Faculté des Mathématiques et de l'Infrmatique
Department de Mathematiques.

polycopié d'Algèbre 01

Coures et exercices d'*algèbre01*

1ère Année Mathématiques

Auteur Dr. **kheir.saadaoui**

2022/2023

Table des matières

Chapitre 1

Notions de logique

À la limite de la philosophie, la logique est une branche fondamentale des mathématiques qui permet d'établir la valeur de vérité de propositions et de construire des raisonnements mathématiques.

Ce document constitue une initiation à cette branche primordiale des mathématiques. Nous définirons les notions de proposition et d'opérateur, construirons des tables de vérité, expliquerons les notions d'implication, d'implication réciproque et d'équivalence avant d'aborder les différents types de raisonnements que l'on peut suivre en mathématique.

1.1 Définition

Une proposition logique (ou assertion) est une affirmation formée d'un assemblage de symboles et de mots, portant sur des objets mathématiques, à laquelle on peut clairement attribuer la valeur vraie ou la valeur faux.

On note P une proposition.

Par définition P satisfait les 3 principes (ou axiomes) suivants :

- Principe d'identité : P est P

  Autrement dit si P est vrai alors P est vrai et si P est faux alors P est faux.

- Principe de non contradiction : P ne peut pas à la fois être vrai et faux

- Principe du tiers exclus : Soit P est vrai, soit P est faux.

Il n'existe pas d'autre valeur de vérité en logique mathématique.

Ces trois principes constituent le fondement de tout raisonnement mathématique. Le dernier point mérite que l'on s'y attarde un instant :

Soit P la proposition «Le carré d'un nombre réel est strictement positif ».

Alors ? Vrai ou faux ?

L'intuition première serait de répondre "ça dépend du nombre", c'est le cas pour la plupart des nombres mais c'est faux pour zéro (car $0^2n'$ 'est pas > 0).

Le problème est que cette réponse est en contradiction avec le principe du tiers exclus. Il faut donc attribuer clairement à cette proposition la valeur vrai ou la valeur faux.

Étant donné qu'il existe au moins un nombre (ici zéro) pour lequel cette proposition est fausse, on dira que la proposition P est fausse.

1.1.1 Quelques exemples

$\boldsymbol{P}_1$: «e nombre de lettres dans l'alphabet français est 10.»

La proposition $\boldsymbol{P}_1$ est fausse.

$\boldsymbol{P}_2$ **:** «$2 + 2 = 4$»

La proposition $\mathbf{P}_2$ est vraie.

$\mathbf{P}_3$ **:** « x>1 »

$\boldsymbol{P}_3$ n'est pas une proposition logique complète car elle contient une variable libre x. On ne sait pas ce qu'est x (un point ? un nombre entier ? un vecteur ? une étoile de l'univers ?). On ne peut donc pas attribuer de valeur de vérité à la proposition $\mathbf{P}_3$.

$\boldsymbol{P'}_3$: «Soit x un nombre réel, alors $x > 1$»

La proposition $\boldsymbol{P'}_3$ est fausse. En effet $\boldsymbol{P'}_3$ est une proposition logique car on a défini la variable x comme étant un nombre réel. Mais elle est fausse car par exemple 0 est un nombre réel et $0 < 1$

On utilise ici un contre-exemple pour prouver que la proposition $\boldsymbol{P'}_3$ est fausse.

(Ce type de raisonnement sera approfondi plus tard).

A retenir

Les propositions logiques ne peuvent prendre que deux valeurs :VRAI Ou FAUX (d'où le nom de logique bivalente).

Il faut bien faire la distinction entre une proposition (qui est une phrase) et sa valeur (qui est soit VRAI soit FAUX). on dira que la proposition p est fausse

1.2 Opérateurs de base

Les opérateurs permettent de construire de nouvelles propositions à partir d'une ou de plusieurs propositions initiales.

Commençons par le premier (et le plus simple !) d'entre eux, l'opérateur «NON».

1.2.1 La négation (non) : Apprenons à dire non !

Soit **P** une proposition. On définit une proposition « non **P**» que l'on note « $\neg$**A**» (avec une sorte de petit L allongé vers le bas) ou encore par $\overline{\boldsymbol{P}}$.

Si $\boldsymbol{P}$ est vraie alors $\overline{\boldsymbol{P}}$ est fausse.

Si $\boldsymbol{P}$ est fausse alors $\overline{\boldsymbol{P}}$ est vraie.

Pour ceux qui font de la programmation, I'opérateur «NON» (noté en maths) est souvent noté « !» en informatique

On peut établir la table de vérité de l'opérateur de négation à partir de sa définition.

Définition. Une table de vérité est un tableau définissant la valeur d'une fonction logique pour chacune des combinaisons possibles des entrées.

Explication. Dans la première colonne, je place toutes les valeurs que peut prendre A (c'est à dire Vrai ou Faux). Dans la seconde colonne, je place la valeur de vérité de $\bar{A}$ correspondante.

Par convention et pour faciliter la lecture de grandes tables, on écrit $\boldsymbol{F}$ pour la valeur $FAUX$ et V pour la valeur $VRAI$

$\boldsymbol{P}$	$\overline{\boldsymbol{P}}$
V	F
F	V

Il est important de bien comprendre comment construire une table de vérité, nous nous en servirons de nombreuses fois dans ce cours.

Ce connecteur est assez intuitif dans la mesure où nous l'utilisons quotidiennement.

Quelques exemples

P : « Alger est la capitale de la Algérie » (ca valeur est $\boldsymbol{V}$)

$\bar{P}$: « Alger n'est pas la capitale de la Algérie » (ca valeur est $\boldsymbol{F}$)

Q : «π est un nombre entier » (F)

$\bar{Q}$: «π n'est pas un nombre entier » (V)

R : «5 est un nombre impair » (V)

$\bar{R}$: «5 est un nombre pair » (F)

Ce premier opérateur doit maintenant vous paraître assez simple. Pour construire des raisonnements logiques on a besoin d'utiliser des opérateurs permettant de lier deux propositions logiques entre elles (on les appelle des **opérateurs binaires**).

1.2.2 La conjonction «et» , noté « $\wedge$ ».

Soient P et Q deux propositions.

On définit une nouvelle proposition «P ET Q » que l'on note «P $\wedge\boldsymbol{Q}$ » Cette nouvelle proposition est

Vraie lorsque $\boldsymbol{P}$ et $\boldsymbol{Q}$ sont vraies en même temps

Fausse dans tous les autres cas.

On déduit de cette définition la table de vérité de la proposition «$P \wedge \boldsymbol{Q}$»

$\boldsymbol{P}$	$\boldsymbol{Q}$	$\boldsymbol{P \wedge Q}$
V	V	V
V	F	F
F	V	F
F	F	F

Les deux premières colonnes permettent de lister tous les cas possibles pour les valeurs de vérité de $\boldsymbol{P}$ et de $\boldsymbol{Q}$. La dernière colonne associe la valeur de vérité de la proposition «$\boldsymbol{P \wedge Q}$ ».

Il est important de bien comprendre la table de vérité de l'opérateur «ET» car il est utilisé dans de nombreux raisonnements.

Quelques exemples

Qxemple 1. «5 est un nombre inférieur à 10 **et** 5 est pair »

Soit $\boldsymbol{P}$: «5 est un nombre inférieur à 10»$\boldsymbol{P}$ est vraie

Soit $\boldsymbol{Q}$: « est pair » $\boldsymbol{Q}$ est fausse

La proposition A est la proposition «$\boldsymbol{P \wedge Q}$»

D'après la table de vérité de l'opérateur binaire «ET», on en déduit que la proposition A est fausse. &xemple 2 : «La lettre A est une voyelle et T est une consonne. " En résonnant de même, on en déduit que la proposition **B** est vraie.

Exemple 2. «La lettre A est une voyelle et T est une consonne.»

En résonnant de même, on en déduit que **la proposition B est vraie**.

1.2.3 La disjonction «ou », noté " V ».

Le deuxième opérateur binaire que nous allons étudier est l'opérateur «OU».

Soient P et Q deux propositions.

On définit une nouvelle proposition « P ou Q » que l'on note «P $\vee Q$ » .

Cette proposition est :

Fausse lorsque $\boldsymbol{P}$ et $\boldsymbol{Q}$ sont fausses en même temps

Vraie sinon

$\boldsymbol{P}$	$\boldsymbol{Q}$	$\boldsymbol{P \vee Q}$
V	V	V
V	F	V
F	V	V
F	F	F

Autrement dit, la proposition « $P \vee Q$ » est vraie uniquement si P ou Q est vraie (ou les deux !).

Exemple. «5 est un nombre inférieur à 10 OU 5 est pair »

Quelle est la valeur de vérité de cette proposition ?

Correction.

Soit $\boldsymbol{P}$: « 5 est un nombre inférieur à 10 ». Est vraie

Soit $\boldsymbol{Q}$: «5 est pair». Est fausse

La proposition " $\boldsymbol{P \vee Q}$ "

D'après la table de vérité de l'opérateur "OU», la proposition de l'exemple est vraie

Les opérateurs binaires «NON», «ET», et «OU» sont les plus importants en mathématiques car ils permettent de définir tous les autres opérateurs.
Nous voilà au cœur du sujet ! En effet les implications et les équivalences sont utilisées dans la grande majorité des démonstrations en mathématiques. Bien les comprendre permet donc d'éviter des erreurs de raisonnement dans une copie... mais aussi dans la vie !

1.2.4 Notion d'implication « $\Rightarrow$ »

L'implication est un opérateur binaire (c'est à dire, qui lie deux propositions entre elles).

Soient deux propositions P et Q.

On note $\boldsymbol{P \Rightarrow Q}$ (et on lit P implique Q)

Plusieurs formulations pour une même notion

$P \Rightarrow Q$ se lit aussi :

- ✓ Si Palors Q
- ✓ Il suffit que P pour que Q
- ✓ Il est nécessaire que Q pour que P
- ✓ Il faut que Q pour que P

Ainsi, à chaque fois que vous entendez dans le langage courant I'une des formulations, c'est en fait une implication

Exemple.

«Il suffit qu'il soit là pour que je sois joyeux. » correspond à «Il est là » $\Rightarrow$ « Je suis joyeux»

«Il pleut. » $\Rightarrow$ «Le sol est mouillé. ». Il pleut alors le sol est mouillé, cela veut dire bien qu'il est impossible qu'il pleuve et que le sol ne soit pas mouillé.

«Si je suis fatigué, je vais me reposer.» C'est à dire que « Je suis fatigué. » $\Rightarrow$ « Je vais me reposer. »

Soient P et Q deux propositions.

On définit une nouvelle proposition «P PQ » (que l'on lit P implique Q)

Cette proposition est :

Fausse lorsque $\boldsymbol{P}$ est Vraie et $\boldsymbol{Q}$ est fausses

Vraie sinon

$\boldsymbol{P}$	$\boldsymbol{Q}$	$\boldsymbol{P \Rightarrow Q}$
V	V	V
V	F	F
F	V	V
F	F	V

Autrement dit, la proposition «P PQ » est fausse uniquement si P est Vraie et Q est fausse).

1.2.5 Implication réciproque « $\rightleftharpoons$ »

Encore un petit quelque chose. P et Q sont toujours deux propositions. La proposition $Q \Rightarrow P$ est appelée l'implication réciproque de la proposition $P \Rightarrow Q$. Retenez cette expression, on va s'en resservir dans deux lignes!

1.2.6 Équivalence « $\Leftrightarrow$ »

Le symbole de l'équivalence est $\Leftrightarrow$. Une double flèche qui n'est pas sans rappeler la flèche de l'implication vue juste au-dessus.

Soient P et Q deux propositions.

On définit une nouvelle proposition «P $\Leftrightarrow Q$ » que l'on lit «P équivaut à Q »

Ou « si et seulement si Q »

C 'est aussi «l'implication $P \Rightarrow Q$ et l'implication réciproque $Q \Rightarrow P$ »

Cette proposition est :

Vraie lorsque P et Q ont la même valeur de vérité (toutes deux vraies, ou toutes deux fausses). Fausse sinon

$\boldsymbol{P}$	$\boldsymbol{Q}$	$\boldsymbol{P \Leftrightarrow Q}$
V	V	V
V	F	F
F	V	F
F	F	V

Pour démontrer une équivalence, on utilise souvent la règle de la double implication :

✓ On démontre dans un premier temps une implication,

✓ puis dans un second temps on démontre l'implication réciproque

Évitez les confusions !

Il ne faut pas confondre implications et équivalences.

À chaque fois que vous devez donner la valeur de vérité d'une équivalence vérifiez bien la valeur de vérité de la double implication.

1.2.7 Propriétés

1. $(P_1 \Leftrightarrow P_2) \Leftrightarrow (P_1 \Rightarrow P_2) \wedge (P_2 \Rightarrow P_1)$

2. $\overline{\overline{P}}_1 \Leftrightarrow P_1$

3. $P_1 \vee P_1 \Leftrightarrow P_1$

4. $P_1 \vee P_1 \Leftrightarrow P_1$

5. $\overline{P_1 \vee P_2} \Leftrightarrow \overline{P_1} \wedge \overline{P_2}$

6. $\overline{P_1 \wedge P_2} \Leftrightarrow \overline{P_1} \vee \overline{P_2}$

7. $P_1 \wedge (P_2 \wedge P_3) \Leftrightarrow (P_1 \wedge P_2) \wedge P_3$

8. $P_1 \vee (P_2 \vee P_3) \Leftrightarrow (P_1 \vee P_2) \vee P_3$

9. $P_1 \wedge (P_2 \vee P_3) \Leftrightarrow (P_1 \wedge P_2) \vee (P_1 \wedge P_3)$

10. $P_1 \vee (P_2 \wedge P_3) \Leftrightarrow (P_1 \vee P_2) \wedge (P_1 \vee P_3)$

11. $\overline{(P_1 \Rightarrow P_2)} \Leftrightarrow P_1 \wedge \overline{P_2}$

12. $P_1 \Rightarrow P_2 \Leftrightarrow \overline{P_2} \Rightarrow \overline{P_1}$ «La loi de contraposition»

Démonstration

✓ Démontrons la propriété 1 : $\overbrace{(P_1 \Leftrightarrow P_2)}^{(1)}\overbrace{(P_1 \Rightarrow P_2) \wedge (P_2 \Rightarrow P_1)}^{(2)}$

On utilise la table de vérité.

P_1	P_2	$P_1 \Rightarrow P_2$	$P_2 \Rightarrow P_1$	$(1) : P_1 \Leftrightarrow P_2$	$(2) : (P_1 \Rightarrow P_2) \wedge (P_2 \Rightarrow P_1)$	$(1) \Leftrightarrow (2)$
V	V	V	V	V	V	$\boldsymbol{V}$
V	F	F	V	F	F	$\boldsymbol{V}$
F	V	V	F	F	F	$\boldsymbol{V}$
F	F	V	V	V	V	$\boldsymbol{V}$

1.3 Les quantificateurs

Soit P la proposition « 8 est un nombre pair». On peut remplacer le nombre 8 par un autre nombre quelconque afin de former de nouvelles propositions. On pourra par exemple écrire la proposition $P(6)$ « 6 est un nombre pair » qui est vraie, ou la proposition $P(3)$ « 3 est un nombre pair » qui est fausse.

On écrira alors la forme générale de cette proposition $P(x)$: « x est un nombre pair ", x est appelé argument de la proposition P. La valeur de vérité de la proposition P(x) dépend de x.

Le problème est que je ne sais pas ce qu'est x dans la proposition $P(x)$. Dans notre exemple, x est un nombre il faut le préciser car sinon notre proposition n'a pas de sens (par exemple P(ABC) : "le triangle ABC est un nombre pair » n'a pas de sens).

On a donc inventé des quantificateurs pour indiquer que l'on prend notre x parmi un ensemble déterminé.

1.3.1 Le quantificateur universel « $\forall$ »

On note "pour tout x élément de E, la proposition $P(x)$ est vraie » ainsi «Iforall x lin IOmega, $P(x)$ »

Oulà ! C'est quoi tous ces symboles ?!

Du calme, du calme. On s'habitue rapidement à lire les quelques symboles mathématiques.

- ✓ Le symbole $\forall$ (un A retourné) se lit "quelque soit". C'est un quantificateur, il indique que la propriété est vraie pour tous les objets satisfaisants la condition qui suit.
- ✓ x est un objet mathématique (un nombre, un point, un vecteur...).
- ✓ Le symbole ϵ signifie "appartient à ». C'est un opérateur qui permet de dire que x appartient à un ensemble précisé.

La notation $\forall$ vient de l'allemand Alle qui signifie «tous » en français.

Exemple.

Traduire la proposition sous sa forme mathématique équivalente (en utilisant le quantificateur et le connecteur logique adéquat).

P : «Pour tout x nombre réel, il suffit que x soit supérieur ou égal à 5 pour que x^2 soit supérieur ou égal à 25 »

Correction.

La formulation «il suffit que P soit vraie pour que Q soit vraie » se traduit par $P \Rightarrow Q$ Cette équivalence est vraie pour tout x nombre réel, on utilise donc le quantificateur $\forall$.

$$P(x) : \underbrace{\forall}_{\text{Quantificateur}} x \in \mathbb{R}, x \geq 5 \underbrace{\Rightarrow}_{\text{connecteur}} x^2 \geq 25$$

1.3.2 Le quantificateur existentiel «$\exists$»

La proposition $\boldsymbol{Q}$: «Tous les étudiants sont présents ".

Essayez de déterminer $\overline{\mathbf{Q}}$ (dans une phrase française).

Attention ! Il y a un piège !

Le contraire de «Tous les étudiants sont présents» n'est pas «Tous les étudiants sont absents» ! En effet, il suffit qu'un seul étudiant soit absent pour que la proposition $\boldsymbol{Q}$ soit fausse.

On dira donc que la proposition contraire de Q est « Au moins un étudiant absent »

Il nous faut un autre quantificateur pour traduire " il existe au moins un ». On pourrait noter ce quantificateur (non $\forall$), car il est simplement la négation du quantificateur universel. Mais pour simplifier la notation, on utilisera le symbole $\exists$ (un E à l'envers).

Et oui $\exists$ vient de l'allemand Existieren (" exister » en français).

$\exists$ s'utilise exactement de la même façon que $\forall$.

Exemple.

$P(x) : \exists x \in \mathbb{R}$ tel que $x^2 = 1$

La proposition P se lit "Il existe au moins un nombre réel x dont le carré est égal à 1. ».

Voyez comme la notation mathématique est plus pratique !

1.3.3 Plusieurs quantificateurs

On peut utiliser deux quantificateurs (ou plus) dans une même proposition. Dans ce cas l'ordre des quantificateurs est important.

Exemple. Traduisez en français les propositions \$P\$ et \$Q\$ et donnez leur valeur de vérité :

$P(x) : \forall x \in \mathbb{N}, \exists y \in \mathbb{N} : x < y$ «N l'ensemble des entiers naturels »

$Q(x) : \exists x \in \mathbb{N}, \forall y \in \mathbb{N} : x < y$

Correction.

La proposition P signifie «Pour tout entier naturel x, il existe un entier naturel y strictement supérieur à x. »La proposition P est **vraie**

La proposition Q signifie «Il existe un entier naturel strictement inférieur à tous les entiers naturels »La proposition Q est **fausse**. Pour le prouver, on peut utiliser un contre-exemple. En effet il n'existe aucun entier naturel strictement inférieur à 0.

Ces deux propositions si proches en apparence n'ont donc absolument rien à voir !

Retenez donc que changer la nature ou l'ordre des quantificateurs change le sens de la proposition.

1.3.4 Propriétés

1. $\overline{(\forall x \boldsymbol{P(x)})} \Leftrightarrow (\exists x \overline{\boldsymbol{P(x)}})$

2. $\overline{(\exists x P(x))} \Leftrightarrow (\forall x \overline{P(x)})$

Exemple. Donner la négation de la proposition de l'inclusion « $\boldsymbol{A \subset B}$»

Correction.

La proposition $\boldsymbol{A \subset B}$ s'écrit « $\forall \boldsymbol{x}; \boldsymbol{x \in A \Rightarrow x \in B}$ »

Donc La négation de $\boldsymbol{A \subset B}$ s'écrit $\overline{\boldsymbol{A \subset B}}$ où $\boldsymbol{A \not\subset B}$ qui revient à chercher $\overline{\forall \boldsymbol{x}; \boldsymbol{x \in A \Rightarrow x \in B}}$.

On utilise la propriété 1 :

Il vient : $\overline{\forall x; x \in A \Rightarrow x \in B} \Leftrightarrow \exists x; \overline{x \in A \Rightarrow x \in B}$ «on utilise $\overline{(P_1 \Rightarrow P_2)} \Leftrightarrow P_1 \wedge \overline{P_2}$ »

$\exists x; \overline{x \in A \Rightarrow x \in B} \Leftrightarrow \exists x; x \in A$ et $x \notin B$

On résumé : $\begin{array}{l} \boldsymbol{A \subset B \Leftrightarrow \forall x; x \in A \Rightarrow x \in B} \\ Et\, A \not\subset B \Leftrightarrow \exists x; x \in A\, et\, x \notin B \end{array}$

1.4 Les types de raisonnement

Nous avons maintenant tous les outils en main pour réaliser des raisonnements mathématiques complets.

Un raisonnement permet d'établir une proposition à partir d'une ou de plusieurs propositions initiales admises (ou précédemment démontrées) en suivant les règles de la logique. Nous allons dans cette dernière partie détailler trois "**types**" de raisonnement, trois "**méthodes**" pour démontrer une proposition :

— Trouver un exemple ou un contre-exemple

— Démontrer la contraposée

— Raisonner par l'absurde

Ces différentes formes de raisonnements devront s'appliquer dans des cas bien particuliers.

1.4.1 Exemple et contre-exemple

Pour montrer qu'une proposition de la forme « exists$\boldsymbol{x} \in \boldsymbol{E}, P(x)$ est vraie", on cherche un x pour lequel $P(x)$ est vraie. C'est donner un ***exemple***.

Exemple. P : «$\exists(x, y, z) \in \mathbb{N}^3 : x^2 = y^2 + z^2$». Démontrer que P est vraie

Correction. Soient $x = 5, y = 4, z = 3$.

x, y et z vérifient $x^2 = y^2 + z^2($ car $25 = 16 + 9)$

Donc la proposition P est vraie.

Pour montrer qu'une proposition de la forme «$\forall x \in E$, $P(x)$ est fausse», on montre que sa négation « $\exists x \in \boldsymbol{E}, \overline{P(x)}$ est vraie ». C'est donner un contre-exemple.

Exemple. Soit P la proposition «$\forall n \in \mathbb{N}, n^2 + 1$, est un nombre premier »

Démontrez que P est fausse.

Correction. Pour démontrer que P est fausse on va montrer que $\bar{P}$ est vraie.

$\bar{P}$ est la proposition « $\exists n \in \mathbb{N}, n^2 + 1$ n'est pas un nombre premier ».

Soit $n = 3$. Et $n^2 + 1 = 10$

10 n'est pas un nombre premier.

$$n \text{ est un exemple de la proposition } \bar{P}.$$

$$n \text{ est un contre-exemple de la proposition } \boldsymbol{P}.$$

Donc la proposition P est fausse.

1.4.2 La contraposée

J'espère que vous vous souvenez de la table de vérité de l'implication ! Comment ça non ?!

Je vous laisse la retrouver (dans votre esprit si possible sinon plus haut sur cette page) avant de passer à l'exercice suivant

Exercice. Soient P et Q deux propositions. Montrer que $(P \Rightarrow Q)$ équivaut à $(\bar{Q} \Rightarrow \bar{P})$

Porrection.

Vous l'avez deviné, on utilise une nouvelle fois une table de vérité pour justifier cette équivalence.

P	Q	$\bar{P}$	$\bar{Q}$	$P \Rightarrow Q$	$\bar{Q} \Rightarrow \bar{P}$	$(P \Rightarrow Q) \Leftrightarrow (\bar{Q} \Rightarrow \bar{P})$
V	V	V	V	V	V	V
V	F	F	V	F	F	V
F	V	V	F	F	F	V
F	F	V	V	V	V	V

Donc $(P \Rightarrow Q) \overbrace{\Leftrightarrow}^{\text{équivaut à}} (\bar{Q} \Rightarrow \bar{P})$

1.4.2.1 Définition

La proposition $(\bar{Q} \Rightarrow \bar{P})$. Est appelée proposition contraposée de la proposition $(P \Rightarrow Q)$

Une proposition et sa contraposée sont équivalentes, ce qui signifie que l'on peut démontrer l'une pour démontrer l'autre. On souhaite par exemple montrer que $(P \Rightarrow Q)$. Le raisonnement par contraposée consiste à prouver que $(\bar{Q} \Rightarrow \bar{P})$.

1.4.2.2 Exemple et exercice

Exemple. Pour démontrer que «S'il pleut, alors le sol est mouillé», je vais démontrer que "Si le sol n'est pas mouillé, alors il ne pleut pas».

Exercice. Démontrez la proposition $P : \forall n \in \mathbb{N}$ si n^2 est pair $\Rightarrow n$ est pair.

Indication 1 : Soit n un entier naturel. Donc deux cas :

- ✓ n est pair : $\exists n \in \mathbb{N} : n = 2k$ avec $k \in \mathbb{N}$
- ✓ n est impair : $\exists n \in \mathbb{N} : n = 2k + 1$ avec $k \in \mathbb{N}$

Correction.

On réalise cette démonstration par contraposition. Ainsi plutôt que de montrer que si n^2 est pair, alors n est pair. Nous allons montrer que si $\boldsymbol{n}$ est impair alors $\boldsymbol{n}^2$ est impair.

n est impair : $\exists k \in \mathbb{N} : n = 2k + 1$ avec $k \in \mathbb{N}$ (d'après l'indication)

donc

$n^2 = (2k+1)^2 = 4k^2 + 2k + 1$ (On élève au carré) alors $n^2 = 2\,(2k^2 + k) + 1$ (on factorise)

(k est un entier naturel, donc $(k^2 + k)$ est aussi un entier naturel)

Finalement : $n^2 = 2h + 1$ avec $h = (2k^2 + k) \in \mathbb{N}$ est impair

On a monté que si n est impair $\overbrace{\text{alors}}^{\Rightarrow}$ n^2 est impair. Donc $\forall n \in \mathbb{N}$ si n^2 est pair $\Rightarrow$ n est pair

On obtient le résultat demandé.

