Algèbre 1

Cours et exercices corrigés (pour la formation préparatoire)

Bensid Yazid

ESAA-TLEMCEN

BENSID.JOOMLA.COM

Première impression, Octobre 2018

Table des matières

Préface

Ce polycopié traite du module d'algèbre générale. Il est le fruit de l'enseignement du module algèbre 1 en première année dans le cadre de la formation préparatoire à l'école supérieure en sciences appliquées de Tlemcen (ESSAT). Cet ouvrage est donc déstiné aux premieres années des classes préparatoires aux grandes écoles mais aussi aux étudiants de première année de tronc commun (MI-ST-SM). Ce mansucrit comprend 3 chapitres qui couvrent l'ensemble du programme du module algèbre 1 :

Le premier chapitre traite de notions fondamentales utiles aussi bien en algèbre qu'en analyse et probabilités telles que la logique, la théorie des ensembles ainsi que les applications.

Le second chapitre est véritablement le coeur de cet ouvrage car on y expose les structures algébriques que sont les groupes, les anneaux et les corps.

Enfin, dans le troisième et dernier chapitre on présente les notions de polynome et de fractions rationnelles, ces derniers seront particulièrement utiles en analyse notemment pour le calcul des integrales.

A la fin de chaque chapitre on retrouve une série d'exercices avec leur corrigés respectifs.

Comme tout travail le notre reste bien evidemment perfectible, nous invitons donc le lecteur à nous faire parvenir toute remarque ou suggestion pour ameliorer notre document.

1. Logique, ensembles et applications

1.1 Notions élémentaires de logique

Définition 1.1.1 — Proposition. Une proposition est une phrase mathématique à laquelle on peut attribuer une valeur de vérité (vraie ou fausse)

■ **Exemple 1.1**

1. "10 est-il pair ?" n'est pas une proposition
2. "4 est un nombre premier" est une proposition fausse
3. le théorème de Phytaghore est une proposition vraie

Définition 1.1.2 — Négation. Soit P une proposition

La négation de P notée $\overline{P}$ est la proposition qui affirme exactement le contraire de P elle est donc vraie si P est fausse et fausse si P est vraie.

Table de vérité :

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

R La table de vérité donne toutes les valeurs possibles d'une proposition. la valeur 1 représente une proposition vraie, alors qu'une proposition fausse est représentée par la valeur 0

1.1.1 Connecteurs logiques

Soit P et Q deux propositions

Définition 1.1.3 — conjonction. La conjonction de P et Q notée $P \wedge Q$ veut dire P et Q

■ **Exemple 1.2** P :10 est pair
Q :12 est impair
$P \wedge Q$: 10 est pair et 12 est impair

Table de vérité :

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

R Pour que $P \wedge Q$ soit vraie il faut que les deux propositions P et Q soient vraies.

Définition 1.1.4 — disjonction. La disjonction de P et Q notée $P \vee Q$ veut dire P ou Q

■ **Exemple 1.3** P :10 est pair
Q :12 est impair
$P \vee Q$: 10 est pair ou 12 est impair

Table de vérité :

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

R Pour que $P \vee Q$ soit vraie il suffit qu'au moins une des deux propositions P et Q soit vraie

Définition 1.1.5 — implication. P implique Q notée $P \Rightarrow Q$ veut dire Si P alors Q
P est souvent dite "condition" ou "hypothèse" et Q est dite résultat.
$Q \Rightarrow P$ est dite réciproque

■ **Exemple 1.4** Soit $x \in \mathbb{R}$
$P : x = 2$
$Q : x^2 = 4$
$P \Rightarrow Q$: si $x = 2$ alors $x^2 = 4$

R Attention, la réciproque n'est pas toujours vraie, par exemple $Q \Rightarrow P$: si $x^2 = 4$ alors $x = 2$ est fausse

Si P est vérifiée, alors Q est automatiquement vérifiée, mais si P n'est pas vérifiée, on ne peut rien dire sur Q

Table de vérité :