1.4.3 Le raisonnement par l'absurde

A quoi bon mettre de l'absurdité dans un raisonnement logique ?!

Drôle d'idée en effet ! Mais rassurez-vous, le raisonnement par l'absurde (comme son nom ne l'indique pas) n'a rien d'absurde. Il est même tout ce qu'il y a de plus logique !

Ce raisonnement repose sur le principe du Tiers-exclus, à savoir que si une proposition n'est pas fausse, alors elle est vraie. Imaginons par exemple que vous savez que quelque chose est vrai, mais vous ne savez pas le démontrer. En raisonnant par l'absurde vous allez commencer par admettre par hypothèse que cette chose est fausse. Puis en suivant les règles de la logique vous allez développer les conséquences de cette hypothèse et aboutir à une contradiction irréfutable (comme $1 = 2$, ou 2 et 4 sont premiers entre eux). Vous allez en déduire que votre hypothèse de départ est nécessairement fausse, c'est à dire que la chose que vous vouliez démontrer n'est pas fausse, donc qu'elle est vraie.*

1.4.3.1 Définition

Le raisonnement par l'absurde est une forme de raisonnement logique. Il consiste

✓ soit à démontrer qu'une proposition P est vraie en prouvant l'absurdité de la proposition $\bar{P}$

✓ soit à démontrer qu'une proposition P est fausse en déduisants logiquement des conséquences absurdes.

Voyons maintenant le raisonnement par l'absurde dans toute sa splendeur à travers l'un de ses exemples les plus classiques : l'irrationalité de $\sqrt{2}$. «P : $\sqrt{2} \notin \mathbb{Q}$»

1.4.3.2 Exemple

On souhaite démontrer que la proposition P est vraie.

$$\boldsymbol{P} : «\sqrt{2} \notin \mathbb{Q}», «\sqrt{2} \text{ est un nombre irrationnel »}$$

On raisonne par l'absurde. On va donc montrer que la proposition $\overline{\boldsymbol{P}}$ est absurde.

$\overline{\boldsymbol{P}}$ Se traduit par « $\sqrt{2} \in \mathbb{Q}$» ou bien « $\sqrt{2}$ est un nombre rationnel ».

Si $\sqrt{2} \in \mathbb{Q}$, il peut se mettre sous la forme d'une fraction. C'est à dire qu'il existe $\boldsymbol{p}$ appartenant à $\mathbb{Z}$ et il existe **q** appartenant à $\mathbb{Z}$ tel que $\sqrt{2} = \frac{p}{q}$ avec $\boldsymbol{p}$ et **q** premiers entre eux.

On simplifie cette égalité :

$$2 = \frac{p^2}{q^2} \text{ (On élève au carré)}$$

$$2q^2 = \boldsymbol{p}^2 \text{ (Par produit de } q^2 \text{)}$$

Donc $\boldsymbol{p}^2$ est pair, donc $\boldsymbol{p}$ est pair (Démonstration par contraposée du paragraphe précédent)
Donc $\exists \boldsymbol{k} \in \mathbb{Z}$ tel que $\boldsymbol{p} = \boldsymbol{2k}$ (propriété vue précédemment)

En remplaçant dans l'égalité précédente, on obtient : $2\boldsymbol{q}^{\mathbf{2}} = (2\boldsymbol{k})^{\mathbf{2}} \Rightarrow \boldsymbol{q}^{\mathbf{2}} = (\mathbf{2k})^{\mathbf{2}} = \mathbf{2k^2}$ Donc $\boldsymbol{q}^2$ est pair, donc $\mathbf{q}$ est pair ce qui est impossible car $\boldsymbol{p}$ est pair et que $\boldsymbol{p}$ et $\mathbf{q}$ sont premiers entre eux.

On aboutit à une contradiction.

Donc la proposition $\overline{\boldsymbol{P}}$ est fausse.

Donc $\sqrt{2}$ est un nombre irrationnel.

Dans le cas où la proposition à démontrer est de la forme $\boldsymbol{P} \Rightarrow \boldsymbol{Q}$, raisonner par l'absurde consiste à démontrer que la proposition $\boldsymbol{P} \wedge \overline{\boldsymbol{Q}}$ est fausse. Pour se faire, on suppose que $\boldsymbol{P}$ est vraie et que $\boldsymbol{Q}$ est fausse, on développe les conséquences et on montre que l'on arrive à une contradiction.

1.5 Exercices corrigé

Exercice 1. Parmi les expressions suivantes lesquelles sont des propositions ? Dans le cas d'une proposition dire si elle est vraie ou fausse

(a) $2+3=5$

(b) $\forall n \in \mathbb{N}, \quad n+2=4$

(c) $\exists n \in \mathbb{N} \quad n+2=3$

(d) Cet exercice est difficile

(e) $x \in \mathbb{N}$

Solution.

a. Cette expréssion est une proposition vraie

b. Cette expréssion est une proposition fausse, car pour $n=1 \in \mathbb{N}$, on a $n+2=3 \neq 4$.

c. Cette expréssion est une proposition vraie, car il existe un élément $n = 1 \in \mathbb{N}$, tel que $n+2=3$.

d. Cette expréssion n'est pas une proposition, car on peut pas lui attribué une valeur de vérité.

e. Cette expréssion n'est pas une proposition, car nous ne savons la nature de l'élément x, donc on peut pas lui attribué une valeur de vérité.

Exercice 2. Dans le LMD mathématique et informatique, un étudiant qui sera admis en deuxième année choisira entre mathématique **OU** informatique mais pas les deux simultanément. C'est le OU 'exclusif ($\underline{\vee}$). Donner la table de vérité.

Solution. Voici la table de vérité du " ou exclusif " est différent de la table de la disjonction " $\vee$" car dans cas particulier, On remarque que le" ou exlusif" est vrai que si les deux assertions P et Q sont différentes. Donc, on peut choisir les deux en même temps.

P	Q	$P\underline{\vee}Q$
1	0	1
0	1	1
1	1	0
0	0	0

Exercice 3. Dans quels cas les propositions suivantes sont elles vraies ?

(a) $(P \Longrightarrow Q) \wedge (\bar{P} \Longrightarrow Q)$

(b) $\overline{P \wedge (\overline{Q \wedge R})} \Leftrightarrow Q$

(c) $((P \vee Q) \Longrightarrow R) \Longleftrightarrow (P \Longrightarrow R) \wedge (Q \Longrightarrow R)$.

Solution.

a. $(P \Longrightarrow Q) \wedge (\bar{P} \Longrightarrow Q)$

P	Q	$\bar{P}$	$P \Longrightarrow Q$	$\bar{P} \Longrightarrow Q$	$(P \Longrightarrow Q) \wedge (\bar{P} \Longrightarrow Q)$
1	0	0	0	1	0
0	1	1	1	1	1
1	1	0	1	1	1
0	0	1	1	0	0

b. $\overline{P \wedge (\overline{Q \wedge R})} \Leftrightarrow Q$ (Devoir pour les étudiants)

c. $\underbrace{((P \vee Q) \Longrightarrow R)}_{(1)} \Longleftrightarrow \underbrace{(P \Longrightarrow R) \wedge (Q \Longrightarrow R)}_{(2)}$

P	Q	R	$P \vee Q$	$P \Longrightarrow R$	$Q \Longrightarrow R$	(1)	(2)	(1) $\Leftrightarrow$ (2)
1	1	1	1	1	1	1	1	1
1	1	0	1	0	0	0	0	1
1	0	1	1	1	1	1	1	1
1	0	0	1	0	1	0	0	1
0	0	1	0	1	1	1	1	1
0	1	0	1	1	0	0	0	1
0	1	1	1	1	1	1	1	1
0	0	0	0	1	1	1	1	1

Exercice 4. Soient les quatres propositions suivantes

a- $\exists x \in \mathbb{R}, \forall y \in \mathbb{R} \quad x + y > 0$

b- $\forall x \in \mathbb{R}, \exists y \in \mathbb{R} \quad x + y > 0$

c- $\forall x \in \mathbb{R}, \forall y \in \mathbb{R} \quad x + y > 0$

d- $\exists x \in \mathbb{R}, \forall y \in \mathbb{R} \quad y^2 > x$.

Ces propositions sont elles vraies ou fausses ? Donner leur négation.

Solution.

a. $\exists x \in \mathbb{R}, \forall y \in \mathbb{R} \quad x + y > 0$

L'assertion (a) est fausse : Est-ce- qu'on peut trouver un réel x pour que pour tout réel y leur somme soit toujours positive ? c'est pas toujours vraie, car il suffit de prendre par exemple $y = -(x+1)$. On obtiendra $x + y = x - x - 1 = -1 < 0$.

La négation de l'assertion (a) est : $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}; \quad x + y \leq 0$, qui est une assertion vraie

b. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R} \quad x + y > 0$.

L'assertion (b) est vraie : en effet, pour tout réel x il exsite un y qui dépend de x. Prenons par exemple $y = -x + 1$ implique que $x + y = x - x + 1 = 1 > 0$.

La négation de l'assertion (b) est : $\exists x \in \mathbb{R}, \forall y \in \mathbb{R} \quad x + y \geq 0$, qui est une assertion fausse

c. L'assertion (c) est fausse. Il suffit de trouver un x et un y qui ne vérifie pas (c). Par exemple $x < 0$ et $y < 0$.

La négqtion de cette assertion est : $\exists x \in \mathbb{R}, \exists y \in \mathbb{R} x + y \leq 0$ qui est une assertion vraie.

d. Devoir pour les étudiants

Exercice 5.

1. En utilisant le raisonnement par l'absurde démontrer que

  (a) $\sqrt{2}$ n'est pas un nombre rationnel

  (b) Si $n \in \mathbb{N}^*$ alors $n^2 + 1$ n'est pas le carré d'un entier naturel

2. Monter par récurrence

  (a) $\forall n \in \mathbb{N}^* 1 + 2^2 + 3^2 + \ldots\ldots\ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$

  (b) $\forall n \in \mathbb{N} 2^n > n.$

3. En utilisant le raisonnement par la contraposé démontrer que si l'entier $(n^2 - 1)$ n'est pas divisible par 8, alors alors n est pair.

Solution.

1. En utilisant le raisonnement par l'absurde démontrer que

  (a) $\sqrt{2}$ n'est pas un nombre rationnel

  Supposons par l'absurde que $\sqrt{2}$ soit rationnel : alors où $a, b > 0$ (sont des nombres entiers positifs). Maintenant, Il est possible de simplifier la fraction jusqu'à ce que a, b soient premiers entre eux (c'est-à-dire la fraction ne puisse plus être simplifiée). tels que

$$\sqrt{2} = \frac{a}{b} \Rightarrow a = \sqrt{2}b \Rightarrow 2b^2 = a^2$$

  alors, on déduit que a^2 est pair, d'où a est pair aussi (voir l'exemple du cours), c'est à dire : $\exists$ un entier positif k tel que

$$a^2 = 4k^2 = 2b^2 \Rightarrow b^2 = 2k^2$$

  Alors, b^2 est pair, d'où b est pair. Par conséquent, il est possible de simplifier la fraction $\frac{a}{b}$ par 2 , ce qui contredit l'hypothèse que a, b sont premiers entre eux.

  (b) Devoir.

2. Monter par récurrence

a. $\forall n \in \mathbb{N}^* 1 + 2^2 + 3^2 + \dots\dots\dots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

1- Vérifions si cette proposition est vraie pour $n = 1$ et 2 .

Pour $n = 1$, on a : $\frac{1(1+1)(2+1)}{6} = 1$, vraie

Pour $n = 2$, on a : $\frac{2(2+1)(4+1)}{6} = 1 + 2^2 = 5$, vraie.

2- Supposons que cette est vraie pour n, c'est à dire ($P(n)$ est vraie). Et montrons que la proposition ($P(n + 1)$ est vraie).

3- D'aprés 2 , on a

$$P(n) \Leftrightarrow \forall n \in \mathbb{N}^* 1 + 2^2 + 3^2 + \dots\dots\dots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

alors,

$$\begin{aligned}
&\underbrace{1 + 2^2 + 3^2 + \dots\dots\dots + n^2}_{P(n)} + (n+1)^2 \\
=&\frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\
=&\frac{n(n+1)(2n+1)}{6} + \frac{6(n+1)^2}{6} \\
=&(n+1)\left[\frac{n(2n+1) + 6(n+1)}{6}\right] = (n+1)\left[\frac{2n^2 + 7n + 6}{6}\right] \\
=&\frac{(n+1)(n+2)(2n+3)}{6} = P(n+1).
\end{aligned}$$

b. $\forall n \in \mathbb{N} 2^n > n$. Devoir.

3. En utilisant le raisonnement par la contraposée démontrons que si l'entier $(n^2 - 1)$ n'est pas divisible par 8 , alors alors n est pair.

$\underbrace{\text{C'est à dire : } \left(n^2 - 1\right) \text{ n'est pas divisible par } 8}_{P} \Rightarrow$

Maintenant, on doit utiliser la contraposée

$\underbrace{n \text{ est impair : alors } \exists \text{ un entier } k \text{ tel que } n = 2k + 1}_{\bar{Q}} \Rightarrow \underbrace{\left(n^2 - 1\right) \text{ est divisible par 8 : alors, } \exists 1}_{\bar{P}}$

Supposons que , n est impair, alors $\exists$ un entier k tel que $n = 2k + 1$, d'où $n^2 = (2k + 1)^2$

Alors,

$$\begin{aligned}
n^2 - 1 &= (2k + 1)^2 - 1 \\
&= 4k^2 + 4k.
\end{aligned}$$

Maintenant, nous avons deux cas : k est pair ou k est impair.

1- Si on suppose que k est pair, alors, il existe un k' telque $k = 2k'$, d'où

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

2- Si k est impair, alors, il existe un k'' tel que $k = 2k'' + 1$, on a :

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

D'où $(n^2 - 1)$ est divisible par 8 .

1.6 Exercices non résolus

Exercice 1. Soient P, Q et R trois propositions. Démontrer les propriétés suivantes :

1. $(P \Rightarrow Q) \Leftrightarrow (\bar{Q} \Rightarrow \bar{P})$

2. $(P \Leftrightarrow Q) \Leftrightarrow ((\overline{P \wedge \bar{Q}}) \wedge (\overline{Q \wedge \bar{P}}))$

3. $(P \wedge (\overline{Q \wedge R})) \Leftrightarrow ((P \wedge \bar{Q}) \vee (P \wedge \bar{R}))$

Exercice 2. Écrire avec des quantificateurs les phrases suivantes :

1. f est une fonction constante sur $\mathbb{R}$.

2. Le graphe de la fonction f coupe la droite d'équation $y = x$.

3. L'équation $\sin x = x$ a une et une seule solution dans $\mathbb{R}$.

4. Pour chaque entier, on peut trouver un entier strictement plus grand.

Exercice 3. Nier les formules suivantes :

1. $0 \leq x \leq 25 \Rightarrow \sqrt{x} \leq 5$.

2. $0 < x \leq 1$ ou $2 \leq y < 3$.

3. $\exists x \in \mathbb{R} \mid \cos(x) = 0$ et $\exists x \in \mathbb{R} \mid \sin(x) = 0$.

4. $\forall \epsilon > 0, \exists \alpha > 0 \mid \forall x \in D_f, (|x - x_0| < \alpha \Rightarrow |f(x) - f(x_0)| \geq \epsilon)$.

Exercice 4. Les assertions suivantes sont-elles vraies ou fausses ?

(a) $\exists x \in \mathbb{R} \mid \forall y \in \mathbb{R} : x + y > 0$;

(b) $\forall x \in \mathbb{R} : \exists y \in \mathbb{R} \mid x + y > 0$;

(c) $\forall x \in \mathbb{R} : \forall y \in \mathbb{R} : x + y > 0$;

(d) $\exists x \in \mathbb{R} \mid \forall y \in \mathbb{R} : y^2 > x$.

Exercice 5. Montrer les formules suivantes :

1. $|x| < 0.1 \Rightarrow |2x^2 - x| < 0.12$ (Raisonnement direct).

2. Pour tout entier $n, n^2 + 3n$ est pair (Cas par cas).

3. $\forall n \in \mathbb{N} : n^2$ est pair $\Rightarrow n$ est pair (Contraposée).

4. $\sqrt{2}$ est irrationnel (L'absurde).

5. $\forall a, b \in \mathbb{R}^+ : \frac{a}{1+b} = \frac{b}{1+a} \Rightarrow a = b$ (L'absurde).

6. $\forall n \in \mathbb{N} : 2^n > n$ (Récurrence).

7. $a; b; c; d$ des nombres réels tels que $a \leq b$ et $c \leq d$, a-t-on toujours $ac \leq bd$? (Contreexemple).

Exercice 6.

1. Soient a et b deux entiers naturels non nuls. Montrer que

$$((\exists k \in \mathbb{N} \mid b = ka) \text{ et } (\exists k \in \mathbb{N} \mid a = kb)) \Rightarrow (a = b)$$

2. Démontrer par récurrence les égalités

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \qquad \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} \qquad \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$$

3. Soit $n \in \mathbb{N}$. Demontrer par l'absurde que $n^2 + 1$ n'est pas le carre d'un entier.

Chapitre 2

Ensembles et applications

2.1 Définitions et exemples

2.1.1 Ensembles et éléments

* Intuitivement, un ensemble est une collection d'objets. Les objets d'un ensemble sont appelés éléments de cet ensemble et qu'un élément a appartient à E (on écrit : $a \in E$) ou n'appartient à E (on écrit : $a \notin E$).

* Un ensemble particulier est l'ensemble vide, noté $\emptyset$ qui est l'ensemble ne contenant aucun élément.

* Un ensemble $E = \{a\}$, formé d'un seul élément, et appelé un singleton. - Soit E un ensemble. Si un ensemble A est contenu dans E, on dit que A est une partie ou un sous ensemble de E. Les éléments de E n'appartenant pas à l'ensemble A constituent une nouvelle partie de E, appelée complémentaire de A dans E et notée A^c ou bien $C_E(A)$. Formellement, $C_E(A) = \{x \in E \mid x \notin A\}$.

2.1.2 Opérations sur les ensembles

A partir de deux ensembles \$A\$ et \$B\$, on peut construire d'autres.

* On dit que A est inclus dans B (A est un sous-ensemble de B ou une partie de B) et on

note $A \subset B$ si tout élément de A est aussi un élément de B.

$$A \subset B \Leftrightarrow (\forall x \in A \Rightarrow x \in B)$$

* On dit que A et B sont égaux si et seulement si $A \subset B$ et $B \subset A$.

* Soient A et B deux ensembles. La réunion de A et de B et noté $A \cup B$ (lire A union de B) est l'ensemble des éléments appartenant à A ou appartenant à B.

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

* Soient A et B deux ensembles. L'intersection de A et de B et noté $A \cap B$ (lire A inter B) est l'ensemble des éléments appartenant à la fois à A et à B.

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

* On dit que A, B sont des ensembles disjoints si $A \cap B = \emptyset$.

Exemple. Dans $\mathbb{N}$, si l'on désigne par $\mathcal{D}(n)$ l'ensemble des diviseurs de l'entier naturel n, on aura

$$\mathcal{D}(24) \cup \mathcal{D}(16) = \{1, 2, 3, 4, 6, 8, 12, 16, 24\} \text{ et } \mathcal{D}(24) \cap \mathcal{D}(16) = \{1, 2, 3, 4, 8\}$$

2.1.3 Propriétés et règles de calculs

Voici quelques propriétés et règles de calculs sur les ensembles.

Proposition 2.1 Soient A, B, C des parties d'un ensemble E. Alors

1. $A \cup A = A, A \cap A = A$.

2. $A \cup \emptyset = A, A \cap \emptyset = \emptyset$.

3. $A \cup B = B \cup A, A \cap B = B \cap A$ (Commutativité).

4. $A \cup (B \cup C) = (A \cup B) \cup C, A \cap (B \cap C) = (A \cap B) \cap C$ (Associativité).

5. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C), A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (Distributivité).

Preuve. On démontre que $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

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

□

Définition 2.1 (L'ensemble des parties) Soit E un ensemble. On admet qu'il existe un ensemble noté $\mathcal{P}(E)$, tel qu'on ait l'équivalence

$$X \in \mathcal{P}(E) \Leftrightarrow X \subset E$$

$\mathcal{P}(E)$ est appelé l'ensemble des parties de E.

Remarque 2.1 Si card $(E) = n$, alors card $\mathcal{P}(E) = 2^n$.

Exemple. Si $E = \{1, 2, 3\}$. Alors, card $\mathcal{P}(E) = 2^3 = 8$ et

$$\mathcal{P}(E) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Définition 2.2 (Différence ensembliste) Soient A, B deux sous-ensembles de E.

1. La différence de A et de B noté $A \backslash B$ est formé des éléments qui sont dans A mais qui ne sont pas dans B c.à.d $A \backslash B = A \cap C_E(B)$.

2. La différence symétrique de A et de B noté $A \triangle B$ est l'ensemble $(A \backslash B) \cup (B \backslash A)$ ou bien l'ensemble $(A \cup B) \backslash (A \cap B)$.

Exemple.

1. Dans $\mathbb{N}$, on a $\mathcal{D}(24) \backslash \mathcal{D}(16) = \{3, 6, 12, 24\}$ et $\mathcal{D}(16) \backslash \mathcal{D}(24) = \{16\}$. Aussi, $\mathcal{D}(24) \triangle \mathcal{D}(24) = \{6, 12, 16, 24\}$

2. L'ensemble $\mathbb{R} \backslash \mathbb{Q}$ contient des nombres irrationnels comme π.

Remarque 2.2 Lorsque $A \subset E$, on $a : E \backslash A = C_E(A)$.

Proposition 2.2 Soient A, B deux sous-ensembles de E. Alors

1. $A \backslash A = \emptyset$.

2. $A \backslash \emptyset = A$.

3. $A \cup C_E(A) = E$.

4. $A \cap C_E(A) = \emptyset$.

5. $C_E\left(C_E(A)\right) = A$.

6. $C_E(A \cap B) = C_E(A) \cup C_E(B)$.

7. $C_E(A \cup B) = C_E(A) \cap C_E(B)$.

Preuve. On démontre que $C_E(A \cap B) = C_E(A) \cup C_E(B)$.

$$\begin{aligned}
&\text{Soit } x \in C_E(A \cap B) \Leftrightarrow x \notin (A \cap B)\\
&\Leftrightarrow \overline{x \in (A \cap B)}\\
&\Leftrightarrow \overline{x \in A \text{ et } x \in B}\\
&\Leftrightarrow \overline{x \in A} \text{ ou } \overline{x \in B}\\
&\Leftrightarrow x \notin A \text{ ou } x \notin B\\
&\Leftrightarrow x \in C_E(A) \cup C_E(B).
\end{aligned}$$

□

Définition 2.3 (Partition) Soit E un ensemble. Une partition de E est un ensemble $\{E_i\}$ de parties de E, qui vérifie les deux conditions suivantes :

1. $E = \bigcup_{i \in I} E_i$

2. $E_i \cap E_j = \emptyset (\forall i \neq j \in I)$.

Exemple. Soit A un sous-ensemble de E. Alors l'ensemble $\{A, C_E(A)\}$ est une partition de E.

Définition 2.4 (Produit cartésien) Soient A, B deux ensembles. Le produit cartésien, noté AB, est l'ensemble des couples (x, y) où $x \in A$ et $y \in B$.

$$AB = \{(x, y) \mid x \in A \text{ et } y \in B\}$$

Exemple.

1. $\mathbb{R}^2 = \mathbb{R}\mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$.

2. Soient $A = \{1, 2, 3\}$ et $B = \{a, b\}$. Alors, $AB = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$.

Généralisation

Si on considère des ensembles $A_1, A_2, \ldots, A_n$ on peut de même définir les n-uples $(x_1, x_2, \ldots, x_n)$ où $x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n$.

$$A_1A_2 \ldots A_n = \{(x_1, x_2, \ldots, x_n) \mid x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n\}.$$

Proposition 2.3 Soient A, B, C, D quatre sous-ensembles de E. Alors

1. $(AC) \cup (BC) = (A \cup B)C$.

2. $(AC) \cup (AD) = A(C \cup D)$.

3. $(AC) \cap (BD) = (A \cap B)(C \cap D)$.

Preuve. On démontre que $(AC) \cup (BC) = (A \cup B)C$.

$$\begin{aligned}(AC) \cup (BC) &= \{(x, y) \mid (x, y) \in AC \text{ ou } (x, y) \in BC\} \\ &= \{(x, y) \mid (x \in A \text{ et } y \in C) \text{ ou } (x \in B \text{ et } y \in C)\} \\ &= \{(x, y) \mid (x \in A \text{ ou } x \in B) \text{ et } y \in C\} \\ &= (A \cup B)C.\end{aligned}$$

□

2.2 Applications

2.2.1 Définitions et exemples

Définition 2.5 Soient E, F deux ensembles. On dit que f est une application de E dans F si pour chaque élément $x \in E$, il existe un élément unique $y \in F$ tel que $f(x) = y$ et on note

$$f : E \longrightarrow F \quad \text{ou bien} \quad E \xrightarrow{f} F$$

* L'ensemble E est dit ensemble de départ et F est dit ensemble d'arrivée. L'élément x est dit l'antécédent et y est dit l'image de x par f.

* On note par $\mathfrak{F}(E,F)$ l'ensemble de toutes les applications de E dans F.

Exemple.

1. $\begin{array}{rcl} f:\{1,2,3\} & \longrightarrow & \{2,4,5\} \\ x & \mapsto & x^2 \end{array}$ n'est pas une application.

2. L'identité $\begin{array}{rcl} f:E & \longrightarrow & E \\ x & \mapsto & x \end{array}$ est une application et sera très utile dans la suite.

3. les projections $\begin{array}{rcl} P_x : EF & \longrightarrow & E \\ (x,y) & \mapsto & P_x\,(x,y) = x \end{array}$ $\begin{array}{rcl} P_y : EF & \longrightarrow & F \\ (x,y) & \mapsto & P_y\,(x,y) = y \end{array}$

   sont des applications aussi.

Définition 2.6 (Restrictions et prolongements) Soit f une application de E vers F

1. On appelle restriction de f à une partie $A \subset E$, l'application notée $f_{|A} : A \longrightarrow F$ définie par

$$f_{|A} = f(x), \quad \forall x \in A$$

2. On appelle prolongement de f à un ensemble E' contenant E, toute application g de E' vers F dont la restriction est f.

Exemple. Si f est l'identité de $\mathbb{R}^{+}$dans lui-même, elle possède une infinité de prolongement à $\mathbb{R}$, parmi lesguels :

1. L'application identité de $\mathbb{R}$.

2. L'application "valeur absolue" de $\mathbb{R}$ dans lui-même.

3. L'application h définie par $h(x) = \frac{1}{2}(x + |x|)$, et qui est identiquement nulle sur $\mathbb{R}^{-}$.

2.2.2 L'image directe et l'image réciproque

Définition 2.7 Soient E, F deux ensembles

1. Soit $A \subset E$ et $f : E \longrightarrow F$, l'image directe de A par f est un sous-ensemble de F définie par

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

2. Soit $B \subset F$ et $f : E \longrightarrow F$, l'image réciproque de B par f est un sous-ensemble de E définie par

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

Exemple. Soit f une application donnée par : $\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \mapsto & 2n+1 \end{array}$

1. Soit $A = \{0, 1, 2\}$, alors $f(A) = \{f(n) \mid n \in A\} = \{f(0), f(1), f(2)\} = \{1, 3, 5\}$.

2. Soit $B = \{5\}$, alors $f^{-1}(B) = \{n \in \mathbb{N} \mid f(n) \in B\} = \{n \in \mathbb{N} \mid f(n) = 5\} = \{2\}$.

Proposition 2.4 Soient $f : E \longrightarrow F$ une application, A_1, A_2 deux parties de E et B_1, B_2 deux parties de F. Alors

(1) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$, $\quad f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$;

(2) Si $A_1 \subset A_2$, alors $f(A_1) \subset f(A_2)$;

(3) $A_1 \subset f^{-1}(f(A_1))$;

(4) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$, $\quad f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$;

(5) Si $B_1 \subset B_2$, alors $f^{-1}(B_1) \subset f^{-1}(B_2)$;

(6) $f(f^{-1}(B_1)) \subset B_1$.

Preuve : On démontre la propriété (2)

Soit $y \in f(A_1)$, alors $\exists x \in A_1 \mid f(x) = y$, et comme $A_1 \subset A_2$, donc $\exists x \in A_2 \mid f(x) = y$. D'où $y \in f(A_2)$.

□

Définition 2.8 (La composition) Soient E, F, G trois ensembles et f, g deux applications telles que

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

On peut en déduire une application de E vers G notée $h = g \circ f$ et appelée application composée de f et g, par

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

Remarque 2.3 En général, on a $f \circ g \neq g \circ f$ ceci est illustré par les fonctions réelles

$$f(x) = x^2, \quad g(x) = 2x + 1$$

$$f \circ g(x) = f[g(x)] = f(2x+1) = (2x+1)^2, \quad g \circ f(x) = g[f(x)] = g\left(x^2\right) = 2x^2 + 1.$$

Alors, $f \circ g \neq g \circ f$.

* Par contre la composition des applications est associative $h \circ (g \circ f) = (h \circ g) \circ f$.

2.2.3 Injection, surjection, bijection

Définition 2.9 Soient E, F deux ensembles et $f : E \longrightarrow F$ une application

1. f est injective si et seulement si

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

2. f est surjective si et seulement si

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

* Une autre formulation : f est surjective si et seulement si $f(E) = F$.

3. f est bijective si f à la fois injective et surjective. Autrement dit :

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

Remarque 2.4 Si f est bijective, et seulement dans ce cas, à tout $y \in F$ on fait correspondre un $x \in E$ et un seul. On définit ainsi une application bijective, notée

$$f^{-1} : F \longrightarrow E$$

et appelée application réciproque de f, et on a l'équivalence

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

Exemple. Soit $f : \mathbb{N} \longrightarrow \mathbb{Q}$ définie par $f(x) = \frac{1}{1+x}$. Montrons que f est injective Soit $x, x' \in \mathbb{N}$ tels que $f(x) = f\left(x'\right)$. Alors $\frac{1}{1+x} = \frac{1}{1+x'}$, donc $1 + x = 1 + x'$ et donc $x = x'$. Alors f est injective.

Par contre f n'est pas surjective. Il s'agit de trouver un élément y qui n'a pas d'antécédent par f. Ici il est facile de voir que l'on a toujours $f(x) \leq 1$ et donc par exemple $y = 2$ n'a pas d'antécédent. Ainsi f n'est pas surjective. Donc n'est pas bijective.

Théorème 2.1 Soient E, F, G trois ensembles et f, g deux applications telles que $f : E \longrightarrow F$ et $g : F \longrightarrow G$

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

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

3. Si f et g sont bijectives, alors $g \circ f$ est bijective.

4. Si f et g sont bijectives, alors $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Preuve.

1. Comme f et g sont injectives, alors

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

2. Comme f et g sont surjectives, alors on a

$$(g \circ f)(E) = g[f(E)] = g(F) = G.$$

3. Directement d'apres (1) et (2).

4. Soit $z \in G$, comme $g \circ f$ est bijective donc $\exists x \in E \mid (g \circ f)(x) = z$.

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

D'autre part $(f^{-1} \circ g^{-1})(z) = (f^{-1} \circ g^{-1})((g \circ f)(x)) = f^{-1}(g^{-1}(g(f(x))) = f^{-1}(f(x)) = x$.

Donc, $(g \circ f)^{-1}(z) = (f^{-1} \circ g^{-1})(z) \quad \forall z \in G$. D'où, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

$\square$

2.3 Exercices corrigé

Exercice1.

1. Soit l'ensemble $A = \{1, 2, 3, 4, 5\}$. Les propositions suivantes sont elles vraies ?

$$2 \in A, 3 \subset A, \emptyset \in A, \{\emptyset\} \subset A, A \cup \{\emptyset\} = A$$

2. Soient $B = \{1, 2\}$ et $C = \{1, 3\}$ deux ensembles.

(a) Déterminer $B \cap C, B \cup C, C_A(B), C_A(C), A \backslash B$ et $B \triangle C$.

(b) Déterminer $BC, B\emptyset, B\{\emptyset\}$ et $\mathcal{P}(\mathcal{P}(B))$.

Exercice2. Soient A, B, C trois parties de l'ensemble E. Montrer que :

1. $A \cap B = \emptyset \Leftrightarrow A \subset C_E(B)$

2. $A \subset B \Leftrightarrow C_E(B) \subset C_E(A)$.

3. $C_E(A \cap B) = C_E(A) \cup C_E(B), \quad C_E(A \cup B) = C_E(A) \cap C_E(B)$

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

5. $C_E(A) \Delta C_E(B) = A \triangle B, \quad C_E(A \triangle B) = C_E(A) \triangle B (*)$

6. $(AC) \cup (BC) = (A \cup B)C$.

7. $A \subset B \Rightarrow \mathcal{P}(A) \subset \mathcal{P}(B)$.

Exercice3. Soient A, B, C trois parties de l'ensemble E. Montrer que :

1. $A = B \Leftrightarrow A \cap B = A \cup B$.

2. $A \cup B = A \cap C \Leftrightarrow B \subset A \subset C$.

3. $A \cap B = \emptyset \Leftrightarrow C_E(A) \cup C_E(B) = E$.

4. $A \triangle B = \emptyset \Leftrightarrow A = B$.

5. $(A \cap B) \backslash C = (A \backslash C) \cap (B \backslash C) = (A \backslash C) \cap B = (B \backslash C) \cap A$.

Exercice4. Soit $f : E \longrightarrow F$ une application. Soient A, B deux parties de l'ensemble E et C, D deux parties de l'ensemble F. Montrer que :

1. $f(A \cap B) \subset f(A) \cap f(B), \quad f(A \cup B) = f(A) \cup f(B) (*)$

2. f est injective $\Leftrightarrow f(A \cap B) = f(A) \cap f(B)$.

3. $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D), \quad f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D) (*)$

4. $f\left(f^{-1}(C)\right) \subset C$.

5. f est surjective $\Leftrightarrow f\left(f^{-1}(C)\right) = C$.

6. $f^{-1}\left(C_F(C)\right) = C_E f^{-1}(C)$. 7. $f^{-1}(C \triangle D) = f^{-1}(C)\Delta f^{-1}(D)$.

Exercice5. Soit l'application f définie par

$$f : \mathbb{R} \longrightarrow \mathbb{R}$$

$$x \longmapsto$$

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

1. f est-elle injective ? surjective ?

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

3. Montrer que l'application g définie par

$$g : [-1, 1] \longrightarrow [-1, 1]$$

$$x \longmapsto g(x) = f(x)$$

est une bijection et trouver l'application réciproque g^{-1}.

Exercice6. Soit E un ensemble non vide. On considère une application f de E dans $\mathbb{R}$ telle que

$$\begin{cases} \text{i) } f(\phi) = 0, \\ \text{ii) } f(E) = 1, \\ \text{iii) } \forall A, B \in \mathcal{P}(E) : f(A \cup B) = f(A) + f(B), \text{ si } A \cap B = \phi. \end{cases}$$

1. Pour toute partie A de E, exprimer $f\left(C_E^A\right)$ en fonction de $f(A)$.

2. Démontrer que : $\forall A, B \in \mathcal{P}(E) : f(A \cup B) = f(A) + f(B) - f(A \cap B)$.

3. On suppose de plus que

$$\text{iv) } \forall A \in \mathcal{P}(E) : f(A) \geq 0.$$

(a) Montrer que $\forall A, B \in \mathcal{P}(E) : A \subset B \Rightarrow f(A) \leq f(B)$.

(b) Montrer que $\forall A \in \mathcal{P}(E) : 0 \leq f(A) \leq 1$.

2.3.1 corrigé

Exercice1.

1.

* $2 \in A$ signifie que 2 est un élément de A. Elle est vraie car les éléments de A sont 1,2 et 3 .

* $3 \subset A$ signifie que 3 est une par lie de A. Elle est fausse car 3 ust un élément de A et non une partie de A.

* $\phi \in A$ signifie que ϕ est un élément de A. Elle est fausse car lu élément de A sont 1, 2 et 3 mais ϕ ne figure pas parmi ce éléments

* $\{\phi\} \subset A$ signifie que le singleton $\{\phi\}$ est une partie de A Elle est fausse car $\{\phi\}$ est une partie de $P(A)$ et non partie de A.

* $A \cup \{\phi\} = \{1, 2, 3, \phi\}$. Ene est fausse car A possède trois éléments.

2.

a) $B \cap C = \{1\}; B \cup C = \{1, 2, 3\}; C_A(B) = \{3, 4, 5\}; C_A(C) = \{2, 4, 5\}; A \backslash B = \{3, 4, 5\}$.

$B \triangle C = \{B \cup C) \backslash (B \cap C) = \{1, 2, 3\} \backslash \{1\} = \{2, 3\}$

b)

* $BC = \{(x, y) \mid x \in B \wedge y \in C\} = \{(1, 1), (1, 3), (2, 1), (2, 3)\}$.

* $B\phi = \{(x, y) \backslash x \in B \wedge y \in \phi\}$ or ϕ ne contient aucun élément, alors $B\phi = \phi$.

* $B\{\phi\} = \{(x, y) \backslash x \in B \wedge y \in \{\phi\}\} = \{(1, \phi), (2, \phi)\}$.

* $P(B) = \{\phi, B, \{1\}, \{2\}\}$, donc

$$\begin{aligned} P(P(B)) = \ & \{\phi; P(B); \{\phi\}; \{B\}; \{\{1\}\}; \{\{2\}\}; \{\phi, B\}; \{\phi, \{1\}\}; \{\phi, \{2\}\}; \{B, \{1\}\}; \{B, \{2\}\}; \\ & \{\{1\}, \{2\}\}; \{\phi, B, \{1\}\}; \{\phi, B, \{2\}\}; \{B, \{1\}, \{2\}\}; \{\phi, \{1\}, \{2\}\}. \end{aligned}$$

Exercice2.

1. $A \cap B = \phi \Leftrightarrow A \subset \underset{E}{C}(B)$.

$\Rightarrow$ On a $A \cap B = \phi$. Soit $x \in A$ et supposons que $x \notin \underset{E}{C}(B)$.

Alors $x \notin \underset{E}{C}(B) \Rightarrow x \in \underset{E}{C}(C_E(B)) = B \Rightarrow x \in A \cap B \Rightarrow A \cap B \neq \phi$

ce qui est absurde . Donc $x \in C_E(B)$

$\Leftarrow$ On suppose que $A \cap B \neq \phi$. Alors, $\exists x \in E / x \in A \cap B \Rightarrow x \in A \wedge x \in B$ et comme $A \subset C_E(B)$, donc

$$x \in \underset{E}{C}(B) \wedge x \in B \Rightarrow x \in \underset{E}{(B)} \cap B = \phi$$

Contradiction. Donc, $A \cap B = \phi$.

2. $A \subset B \Longleftrightarrow C_E(B) \subset C_E(A)$.

$\Rightarrow$ Supposons que $A \subset B$ et $x \in C_E(B)$. Alors $x \in \underset{E}{C}(B) \Rightarrow x \notin B$ et comme $A \subset B$.

donc $x \notin A \Rightarrow x \in {}_E(A) \Rightarrow C_E(B) \subset (A)$.

$\Leftarrow$ On a $\underset{E}{C}(B) \subset \underset{E}{C}(A)$ Alors, $x \in A \Rightarrow x \notin \underset{E}{C}(A) \Rightarrow x \notin \underset{E}{C}(B) \Rightarrow x \in B$.

Danc, $A \subset B$.

3. $C_E(A \cap B) = C_E(A) \cup C_E(B)$

$$\begin{aligned} x \in C_E(A \cap B) &\Leftrightarrow x \notin (A \cap B) \Longleftrightarrow x \notin A \vee x \notin B \\ &\Leftrightarrow x \in \underset{E}{C}(A) \vee x \in \underset{E}{C}(B) \\ &\Leftrightarrow x \in \underset{E}{C}(A) \cup \underset{E}{C}(B). \end{aligned}$$

De même pour la réunion.

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

$$\begin{aligned} A \backslash (B \cup C) &\overset{\text{Déf}}{=} A \cap C(B \cup C) \overset{(3)}{=} A \cap \Big(C_E(B) \ \cap \ C_E(C) \Big) \\ &= \Big(A \cap C_E(B) \Big) \cap \Big(A \cap C_E(C) \Big) \overset{\text{Déf}}{=} (A \backslash B) \cap (A \backslash C). \end{aligned}$$

5. $C_E(A) \Delta C_E(B) = A \triangle B$,

D après la définition : $A \Delta B = (A \backslash B) \cup (B \backslash A) = (A \cap C_E(B)) \cup (B \cap C_E(A))$ En remplaçant A par $C_E(A)$ et B par $\underset{E}{C}(B)$ dans la formule précédente

$$\underset{E}{C}(A) \Delta \underset{E}{C}(B) = (\underset{E}{C}(A) \backslash \underset{E}{C}(B)) \cup (\underset{E}{C}(B) \backslash \underset{E}{C}(A) = (C\underset{E}{(A)} \cap B) \cup (\underset{E}{C}(B) \cap A)$$

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

Car $\cap, U$ sont des lois commutatives.

6. $(AC) \cup (BC) = (A \cup B)C$.

$$\begin{aligned}(AC) \cup (BC) &= \{(x,y)/(x,y) \in AC \text{ ou } (x,y) \in BC\} \\ &= \{(x,y) \mid (x \in A \text{ et } y \in C) \text{ ou } (x \in B \text{ et } y \in C\} \\ &= \{(x,y) \mid (x \in A \text{ ou } x \in B) \text{ et } y \in C\} \\ &= (A \cup B)C.\end{aligned}$$

7. $A \subset B \Rightarrow P(A) \subset P(B)$.

D'après la définition : $P(A) = \{X \mid X \subset A\}$ on trouve :

$X \in P(A) \Rightarrow X \subset A$ et comme $A \subset B$. Alors, $X \subset B \Rightarrow x \in P(B)$. Donc l' inclusion.

Exercice4.

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

Soit $y \in f(A \cap B)$, il existe $x \in A \cap B$ tel que $y = f(x)$, or $x \in A$ donc $y = f(x) \in f(A)$ et de même $x \in B$ donc $y \in f(B)$.

D'ou , $y \in f(A) \cap f(B)$.

2. $f$est injective $\Leftrightarrow f(A \cap B) = f(A) \cap f(B)$.

$\Longleftarrow$ Soient $x_1, x_2 \in E$ tels que $f(x_1) = f(x_2)$. Posons $A = \{x_1\}$

$B = \{x_2\}$ **. Ona** $g(x_1) = g(x_2) \in g(A) \cap g(B) = g(A \cap B)$**.**

Donc, $g(A \cap B) \neq \phi$ et par suite, $A \cap B \neq \phi$. Ceci implique $x_1 = x_2$.

$\Longrightarrow$ On a dáprès (1) $f(A \cap B) \subset f(A) \cap f(B)$.

On démontre maintenant que$f(A) \cap f(B) \subset f(A \cap B)$.

Soit $y \in f(A) \cap f(B) \Rightarrow y \in f(A) \wedge y \in f(B)$.

$\Rightarrow \exists x \in A | y = f(x) \wedge \exists \bar{x} \in B | y = f(x')$ **.**

Alors, $f(x) = f(x')$ et comme$f$ est invective donc $x = \bar{x}$

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

Donc, $f(A) \cap f(B) \subset f(A \cap B)$. D'ou, $f(A \cap B) = f(A) \cap f(B)$.

3. $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$

$$\begin{aligned} f^{-1}(C \cap D) &= \{x; f(x) \in C \cap D\} \\ &= \{x; f(x) \in C \wedge f(x) \in D\} \\ &= \{(x; f(x) \in C) \text{ et } (x; f(x) \in D)\} \\ &= f^{-1}(C) \cap f^{-1}(D). \end{aligned}$$

4. Soit $f(x) \in f\left(f^{-1}(c)\right) \Rightarrow x \in f^{-2}(C) \Rightarrow f(x) \in C$

Donc, $f\left(f^{-1}(c)\right) \subset C$.

5. f est surjective $\Leftrightarrow f\left(f'(c)\right) = C$.

$\Longleftarrow$ on démontre que $\forall y \in F, \exists x \in E \mid y = f(x)$.

$\forall y \in F : y \in \{y\}$ et d'après l'hypothèse on pent écrit $\{y\} = f\left(f^{-1}(\{y\})\right)$

Alors, Il existe un élément E avec $x \in f^{-1}(\{y\}) \Rightarrow f(x) \in \{y) \Rightarrow f(x) = y$

$\Longrightarrow$ On a d' après (4) $f\left(f^{-1}(c)\right) \subset C$, on démontre main tannant que $C \subset f\left(f'(c)\right)$.

Soit $y \in C$, donc $y \in F$ et commefert surjective. Alors

$$\exists x \in E \mid y = f(x). \text{ Donc, } f(x) \in C \Rightarrow x \in f^{-1}(c) \Rightarrow f(x) \in f\left(f^{-1}(c)\right)$$

Aloß, $y \in f\left(f^{-1}(C)\right)$. D' où, $f\left(f^{-1}(C)\right) \supset C$.

(6) $f^{-1}\left(C_F(C)\right) = C_E f^{-1}(C)$.

$$\begin{aligned} x \in f^{-1}\left(C_F(C)\right) \Leftrightarrow f(x) \in C_E(C) \Leftrightarrow f(x) \notin C \Leftrightarrow x \notin f^{-1}(C) \\ \Leftrightarrow x \in \int_F^{f^{-1}(C)} . \end{aligned}$$

(7) $f^{-1}(C \triangle D) = f^{-1}(C) \Delta f^{-1}(D)$.

$$\begin{aligned} f^{-1}(C \Delta D) &= f^{-1}((C \backslash D) \cup (D \backslash C)) = f^{-1}(C \backslash D) \cup \hat{f}^{-1}(D \backslash C) \\ &= f^{-1}(C \cap C_F(D)) \cup f^{-1}(D \cap C_F(C)) \\ &= \left(f^{-1}(C) \cap f^{-1}(C_F(D))\right) \cup \left(f^{-1}(D) \cap f^{-1}(C_F(C))\right). \\ &= \left(f^{-1}(C) \cap C_E f^{-1}(D)\right) \cup \left(f^{-1}(D) \cap C_E f^{-1}(C)\right). \\ &= \left(f^{-1}(C) \backslash f^{-1}(D)\right) \cup \left(f^{-1}(D) \backslash f^{-1}(C)\right) \\ &= f^{-1}(C) \Delta f^{-1}(D). \end{aligned}$$

Exercice5.

1. f n'est pas injective car $f(2) = f(1/2) = \frac{4}{5}$ mais $2 + \frac{1}{2}$.

f nést pas surjective car "2" n'apas d'antécédent

En effet : L'equation $f(x) = 2$ devient $x^2 - x + 1 = 0$ qui ná pas de solutions réelles.

2. On sait que $f(\mathbb{R}) = [-1, 1]$ si léquation $f(x) = y$ admet une solution $x, \forall y \in [-1, 1]$.

$$f(x) = y \Rightarrow yx^2 - 2x + y = 0.......(*)$$

$$\Delta = 1 - y^2$$

$(*)$ admet une solution ssi $\triangle' \geqslant 0$, donc il y a des solutions siet seulement si $y \in [-1, 1]$.

Donc, $f(R) = [-1, 1]$.

3. g est bijechive $\Leftrightarrow$ gest injective et surjective

$\Leftrightarrow \forall y \in [-1, 1]$, léquation $g(x) = y$ a une sodution unique

$\Leftrightarrow \forall y \in [-1, 1], \exists! x \in [-1, 1] : g(x) = y$.

Soit $y \in [-1, 1]$. Alor, les solvtions de $g(x) = x$ soit $\begin{cases} x = \frac{1-\sqrt{1-y^2}}{y} \\ x = \frac{1+\sqrt{1-y^2}}{y} \end{cases}$

$\Longrightarrow \begin{cases} x = \frac{y}{1+\sqrt{1-y^2}} & \in [1, -1] \\ x = \frac{1+\sqrt{1-y^2}}{y} & \notin [1, -1] \end{cases}$

Donc, la senle solution est $x = \frac{y}{1+\sqrt{1-y^2}}$. D'ou g est bijective.

$$g^{-1} : [-1, 1] \longrightarrow [-1, 4]$$
$$y \longmapsto g^{-1}(y) = \frac{1 - \sqrt{1 - y^2}}{y}$$

Chapitre 3

Relations binaires sur un ensemble

3.1 Définitions de base

Définition 3.1 (Relation binaire) Soit E un ensemble. Une relation binaire $\mathcal{R}$ sur E est une propriété portant sur les couples d'éléments de E. On notera $x\mathcal{R}y$ le fait que la propriété est vraie pour le couple $(x, y) \in EE$.

Exemple.

1. L'inégalité $\leq$ est une relation sur $\mathbb{N}, \mathbb{Z}$ et $\mathbb{R}$.
2. La relation d'inclusion dans l'ensemble des parties de E : $A\mathcal{R}B \Leftrightarrow A \subset B$.
3. La relation de divisibilité sur les entiers relatifs : $m\mathcal{R}n \Leftrightarrow m$ divise n.

Définition 3.2 Soit $\mathcal{R}$ une relation sur un ensemble E.

1. $\mathcal{R}$ est réflexive si pour tout $x \in E$ on a $x\mathcal{R}x$;
2. $\mathcal{R}$ est symétrique si pour tout $x, y \in E$ on a $x\mathcal{R}y \Rightarrow y\mathcal{R}x$;
3. $\mathcal{R}$ est antisymétrique si pour tout $x, y \in E, (x\mathcal{R}y \wedge y\mathcal{R}x) \Rightarrow x = y$;
4. $\mathcal{R}$ est transitive si pour tout $x, y, z \in E, (x\mathcal{R}y \wedge y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.

3.2 Relation d'équivalence

Définition 3.3 (Relation d'équivalence) Une relation binaire $\mathcal{R}$ sur E est une relation d'équivalence si et seulement si elle est réflexive, symétrique et transitive.

Exemple 1. La relation $\mathcal{R}$ «être parallèle » est une relation d'équivalence pour l'ensemble E des droites affines du plan :

1. réflexivité : une droite est parallèle à elle-même ;

2. symétrie : si D est parallèle à D' alors D' est parallèle à D ;

3. transitivité : si D parallèle à D' et D' parallèle à D'' alors D est parallèle à D''.

Exemple 2. On considère la relation suivante sur $\mathbb{Z}$

$$x\mathcal{R}y \Leftrightarrow \exists k \in \mathbb{Z} \mid x - y = 2k$$

1. $\mathcal{R}$ est réflexive, car $\exists k = 0 \mid x - x = 2k = 0$, donc $x\mathcal{R}x$.

2. Supposons que $x\mathcal{R}y$, alors $\exists k \in \mathbb{Z} \mid x - y = 2k \Rightarrow y - x = 2k'$ avec $k' = -k \in \mathbb{Z}$. Donc, $y\mathcal{R}x$. D'où, $\mathcal{R}$ est symétrique.

3. Supposons que $x\mathcal{R}y$ et $y\mathcal{R}z$. Alors, $(\exists k \in \mathbb{Z} \mid x - y = 2k)$ et $(\exists k' \in \mathbb{Z} \mid y - z = 2k')$ avec l'addition nous trouvons $x - z = 2k''$ avec $k'' = (k + k') \in \mathbb{Z}$. Donc, $x\mathcal{R}z$. D'où, $\mathcal{R}$ est transitive. Alors, $\mathcal{R}$ est une relation d'équivalence.

Définition 3.4 Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. On appelle classe d'équivalence d'un élément $x \in E$ l'ensemble des éléments de E en relation avec x par $\mathcal{R}$, notée par $\mathcal{C}(x)$ ou bien $\bar{x}$

$$\bar{x} = \{y \in E \mid y\mathcal{R}x\}$$

Définition 3.5 Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. L'ensemble quotient de E par $\mathcal{R}$ est l'ensemble des classes d'équivalence de $\mathcal{R}$, notée $E/\mathcal{R}$

$$E/\mathcal{R} = \{\bar{x} \mid x \in E\}$$

Exemple. Dans l'exemple précédent on a

$$\begin{aligned}\bar{x} &= \{y \in E \mid y\mathcal{R}x\}\\ &= \{y \in E \mid x - y = 2k\}\\ &= \{x - 2k : k \in \mathbb{Z}\}\\ &= \{\ldots, x - 4, x - 2, x, x + 2, x + 4, \ldots\}.\end{aligned}$$

$$\overline{0} = \{y \in E \mid 0\mathcal{R}y\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}, \overline{1} = \{y \in E \mid 1\mathcal{R}y\} = \{\ldots, -3, -1, 1, 3, \ldots\}$$

et $\overline{2} = \overline{0}$. **Alors,** $\mathbb{Z}/\mathcal{R} = \{\bar{x} \mid x \in E\} = \{\overline{0}, \overline{1}\}$

Proposition 3.1 Soit $\mathcal{R}$ une relation d'équivalence sur E. Alors

1. Une classe d'équivalence est un sous-ensemble de l'ensemble E, c.à.d

$$\forall x \in E, \bar{x} \subset E$$

2. Une classe d'équivalence n'est jamais vide, c.à.d

$$\forall x \in E, \bar{x} \neq \phi$$

3. L'intersection de deux classes d'équivalence distinctes est vide, c.à.d

$$\forall x, y \in E, \bar{x} \cap \bar{y} = \phi$$

4. $\forall x, y \in E, x\mathcal{R}y \Leftrightarrow \bar{x} = \bar{y}$

Théorème 3.1 Soit $\mathcal{R}$ une relation d'équivalence sur E. Les classes d'équivalence $(\bar{x})_{x \in E}$ constituent une partition de E

$$E = \cup_{x \in E} \bar{x}$$

3.3 Relation d'ordre

Définition 3.6 (Relation d'ordre) Une relation binaire $\mathcal{R}$ sur E est une relation d'ordre si et seulement si elle est réflexive, antisymétrique et transitive. On dit alors que $(E, \mathcal{R})$ est un ensemble ordonné.

Exemple.

1. L'inégalité $\leq$ est une relation d'ordre sur $\mathbb{N}, \mathbb{Z}$ et $\mathbb{R}$.

2. La relation d'inclusion dans l'ensemble des parties de E est une relation d'ordre : $A\mathcal{R}B \Leftrightarrow A \subset B$

Définition 3.7 Soit $\mathcal{R}$ une relation d'ordre sur E. Deux éléments x et y de E sont dits comparables si $x\mathcal{R}y$ ou $y\mathcal{R}x$.

Définition 3.8 (L'ordre total et l'ordre partiel) Soit $\mathcal{R}$ une relation d'ordre sur E. Si deux éléments quelconques x et y sont toujours comparables on dit que $\mathcal{R}$ est une relation d'ordre total et l'ensemble E est dit totalement ordonné. Sinon (c'est-à-dire s'il existe au moins deux éléments non comparables x et y), on dit que $\mathcal{R}$ est une relation d'ordre partiel et l'ensemble E est dit partiellement ordonné.

Exemple.

1. $\leq$ est un ordre total sur $\mathbb{N}, \mathbb{Z}$ et $\mathbb{R}$.

2. La divisibilité dans $\mathbb{N}^*$ est un ordre partiel.

Définition 3.9 Soient $\mathcal{R}$ une relation d'ordre sur E et M, m deux élément de E.

1. M est un majorant d'une partie A de E si $x\mathcal{R}M$ pour tout $x \in A$;

2. m est un minorant d'une partie A de E si $m\mathcal{R}x$ pour tout $x \in A$.

Exemple.

1. L'ensemble $\{8, 10, 12\}$ est minoré par 2 et majoré par 120 pour la relation de divisibilité "/ sur $\mathbb{N}$;

2. $\mathcal{P}(E)$ est minoré par ϕ et majoré par E pour la relation d'inclusion $\subset$.

3.4 Exercices corrigé

Exercice1. Dans $\mathbb{R}$, on définit la relation binaire $\mathcal{R}$ par

$$\forall x, y \in \mathbb{R} : x\mathcal{R}y \Longleftrightarrow x^2 - 1 = y^2 - 1$$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{R}$.

2. Donner l'ensemble quotient $\mathbb{R}/\mathcal{R}$.

Exercice2. Pour tout $n \in \mathbb{N}^*$, on définit une relation binaire sur $\mathbb{Z}$ par

$$\forall x, y \in \mathbb{Z} : x\mathcal{R}y \Longleftrightarrow \exists k \in \mathbb{Z} \mid x - y = kn$$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{Z}$.

2. Supposons que $n = 3$:

(a) Déterminer la classe d'équivalence de $x \in \mathbb{Z}$. En déduire les classes $\overline{0}, \overline{1}, \overline{2}$.

(b) Montrer que $\forall m \in \mathbb{Z} : \overline{0} = \overline{3m}, \overline{1} = \overline{3m+1}, \overline{2} = \overline{3m+2}$.

(c) Montrer que $\overline{0} \cap \overline{1} = \emptyset, \overline{1} \cap \overline{2} = \emptyset, \overline{0} \cap \overline{2} = \emptyset$. En déduire l'ensemble quotient $\mathbb{Z}/\mathcal{R}$.

Exercice3. Soit E un ensemble et soit A une partie de E. On définit sur $\mathcal{P}(E)$ la relation binaire $\mathcal{R}$ par

$$\forall X, Y \in \mathcal{P}(E) : X\mathcal{R}Y \iff A \cap X = A \cap Y$$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathcal{P}(E)$.

2. Déterminer les classes d'équivalence de $\emptyset$ et E. En déduire $\bar{A}$ et $\overline{C_E(A)}$.

Exercice4. Soit $\mathcal{R}$ une relation binaire sur $\mathbb{R}^3$ définie par

$$(x, y, z)\mathcal{R}(a, b, c) \iff (|x - a| \leq b - y \text{ et } z = c).$$

1. Montrer que $\mathcal{R}$ est une relation d'ordre sur $\mathbb{R}^3$.

2. L'ordre est-il total sur $\mathbb{R}^3$?

Exercice5. On définit sur $\mathbb{R}^2$ une relation binaire $\mathcal{R}$ par

$$\forall (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2 : (x_1, y_1)\, \mathcal{R}\, (x_2, y_2) \iff x_1 \leq x_2 \text{ et } y_1 \leq y_2.$$

1. Montrer que $\mathcal{R}$ est une relation d'ordre sur $\mathbb{R}^2$.

2. Les éléments $(2, 4), (3, 1)$ de $\mathbb{R}^2$ sont-ils comparables par $\mathcal{R}$?

3. L'ordre est-il total sur $\mathbb{R}^2$?

4. Déterminer l'ensemble des majorants de $A = \{(1, 2), (3, 1)\} \subset \mathbb{R}^2$.

Exercice6. Les relations $\mathcal{R}$ définies ci-dessous sont-elles des relations d'ordre ?

1. $\forall x, y \in \mathbb{R} : x\mathcal{R}y \iff e^x \leq e^y$;

2. $\forall x, y \in \mathbb{R} : x\mathcal{R}y \iff |x| \leq |y|$

3. $\forall x, y \in \mathbb{N} : x\mathcal{R}y \iff \exists p, q \geq 1 \mid y = px^q$ (p et q sont des entiers) ;

4. $\forall x, y \in \mathbb{N}^* : x\mathcal{R}y \iff \exists m \in \mathbb{N}^* \mid y = mx$;

5.$\forall x, y \in]1, +\infty[: x\mathcal{R}y \iff \frac{x}{1+x^2} \geq \frac{y}{1+y^2}$

3.4. Exercices corrigé

3.4.1 corrigé

Exercice1.

1. $\forall x, y \in \mathbb{R} : x\mathcal{R}y \Longleftrightarrow x^2 - 1 = y^2 - 1$

(i) La réflexivité : $\forall x \in \mathbb{R}, x^2 - 1 = x^2 - 1 \Rightarrow xRx$.

ii) La symétrie : $x\mathcal{R}y \Leftrightarrow x^2 - 1 = y^2 - 1 \Rightarrow y^2 - 1 = x^2 - 1 \Rightarrow y\mathcal{R}x$.

iii) La kansitivité :

$$\begin{cases} x\mathcal{R}y \\ y\mathcal{R}z \end{cases} \Leftrightarrow \begin{cases} x^2 - 1 = y^2 - 1 \\ y^2 - 1 = z^2 - 1 \end{cases} \Rightarrow x^2 - 1 = z^2 - 1 \Rightarrow x\mathcal{R}z.$$

Donc, $\mathcal{R}$ est une relation équivalents.

2. $\mathbb{R}/\mathbb{R} = \{\bar{x} : x \in \mathbb{R}\}$.

On a $\bar{x} = \{y \in \mathbb{R} \mid y\mathbb{R}x\} = \{y \in \mathbb{R} \mid y^2 - 1 = x^2 - 1\} = \{x, -x \mid x \in \mathbb{R}\}$

Alors $, \mathbb{R}/\mathbb{R} = \{\{x_1 - x\}, x \in \mathbb{R}\}$.

Exercice2.

1. $\forall x, y \in \mathbb{Z} : xRy \Leftrightarrow \exists k \in \mathbb{Z} \mid x - y = kn$.

- La réflexivité : On sait que $\forall x \in \mathbb{Z} : x - x = 0 = 0.n$, avec $k = 0 \in \mathbb{Z}$,donc $x\mathcal{R}x$
- Lu symétrique : $xRy \Leftrightarrow x - y = kn \Rightarrow y - x = (-k) \cdot n = k' \cdot n$ avec $k' = -k \in \mathbb{Z}$ Donc, $y\mathcal{R}x$
- La transitivité :

$$\begin{cases} xRy \\ xRz \end{cases} \Leftrightarrow \begin{cases} x - y = k_1 \cdot n / k_1 \in \mathbb{Z} \\ y - z = k_2 \cdot n / k_2 \in \mathbb{Z} \text{ donne :} \end{cases} \text{; La sommation membre à nembre dome :}$$

$$x - z = (k_1 + k_2)n = k_3.n \text{ avec } k_3 = k_1 + k_2 \in \mathbb{Z}$$

Donc, $x\mathcal{R}z$

2. Pour $n = 3$: $\quad \forall x, y \in \mathbb{Z} : x\mathcal{R}y \Leftrightarrow \exists k \in \mathbb{Z} : x - y = 3k$.

(a) Pour tout

$$x \in \mathbb{Z} : \bar{x} = \{y \in \mathbb{Z} : yRx\} = \{y \in \mathbb{Z} : y = x + 3k\}$$
$$= \{x + 3k \mid k \in \mathbb{Z}\}.$$

En particulier :

$$\bar{O} = \{y \in \mathbb{Z} : yRO\} = \{3k \mid k \in \mathbb{Z}\} = 3\mathbb{Z}$$

$$\overline{1} = \{y \in \mathbb{Z} : y\mathbb{R}1\} = \{3k + 1/k \in \mathbb{Z}\} = 3\mathbb{Z} + 1$$

$$\bar{z} = \{y \in \mathbb{Z} : yR2\} = \{3k + 2 \mid k \in \mathbb{Z}\} = 3\mathbb{Z}.2.$$

(b)

$$\forall m \in \mathbb{Z} : \begin{cases} \overline{0} = \overline{3m} \\ \overline{1} = \overline{3m+1} \\ \overline{2} = \overline{3m+2} \end{cases} \quad \text{car} \quad \forall m \in \mathbb{Z} : \begin{cases} 0R(3m) \\ 1R(3m+1) \\ 2R(3m+2) \end{cases}.$$

$$\text{En effet } \forall m \in \mathbb{Z} : \begin{cases} 0 - (3m) = 3(-m) \\ 1 - (3m+1) = 3(-m) \\ 2 - (3m+2) = 3(-m) \end{cases}, \quad -m \in \mathbb{Z}.$$

(C)

$$\text{On a } \begin{cases} \overline{0} \cap \overline{1} = \phi \\ \overline{1} \cap \overline{2} = \phi \\ \overline{0} \cap \overline{2} = \phi \end{cases}, \text{ car } \begin{cases} 0\not R1 \\ 1\not R2 \\ 0\not R2 \end{cases} \text{ En effet } \begin{cases} 0 - 1 = -1 \neq 3k_1 \\ 1 - 2 = -1 \neq 3k_2 \\ 0 - 2 = -2 \neq 3k_3 \end{cases} \quad \mid k_1, k_2, k_3 \in \mathbb{Z}$$

On sait que

$$\mathbb{Z}/R = \{\bar{x} : x \in \mathbb{Z}\}$$
$$= \{\bar{x} : x = 3m\} \cup \{\bar{x} : x = 3m + 1\} \cup \{\bar{x} : x = 3x + 2\}.$$
$$= \{\overline{0}, \overline{1}, \overline{2}\}.$$

Exercice4. $(x, y, z)R(a, b, c) \Leftrightarrow (|x - a| \leqslant b - y \text{ et } z = c)$

(1)

(i) La réflexivité, $(x, y, z)R(x, y, z) \Leftrightarrow (|x - x| = 0 \leqslant y - y = 0 \text{ et } z = z)$ alors R et réflexive.

(ii) L' anti-symétrique : Supposons $(v, y, z)R(a, b, c)$ et $(a, b, c)R(x, y, z)$

Ceci implique $[(|x - a| \leqslant b - y \quad (*) \text{ et } |a - x| \leqslant y - b \quad (**)) \text{ et } z = c]$

Alors, $(*) + (**)$ donne : $x = a$, on remplace $x = a$ dans $(*)$ et $(**)$ on trouve $y = b$

Donc, $(x, y, z) = (a, b, c)$. D'ou, R est anti-symétrique.

(iii) La transitivité : Supposons $(v, y, z)R(a, b, c)$ et $(a, b, c)R(\alpha, \beta, \gamma)$

Ceci implique $[(|x - a| \leqslant b - y \ \ (*)$ et $|a - \alpha| \leqslant \beta - b \ \ (**))$ et $z = c = \gamma]$

alors, $(*) + (**)$ donne $(|x - a| + |a - \alpha| \leqslant b - y + \beta - b$ et $z = c = \gamma)$.

et comme $(|x - \alpha| = |x - a + a - \alpha| \leqslant |x - a| + |a - \alpha| \leqslant y + \beta$ et $z = \gamma)$ implique $(x, y, z)R(\alpha, \beta, \gamma)$. Donc, R est transitive.

D'ou, R est une relation d' ordre sur $\mathbb{R}^3$.

(2) R n'est pas total car $\exists(x, y, z) = (0, 0, 2) \in \mathbb{R}^3$ et $(a, b, c) = (0, 0, 3) \in \mathbb{R}^3$ tels que $(0, 0, 2)\not{R}(0, 0, 3)$ et $(0, 0, 3)\not{R}(0, 0, 2)$.

Exercice5. $\forall\, (x_1, y_1)\,, (x_2, y_2) \in \mathbb{R}^2 : x_1 \leqslant x_2$ et $y_1 \leqslant y_2$.

(1)

(i) La réflexivité, on sait que

$$\forall (x, y) \in \mathbb{R}^2 : \begin{cases} x \leqslant x \\ y \leqslant y \end{cases} \Rightarrow (x, y)R(x, y) \Rightarrow R\text{est réflexive.}$$

(ii) L' anti-symétrique : supposons $(x_1, y_1)\, R\, (x_2, y_2)$ et $(x_1, y_2)\, R\, (x_1, y_1)$

$$\Rightarrow \begin{cases} x_1 \leqslant x_2 \wedge y_1 \leqslant y_2 \\ \wedge \\ x_2 \leqslant x_1 \wedge y_2 \leqslant y_1 \end{cases} \Rightarrow \begin{cases} x_1 = x_2 \\ \wedge \\ y_1 = y_2 \end{cases} \Rightarrow (x_1, y_1) = (x_2, y_2)\ \text{. Donc } R \text{ est anti-symétrique}$$

(iii) La transitivité : Soient $(x_1, y_1)\,, (x_2, y_2)\,, (x_3, y_3) \in \mathbb{R}^2$

$$\begin{cases} (x_1, y_1)\, R\, (x_2, y_2) \\ \wedge \\ (x_2, y_2)\, R\, (x_3, y_3) \end{cases} \Rightarrow \begin{cases} x_1 \leqslant x_2 \wedge y_1 \leqslant y_2 \\ \wedge \\ x_2 \leqslant x_3 \wedge y_2 \leqslant y_3 \end{cases} \Rightarrow \begin{cases} x_1 \leqslant x_3 \\ \wedge \\ y_1 \leqslant y_3 \end{cases} \Rightarrow (x_1, y_1)\, R\, (x_3, y_3)$$

Donc, R est transitive. D'où, R est une relation d'ordre sur $\mathbb{R}^2$.

(2) $(2, 4)$ et $(3, 1)$ ne sont pas comparables car $(1, 4)$ et $(3, 1)$ ne vérifient pas la relation. En effet

$$\begin{cases} 2 \leqslant 3 \\ \wedge \\ 4 \not\leqslant 1 \end{cases} \text{et} \begin{cases} 3 \not\leqslant 2 \\ \wedge \\ 1 \leqslant 2 \end{cases} \Rightarrow \begin{cases} (2, 4)\not{R}(3, 1) \\ \wedge \\ (3, 1)\not{R}(2, 4) \end{cases}$$

(3) L'ordre est partiel car $\exists a = (2,4)$ et $b = (3,1) / a \not{R} b \wedge b \not{R} a$.

(4) $t = (x,y) \in \mathbb{R}^2$ est un majorant de $A \Leftrightarrow \forall a \in A : aRt$.

$$\Rightarrow \begin{cases} (1,2)R(x,y) \\ \wedge \\ (3,1)R(x,y) \end{cases} \Rightarrow \begin{cases} 1 \leqslant x \wedge 2 \leqslant y. \\ \wedge \\ 3 \leqslant x \wedge 1 \leqslant y. \end{cases} \Rightarrow \begin{cases} x \geqslant 3 \\ \wedge \\ y \geqslant 2 \end{cases}$$

$$\Rightarrow \underset{\mathbb{R}^2}{\mathrm{Maj}}(A) = \{(x,y) : x \geqslant 3 \wedge y \geqslant 2\}.$$

Chapitre 4

Structures algébriques

4.1 Lois de composition internes et ses propriétés

4.1.1 Lois de composition internes

Définition 4.1 Soit E un ensemble. Une loi de composition interne $*$ sur E est une application de EE vers E

$$\begin{aligned} * : EE &\longrightarrow E \\ (x, y) &\mapsto x * y \end{aligned}$$

Notations

1. Plutôt que loi de composition interne, on dit aussi opération de composition interne, ou plus simplement opération interne ;

2. On note souvent $(E, *)$ pour désigner un ensemble E muni d'une opération interne $*$.

Exemple.

1. Les lois $\cup$ (union), $\cap$ (intersection) et $\triangle$ (différence symétrique) sur $\mathcal{P}(E)$;

2. La loi (la composition) sur $\mathcal{F}(E)$ (l'ensemble des applications de E vers E).

3. Les lois $+$ et sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$.

4. Soit * définie sur $\mathbb{R}$ par : $x * y = \frac{1}{x+y}$. Alors $*$ n'est pas une opération interne, car $(-1, 1)$ n'admet pas une image.

Définition 4.2 (Partie stable pour une loi) Soit E un ensemble muni par une loi de composition interne * et F une partie de E. On dit que F est stable pour la loi $*$ si

$$\forall (x, y) \in FF : x * y \in F$$

Exemple.

1. $\mathbb{R}^+$et $\mathbb{R}^-$sont deux partie stable de $\mathbb{R}$ pour la loi $+$.

2. Pour la loi ,$\mathbb{R}^+$est encore une partie stable, mais ce n'est pas le cas de $\mathbb{R}^-$.

4.1.2 Propriétés des lois de composition internes

Définition 4.3 (Commutativité et associativité) Soit E un ensemble muni par une loi de composition interne $*$

On dit que $*$ est commutative si $\forall (x, y) \in E^2 : x * y = y * x$.

On dit que $*$ est associative si $\forall (x, y, z) \in E^3 : (x * y) * z = x * (y * z)$.

Exemple.

1. Les lois $+$ et sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont commutative et associative ;

2. Aussi, les lois $\cup, \cap$ et $\triangle$ sur $\mathcal{P}(E)$ sont commutative et associative ;

3. La loi o sur $\mathcal{F}(E)$ est associative mais pas commutative, car $f \circ g \neq g \circ f$ en général ;

4. Soit la loi $*$ définie sur $\mathbb{Q}$ par : $x * y = \frac{x+y}{2}$. Alors $*$ est commutative,

car $x * y = \frac{x+y}{2} = \frac{y+x}{2} = y * x$ mais n'est pas associative,

car $(-1 * 0) * 1 = \frac{1}{4} \neq -1 * (0 * 1) = \frac{-1}{4}$.

Définition 4.4 (Element neutre) Soit E un ensemble muni d'une loi de composition interne *. Soit e un élément de E. On dit que e est élément neutre pour la loi *, si

$$\forall x \in E : x * e = e * x = x$$

Remarque 4.1 Si la loi $*$ est commutative, l'égalité $x * e = e * x$ est automatiquement réalisée.

Exemple.

1. Dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$, 0 est neutre pour la lois $+$, et 1 est neutre pour la loi ;

2. Dans $\mathcal{P}(E), \emptyset$ est neutre pour la lois $\cup$, et E est neutre pour la loi $\cap$;

3. Soit la loi $*$ définie sur $\mathbb{R}$ par : $x * y = x + y - 1$. Alors $e = 1$ est un élément neutre, car $x * e = x \Rightarrow x + e - 1 = x$. Donc $e = 1$.

Proposition 4.1 (Unicité de l'élement neutre) L'élement neutre de E pour la loi * s'il existe, est unique.

Preuve. En effet, soit e' un autre élément neutre pour $*$ alors $e' = e' * e = e * e' = e$. Donc, l'élement neutre est unique.

Définition 4.5 (Element symétrique) Soit E un ensemble muni d'une loi de composition interne * ait un élément neutre e. On dit que l'élément x de E admet un élément symétrique (inversible) x' de E, si $\forall x \in E : x * x' = x' * x = e$.

Exemple.

1. Dans $\mathbb{R}$, les éléments inversibles pour la lois , sont les éléments non nuls ;

2. Soit la loi * définie sur $\mathbb{R}$ par : $x * y = x + y - 1$. Alors $x \in \mathbb{R}$ admet un élément symétrique $x' = 2 - x$, car $x * x' = 1 \Rightarrow x + x' - 1 = 1$. Donc $x' = 2 - x$.

Proposition 4.2 Soit E un ensemble muni d'une loi de composition interne $*$ qui est associative et admet un élément neutre.

1. L'élement symétrique x' de x pour la loi * dans E, s'il existe, est unique ;

2. Si $x, y \in E$ sont symétrisables alors $x * y$ est symétrisable et son symétrique donné par

$$(x * y)' = y' * x'$$

Définition 4.6 (Distributivité) Soit E un ensemble muni par deux lois de composition internes $*$ et $\top$

On dit que $*$ est distributive à gauche par rapport a $\top$ si

$$\forall (x, y, z) \in E^3 : x * (y \top z) = (x * y) \top (x * z)$$

.

On dit que $*$ est distributive à droite par rapport a $\top$ si

$$\forall(x,y,z)\in E^3 : (x)*z=(x*z)\top(y*z)$$

.

Remarque 4.2 Si la loi $*$ est commutative, alors l'une de ces deux propriétés implique l'autre.

Exemple.

1. Dans $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$ et $\mathbb{C}$, la loi est distributive par rapport à la loi $+$;

2. Dans $\mathcal{P}(E)$, les lois $\cup,\cap$ sont distributives l'une par rapport à l'autre ;

3. Soit la loi * définie sur $\mathbb{R}$ par : $x*y=x+y-xy$ et la loi $\top$ définie sur $\mathbb{R}$ par : $x\top y=x+y-1$. Comme la loi * est commutative donc il suffit de démontrer la distributivité à gauche par rapport a $\top$

$$x*(y\top z)=x*(x+y-1)=2x+y+z-xy-xz-1\ldots\ldots.(1)$$

$$(x*y)\top(x*z)=(x+y-xy)\top(x+z-xz)=2x+y+z-xy-xz-1\ldots.(2)$$

$$(1)=(2),\ \text{donc la loi } * \text{ est distributive par rapport à la loi } \top.$$

4.2 Structures algébriques

4.2.1 Groupes

4.2.1.1 Définitions et exemples

Définition 4.7 (Groupe) Un groupe est un ensemble non vide muni d'une loi de composition interne $(G,*)$ tels que :

- * est associative ;

- * admet un élément neutre e ;

- tout élément de G est symétrisable (admet un symétrique) pour *.

Remarque 4.3 Si * est commutative, on dit que $(G,*)$ est commutatif, ou abélien.

Exemple.

1. $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes abéliens ;

2. L'ensemble $\mathcal{P}(E)$ muni de la différence symétrique $\triangle$ est un groupe abélien ;

3. $(\mathbb{N},+),(\mathbb{R},),(\mathcal{P}(E),\cap)$ et $(\mathcal{P}(E),\cup)$ ne sont pas des groupes.

Définition 4.8 (Sous-groupe) Soit $(G,*)$ un groupe et soit H une partie non vide de G. On dit que H est un sous-groupe de G si :

1. H est stable pour la lois $*$: $\forall(x,y)\in H^2, x*y\in H$;

2. H est stable pour le passage à l'inverse $\forall x\in H, x'\in H$.

Exemple.

1. Soit $(G,*)$ un groupe, alors e_G et G sont des sous-groupes (dits triviaux) ;

2. Soit $(\mathbb{Z},+)$ un groupe. Alors $3\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$ avec

$$3\mathbb{Z}=\{3z : z\in\mathbb{Z}\}=\{\ldots,-6,-3,0,3,6,\ldots\}$$

3. Soit $(G,\cdot)$ un groupe, alors l'ensemble $Z(G)=\{x\in G : \forall y\in G, xy=yx\}$ est un sous groupe de G appelé centre de G.

Théorème 4.1 (Caractérisation des sous-groupes) Soit $(G,*)$ un groupe et soit H une partie non vide de G. Alors H est un sous-groupe de G si et seulement si :

$$\forall(x,y)\in H^2, x*y'\in H$$

Proposition 4.3 (Intersection de sous-groupes) Soit $(G,*)$ un groupe et soit $\{H_i\}_{i\in I}$ une famille de sous groupe de G. Alors $\cap_{i\in I}H_i$ est un sous-groupe de G.

Remarque 4.4 La réunion de deux sous-groupes de G n'est pas nécessairement un sous-groupe de G. Par exemple $2\mathbb{Z}$ et $3\mathbb{Z}$ sont deux sous-groupes de $(\mathbb{Z},+)$, mais la réunion ne l'est pas puisque 2 et 3 sont dans $2\mathbb{Z}\cup3\mathbb{Z}$ alors que $2+3=5\notin 2\mathbb{Z}\cup3\mathbb{Z}$.

4.2.1.2 Homomorphisme de groupes

Définition 4.9 Soient $(G_1,*)$ et $(G_2,\perp)$ deux groupes. On appelle homomorphisme (ou morphisme) de groupes de G_1 dans G_2, une application $f : G_1\longrightarrow G_2$ telle que,

$$\forall x,y\in G_1, f(x*y)=f(x)\perp f(y)$$

Exemple.

Soit l'application f donnée par : $\begin{array}{rlll} f: & \mathbb{R} & \longrightarrow \mathbb{R}^* \\ & x & \mapsto f(x)=2^x \end{array}$ est un homomorpphisme de $(\mathbb{R},+)$ dans $(\mathbb{R},)$ car :

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

Remarque 4.5 Soient $(G_1,*)$ et $(G_2,\perp)$ deux groupes et f un homomorphisme de G_1 dans G_2. Alors

1. Si f est bijective, alors on dit que f est isomorphisme ;

2. Si f est définie dans $(G_1,*)$ dans lui mème, alors on dit que f est endomorphisme ;

3. Si f est endomorphisme bijective, alors on dit que f est automorphisme.

Exemple.

1. La fonction exponentielle est un isomorphisme des groupes de $(\mathbb{R},+)$ dans $\left(\mathbb{R}_+^*,\right)$;

2. La fonction logarithme népérien est un isomorphisme de groupes de $\left(\mathbb{R}_+^*,\right)$ dans $(\mathbb{R},+)$;

Proposition 4.4 Soient $(G_1,*)$ et $(G_2,\perp)$ deux groupes d'éléments neutres e e_1 et et soit f un homomorphisme de G_1 dans G_2. Alors

1. $f(e_1)=e_2$;

2. $\forall x \in G_1, (f(x))'=f(x')$.

Proposition 4.5 Soient $(G_1,*)$ et $(G_2,\perp)$ deux groupes d'éléments neutres e e_1 et e_2 et soit f un homomorphisme de G_1 dans G_2. Alors

1. Si H est un sous-groupe de G_1, alors $f(H)$ est un sous-groupe de G_2 ;

2. Si H' est un sous-groupe de G_2, alors $f^{-1}(H)$ est un sous-groupe de G_1.

Définition 4.10 (Le noyau et l'image d'un homomorphisme) Soient $(G_1,*)$ et $(G_2,\perp)$ deux groupes et f un homomorphisme de G_1 dans G_2. Alors

1. On appelle noyau de f l'ensemble

$$\operatorname{Ker}(f)=f^{-1}(e)=\{x \in G_1 : f(x)=e_2\}$$

2. On appelle image de f l'ensemble

$$\mathrm{Im}(f) = f\left(G_1\right) = \left\{f(x) \in G_2 : x \in G_1\right\}.$$

Exemple. Soit f un homomorphisme donné dans l'exempl&4.9, alors

$$\mathrm{Ker}(f) = \{x \in \mathbb{R}, f(x) = 1\} = \{x \in \mathbb{R}, 2^x = 1\} = \{0\}$$

et $\mathrm{Im}(f) = \{f(x) : x \in \mathbb{R}\}$. On a $f(x) = y$, alors $2^x = y$ ceci implique que $x \ln 2 = \ln y$, donc $x = \frac{\mathrm{lng}}{\ln 2}$. D'où, $\mathrm{Im}(f) = \mathbb{R}_+^*$.

Théorème 4.2 Soit f un homomorphisme de $(G_1, *)$ dans $(G_2, \perp)$. Alors

1. $\mathrm{Ker}(f)$ est un sous-groupe de G_1 ;

2. $\mathrm{Im}(f)$ est un sous-groupe de G_2 ;

3. f est injective si et seulement si $\mathrm{Ker}(f) = \{e_1\}$;

4. f est surjective si et seulement si $\mathrm{Im}(f) = G_2$.

4.2.2 Anneaux

4.2.2.1 Définitions

Définition 4.11 (Anneau) Soit A un ensemble muni de deux lois de composition, $*$ et $\perp$. On dit que $(A, *, \perp)$ est un anneau si :

1. $(A, *)$ est un groupe commutatif ;

2. la loi $\perp$ est associative ;

3. la loi $\perp$ distributive par rapport à la loi $*$.

Remarque 4.6

1. Si $\perp$ est commutative, on dit que $(A, *, \perp)$ est un anneau commutatif.

2. Si $\perp$ admet un élément neutre, on dit que $(A, *, \perp)$ est un anneau unitaire.

Exemple.

1. $(\mathbb{Z}, +,), (\mathbb{Q}, +,), (\mathbb{R}, +,)$ et $(\mathbb{C}, +,)$ sont des anneaux commutatifs ;

2. Soit E un ensemble, $(\mathcal{P}(E), \triangle, \cap)$ est un anneau commutatif ;

3. Soit A l'ensemble des applications de $\mathbb{C}$ dans $\mathbb{C}$, de la forme $z \mapsto \alpha z + \beta \bar{z}$.

$(A, +, \circ)$ est un anneau non commutatif.

Définition 4.12 (Sous-anneau) Soit $(A, +, \cdot)$ un anneau et soit B une partie de A. On dit que B est un sous-anneau de $(A, +, \cdot)$ si et seulement si :

1. $B \neq \emptyset \, (0_A \in B)$;

2. $(B, +)$ est un sous-groupe de A ;

3. B stable pour la loi .

Ce qui équivaut à

1. $0_A \in B$

2. $\forall a, b \in B, a - b \in B$;

3. $\forall a, b \in B, a \cdot b \in B$.

Exemple.

1. $(\mathbb{Z}, +,), (\mathbb{Q}, +,), (\mathbb{R}, +,)$ et $(\mathbb{C}, +,)$, chacun est un sous-anneau du suivant ;

2. l'ensemble, $\left\{r + s\sqrt{2}, (r, s) \in \mathbb{Q}^2\right\}$ est un sous-anneau de $(\mathbb{R}, +,)$.

Définition 4.13 (Homomorphisme d'anneaux) Soient $(A, +, \cdot)$ et $(B, +, \cdot)$ deux anneaux. On dit qu'une application f de A vers B est un homomorphisme (ou morphisme) si :

1. $f\,(1_A) = 1_B$

2. $\forall a, b \in A, f(a + b) = f(a) + f(b)$;

3. $\forall a, b \in A, f(a \cdot b) = f(a) \cdot f(b)$.

Remarque 4.7 En particulier, f est un homomorphisme de groupes, de $(A, +)$ vers $(A, +)$;

Définition 4.14 (L'élément inversible) Un élément d'un anneau $(A, +, \cdot)$ est dit inversible si et seulement s'il est symétrisable pour la seconde opération (s'il admet un symétrique pour la loi.).

Définition 4.15 (Diviseur de zéro) Un élément non nul x d'un anneau A est un diviseur de zéro si et seulement si son produit avec un autre élément non nul vaut zéro :

$$\exists y \neq 0 \mid xy = 0 \quad \text{ou } yx = 0.$$

Exemple.

1. Dans $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$, tous les éléments non nuls sont inversibles ;
2. Dans l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, toute fonction f qui s'annulle est diviseur de 0 et les éléments inversibles sont les fonctions qui ne s'annullent pas.

4.2.2.2 Idéal dans un anneau

Définition 4.16 (Idéal) Soit $(A, +, \cdot)$ un anneau. Une partie I non vide de A est dite un idéal de A si et seulement si

1. I est un sous-groupe de $(A, +, \cdot)$;
2. pour $x \in I$ et $a \in A$ on $a : x \cdot a \in I$ et $a \cdot x \in I$

Exemple. L'ensemble $\mathbb{Z}$ n'est pas un idéal de $(\mathbb{R}, +,)$, car $\frac{1}{5} \in \mathbb{R}$ et $3 \in \mathbb{Z}$ alors que $\frac{3}{5} \notin \mathbb{Z}$

Remarque 4.8 Il est facile de vérifier que

1. L'intersection des idéaux de A est un idéal de A.
2. L'image directe d'un idéal par un morphisme d'anneau surjective est un idéal.
3. Le noyau d'un morphisme d'anneaux est un idéal.

4.2.2.3 Règles de calculs dans un anneau

On rappelle la formule du binôme de Newton, qui s'étend de $\mathbb{Z}$ aux anneaux commutatifs, mais aussi dans un anneau quelconque.

Proposition 4.6 Soient $(A, +, \cdot)$ un anneau et $a, b \in A$, avec $a \cdot b = b \cdot a$, et $n \in \mathbb{N}^*$. Alors :

$$(a + b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}.$$

Preuve. Récurrence sur $\mathbb{N}$ et formule du triangle de Pascal.

Remarque 4.9 Soient $x, y \in A$ et $n \in \mathbb{N}^*$, alors $x - y \mid x^n - y^n$ et plus précisément :

$$x^n - y^n = (x - y) \sum_{k=0}^{n-1} x^k y^{n-1-k}.$$

* Cas particulier de ce qui précède : si $1 - x$ est inversible, on peut calculer $\sum_{k=0}^{n-1} x^k$ grâce à la formule :

$$1 - x^n = (1 - x) \sum_{k=0}^{n-1} x^k$$

4.2.3 Corps

Définition 4.17 (Corps) Un corps est un anneau commutatif dans lequel tout élément non nul est inversible pour la deuxième loi.

Remarque 4.10 Si de plus la deuxième loi est commutative, le corps $(K, +, \cdot)$ est dit corps commutatif.

Exemple.

$\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$, sont des corps, mais pas $\mathbb{Z}$ (2 n'est pas inversible).

Définition 4.18 (Sous-corps) Soit $(K, +, \cdot)$ un corps, un sous-corps de K est une partie K_1 de K telle que $(K_1, +, \cdot)$ soit un corps, c'est-à-dire, pour tous x, y de K_1, on a

$$x - y \in K_1 \quad \text{et } xy^{-1} \in K_1.$$

Exemple.

1. $(\mathbb{Q}, +,), (\mathbb{R}, +,)$ et $(\mathbb{C}, +,)$, chacun est un sous-corps du suivant ;

2. L'ensemble $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$ est un corps commutatif qui admet $\mathbb{Q}$ comme sous-corps.

4.3 Exercices corrigé

Exercice1. On définit sur $\mathbb{R}$ une loi de composition interne $*$ par

$$\forall a, b \in \mathbb{R} : a * b = \ln\left(e^a + e^b\right)$$

1. La loi $*$ est elle commutative ? Associative ? Possède-t-elle un élément neutre ?

2. Soient $a, b \in \mathbb{R}$. On définit dans $\mathbb{R}$ une loi de composition interne $\perp$ par

$$\forall x, y \in \mathbb{R} : x \perp y = ax + by$$

Déterminer a, b pour que la loi $\perp$: (1) Soit associative (2) Possède un élément neutre.

Exercice2. Soit $G = \mathbb{R}^*\mathbb{R}$ et $*$ la loi de composition interne définie sur G par

$$\forall (x, y), (x', y') \in G : (x, y) * (x', y') = (xx', xy' + y)$$

1. Montrer que $(G, *)$ est un groupe non commutatif.

2. Montrer que l'ensemble $H = \mathbb{R}_+^* \mathbb{R}$ est un sous groupe de $(G, *)$.

Exercice3.

Soient $\left(\mathbb{R}_+^*, \right)$ et $(\mathbb{R}, +)$ deux groupes et soit l'application

$$\begin{aligned} f : \mathbb{R}_+^* &\longrightarrow \mathbb{R} \\ x &\mapsto f(x) = \ln(x) \end{aligned}$$

1. Montrer que f est un homomorphisme de $\left(\mathbb{R}_+^*, \right)$ dans $(\mathbb{R}, +)$.

2. Calculer $Ker(f)$. Que vous conclus.

3. Est ce que f est surjective ?

Exercice4. On munit l'ensemble $A = \mathbb{Z}^2$ de deux lois définies par :

$$(x, y) + (x', y') = (x + x', y + y') \text{ et } (x, y) \star (x', y') = (xx', xy' + x'y)$$

1. Montrer que $(A, +)$ est un groupe commutatif. $(*)$

2. Montrer que la loi $\star$ est commutative et associative.

3. Déterminer l'élément neutre pour la loi $\star$.

4. Montrer que $(A, +, \star)$ est un anneau unitaire commutatif.

5. Montrer que $B = \{(a, 0) \mid a \in \mathbb{Z}\}$ est un sous-anneau de $(A, +, \star)$.

6. On munit l'ensemble $K = \mathbb{R}$ par l'addition et la multiplication usuelle.

(a) Pourquoi $(K, +, \cdot)$ est-il un corps ?

(b) On pose $L = \{x \in \mathbb{R}, \exists \alpha, \beta \in \mathbb{Q} \mid x = \alpha + \beta\sqrt{3}\}$ une partie de $\mathbb{R}$.

Montrer que $(L, +, .) estunsous - corpsde(K, +, .)$

Exercice5.

(1) On considère un ensemble E défini par $E = \{(a, b) \in \mathbb{R}^2 : a \neq 0\}$ et on définit sur E une loi de composition $*$ par

$$\forall (a_1, b_1), (a_2, b_2) \in E : (a_1, b_1) * (a_2, b_2) = (a_1 a_2, a_1 b_2 + b_1)$$

(a) Vérifier que $*$ est une loi interne sur E et trouver $(2,0)*(1,1)$

(b) Montrer que $(E,*)$ est un groupe non commutatif.

(c) Déterminer l'ensemble $H = \{(x,y) \in E, \forall (a,b) \in E : (x,y)*(a,b) = (a,b)*(x,y)\}$

(2) Soit $F = \{(a,b) \in E : b = 0\}$ une partie de E.

(a) Montrer que F est un sous-groupe de E.

(3) On considère une application f définie par

$$f : (E,*) \longrightarrow (\mathbb{R}^*,.)$$
$$(a,b) \longmapsto f((a,b)) = a$$

(a) Montrer que f est un morphisme de groupe $(E,*)$ dans le groupe $(\mathbb{R}^*,.)$

(b) Déterminer le noyau de f.

(4) On pose $\mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2}, m,n \in \mathbb{Z}\}$ une partie de $\mathbb{R}$.

(a) Montrer que $\mathbb{Z}[\sqrt{2}]$ muni de l'addition et de la multiplication des réels, est un sous anneau de $\mathbb{R}$.

4.3.1 corrigé

Exercice1.

(1)

- $\forall a,b \in \mathbb{R}, b*a = \ln\left(e^b + e^a\right) = \ln\left(e^a + e^b\right) = a*b$

  Donc, $*$ est commutative.

- $$\begin{aligned}\forall a,b,c \in \mathbb{R}, (a*b)*c &= \ln\left(e^{a*b} + e^c\right) = \ln\left(e^a + e^b + e^c\right)\\ &= a*(b*c).\end{aligned}$$

  Donc, $*$ est associative.

- $a*e = a \Leftrightarrow \ln\left(e^a + e^e\right) = a \Leftrightarrow e^e = 0.$

  Il n'y a donc pas de neutre.

(2)

- $\perp$ associative $\Leftrightarrow \forall x, y, z \in \mathbb{R} : (x \perp y) \perp z = x \perp (y \perp z)$.

  $\Leftrightarrow \forall x, y, z \in \mathbb{R} : a^2x + aby + bz = ax + aby + b^2z$.

  Donc, $a^2 = a$ et $ab = ba$ et $b = b^2$

  D'où, $(a = 0$ or $a = 1)$ et $(b = 0$ or $b = 1)$.

- $\perp$ possède un élément neutre $e \in \mathbb{R} \Leftrightarrow \forall x \in \mathbb{R} : x \perp e = e \perp x = x$

  $\Leftrightarrow \forall x \in \mathbb{R} : ax + be = ae + bx = x$.

  $\Leftrightarrow a = 1$ et $e = 0$ et $b = 1$.

Exercice2.

(1)

- $((x, y) * (x', y')) * (x'', y'') = (xx', xy' + y) * (x'', y'') = (xx'x'', xx'y'' + xy' + y)$ et

$(x, y) * ((x', y') * (x'', y'')) = (x, y) * (x'x'', x'y'' + y') = (xx'x'', xx'y'' + xy' + y)$

Donc, $*$ est associative.

- $(x, y) * (1, 0) = (x, y)$ et $(1, 0) * (x, y) = (x, y)$.

Donc, $(1, 0)$ est élément neuve.

- $(x, y) * \left(\frac{1}{x}, \frac{-y}{x}\right) = (1, 0)$ et $\left(\frac{1}{x}, -\frac{y}{x}\right) * (x, y) = (1, 0)$.

Donc, tout élément est symétrisable. D'où, $(G_1, *)$ est un groupe.

- $(1, 2) * (3, 4) = (3, 6)$ et $(3, 4) * (1, 2) = (3, 10)$.

Alors, le groupe n'est pas commutatif.

(2) $H = \mathbb{R}_+^*.\mathbb{R}$ est inclus dans G.

- $(1, 0) \in H$,

- $\forall (x, y), (x', y') \in H, (x, y) * (x', y') \in H$ Car $x\bar{x} > 0$,

- $\forall (x, y) \in H, (x, y)^{-1} = \left(\frac{1}{x}, \frac{-y}{x}\right) \in H$ car $\frac{1}{x} > 0$.

Donc H est un sous-groupe de G.

Exercice3.

(1) f est un homomorphisme de $\left(\mathbb{R}_+^*, .\right)$ dans$(\mathbb{R}, +)$.Soient :

$$\begin{aligned} x_1, x_2 \in \mathbb{R}_+^* : f\left(x_1.x_2\right) &= \ln\left(x_1.x_2\right) = \ln x_1 + \ln x_2 \\ &= f\left(x_1\right) + f\left(x_l\right) \end{aligned}$$

(2)

$$\begin{aligned} \ker(f) &= \left\{x \in \mathbb{R}_+^* : f(x) = 0\right\} \\ &= \left\{x \in \mathbb{R}_+^* : \ln x = 0\right\} \\ &= \left\{x \in \mathbb{R}_+^* : e^{\ln(x)} = e^0 = 1\right\} \\ &= \left\{x \in \mathbb{R}_+^* : x = 1\right\} \\ &= \{1\} \end{aligned}$$

Alors, f us injective.

(3) f est surjective car :

$$\forall y \in \mathbb{R}, \exists x = e^y \in \mathbb{R}_+^* \mid f(x) = f\left(e^y\right) = \ln\left(e^y\right) = y.$$

Exercice4.

(1) $(*)$

(2) $(x, y) * (x', y') = (xx', xy' + x'y) = (x'x, x'y + xy') = (x', y') * (x, y)$.

Donc,$*$ est commutative.

$$\begin{aligned} [(x, y) * (x', y')] * (x'', y'') &= (xx', xy' + x'y) * (x'', y'') = (xx'x'', xx'y'' + x''(xy' + x'y)) \\ &= (xx'x'', xx'y'' + x''xy' + x''x'y) \\ (x, y) * [(x', y') * (x'', y'')] &= (x, y) * (x', x'', x'y'' + x''y') = (xx'x'', x\left(x'y'' + x''y'\right) + x'x''y) \\ &= (xx'x'', xx'y'' + xx''y' + x'x''y)\,\mathbf{.} \end{aligned}$$

La loi $*$ est associative

(3) Soit (e, e') tel que pour tout $(x, y) \in A = (x, y) * (e, e') = (x, y)$.

Alors, $\begin{cases} x \cdot e = x \\ xe' + ye = y \end{cases} \Rightarrow \begin{cases} e = x \\ xe' + y = y \end{cases} \Rightarrow \begin{cases} e = 1 \\ e' = 0 \end{cases}$

$(1, 0)$ est l'élément neutre de A pour la loi $*$.

(4) Toutes les propriétés d'un anneau sont dans les questions précédentes sauf la distributivité de $*$ par rapport à l'addition

$$\begin{aligned}(x,y)*[(x',y')+(x'',y'')] &= (x,y)*(x'+x'',y'+y'') \\ &= (x(x'+x''),x\,(y'+y'')+(x'+x'')\,y) \\ &= (xx'+xx'',xy'+x'y+xy''+x''y) \\ &= (xx',xy'+x'y)+(xx'',xy''+x''y) \\ &= [(x,y)*(x',y')]+[(x,y)*(x'',y'')]\,.\end{aligned}$$

$(A+,*)$ est un anneau commutatif.

(5) $B=\{(a,0)\mid a\in\mathbb{Z}\}$

- $B\subset\mathbb{Z}^2$ et $(1,0)\in A$.
- $\forall(a,0),(b,0)\in B$, an a $(a,0)-(b,0)=(a-b,0)\in B$.
- $\forall(a,0),(b,0)\in B$, on a $(a,0)*(b,0)=(ab,0)\in B$.

B est donc un sous-anneau de $(\mathbb{Z}^2,+,*)$.

(6)

(a) $(k,+,\cdot)$ est un corps car

$$\begin{cases}\text{(i) } (K,+,\cdot) \text{ est un anneau commutatif } (*) \\ \text{(ii) tout élément non nul est inversible pour la multiplication.}\end{cases}$$

(b) $(L,+,\cdot)$ est un sous-corps de $(k,+,\cdot)$ si et seulement si :

(i) $\forall x,y\in L: x-y\in L$

(ii) $\forall x,y\in L: xy\in L$

(iii) $\forall x\in L^*: x^{-1}\in L$.

Posons que : $x=\alpha_1+\beta_1\sqrt{3}, y=\alpha_2+\beta_2\sqrt{3}\in L$

(i) On a : $x-y=(\alpha_1-\alpha_2)+(\beta_1-\beta_2)\sqrt{3}=\alpha_3+\beta_3\sqrt{3}\in L$.

car : $\alpha_3=\alpha_1-\alpha_2, \beta_3=\beta_1-\beta_2\in\mathbb{Q}$.

(ii) On a aussi :

$$\begin{aligned}xy=\left(\alpha_1+\beta_1\sqrt{3}\right)\left(\alpha_2+\beta_2\sqrt{3}\right) &= (\alpha_1\alpha_2+3\beta_1\beta_2)+(\alpha_1\beta_2+\beta_1\alpha_2)\sqrt{3} \\ &= \alpha'+\beta'\sqrt{3}\in L.\end{aligned}$$

car : $\alpha' = \alpha_1\alpha_2 + 3\beta_1\beta_2 \quad , \quad \beta' = \alpha_1\beta_2 + \beta_1\alpha_2 \in \mathbb{Q}$.

(iii) Soit $x = \alpha_1 + \beta_1\sqrt{3} \in L^*$, c'est-à-dire $\alpha_1 \neq 0$ ore $\beta_1 \neq 0$. Alors,

$$x^{-1} = \frac{1}{x} = \frac{1}{\alpha_1 + \beta_1\sqrt{3}} = \frac{\alpha_1 - \beta_1\sqrt{3}}{\alpha_1^2 - 3\beta_1^2} = \frac{\alpha_1}{\alpha_1^2 - 3\beta_1^2} + \frac{-\beta_1}{\alpha_1^2 - 3\beta_1^2}\sqrt{3} = a + b\sqrt{3} \in L.$$

car : $a = \frac{\alpha_1}{\alpha_1^2 - 3\beta_1^2}, b = \frac{-\beta_1}{\alpha_1^2 - 3\beta_1^2} \in Q$

Donc, $(L, +, \cdot)$ est un sous-corps de $(k, +, \cdot)$.

Chapitre 5

Anneaux de polynômes

Dans ce chapitre, on introduit la notion de polynôme sur un corps ou un anneau. Tout au long du chapitre, $\mathbb{K}$ désigne un corps et $\mathbb{A}$ un anneau commutatif unitaire.

5.1 Définitions

Définition 5.1. Soit $(\mathbb{A}, +, .)$ un anneau unitaire et commutatif.

On appelle polynôme P à une indéterminée X et à coefficjents dans $\mathbb{A}$ toutes écriture algébrique de la forme

$$a_0 + a_1X + a_2X^2 + \ldots + a_nX_n + \ldots$$

où les $a_i \in \mathbb{A}$ sont nuls sauf un nombre fini,

Une autre définition est donné par.

Définition 5.2, On appelle polynôme à une indéterminée x à cocficicuts dans $\mathbb{A}$ toute suite $P = (a_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{A}$ tous nul à partir d'un certain rang.

1. Les a_n sont appelés les coefficients de P.

2. Le plus grand indice n vérifant $a_n \neq 0$ (s'il existe) est appelé degré de P et noté $\deg(P)$ et dans ce cas a_nx^n est appelé terme dominant de P.

3. Si tous les a_i sont nuls, P est appelé polynôme nul noté 0 et par convention $\deg(0) = -\infty$.

4. Si le terme dominant de P est $1X^n$ le polynôme P est dit unitaire.

5. Chaque élément a de $\mathbb{A}$ est un polynôme, appelé polynôme constant.

6. L'ensemble des polynômes à une indéterminée X à coefficients dans $\mathbb{A}$ est noté $\mathbb{A}[X]$.

Les polynômes sont munis des opérations usuelles d'addition, de produit de polynômes et de multiplication par un scalaire $\lambda \in \mathbb{A}$: soient $P = (a_n)_{n\in\mathbb{N}}, Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes à une indéterminée à coefficients dans $\mathbb{A}$. On a alors :

1. $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$,

2. $PQ = (c_n)_{n\in\mathbb{N}}$ avec $c_n = \sum_{0\leq k\leq n} a_k b_{n-k}$,

3. $\lambda P = (\lambda a_n)_{n\in\mathbb{N}}$.

Définition 5.3

L'ensemble $\mathbb{A}[X]$ des polynômes à une indéterminée à coefficients dans $\mathbb{A}$ muni de l'addition et de la multiplication définies ci-dessus est un anneau commutatif.

Proposition 5.1. Si $\mathbb{A}$ est intègre alors pour tout $P, Q \in A[X]$ on a

1. $\deg(PQ) = \deg(P) + \deg(Q)$.

2. $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$.

Démonstration

1. Si un des deux polynômes est nul alors $PQ = 0$ et l'égalité devient $-\infty = -\infty$ ce qui est vrai. On suppose donc que P et Q sont non nuls. Soit $n = \deg(P)$ et $m = \deg(Q)$. On pose $P = \sum a_i X^i$ et $Q = \sum b_i X^i$ où $a_i, b_i \in \mathbb{A}$. Alors le coefficient du terme dominant de PQ est $a_n b_m$. Or $a_n \neq 0$ et $b_n \neq 0$ et donc, puisque $\mathbb{A}$ est intègre, $a_n b_n \neq 0$. Ce qui implique $\deg(PQ) = n + m$.

2. Évident

Soit $\mathbb{U}(A)$ désigne les éléments inversibles de $\mathbb{A}$.

Proposition 5.2

Si $\mathbb{A}$ est intègre, alors les éléments inversibles de $\mathbb{A}[X]$ sont les polynômes constants $P = a$ où $a \in \mathbb{U}(A)$.

Démonstration.

Soit P inversible dans $\mathbb{A}[X]$. Il existe $Q \in \mathbb{A}[X]$ tel que $PQ = 1$. On a alors $\deg(P) + \deg(Q) = 0$ et $\deg(P) = \deg(Q) = 0$. Ainsi P et Q sont des constantes inversibles

5.2 Arithmétique des polynômes

5.2.1 Polynômes associés

Définition 5.4.

Deux polynômes P et Q de $\mathbb{A}[X]$ sont dits associés s'il existe $a \in \mathbb{U}(A)$ tel que $P = aQ$

Exemple.

L'ensembles des polynômes associés à $X^2 + 1$ dans $\mathbb{Z}[X]$ est

$$\left\{X^2 + 1, -\left(X^2 + 1\right)\right\}$$

puisque les seuls inversibles de $\mathbb{Z}$ sont 1 et -1 .

Proposition 5.3.

1. La relation «être associé » est une relation d'équivalence sur $\mathbb{A}[X]$.
2. Si P et Q sont associés et ont le même coefficient dominant alors $P = Q$.
3. Si $\mathbb{A}$ est un corps alors tout polynôme P est associé à un unique polynôme unitaire.

Proposition 5.4 Soient P et Q deux polynômes de $A[X]$, alors : $\deg(P+Q) \leq \max(\deg(P); \deg(Q))$ et $\deg(P \cdot Q) = \deg(P) + \deg(Q)$

Exemple. Dans $\mathbb{Q}[X]$, soient les polynômes : $P = 3X^2 - 1$ et $Q = \frac{1}{2}X^3 + 4X$ alors $P + Q = \frac{1}{2}X^3 + 3X^2 + 4X - 1$ et $P \cdot Q = \frac{3}{2}X^5 - \frac{23}{2}X^3 - 4X$

Définition 5.5 (Divisibilité) Soient P, B deux polynômes de $A[X]$. On dit que B divise P, s'il existe $Q \in A[X]$ tel que $P = Q \cdot B$. On note alors $B \mid P$.

On dit aussi que P est multiple de B ou que P est divisible par B.

Exemple.

1. Tout élément inversible a de l'anneau A divise tout polynôme P de $A[X]$. En effet, $P = a \cdot (a^{-1}P)$;

2. $X+1$ divise X^2+X. En effet, $X^2+X = X(X+1)$.

Remarque. Si B divise P et $P \neq 0$, alors $\deg(B) \leq \deg(P)(P = Q \cdot B$ et $\deg(P) = \deg(Q) + \deg(B))$

Proposition 5.5 Soient $A, B, C \in K[X]$. Alors

1. Si $A \mid B$ et $B \mid A$, alors il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$.

2. Si $A \mid B$ et $B \mid C$ alors $A \mid C$.

3. Si $C \mid A$ et $C \mid B$ alors $C \mid (AU + BV)$, pour tout $U, V \in K[X]$.

Définition 5.6 (Division euclidienne des polynômes) Soient P, B deux polynômes de $A[X]$.

Si le coefficient du terme dominant de B est inversible dans A, alors il existe un couple $(Q; R) \in A[X]^2$ tels que $P = QB + R$ et $\deg(R) < \deg(B)$

Exemple. Divison $P = 3X^5 - 2X^3 - 5X^2 + 1$ par $B = 2X^3 + \frac{1}{2}X^2 - X$

$$\begin{array}{r|l} 3X^5 + 0X^4 - 2X^3 - 5X^2 + 0X + 1 & \frac{1}{2}X^3 + 2X^2 - X + 0 \\ \hline -12X^4 + 4X^3 - 5X^2 + 0X + 1 & 6X^2 - 24X + 104 \\ 52X^3 - 29X^2 + 0X + 1 & \\ -237X^2 + 104X + 1 & \end{array}$$

Donc le quotient $Q = 6X^2 - 24X + 104$ et le reste $R = -237X^2 + 104X + 1$.

L'existence de la division euclidienne permet de développer les propriétés de divisibilité : PGCD,PPCM, théorème de Bézout, algorithme d'Euclide, théorème de Gauss, décomposition en produit de facteurs, de manière entièrement analogue à $\mathbb{Z}$.

Définition 5.7 Le plus grand diviseur commun ($PGCD$) de deux polynômes A et B est un polynôme D qui divise A et B et tel que tout polynôme divisant A et B divise nécessairement D. Le plus petit commun multiple ($PPCM$) est un polynôme M multiple de A et B et tel que tout polynôme multiple de A et B soit divisible par M.

Remarque. 5.3 Soient $P1, P2, \ldots, P$ des polynômes de $K[X]$.

1. Le $PGCD$ et le $PPCM$ ne changent pas en permuttant les Pi ;

2. $PGCD\,(\lambda_1 P1; \lambda_2 P2, \ldots, \lambda_s Ps) = PGCD(P1, P2, \ldots, Ps)$ et

$PPCM\,(\lambda_1 P1, \lambda_2 P2, \ldots, \lambda_s Ps) = \text{PPCM}(P1, P2, \ldots, Ps)$ pour $\lambda_1, \lambda_2, \ldots, \lambda_s \in K$

Exemple. Soient $A := X^6 + X^5 + X^4 + X^2 + X + 1$ et $B = X^5 + X^4 + X^3 + X^2 + X + 1$ alors

$A = BQ_1 + R_1$ (avec $Q_1 = X$ et $R_1 = 1 - X^3$)

$B = R_1Q_2 + R_2$ (avec $Q_2 = -X^2 - X - 1$ et $R_2 = 2X^2 + 2X + 2$)

$R_1 = R_2Q_3 + R_3$ (avec $Q_3 = \frac{1}{2}$ et $R_3 = 0$)

Donc, $R_2 = 2X^2 + 2X + 2$ est le $PGCD$ et le $\mathrm{PPCM}(A, B) \cdot \mathrm{PGCD}(A, B) = A \cdot B$, alors $\mathrm{PPCM}(A, B) = X^9 + X^8 + X^7 + X^6 + 2X^5 + 2X^4 + X^3 + X^2 + X + 1$.

Définition 5.8 (Polynôme irréductible) Un polynôme $P \in K[X]$ est dit irréductible s'il n'est pas constant et si les seules factorisations $P = QR$ (avec $Q, R \in K[X]$) s'obtiennent avec P ou Q constant.

Remarque 5.4

1. La notion de polynôme irréductible correspond à celle de nombre premier dans $\mathbb{Z}$

2. Les polynômes irréductibles dans $\mathbb{C}[X]$ sont les polynômes du premier degré ;

3. Les polynômes irréductibles dans $\mathbb{R}[X]$ sont les polynômes du premier degré et les polynômes du second degré de la forme $P = aX^2 + bX + c$ avec $b^2 - 4ac < 0$.

Exemple. $X^2 + 1$ est irréductible dans $R[X]$ car on ne peut pas l'écrire comme produit de deux polynômes de degré 1 à coefficients dans $\mathbb{R}$.

Le même polynôme $X^2 + 1$ est réductible dans $C[X]$, car $X^2 + 1 = (X + i)(X - i)$.

Théorème 5.1

1. (Euclide) Soit P irréductible dans $K[X]$ et divisant QR alors P divise Q ou R.

2. (Gauss) Si $PGCD(P, Q) = 1$ et P divise QR alors P divise R.

Preuve. La démonstration est entièrement analogue à celle faite dans $\mathbb{Z}$.

5.3 Racines d'un polynôme et factorisation

Définition 5.9 Soit $P \in K[X]$ et $\alpha \in K$. On dit que α est une racine (ou un zéro) de P si $P(\alpha) = 0$.

Proposition 5.6 Soit $P \in K[X]$, alors

$$P(\alpha) = 0 \Leftrightarrow X - \alpha \text{ divise } P$$

Définition 5.10 Soit $k \in \mathbb{N}^*$. On dit que α est une racine de multiplicité (ou bien 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.

Exemple 5.7 -3 est une racine double et 1 une racine simple du polynôme $P = X^3 + 5X^2 + 3X - 9$ de $\mathbb{R}[X]$; car $P = (X+3)^2(X-1)$.

Définition 5.11 Soit $P = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ un polynôme, le polynôme dérivé est $P' = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \ldots + a_1$. On note $P^{(r)}$ la dérivée $n-$ ème définit par $P^{(r+1)} = \left(P^{(r)}\right)'$

Remarque 5.5 Les propriétés suivantes sont équivalentes :

1. P possède une racine d'ordre r en $X = \alpha$

2. $P(\alpha) = P'(\alpha) = \ldots = P^{(r-1)}(\alpha) = 0$ et $P^{(r)}(\alpha) \neq 0$

Exemple. Soit le polynôme $B = X^4 - 2X^3 + 2X^2 - 2X + 1$ de $\mathbb{R}[X]$. On a $\alpha = 1$ est une racine double de B car $B(1) = 0, B'(1) = 0, B''(1) \neq 0$

Théorème 5.2 (Théorème fondamental de l'algèbre) Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine dans $\mathbb{C}$. Autrement dit : Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1 .

La preuve de ce théorème dépasse le cadre du cours d'algèbre de 1 ère année LMD.

Théorème 5.3 (Décomposition en facteurs irréductibles) Pour tout polynôme P de $K[X]$ tel que deg $P \geq 1$; il existe, de façon unique, des polynômes irréductibles $P_1, P_2, \ldots, P_r$ unitaires, deux à deux distincts de $K[X]$ et des nombres entiers naturels strictement positifs $\alpha_1, \alpha_2, \ldots, \alpha_r$ et il existe un élément unique $\lambda \in K^*$ tels que $P = \lambda \prod_{i=1}^{r} P_i^{\alpha_i}$

Il s'agit bien sûr de l'analogue de la décomposition d'un nombre en facteurs premiers.

Théorème 5.4 (Factorisation dans C) Soit $P \in \mathbb{C}[X]$ de degré $n \geq 1$. La factorisation de P s'écrit $P = \lambda\left(X - \alpha_1\right)^{k_1}\left(X - \alpha_2\right)^{k_2} \ldots \left(X - \alpha_r\right)^{k_r}$, où $\alpha_1, \alpha_2, .., \alpha_r$ sont les racines distinctes de P et $k_1, k_2, \ldots, k_r$ sont leurs multiplicités.

Théorème 5.5 (Factorisation dans R) Soit $P \in \mathbb{C}[X]$ de degré $n \geq 1$. La factorisation de P s'écrit $P = \lambda\,(X-\alpha_1)^{k_1}\,(X-\alpha_2)^{k_2}\dots(X-\alpha_r)^{k_r}\,Q_1^{l_1}\dots Q_s^{l_s}$, où α_i sont exactement les racines réelles distinctes de multiplicité k_i et les Q_i sont des polynômes irréductibles de degré 2 : $Q_i = X^2+\beta_i X+\gamma_i$ avec $\Delta = \beta_i^2 - 4\gamma_i < 0$.

Exemple. Soit $P = 2X^4(X-1)^3\,(X^2+1)^2\,(X^2+X+1)$ est déjà décomposé en facteurs irréductibles dans $\mathbb{R}[X]$ mais sa décomposition dans $\mathbb{C}[X]$ est

$$P = 2X^4(X-1)^3(X-i)^2(X+i)^2\left(X-\tfrac{-1+i\sqrt{3}}{2}\right)\left(X-\left(\tfrac{-1+i\sqrt{3}}{2}\right)^2\right).$$

5.4 Exercices

Exercice1. Soit le polynôme $P = X^4+5X^3+10X^2+12X+8$.

1. Démontrer que -2 est racine double du polynôme P.

2. Factoriser P dans $\mathbb{R}[X]$.

3. Déduire les racines de P dans $\mathbb{C}$.

Exercice2. Soit le polynôme $P = X^4+X^2+1$.

1. Déterminer les racines de P dans $\mathbb{C}$.

2. Factoriser P dans $\mathbb{C}[X]$.

3. En déduire une factorisation de P dans $\mathbb{R}[X]$.

Exercice3. Soit $n \in \mathbb{N}$. Soit le polynôme $P_n = X^n$.

1. Déterminer le reste de la division euclidienne de P_n par $A_1 = X^2-3X-4$.

2. Déterminer le reste de la division euclidienne de P_n par $A_2 = X^2+1$.

Exercice4. Soit le polynôme $P = X^4-4X^3+5X^2-2X-6$.

1. On se propose de démontrer que P n'a pas de racine double.

(a) On se propose d'effectuer la division euclidienne de $2P$ par $\frac{1}{2}P'$. On note R le reste de cette division euclidienne.

(b) Effectuer la division euclidienne de $\frac{1}{2}P'$ par R. On note T le reste de cette division euclidienne.

(c) Démontrer que si a est une racine double de P, alors a est racine de R et de T.

(d) Démontrer que P n'a pas de racine double.

2. On se propose de factoriser P dans $\mathbb{R}[X]$.

(a) On pose $X = Y + 1$ et $Q(Y) = P(Y + 1)$. Calculer $Q(Y)$.

(b) Calculer les racines de Q dans $\mathbb{C}$. En déduire les racines de P dans $\mathbb{C}$.

(c) Factoriser P dans $\mathbb{C}[X]$, puis dans $\mathbb{R}[X]$.

Exercice5. Soit le polynôme $P = X^4 + 2X^3 - X^2 - 2X + 10$. Pour tout $z \in \mathbb{C}$, on pose $P(z) = z^4 + 2z^3 - z^2 - 2z + 10$

1. Soit $x \in \mathbb{R}\backslash\{0\}$. Donner l'expression de $P(x(1 + \imath))$ sous forme $P(x(1 + \imath)) = Q(x) + \imath R(X)$, où Q et R sont des polynômes à coefficients réels.

2. Les équations $Q(x) = 0$ et $R(x) = 0$ ont-elles des racines communes ?

3. Donner deux racines complexes conjuguées de l'équation $P(z) = 0$.

4. Factoriser P sous forme d'un produit de deux trinômes du second degré à coefficients réels et en déduire les racines complexes de P.

Exercice6. Déterminer les réels p et q pour que le polynôme $P = X^3 + pX + q$ soit divisible par le polynôme $Q = X^2 + 3X - 1$

Exercice7. Soit $n \in \mathbb{N}$. Montrer que le polynôme $X^2 - X + 1$ divise le polynôme $P_n = (X - 1)^{n+2} + X^{2n+1}$.

Exercice8. Soit $n \in \mathbb{N}\backslash\{0, 1\}$. Calculer le reste de la division euclidienne du polynôme $P_n = (X - 3)^{2n} + (X - 2)^n - 2$ par le polynôme $(X - 2)^2$.

Exercice9. Factoriser dans $\mathbb{R}[X]$ le polynôme $P = X^6 + 1$.

Exercice10. Déterminer $\lambda \in]0, \infty[$ tel que le polynôme $P = X^3 - 3X + \lambda$ ait une racine double. Quelle est alors l'autre racine de P ?

Exercice11. Soit $n \in \mathbb{N}$. Montrer que le polynôme $P_n = 1 + X + \frac{X^2}{2} + \frac{X^3}{3!} + \ldots + \frac{X^n}{n!}$ n'a pas de racine multiple.

Exercice12. Déterminer tous les polynômes P tels que $(X^2 + 1)\, P'' - 6P = 0$ et $P(1) = 2$.

Exercice13. Soit le polynôme $P = X^4 + 12X - 5$. Factoriser P dans $\mathbb{R}[x]$ puis dans $\mathbb{C}[X]$ sachant qu'il admet deux racines dont le produit vaut -1 .

Exercice14. Résoudre le système en $(x, y, z) \in \mathbb{R}^3$:

$$\begin{cases} x + y + z = 2 \\ xyz = -\frac{1}{2} \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{1}{2} \end{cases}$$

Exercice15. Soit $n \in \mathbb{N}\backslash\{0\}$. Factoriser le polynôme

$$P_n = 1 - X + \frac{X(X-1)}{2!} - \frac{X(X-1)(X-2)}{3!} + \ldots + (-1)^n \frac{X(X-1)(X-2)\ldots(X-n+1)}{n!}$$

Exercice16. Déterminer tous le polynômes $P \in \mathbb{R}[X]$ tels que P' divise P.

Chapitre 6

examens corrigés

6.1 Examen 01

Exercice1. (6p)

I) Soit $\mathrm{P}_1, \mathrm{P}_2$ deux propositions. Démontrer les propriétés suivantes dans le même tableau de vérité

1. $\left(\overline{\mathrm{P}_1 \Longrightarrow \mathrm{P}_2}\right) \Leftrightarrow \left(\mathrm{P}_1 \wedge \overline{\mathrm{P}_2}\right)$

2. $(\mathrm{P}_1 \Longrightarrow \mathrm{P}_2) \Leftrightarrow \left(\overline{\mathrm{P}_2} \Longrightarrow \overline{\mathrm{P}_1}\right)$

II) Soit P, Q deux polynômes de $\mathbb{K}[X]$ si $PQ = 0$. Montrer que : $P = 0$ ou $Q = 0$.

Exercice02. (8p) Soient A et B deux sous-ensembles d'un ensemble E. La différence symétrique de A et B est l'ensemble, noté $A\Delta B$, défini par

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

1. La différence symétrique de deux ensemble est-elle commutative ?

2. Expliciter les ensembles suivants : $A\Delta\phi, A\Delta A$ et $A\Delta B$ si $A \subset B$.

3. Montrer que $A\Delta B = C_E A \Delta C_E B$.

4. Montrer que $A\Delta B = (A \cap C_E B) \cup (B \cap C_E A)$.

5. Expliciter l'ensemble $(A\Delta B) \cup (A\Delta C_E B)$.

Exercice03. (6p) Soit $(G, \cdot)$ un groupe, pour toute $a \in G$ on définit l'application

$$f_a : G \longrightarrow G$$
$$x \mapsto f_a(x) = axa^{-1}$$

1. Montrer que f_a est un homomorphisme de G.

2. Calculer le $\ker(f_a)$. Que vous conclus.

3. Montrer que $f_a \circ f_b = f_{ab}$.

4. Est ce que $f_a \circ f_b$ est un automorphisme de G.

6.1.1 solution

Exercice1. (6p)

I) -

P_1	P_2	$\overline{\mathrm{P}_1}$	$\overline{\mathrm{P}_2}$	$\mathrm{P}_1 \Longrightarrow \mathrm{P}_2$	$\overline{\mathrm{P}_2} \Longrightarrow \overline{\mathrm{P}_1}$	$\overline{\mathrm{P}_1 \Longrightarrow \mathrm{P}_2}$	$\mathrm{P}_1 \wedge \overline{\mathrm{P}_2}$	$\Leftrightarrow (1°)$	$\Leftrightarrow (2°)$
1	1	0	0	1	1	0	0	1	1
1	0	0	1	0	0	1	1	1	1
0	1	1	0	1	1	0	0	1	1
0	0	1	1	1	1	0	0	1	1

II) Soit $(P; Q) \in \mathbb{K}[X]$ tel que $PQ = 0$. Alors on a $\deg(P) + \deg(Q) = \deg(PQ) = -\infty$.

Donc $\deg(P)$ ou $\deg(Q)$ vaut $-\infty$, ce qui est exactement la propriété demandée.

Exercice02. (8p)

1. Elle est commutative car $\cup$ l'est.

2. A $\Delta\phi = (A\backslash\phi) \cup (\phi\backslash A) = A, A\Delta A = A$ et si $A \subset B$ alors $A\Delta B = B\backslash A$.

3.

$$\begin{aligned} A\Delta B &= \{x \in E, \quad (x \in A\backslash B) \vee (x \in B\backslash A)\} \\ &= \{x \in E, \quad (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\} \\ &= \{x \in E, \quad (x \notin C_E A \wedge x \in C_E B) \vee (x \notin C_E B \wedge x \in C_E A)\} \\ &= \{x \in E, \quad (x \in C_E B\backslash C_E A) \vee (x \in C_E A\backslash C_E B)\} \\ &= C_E A \Delta C_E B. \end{aligned}$$

4. $A\Delta B = (A\cap C_E B)\cup(B\cap C_E A)$

$$\begin{aligned} A\Delta B &= \{x\in E,\quad (x\in A\backslash B)\vee(x\in B\backslash A)\} \\ &= \{x\in E,\quad (x\in A\wedge x\notin B)\vee(x\in B\wedge x\notin A)\} \\ &= \{x\in E,\quad (x\in A\wedge x\in C_E B)\vee(x\in B\wedge x\in C_E A)\} \\ &= \{x\in E,\quad x\in(A\cap C_E B)\vee x\in(B\cap C_E A)\} \\ &= (A\cap C_E B)\cup(B\cap C_E A)\,. \end{aligned}$$

5. On a

$$\begin{aligned} (A\Delta B)\cup(A\Delta C_E B) &= ((A\cap C_E B)\cup(B\cap C_E A))\cup((A\cap B)\cup(C_E B\cap C_E A)) \\ &= ((A\cap C_E B)\cup(A\cap B))\cup((B\cap C_E A)\cup(C_E B\cap C_E A)) \\ &= (A\cap(C_E B\cup B))\cup((B\cup C_E B)\cap C_E A) \\ &= (A\cap E)\cup(E\cap C_E A) \\ &= A\cup C_E A = E \end{aligned}$$

Exercice03. (6p)

1. f_a est un homomorphisme de G.

Soit $x,y\in G \quad f_a(xy) = a(xy)a^{-1} = a\left(xa^{-1}ay\right)a^{-1} = \left(axa^{-1}\right)\left(aya^{-1}\right) = f_a(x)f_a(y)$.

2.

$$\begin{aligned} \ker(f_a) &= \{x\in G,\quad f_a(x)=1\} \\ &= \left\{x\in G,\quad axa^{-1}=1\right\} \\ &= \left\{x\in G,\quad a^{-1}axa^{-1}a = a^{-1}a\right\} \\ &= \{x\in G,\quad x=1\} \\ &= \{1\} \end{aligned}$$

alors f_a est injective.

3. Soit $x\in G$

$$(f_a\circ f_b)(x) = (f_a(f_b(x))) = \left(f_a\left(bxb^{-1}\right)\right) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = f_{ab}(x)$$

4. $(f_a\circ f_b$ est un automorphisme de $G) \Longleftrightarrow (f_{ab}$ est un homomorphisme bijective $)$

i) f_{ab} est un homomorphisme

$$f_{ab}(xy) = (ab)xy(ab)^{-1} = (ab)x(ab)^{-1}(ab)y(ab)^{-1} = f_a(x)f_a(y)$$

ii)

(a) f_{ab} est bijective

$$\begin{aligned}\ker(f_{ab}) &= \{x \in G, \quad f_{ab}(x) = 1\} \\ &= \{x \in G, \quad (ab)x(ab)^{-1} = 1\} \\ &= \{1\}\end{aligned}$$

alors f_{ab} est injective

(b) f_{ab} est surjective : Soit $y \in G \quad \exists x = (ab)^{-1}yab \in G$ tel que $f_{ab}(x) = f_{ab}\left((ab)^{-1}y(ab)\right) = y$.

6.2 Examen 02

Exercice01 (8p)

Soit $\mathrm{P}_1, \mathrm{P}_2$ et P_3 trois propositions. Démontrer les propriétés suivantes.

1. $(\mathrm{P}_1 \vee (\mathrm{P}_2 \wedge \mathrm{P}_3)) \Leftrightarrow ((\mathrm{P}_1 \vee \mathrm{P}_2) \wedge (\mathrm{P}_1 \vee \mathrm{P}_3))$

2. $\left(\mathrm{P}_1 \vee \left(\overline{\mathrm{P}_2 \vee \mathrm{P}_3}\right)\right) \Leftrightarrow \left(\left(\mathrm{P}_1 \vee \overline{\mathrm{P}_2}\right) \wedge \left(\mathrm{P}_1 \vee \overline{\mathrm{P}_3}\right)\right)$

Exercice02 (8p) Soient A et B deux sous-ensembles d'un ensemble E. La différence symétrique de A et B est l'ensemble, noté $A\Delta B$, défini par

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

1. La différence symétrique de deux ensemble est-elle commutative ?

2. Expliciter les ensembles suivants : $A\Delta\phi, A\Delta A$ et $A\Delta B$ si $A \subset B$.

3. Montrer que $A\Delta B = C_E A \Delta C_E B$.

4. Montrer que $A\Delta B = (A \cap C_E B) \cup (B \cap C_E A)$.

5. Expliciter l'ensemble $(A\Delta B) \cup (A\Delta C_E B)$.

Exercice03 (4p) Parmi les applications suivantes, déterminer les injections, les surjections et les bijections :

$$f : \mathbb{R} \to \mathbb{R} \quad g : \mathbb{R}_+ \to \mathbb{R}$$

$$x \longmapsto f(x) = x^2 \longmapsto g \longmapsto g(x) = x^2$$

$$h : \mathbb{R} \to \quad \mathbb{R}_+ \quad k : \mathbb{R}_+ \to \quad \mathbb{R}_+$$

$$x \longmapsto h(x) = x^2 \longmapsto k(x) = x^2$$

6.2.1 solution

Exercice01 (8p)

1. $(\mathrm{P}_1 \vee (\mathrm{P}_2 \wedge \mathrm{P}_3)) \Leftrightarrow ((\mathrm{P}_1 \vee \mathrm{P}_2) \wedge (\mathrm{P}_1 \vee \mathrm{P}_3))$

P_1	P_2	P_3	$(\mathrm{P}_2 \wedge \mathrm{P}_3)$	$\mathrm{P}_1 \vee (\mathrm{P}_2 \wedge \mathrm{P}_3)$	$\mathrm{P}_1 \vee \mathrm{P}_2$	$\mathrm{P}_1 \vee \mathrm{P}_3$	$(\mathrm{P}_1 \vee \mathrm{P}_2) \wedge (\mathrm{P}_1 \vee \mathrm{P}_3)$	$\Longleftrightarrow$
1	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1	1
1	0	1	0	1	1	1	1	1
1	0	0	0	1	1	1	1	1
0	1	1	1	1	1	1	0	1
0	1	0	0	0	1	0	1	1
0	0	1	0	0	0	1	0	1
0	0	0	0	0	0	0	1	1

2. $\left(\mathrm{P}_1 \vee \left(\overline{\mathrm{P}_2 \vee \mathrm{P}_3}\right)\right) \Leftrightarrow \left(\left(\mathrm{P}_1 \vee \overline{\mathrm{P}_2}\right) \wedge \left(\mathrm{P}_1 \vee \overline{\mathrm{P}_3}\right)\right)$

On a $\left(\overline{\mathrm{P}_2 \vee \mathrm{P}_3}\right) \Longleftrightarrow \left(\overline{\mathrm{P}_2} \wedge \overline{\mathrm{P}_3}\right)$ alors

$$\left(\mathrm{P}_1 \vee \left(\overline{\mathrm{P}_2 \vee \mathrm{P}_3}\right)\right) \Leftrightarrow \left(\mathrm{P}_1 \vee \left(\overline{\mathrm{P}_2} \wedge \overline{\mathrm{P}_3}\right)\right) \overset{(1)}{\Leftrightarrow} \left(\left(\mathrm{P}_1 \vee \overline{\mathrm{P}_2}\right) \wedge \left(\mathrm{P}_1 \vee \overline{\mathrm{P}_3}\right)\right)$$

Exercice02(8p)

1. Elle est commutative car $\cup$ l'est.

2. $A\Delta\phi = (A\backslash\phi) \cup (\phi\backslash A) = A, A\Delta A = A$ et si $A \subset B$ alors $A\Delta B = B\backslash A$.

3.

$$\begin{aligned} A\Delta B &= \{x\in E,\quad (x\in A\backslash B)\vee(x\in B\backslash A)\} \\ &= \{x\in E,\quad (x\in A\wedge x\notin B)\vee(x\in B\wedge x\notin A)\} \\ &= \{x\in E,\quad (x\notin C_EA\wedge x\in C_EB)\vee(x\notin C_EB\wedge x\in C_EA)\} \\ &= \{x\in E,\quad (x\in C_EB\backslash C_EA)\vee(x\in C_EA\backslash C_EB)\} \\ &= C_EA\Delta C_EB. \end{aligned}$$

4. $A\Delta B=(A\cap C_EB)\cup(B\cap C_EA)$

$$\begin{aligned} A\Delta B &= \{x\in E,\quad (x\in A\backslash B)\vee(x\in B\backslash A)\} \\ &= \{x\in E,\quad (x\in A\wedge x\notin B)\vee(x\in B\wedge x\notin A)\} \\ &= \{x\in E,\quad (x\in A\wedge x\in C_EB)\vee(x\in B\wedge x\in C_EA)\} \\ &= \{x\in E,\quad x\in(A\cap C_EB)\vee x\in(B\cap C_EA)\} \\ &= (A\cap C_EB)\cup(B\cap C_EA). \end{aligned}$$

5. Ona

$$\begin{aligned} (A\Delta B)\cup(A\Delta C_EB) &= ((A\cap C_EB)\cup(B\cap C_EA))\cup((A\cap B)\cup(C_EB\cap C_EA)) \\ &= ((A\cap C_EB)\cup(A\cap B))\cup((B\cap C_EA)\cup(C_EB\cap C_EA)) \\ &= (A\cap(C_EB\cup B))\cup((B\cup C_EB)\cap C_EA) \\ &= (A\cap E)\cup(E\cap C_EA) \\ &= A\cup C_EA=E \end{aligned}$$

Exercice03(4p) les injections, les surjections et les bijections :

- g est injective car $\forall x_1,x_2\in\mathbb{R}_+$si $f(x_1)=f(x_2)$ on a $x_1=x_2$.
- h est surjective car $\forall y\in\mathbb{R}_+\exists x\in\mathbb{R}$ tel que $f(x)=y$.
- k est bijective.

6.3 Examen 03

Exercice01 (5p)

I) Soit $\mathrm{P}_1,\mathrm{P}_2$ et P_3 des propositions. Démontrer que :

1. $(\mathrm{P}_1 \vee (\mathrm{P}_2 \wedge \mathrm{P}_3)) \Leftrightarrow ((\mathrm{P}_1 \vee \mathrm{P}_2) \wedge (\mathrm{P}_1 \vee \mathrm{P}_3))$

II) Soit $\mathcal{R}$ une relation d'équivalence dans un ensemble E. Montrer que :

1. $\forall x, y \in E, \quad x\mathcal{R}y \Longleftrightarrow \bar{x} = \bar{y}$.

2. $\forall x, y \in E, \quad x\mathcal{R}y \Longrightarrow \bar{x} \cap \bar{y} = \phi$

Exercice02 (7p) Soit $g : E \longrightarrow F$ une application. Soit A et B deux parties de F. Montrerque :

1. $A \backslash B = A \cap C_F B$

2. $C_F(A \cup B) = C_F A \cap C_F B$

3. $g^{-1}(A \cup B) = g^{-1}(A) \cup g^{-1}(B)$

4. $g^{-1}(A \cap B) = g^{-1}(A) \cap g^{-1}(B)$

5. $g^{-1}(C_F B) = C_E g^{-1}(B)$

6. Expliciter l'ensemble $g^{-1}(A \Delta B)$

Exercice03 (5p) Soient $(\mathbb{R}, +)$ et $\left(\mathbb{R}_+^*, \right)$ deux groupes. Soit l'application

$$f : \mathbb{R} \longrightarrow \mathbb{R}_+^*$$

$$x \mapsto f(x) = 2^x$$

1. Montrer que f est un homomorphisme de $(\mathbb{R}, +)$ dans $\left(\mathbb{R}_+^*, \right)$.

2. Calculer le $\ker(f)$. Que vous conclus.

3. Est ce que f est surjective.

Exercice04 (5p) Soit $h : E \longrightarrow F$ une application. B partie de F. Montrer que.

$$\left(B = h\left(h^{-1}(B)\right)\right) \Longleftrightarrow (h \text{ est surjective })$$

6.3.1 solution

Exercice01 (5p)

I) $(\mathrm{P}_1 \vee (\mathrm{P}_2 \wedge \mathrm{P}_3)) \Leftrightarrow ((\mathrm{P}_1 \vee \mathrm{P}_2) \wedge (\mathrm{P}_1 \vee \mathrm{P}_3))$.

P_1	P_2	P_3	$(P_2 \wedge P_3)$	$P_1 \vee (P_2 \wedge P_3)$	$P_1 \vee P_2$	$P_1 \vee P_3$	$(P_1 \vee P_2) \wedge (P_1 \vee P_3)$	$\Longleftrightarrow$
1	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1	1
1	0	1	0	1	1	1	1	1
1	0	0	0	1	1	1	1	1
0	1	1	1	1	1	1	1	1
0	1	0	0	0	1	0	0	1
0	0	1	0	0	0	1	0	1
0	0	0	0	0	0	0	0	1

II)

1) soit $z \in \bar{x}$.

$$\begin{aligned} z \in \bar{x} &\Longleftrightarrow x\mathcal{R}z \\ (\text{car } x\mathcal{R}y) &\Longleftrightarrow z\mathcal{R}x \\ &\Longleftrightarrow z\mathcal{R}y \\ &\Longleftrightarrow z \in \bar{y} \end{aligned}$$

2) Nous allons raisonner par contraposée $(\bar{x} \cap \bar{y} \neq \phi \Longrightarrow x\mathcal{R}y)$

$$\begin{aligned} z \in \bar{x} \cap \bar{y} &\Longrightarrow z \in \bar{x} \text{ et } z \in \bar{y} \\ &\Longrightarrow x\mathcal{R}z \text{ et } z\mathcal{R}y \\ &\Longrightarrow x\mathcal{R}y \end{aligned}$$

Exercice02 (7p) Soit $g : E \longrightarrow F$ une application. Soit A et B deux parties de F. Montrer que :

1. $x \in A \backslash B \Longleftrightarrow x \in A \wedge x \notin B \Longleftrightarrow x \in A \wedge x \in C_F B \Longleftrightarrow x \in A \cap C_F B$

2.

$$x \in C_F(A \cup B) \Longleftrightarrow x \in F \wedge (x \notin (A \cup B)) \Longleftrightarrow x \in F \wedge (x \notin A \wedge x \notin B) \Longleftrightarrow$$

$$(x \in F \wedge x \notin A) \wedge (x \in F \wedge x \notin B) \Longleftrightarrow x \in F \backslash A \wedge x \in F \backslash B \Longleftrightarrow x \in C_F A \cap C_F B$$

3.

$$x \in g^{-1}(A \cup B) \Longleftrightarrow g(x) \in A \cup B \Longleftrightarrow g(x) \in A \vee g(x) \in B$$

$$\Longleftrightarrow x \in g^{-1}(A) \vee x \in g^{-1}(B) \Longleftrightarrow x \in g^{-1}(A) \cup g^{-1}(B)$$

6.3. Examen 03

4.

$$x \in g^{-1}(A \cap B) \Longleftrightarrow g(x) \in (A \cap B) \Longleftrightarrow g(x) \in A \wedge g(x) \in B$$
$$\Longleftrightarrow x \in g^{-1}(A) \wedge x \in g^{-1}(B) \Longleftrightarrow x \in g^{-1}(A) \cap g^{-1}(B)$$

5. $x \in g^{-1}(C_F B) \Longleftrightarrow g(x) \in C_F B \Longleftrightarrow g(x) \notin B \Longleftrightarrow x \notin g^{-1}(B) \Longleftrightarrow x \in C_E g^{-1}(B)$

6. $g^{-1}(A \Delta B) = g^{-1}((A \backslash B) \cup (B \backslash A)) \overset{(2)}{=} g^{-1}(A \backslash B) \cup g^{-1}(B \backslash A) \overset{(1)}{=} g^{-1}(A \cap C_F B) \cup g^{-1}(C_F A \cap B)$

$\overset{(3)}{=} (g^{-1}(A) \cap g^{-1}(C_F B)) \cup (g^{-1}(C_F A) \cap g^{-1}(B)) \overset{(4)}{=} (g^{-1}(A) \cap C_E g^{-1}(B)) \cup (C_E g^{-1}(A) \cap g^{-1}(B))$

$\overset{(4)}{=} (g^{-1}(A) \cap C_E g^{-1}(B)) \cup (C_E g^{-1}(A) \cap g^{-1}(B)) \overset{(1)}{=} (g^{-1}(A) \backslash f^{-1}(B)) \cup (g^{-1}(B) \backslash g^{-1}(A)) =$

$g^{-1}(A) \Delta g^{-1}(B)$.

Exercice03 (5p)

1. f est un homomorphisme de $(\mathbb{R}, +)$ dans $\left(\mathbb{R}_+^*, \cdot\right)$.

Soit $x_1, x_2 \in \mathbb{R} \quad f(x_1 + x_2) = 2^{x_1 + x_2} = 2^{x_1} 2^{x_2} = f(x_1) f(x_2)$.

2.

$$\begin{aligned} \ker(f) &= \{x \in \mathbb{R} : \ f(x) = 1\} \\ &= \{x \in \mathbb{R} : \ 2^x = 1\} \\ &= \{x \in \mathbb{R} : \ \ln(2^x) = \ln(1) = 0\} \\ &= \{x \in \mathbb{R} : \ x \ln(2) = 0\} \\ &= \{x \in \mathbb{R} : \ x = 0\} \\ &= \{0\} \end{aligned}$$

alors f est injective

3. f est surjective car $: \forall y \in \mathbb{R}_+^*, \exists x = \frac{\ln(y)}{\ln(2)} \in \mathbb{R} : f(x) = f\left(\frac{\ln(y)}{\ln(2)}\right) = 2^{\frac{\ln(y)}{\ln(2)}} = e^{\ln\left(2^{\ln(y)} \ln(2)\right)} =$ $e^{\frac{\ln(y)}{\ln(2)} \ln(2)} = e^{\ln(y)} = y$

Exercice04(3p)

1) $(B = h(h^{-1}(B))) \Longrightarrow (h$ est surjective) supposons que $B = h(h^{-1}(B))$pour toute partie de F.

$[(h$ est surjective $) \Longleftrightarrow (h(E) = F)]$ on a $h(E) \subset F$ car h est une application, il reste à dé-monté que $F \subset h(E)$ d'après la proposition on a $F = h(h^{-1}(F))$ mais $h^{-1}(F) \subset E$ alors$h(h^{-1}(F)) \subset h(E)$ donc $F \subset h(E)$.

2) (h est surjective) $\Longrightarrow (B = h(h^{-1}(B)))$ supposons que h est surjective, il reste à démontéque $B = h(h^{-1}(B))$:

- **(i)** $B \subset h(h^{-1}(B))$, soit $y \in B$ alors $\exists x \in E h(x) = y$ (car h est surjective), donc $h(x) \in B \Longrightarrow x \in h^{-1}(B) \Longrightarrow h(x) \in h(h^{-1}(B)) \Longrightarrow y \in h(h^{-1}(B))$
- **(ii)** $h(h^{-1}(B)) \subset B$, soit $y \in h(h^{-1}(B))$ alors $\exists x \in h^{-1}(B), h(x) = y$ donc $h(x) = y \in B$.

6.4 Examen 04

Exercice01 (6p) Soit $(G_1, *)$ et $(G_2, \perp)$ deux groupe et f est un homomorphisme de $(G_1, *)$ dans $(G_2, \perp)$. Montrer que :

1. $f(e_1) = e_2$
2. $\forall x \in G_1 : \quad [f(x)]' = f(x')$.
3. $\ker(f)$ est un sous-groupe de G_1.
4. $(\ker(f) = \{e_1\}) \Longleftrightarrow (f$ est injective).

Exercice012 (8p) Soit $g : E \longrightarrow F$ une application. Soit A et B deux parties de F. Montrer que :

1. $A \backslash B = A \cap C_F B$
2. $C_F(A \cup B) = C_F A \cap C_F B$
3. $g^{-1}(A \cup B) = g^{-1}(A) \cup g^{-1}(B)$
4. $g^{-1}(A \cap B) = g^{-1}(A) \cap g^{-1}(B)$
5. $g^{-1}(C_F B) = C_E g^{-1}(B)$
6. Expliciter l'ensemble $g^{-1}(A \Delta B)$

Exercice03 (6p) Démontrer les propositions suivants par contraposée ou par l'absurde :

1. $(n^2$ est pair $) \Longrightarrow (n$ est pair $).(\forall n \in \mathbb{N})$
2. $\sqrt{2} \notin \mathbb{Q}$

6.4.1 solution

Exercice01 (6p)

1. $f(e_1) = e_2$.

On a $e_1 = e_1 * e_1$ alors $f(e_1) = f(e_1 * e_1) \overset{f \text{ hom}}{=} f(e_1) \perp f(e_1) \Longrightarrow f(e_1) = e_2$

2. $\forall x \in G_1 : \quad [f(x)]' = f(x')$.

On a $f(x') \perp f(x) = f(x' * x) = f(e_1) \overset{(1)}{=} e_2 \Longrightarrow (f(x))' = f(x')$.

3. $\ker(f)$ est un sous-groupe de G_1.

$\ker(f)$ est un sous-groupe de G_1 si et seulement si

$$\forall (x, y) \in \ker(f) \ker(f) \Longrightarrow x * y' \in ker(f)$$

Soient $x, y \in \ker(f) \Rightarrow f(x) = e_2$ et $f(y) = e_2$ on démontre que $x * y' \in ker(f)$ on a $f(x * y') = f(x) \perp f(y') \overset{(1)}{=} f(x) \perp [f(y)]' = e_2 \perp e_2 = e_2$. Donc $f(x * y') = e_2$ implique $x * y' \in \ker(f)$.

4. $(\ker(f) = \{e_1\}) \Longleftrightarrow (f$ est injective $)$.

$\Longleftarrow)$ Supposons que $\ker(f) = \{e_1\}$ alors, soient $x_1, x_2 \in G_1$ tel que $f(x_1) = f(x_2)$ donc $f(x_1') \perp f(x_1) = f(x_1') \perp f(x_2)$ lorsque f est un homomorphisme alors $e_1 = f(x_1' * x_2)$ implique $x_1' * x_2 \in \ker(f) = \{e_1\}$ donc $x_1' * x_2 = e_1$ alors $x_1 = x_2$ ce implique que f est injective.

$\Longrightarrow)$ Supposons que f est injective

soit $x \in \ker(f) \Longrightarrow f(x) = e_2 = f(e_1) \Longrightarrow x = e_1$ (car f est injective) alors $\ker(f) = \{e_1\}$

Exercice02 (8p) Soit $g : E \longrightarrow F$ une application. Soit A et B deux parties de F. Montrer que :

1. $x \in A \backslash B \Longleftrightarrow x \in A \wedge x \notin B \Longleftrightarrow x \in A \wedge x \in C_F B \Longleftrightarrow x \in A \cap C_F B$

2.

$$x \in C_F(A \cup B) \Longleftrightarrow x \in F \wedge (x \notin (A \cup B)) \Longleftrightarrow x \in F \wedge (x \notin A \wedge x \notin B) \Longleftrightarrow$$
$$(x \in F \wedge x \notin A) \wedge (x \in F \wedge x \notin B) \Longleftrightarrow x \in F \backslash A \wedge x \in F \backslash B \Longleftrightarrow x \in C_F A \cap C_F B$$

3.

$$x \in g^{-1}(A \cup B) \Longleftrightarrow g(x) \in A \cup B \Longleftrightarrow g(x) \in A \vee g(x) \in B$$
$$\Longleftrightarrow x \in g^{-1}(A) \vee x \in g^{-1}(B) \Longleftrightarrow x \in g^{-1}(A) \cup g^{-1}(B)$$

4.

$$x \in g^{-1}(A \cap B) \Longleftrightarrow g(x) \in (A \cap B) \Longleftrightarrow g(x) \in A \wedge g(x) \in B$$
$$\Longleftrightarrow x \in g^{-1}(A) \wedge x \in g^{-1}(B) \Longleftrightarrow x \in g^{-1}(A) \cap g^{-1}(B)$$

5. $x \in g^{-1}\left(C_F B\right) \Longleftrightarrow g(x) \in C_F B \Longleftrightarrow g(x) \notin B \Longleftrightarrow x \notin g^{-1}(B) \Longleftrightarrow x \in C_E g^{-1}(B)$

6. $g^{-1}(A \Delta B) = g^{-1}((A \backslash B) \cup (B \backslash A)) \overset{(2)}{=} g^{-1}(A \backslash B) \cup g^{-1}(B \backslash A) \overset{(1)}{=} g^{-1}\left(A \cap C_F B\right) \cup g^{-1}\left(C_F A \cap B\right)$

$\overset{(3)}{=} (g^{-1}(A) \cap g^{-1}\left(C_F B\right)) \cup (g^{-1}\left(C_F A\right) \cap g^{-1}(B)) \overset{(4)}{=} (g^{-1}(A) \cap C_E g^{-1}(B)) \cup (C_E g^{-1}(A) \cap g^{-1}(B))$

$\overset{(4)}{=} (g^{-1}(A) \cap C_E g^{-1}(B)) \cup (C_E g^{-1}(A) \cap g^{-1}(B)) \overset{(1)}{=} (g^{-1}(A) \backslash f^{-1}(B)) \cup (g^{-1}(B) \backslash g^{-1}(A)) =$

$g^{-1}(A) \Delta g^{-1}(B)$

Exercice03 (6p) Démontrer les propositions suivants par contraposée ou par l'absurde :

1. (n^2 est pair) $\Longrightarrow$ (n est pair).($\forall n \in \mathbb{N}$)

En passant à la contraposée, nous voyons qu'il suffit que nous montrions l'implication

$$(n \text{ est impair }) \Longrightarrow \left(n^2 \text{ est impair }\right)$$

Supposons que n est impair, alors $n = 2k+1$ implique que $n^2 = (2k+1)^2 = 2\left(k^2 + k\right)+1 = 2k' + 1$, on voit que n^2 est impair. Ceci prouve l'implication $(*)$, ce qui termine la preuve.

2. $\sqrt{2} \notin \mathbb{Q}$.en utilise l'absurde

Supposons que $\sqrt{2} \in \mathbb{Q}$ alors $\sqrt{2} = \frac{p}{q}$ avec $p \wedge q = 1$, alors on a $2 = \frac{p^2}{q^2}$ donc $p^2 = 2q^2$ implique p est paie et par la même manière on trouve $q^2 = 2p^2$ implique que q est paie donc $p \wedge q \neq 1$. Ceci est absurde puisque nous savons que $p \wedge q = 1$

6.5 Examen 05

Exercice01 (5p) Soient $\left(\mathbb{R}_+^*, \right)$ et $(\mathbb{R}, +)$ deux groupes. Soit l'application

$$\begin{aligned} f : \mathbb{R}_+^* &\longrightarrow \mathbb{R} \\ x &\mapsto f(x) = \ln(x) \end{aligned}$$

1. Montrer que f est un homomorphisme de $\left(\mathbb{R}_{+}^{*},\right)$ dans $(\mathbb{R},+)$.

2. Calculer le $\ker(f)$. Que vous conclus.

3. Est ce que f est surjective.

Exercice02 (5p) Soit $g : E \longrightarrow F$ une application. Soit A, B et C trois parties de E. Montrer que :

1. $A \backslash B = A \cap C_E B$

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

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

4. $[g(A \cap B) = g(A) \cap g(B)] \Longrightarrow [g$ est injective $]$.

Exercice03 (5p) Soient :

$$\begin{aligned} f : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\mapsto f(n) = n+1 \end{aligned} \quad \text{et} \quad \begin{aligned} g : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\mapsto g(n) = \begin{cases} 0 & \text{si } n = 0 \\ n-1 & \text{si } n \neq 0 \end{cases} \end{aligned}$$

1. Etudier l'injectivité et la surjectivité de f et g.

2. Calculer $f \circ g$ et $g \circ f$.

Exercice04(4p) Soit $\mathcal{R}$ une relation binaire sur $\mathbb{R}^3$ défini par

$$(x, y, z) \mathcal{R} (a, b, c) \Longleftrightarrow (|x-a| \leq b-y \quad \text{et} \quad z = c)$$

1. Montrer que c'est une relation d'ordre ; est-il total ?

6.5.1 solution

Exercice01 (5p)

1. f est un homomorphisme de $\left(\mathbb{R}_{+}^{*}, \cdot\right)$ dans $(\mathbb{R},+)$.

Soit $x_1, x_2 \in \mathbb{R}_{+}^{*}$ $\quad f\left(x_1 \cdot x_2\right) = \ln\left(x_1 \cdot x_2\right) = \ln\left(x_1\right) + \ln\left(x_2\right) = f\left(x_1\right) + f\left(x_2\right)$.

2.

$$\begin{aligned}\ker(f) &= \left\{x \in \mathbb{R}_+^* : f(x) = 0\right\} \\ &= \left\{x \in \mathbb{R}_+^* : \ln(x) = 0\right\} \\ &= \left\{x \in \mathbb{R}_+^* : e^{\ln(x)} = e^0 = 1\right\} \\ &= \left\{x \in \mathbb{R}_+^* : x = 1\right\} \\ &= \{1\}\end{aligned}$$

alors f est injective

3. f est surjective car :

$\forall y \in \mathbb{R}, \exists x = e^y \in \mathbb{R}_+^* : f(x) = f\left(e^y\right) = \ln\left(e^y\right) = y$

Exercice02 (5p) Soit $g : E \longrightarrow F$ une application. Soit A, B et C trois parties de E. Montrer que :

1. $x \in A \backslash B \Longleftrightarrow x \in A \wedge x \notin B \Longleftrightarrow x \in A \wedge x \in C_E B \Longleftrightarrow x \in A \cap C_E B$

2. $x \in C_E(A \cup B) \Longleftrightarrow x \in E \wedge (x \notin (A \cup B)) \Longleftrightarrow x \in E \wedge (x \notin A \wedge x \notin B) \Longleftrightarrow$

$(x \in E \wedge x \notin A) \wedge (x \in E \wedge x \notin B) \Longleftrightarrow x \in E \backslash A \wedge x \in E \backslash B \Longleftrightarrow x \in C_E A \cap C_E B$

3. $A \backslash (B \cup C) \overset{(1)}{=} A \cap C_E(B \cup C) \overset{(2)}{=} A \cap (C_E B \cap C_E C) = (A \cap C_E B) \cap (A \cap C_E C) = (A \backslash B) \cap (A \backslash C)$

4. Soient $x_1, x_2 \in E$ tels que $g\left(x_1\right) = g\left(x_2\right)$.

Posons $A = \{x_1\}$ et $B = \{x_2\}$.

On a $g\left(x_1\right) = g\left(x_2\right) \in g(A) \cap g(B) = g(A \cap B)$.

Donc $g(A \cap B) \neq \phi$ et par suite, $A \cap B \neq \phi$.

Ceci implique $x_1 = x_2$.

Exercice03 (6p)

1)

- f est injective ssi $\forall n_1, n_2 \in \mathbb{N} : f\left(n_1\right) = f\left(n_2\right) \Longrightarrow n_1 = n_2$.

  Soient $n_1, n_2 \in \mathbb{N}$ tels que $f\left(n_1\right) = f\left(n_2\right)$ alors $n_1 + 1 = n_2 + 1$ ceci implique $n_1 = n_2$.

  Donc f est injective

- f n'est pas surjective car : $\exists y = 0 \in \mathbb{N}, \forall n \in \mathbb{N} \quad f(n) \neq y$.

- g n'est pas injective car : $\exists n_1 = 0, n_2 = 1 \in \mathbb{N} : g(0) = 0 = g(1) \wedge 0 \neq 1$.
- g est surjective ssi : $\forall y \in \mathbb{N}, \exists n = y + 1 \in \mathbb{N} g(n) = g(y+1) = y$.

2)

- Soit $n \in \mathbb{N}, (f \circ g)(n) = f(g(n)) = g(n) + 1 = \begin{cases} 1 & \text{si } n = 0 \\ n & \text{si } n \neq 0 \end{cases}$.
- Soit $n \in \mathbb{N}, (g \circ f)(n) = g(f(n)) = g(n+1) = n$.

Exercice04. (4p)

1) $\mathcal{R}$ est réflexive ssi $(x, y, z)\mathcal{R}(x, y, z)$. Comme $(|x - x| = 0 \leq y - y = 0$ et $z = z)$ alors $\mathcal{R}$ est réflexive

2) $\mathcal{R}$ est anti-symétrique si $[(x, y, z)\mathcal{R}(a, b, c)$ et $(a, b, c)\mathcal{R}(x, y, z)] \Longrightarrow (x, y, z) = (a, b, c)$. Supposons $(x, y, z)\mathcal{R}(a, b, c)$ et $(a, b, c)\mathcal{R}(x, y, z)$. Ceci implique $[(|x - a| \leq b - y(*)$ et $|a - x| \leq y - b(**))$ et $z = c)$, alors $(*) + (**)$ donne $x = a$, on remplace $x = a$ dans $(*)$ et $(**)$ on trouve $y = b$.

Donc $(x, y, z) = (a, b, c)$ alors $\mathcal{R}$ est anti-symétrique.

3) $\mathcal{R}$ est transitive si $(x, y, z)\mathcal{R}(a, b, c)$ et $(a, b, c)\mathcal{R}(\alpha, \beta, \gamma) \Longrightarrow (x, y, z)\mathcal{R}(\alpha, \beta, \gamma)$. Supposons $(x, y, z)\mathcal{R}(a, b, c)$ et $(a, b, c)\mathcal{R}(\alpha, \beta, \gamma)$, ceci implique $[(|x - a| \leq b - y \quad (*)$ et $|a - \alpha| \leq \beta - b(**))$ et $z = c = \gamma]$, alors $(*) + (**)$ donne $(|x - a| + |a - \alpha| \leq b - y + \beta - b$ et $z = c = \gamma)$ et comme $(|x - \alpha| = |x - a + a - \alpha| \leq |x - a| + |a - \alpha| \leq y + \beta$ et $z = \gamma)$ implique $(x, y, z)\mathcal{R}(\alpha, \beta, \gamma)$.

Donc $\mathcal{R}$ est transitive. De $(1), (2)$ et $(3)\mathcal{R}$ une relation d'order sur $\mathbb{R}^3$.

- $\mathcal{R}$ n'est pas total car $\exists (x, y, z) = (0, 0, 2) \in \mathbb{R}^3$ et $(a, b, c) = (0, 0, 3) \in \mathbb{R}^3$ tels que $(0, 0, 2)\mathcal{R}(0, 0, 3)$ et $(0, 0, 3)\mathcal{R}(0, 0, 2)$.

Exercice05 (4p) Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications quelconques.

1. (Si f et g sont injectives) $\Longrightarrow g \circ f$ est injective.

2. (Si f et g sont surjectives) $\Longrightarrow g \circ f$ est sont surjective.

3. (Si f et g sont bijectives) $\Longrightarrow ((g \circ f)^{-1} = f^{-1} \circ g^{-1})$

6.6 Examen 06

Exercice01(6p)

I) Soit $\mathrm{P}_1, \mathrm{P}_2$ et P_3 des propositions. Démontrer que :

1. $(\mathrm{P}_1 \vee (\mathrm{P}_2 \wedge \mathrm{P}_3)) \Leftrightarrow ((\mathrm{P}_1 \vee \mathrm{P}_2) \wedge (\mathrm{P}_1 \vee \mathrm{P}_3))$

II) Soit $\mathcal{R}$ une relation d'équivalence dans un ensemble E. Montrer que :

1. $\forall x, y \in E, \quad x\mathcal{R}y \Longleftrightarrow \bar{x} = \bar{y}$.

2. $\forall x, y \in E, \quad x\mathcal{R}y \Longrightarrow \bar{x} \cap \bar{y} = \phi$

Exercice02 (6p) Soit $g : E \longrightarrow F$ une application. Soit A et B deux parties de F. Montrer que :

1. $A \backslash B = A \cap C_F B$

2. $C_F(A \cup B) = C_F A \cap C_F B$

3. $g^{-1}(A \cup B) = g^{-1}(A) \cup g^{-1}(B)$

4. $g^{-1}(A \cap B) = g^{-1}(A) \cap g^{-1}(B)$

5. $g^{-1}(C_F B) = C_E g^{-1}(B)$

6. Expliciter l'ensemble $g^{-1}(A \Delta B)$

Exercice03 (3p) Soient $(\mathbb{R}, +)$ et $\left(\mathbb{R}_+^*, \right)$ deux groupes. Soit l'application

$$f : \mathbb{R} \longrightarrow \mathbb{R}_+^*$$
$$x \mapsto f(x) = 2^x$$

1. Montrer que f est un homomorphisme de $(\mathbb{R}, +)$ dans $\left(\mathbb{R}_+^*, \right)$.

2. Calculer le $\ker(f)$. Que vous conclus.

3. Est ce que f est surjective.

Exercice04 (5p) Soit $h : E \longrightarrow F$ une application. B partie de F. Montrer que.

$$\left(B = h\left(h^{-1}(B)\right)\right) \Longleftrightarrow (h \text{ est surjective })$$

6.6.1 solution

Exercice01 (5p)

I) $(\mathrm{P}_1 \vee (\mathrm{P}_2 \wedge \mathrm{P}_3)) \Leftrightarrow ((\mathrm{P}_1 \vee \mathrm{P}_2) \wedge (\mathrm{P}_1 \vee \mathrm{P}_3))$.

P_1	P_2	P_3	$(\mathrm{P}_2 \wedge \mathrm{P}_3)$	$\mathrm{P}_1 \vee (\mathrm{P}_2 \wedge \mathrm{P}_3)$	$\mathrm{P}_1 \vee \mathrm{P}_2$	$\mathrm{P}_1 \vee \mathrm{P}_3$	$(\mathrm{P}_1 \vee \mathrm{P}_2) \wedge (\mathrm{P}_1 \vee \mathrm{P}_3)$	$\Longleftrightarrow$
1	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1	1
1	0	1	0	1	1	1	1	1
1	0	0	0	1	1	1	1	1
0	1	1	1	1	1	1	1	1
0	1	0	0	0	1	0	0	1
0	0	1	0	0	0	1	0	1
0	0	0	0	0	0	0	0	1

II)

1) soit $z \in \bar{x}$.

$$\begin{aligned} z \in \bar{x} &\Longleftrightarrow x\mathcal{R}z \\ (\text{car}\, x\mathcal{R}y) &\Longleftrightarrow z\mathcal{R}x \\ &\Longleftrightarrow z\mathcal{R}y \\ &\Longleftrightarrow z \in \bar{y} \end{aligned}$$

2) Nous allons raisonner par contraposée $(\bar{x} \cap \bar{y} \neq \phi \Longrightarrow x\mathcal{R}y)$

$$\begin{aligned} z \in \bar{x} \cap \bar{y} &\Longrightarrow z \in \bar{x} \text{ et } z \in \bar{y} \\ &\Longrightarrow \quad x\mathcal{R}z \text{ et } z\mathcal{R}y \\ &\Longrightarrow \quad x\mathcal{R}y \end{aligned}$$

Exercice02 (7p) Soit $g : E \longrightarrow F$ une application. Soit A et B deux parties de F. Montrer que :

1. $x \in A \backslash B \Longleftrightarrow x \in A \wedge x \notin B \Longleftrightarrow x \in A \wedge x \in C_F B \Longleftrightarrow x \in A \cap C_F B$

2. $x \in C_F(A \cup B) \Longleftrightarrow x \in F \wedge (x \notin (A \cup B)) \Longleftrightarrow x \in F \wedge (x \notin A \wedge x \notin B) \Longleftrightarrow$

$(x \in F \wedge x \notin A) \wedge (x \in F \wedge x \notin B) \Longleftrightarrow x \in F \backslash A \wedge x \in F \backslash B \Longleftrightarrow x \in C_F A \cap C_F B$

3. $x \in g^{-1}(A \cup B) \Longleftrightarrow g(x) \in A \cup B \Longleftrightarrow g(x) \in A \vee g(x) \in B$

$\Longleftrightarrow x \in g^{-1}(A) \vee x \in g^{-1}(B) \Longleftrightarrow x \in g^{-1}(A) \cup g^{-1}(B)$

4. $x \in g^{-1}(A \cap B) \Longleftrightarrow g(x) \in (A \cap B) \Longleftrightarrow g(x) \in A \wedge g(x) \in B \Longleftrightarrow$

$x \in g^{-1}(A) \wedge x \in g^{-1}(B) \Longleftrightarrow x \in g^{-1}(A) \cap g^{-1}(B)$

5. $x \in g^{-1}(C_F B) \Longleftrightarrow g(x) \in C_F B \Longleftrightarrow g(x) \notin B \Longleftrightarrow x \notin g^{-1}(B) \Longleftrightarrow x \in C_E g^{-1}(B)$

6. $g^{-1}(A\Delta B) = g^{-1}((A\backslash B)\cup(B\backslash A)) \overset{(2)}{=} g^{-1}(A\backslash B)\cup g^{-1}(B\backslash A) \overset{(1)}{=} g^{-1}(A \cap C_F B)\cup g^{-1}(C_F A \cap B)$

$\overset{(3)}{=} (g^{-1}(A) \cap g^{-1}(C_F B))\cup(g^{-1}(C_F A) \cap g^{-1}(B)) \overset{(4)}{=} (g^{-1}(A) \cap C_E g^{-1}(B))\cup(C_E g^{-1}(A) \cap g^{-1}(B))$

$\overset{(4)}{=} (g^{-1}(A) \cap C_E g^{-1}(B))\cup(C_E g^{-1}(A) \cap g^{-1}(B)) \overset{(1)}{=} (g^{-1}(A)\backslash f^{-1}(B))\cup(g^{-1}(B)\backslash g^{-1}(A)) =$

$g^{-1}(A)\Delta g^{-1}(B)$.

Exercice03 (5p)

1. f est un homomorphisme de $(\mathbb{R}, +)$ dans $\left(\mathbb{R}_+^*, \cdot\right)$.

Soit $x_1, x_2 \in \mathbb{R} \quad f(x_1 + x_2) = 2^{x_1+x_2} = 2^{x_1}2^{x_2} = f(x_1) f(x_2)$.

2.

$$\begin{aligned}
\ker(f) &= \{x \in \mathbb{R} : f(x) = 1\} \\
&= \{x \in \mathbb{R} : 2^x = 1\} \\
&= \{x \in \mathbb{R} : \ln(2^x) = \ln(1) = 0\} \\
&= \{x \in \mathbb{R} : x\ln(2) = 0\} \\
&= \{x \in \mathbb{R} : x = 0\} \\
&= \{0\}
\end{aligned}$$

alors f est injective

3. f est surjective car :

$$\forall y \in \mathbb{R}_+^*, \exists x = \tfrac{\ln(y)}{\ln(2)} \in \mathbb{R} : f(x) = f\left(\tfrac{\ln(y)}{\ln(2)}\right) = 2^{\frac{\ln(y)}{\ln(2)}} = e^{\ln\left(2^{\ln(y)}\ln(2)\right)} = e^{\frac{\ln(y)}{\ln(2)}\ln(2)} = e^{\ln(y)} = y$$

Exercice04 (3p)

1) $(B = h(h^{-1}(B))) \Longrightarrow (h$ est surjective$)$ supposons que $B = h(h^{-1}(B))$ pour toute partie de F.

$[(h \text{ est surjective }) \iff (h(E) = F)]$ on a $h(E) \subset F$ car h est une application, il reste à démonté que $F \subset h(E)$ d'après la proposition on a $F = h\left(h^{-1}(F)\right)$ mais $h^{-1}(F) \subset E$ alors $h\left(h^{-1}(F)\right) \subset h(E)$ donc $F \subset h(E)$.

2) (h est surjective) $\Longrightarrow (B = h\left(h^{-1}(B)\right))$ supposons que h est surjective, il reste à démonté que $B = h\left(h^{-1}(B)\right)$:

(i) $B \subset h\left(h^{-1}(B)\right)$, soit $y \in B$ alors $\exists x \in E h(x) = y$ (car h est surjective), donc $h(x) \in B \Longrightarrow x \in h^{-1}(B) \Longrightarrow h(x) \in h\left(h^{-1}(B)\right) \Longrightarrow y \in h\left(h^{-1}(B)\right)$

(ii) $h\left(h^{-1}(B)\right) \subset B$, soit $y \in h\left(h^{-1}(B)\right)$ alors $\exists x \in h^{-1}(B), h(x) = y$ donc $h(x) = y \in B$.

6.7 Examen 07

Exercice01 (4p)

1) Soit $n \in \mathbb{N}$. Montrer par disjonction des cas que $n\left(n^2+2\right)$ est un multiple de 3 .

2) Montrer par l'absurde que $(\forall n \in \mathbb{N}^*, \exists p \in \mathbb{N}^* : n = p^2) \Rightarrow (\forall q \in \mathbb{N}^* : 2n \neq q^2)$.

Exercice02 (6p)

1. Résoudre dans $\mathbb{R}$1 'équation $-x^2 + x = 0$.

2. Pour chaque $a \in \mathbb{R}$, resoudre dans $\mathbb{R}$ l'équation $-x^2 + x - a = 0$.

3. Soit $f : \mathbb{R} \to \mathbb{R}l'$ application définie par : Pour tout $x \in \mathbb{R}, f(x) = x(1-x)$. f est-elle injectivité ? Est-elle surjectivité ?

4. Montrer que l'application $g : \left[\frac{1}{2}, +\infty[\to] - \infty, \frac{1}{4}\right]$ définie par $g(x) = f(x)$ est bijective.

Exercice03 (4p)

Soit $\mathcal{R}$ la relation définie sur $\mathbb{Z}$ par :

$$\forall a, b \in \mathbb{Z} \quad : a\mathcal{R}b \Leftrightarrow (a - b \text{ est divisible par 2 ou par 3})$$

- Étudier la réflexivité, la symétrie, l'antisymétrie et la transitivité de $\mathcal{R}$. Conclure.

Exercice04 (6p)

Soit $*$ la loi de composition définie dans $\mathbb{R}$ par : $\forall x, y \in \mathbb{R} : x * y = x + y + \frac{1}{10}$.

1. Montrer que $(\mathbb{R}, *)$ est un groupe abélien.

2. Montrer que l'application g définie par : $g(x) = 5x + \frac{1}{2}$ est un homomorphisme du groupe $(\mathbb{R}, *)$ dans le groupe $(\mathbb{R}, +)$.

3. Soit $H = \left\{\frac{2n-1}{10}, n \in \mathbb{Z}\right\}$, Montrer que $(H, *)$ est un sous-groupe de $(\mathbb{R}, *)$

6.7.1 solution

Exercice01 (4p)

1) Soit $n \in \mathbb{N}$. On a :

<u>1^{er}**cas**</u> : Si $n = 3k$, avec $k \in \mathbb{N}$ alors $n\left(n^2+2\right) = 3k\left((3k)^2+2\right)$ qui est un multiple de 3

<u>2^{eme}**cas**</u> : Si $n = 3k+1$, avec $k \in \mathbb{N}$ alors $n\left(n^2+2\right) = (3k+1)\left((3k+1)^2+2\right) = (3k+1)\left(9k^2+6k+1+2\right)$

$$= 3(3k+1)\left(3k^2+2k+1\right) \text{ qui est un multiple de 3.}$$

<u>3^{eme}**cas**</u> **:** Si $n = 3k+2$, avec $k \in \mathbb{N}$ alors

$$\begin{aligned} n\left(n^2+2\right) &= (3k+2)\left((3k+2)^2+2\right) = (3k+2)\left(9k^2+12k+4+2\right) \\ &= 3(3k+2)\left(3k^2+4k+2\right) \text{ qui est un multiple de 3} \end{aligned}$$

Par suite, dans tous les cas $n\left(n^{2}+2\right)$ est un multiple de 3

2) Supposons que $(\forall n \in \mathbb{N}^*, \exists p \in \mathbb{N}^* : n = p^2)$ et $(\exists q \in \mathbb{N}^* : 2n = q^2)$.

Soit $n \in \mathbb{N}^*$, alors $n = p^2$ et $2n = q^2$ avec $p, q \in \mathbb{N}^*$, ainsi $2p^2 = q^2$, d'où $\sqrt{2} = \frac{q}{p} \in \mathbb{Q}$, ce qui est absurde car $\sqrt{2}$ est irrationnel.

Exercice02 (6p)

1) $-x^2 + x = 0 \Leftrightarrow x(1-x) = 0 \Leftrightarrow (x = 0 \text{ ou } x = 1)$, donc l'ensemble des solutions $S = \{0, 1\}$

2) $-x^2 + x - a = 0$ est une équation de second degré, calculons son discriminant : $\Delta = 1 - 4a$

Si $a > \frac{1}{4}$, alors $\Delta < 0$, donc il n'y a pas de solutions dans $\mathbb{R}$.

Si $a \leq \frac{1}{4}$, alors $\Delta \geq 0$, donc on a les solutions : $x_1 = \frac{1+\sqrt{1-4a}}{2}$ et $x_2 = \frac{1-\sqrt{1-4a}}{2}$

3) D'après 1), on a : $f(1) = f(0)$ mais $1 \neq 0$ donc f n'est pas injective.

D'après 2), on a : $y = 1$ n'a pas d'antécédent, alors f n'est pas surjective.

4.1) Soient $x_1, x_2 \in \left[\frac{1}{2}, +\infty\right[$:

$$g(x_1) = g(x_2) \Rightarrow x_1(1-x_1) = x_2(1-x_2) \Rightarrow x_1 - x_2 = {x_1}^2 - {x_2}^2$$

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

$$\Rightarrow (x_1 - x_2 = 0) \text{ ou } (x_1 + x_2 - 1 = 0) \Rightarrow (x_1 = x_2) \text{ ou } (x_1 = 1 - x_2)$$

$$\Rightarrow (x_1 = x_2) \text{ ou } \left(x_1 = x_2 = \frac{1}{2}\right), \text{ car } 1 - x_2 \geq \frac{1}{2} \Rightarrow x_2 \leq \frac{1}{2} \Rightarrow x_2 = \frac{1}{2}$$

$$\Rightarrow x_1 = x_2$$

Alors g est injective.

4.2) Soit $y \in]-\infty, \frac{1}{4}]$, d'après 2), l'équation $g(x) = y$ admet au moins une solution x dans $\mathbb{R}$.

On a $x_1 - \frac{1}{2} = \frac{1+\sqrt{1-4y}}{2} - \frac{1}{2} = \frac{\sqrt{1-4y}}{2} \geq 0$ d'où $x_1 \geq \frac{1}{2}$.

et $x_2 - \frac{1}{2} = \frac{1-\sqrt{1-4y}-1}{2} = \frac{-\sqrt{1-4y}}{2} \leq 0$ d'où $x_2 \leq \frac{1}{2}$.

Alors il suffit de prendre $x = \frac{1+\sqrt{1-4y}}{2} \in \left[\frac{1}{2}, +\infty\right[$, pour avoir $y = g(x)$.

Alors g est surjective.

Par suite g est bijective.

Exercice03 (4p)

1) Soit $a \in \mathbb{Z}$ on a : $a - a = 0$ est divisible par 2 ou par 3, c-à-d : $a\mathcal{R}a$

Alors $\mathcal{R}$ est réflexive.

2) Soient $a, b \in \mathbb{Z}$, on a :

$a\mathcal{R}b \Rightarrow a - b$ est divisible par 2 ou par 3

$\Rightarrow -(a - b)$ est divisible par 2 ou par 3

$\Rightarrow b - a$ est divisible par 2 ou par 3

$\Rightarrow b\mathcal{R}a$

Alors $\mathcal{R}$ est symétrique.

3) On a par exemple ($6 - 3$ est divisible par 2 ou par 3) et ($3 - 6$est divisible par 2 ou par 3) et $(3 \neq 6)$

C.à.d : $\exists a, b \in \mathbb{Z}, a\mathcal{R}b$ et $b\mathcal{R}a$ et $a \neq b$.

Alors $\mathcal{R}$ n'est pas antisymétrique.

4) On a par exemple (6-3 est divisible par 2 ou par 3) et (3-1 est divisible par 2 ou par 3) et (6-1 n'est pas divisible ni par 2, ni par 3).

C.à.d : $\exists a, b, c \in \mathbb{Z}, a\mathcal{R}b$ et $b\mathcal{R}_c$ et $\overline{a\mathcal{R}_c}$.

Alors $\mathcal{R}$ n'est pas transitive.

On conclut que $\mathcal{R}$ n'est pas une relation d'ordre et n'est pas une relation d'équivalence.

Exercice04 (6p)

1.1) Soient $x, y \in \mathbb{R}$, on a : $x + y + \frac{1}{10} \in \mathbb{R}$ c-à-d $x * y \in \mathbb{R}$.

Alors $*$ est une loi interne dans $\mathbb{R}$.

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

$x * y = x + y + \frac{1}{10} = y + x + \frac{1}{10} = y * x$

Alors $*$ est une loi commutative.

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

$$(x * y) * z = \left(x + y + \tfrac{1}{10}\right) * z = x + y + \tfrac{1}{10} + z + \tfrac{1}{10} = \left(x + \left(y + z + \tfrac{1}{10}\right) + \tfrac{1}{10}\right)$$
$$= \left(x + (y * z) + \frac{1}{10}\right) = x * (y * z)$$

Alors $*$ est associative.

1.4) Cherchons $e \in \mathbb{R}$, tel que $\forall x \in \mathbb{R} : x * e = e * x = x$.

On a : $x * e = x \Leftrightarrow x + e + \frac{1}{10} = x \Leftrightarrow e = -\frac{1}{10}$

Puisque $-\frac{1}{10} \in \mathbb{R}$ et $*$ est commutative, alors $e = -\frac{1}{10}$ est l'élément neutre de la loi $*$

1.5) Soit $x \in \mathbb{R}$, cherchons $x' \in \mathbb{R}$, tel que $x * x' = x' * x = -\frac{1}{10}$

On a : $x * x' = -\frac{1}{10} \Leftrightarrow x + x' + \frac{1}{10} = -\frac{1}{10} \Leftrightarrow x' = -x - \frac{1}{5}$

Puisque $-x - \frac{1}{5} \in \mathbb{R}$ et $*$ est commutative, alors $x' = -x - \frac{1}{5}$ est le symétrique de x par rapport à la loi $*$

Par suite $(\mathbb{R}, *)$ est un groupe abélien.

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

$g(x * y) = g\left(x + y + \frac{1}{10}\right) = 5\left(x + y + \frac{1}{10}\right) + \frac{1}{2} = 5x + 5y + \frac{1}{2} + \frac{1}{2} = \left(5x + \frac{1}{2}\right) + \left(5y + \frac{1}{2}\right) = g(x) + g(y)$.

Alors g est un homomorphisme du groupe $(\mathbb{R}, *)$ dans le groupe $(\mathbb{R}, +)$.

3) On a : $e = -\frac{1}{10} = \frac{2(0)-1}{10} \in H$.

Soient $x, y \in H$, alors $\exists n, m \in \mathbb{Z}, x = \frac{2n-1}{10}, y = \frac{2m-1}{10}$, on a :

$$x * y^{-1} = x * \left(-y - \frac{1}{5}\right) = \left(\frac{2n-1}{10}\right) * \left(-\frac{2m-1}{10} - \frac{1}{5}\right) = \left(\frac{2n-1}{10}\right) * \left(\frac{-2m-1}{10}\right) = \frac{2n-1}{10} + \frac{-2m-1}{10} + \frac{1}{10}$$
$$= \frac{2(n-m)-1}{10} \in H, \text{ car } n-m \in \mathbb{Z}.$$

Par suite $(H, *)$ est un sous groupe de $(\mathbb{R}, *)$

6.7. Examen 07

Bibliographie

[**1**] J. Franchini et J. C. Jacquens, Algèbre : cours, exercices corrigés, travaux dirigés, Ellipses, Paris, 1996.

[**2**] C. Degrave et D. Degrave, Algèbre 1ère année : cours, méthodes, exercices résolus, Bréal, 2003.

[**3**] S. Balac et F. Sturm, Algèbre et analyse : cours de mathématiques de première année avec exercices corrigés,, Presses Polytechniques et Universitaires romandes, 2003

[**4**] M. Gran, fiches de TD (L1), Université du Littoral Côte d'Opale.

[**5**] M. Serfati, Exercices de mathématiques. 1. Algèbre, Belin, Collection DIA, 1987.

[**6**] D. Duverney, S. Heumez, G. Huvent, Toutes les mathématiques – Cours, exercices corrigés – MPSI, PCSI, PTSI, TSI, Ellipses, 2004.