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

Définition 1.1.6 — équivalence. On dit que P est équivalente à Q et on note $P \Leftrightarrow Q$ si :
$(P \Rightarrow Q)$ et $(Q \Rightarrow P)$

■ **Exemple 1.5** $P : n$ pair
$Q : (n+2)$ pair
$P \Leftrightarrow Q$: n pair est équivalente à $(n+2)$ pair

Table de vérité :

P	1	1	0	0
Q	1	0	0	1
$P \Rightarrow Q$	1	0	1	1
$Q \Rightarrow P$	1	1	1	0
$P \Leftrightarrow Q$	1	0	1	0

R Pour que $P \Leftrightarrow Q$ soit vraie il faut que les deux propositions P et Q sont toutes les deux vraies ou toutes les deux fausses simultanément.

1.1.2 Propriétés des connecteurs logiques

Réflexivité

$$P \Leftrightarrow P$$

Négation

$$\overline{P \Rightarrow Q} \Leftrightarrow [P \wedge \overline{Q}]$$

Contraposée

$$[P \Rightarrow Q] \Leftrightarrow [\overline{Q} \Rightarrow \overline{P}]$$

Double négation

$$\overline{\overline{P}} \Leftrightarrow P$$

Transitivité

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

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

Idempotence

$$P \wedge P \Leftrightarrow P$$

$$P \vee P \Leftrightarrow P$$

Commutativité

$$P \wedge Q \Leftrightarrow Q \wedge P$$

$$P \vee Q \Leftrightarrow Q \vee P$$

Associativité

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

$$P \vee (Q \vee R) \Leftrightarrow (P \vee Q) \vee R$$

Distributivité

$$P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$$
$$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$$

Lois de Morgan

$$\overline{P \wedge Q} \Leftrightarrow \overline{P} \vee \overline{Q}$$
$$\overline{P \vee Q} \Leftrightarrow \overline{P} \wedge \overline{Q}$$

1.1.3 Quantificateurs logiques

Définition 1.1.7 — Quantificateur universel. $\forall x\, P(x)$ veut dire pour tout objet x P est vraie.

Définition 1.1.8 — Quantificateur existentiel. $\exists x\, P(x)$ veut dire il existe au moins un objet x tel que P est vraie.

R $\exists! x\, P(x)$ veut dire il existe un unique objet x tel que P est vraie.

■ **Exemple 1.6**

$$\forall n \in \mathbb{N} \quad n \geq 0$$
$$\exists n \in \mathbb{Z} \quad n \geq -2$$
$$\exists! n \in \mathbb{N}^* \quad n \leq 1$$

R L'ordre des quantificateurs est important, par exemple les deux propositions suivantes n'ont pas le même sens :

$$(1) \quad \forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\ x < y \qquad\qquad (2) \quad \exists y \in \mathbb{R},\ \forall x \in \mathbb{R},\ x < y$$

Théorème 1.1.1 — Négation des quantificateurs. Soit P une proposition, alors :
1. $\overline{[\forall x\, P(x)]} \Leftrightarrow \exists x\, \overline{P(x)}$
2. $\overline{[\exists x\, P(x)]} \Leftrightarrow \forall x\, \overline{P(x)}$

■ **Exemple 1.7** $P : \forall x \in \mathbb{R}, \quad x > x^2 \Rightarrow x > 0$

$$\exists x \in \mathbb{R}, \quad x > x^2 \text{ et } x \leq 0 \qquad \text{négation}$$
$$\forall x \in \mathbb{R}, \quad x \leq 0 \Rightarrow x \leq x^2 \qquad \text{Contraposée}$$

1.2 Types de raisonnement mathématique

1.2.1 raisonnement par contraposée

Pour montrer $P \Rightarrow Q$ il suffit de montrer $\overline{Q} \Rightarrow \overline{P}$

■ **Exemple 1.8** Montrons par contraposée que :

$$\forall n \in \mathbb{Z} \quad [n^2 - 6n + 5]\,\text{pair} \Rightarrow n\ \text{impair}$$

il est plus simple de montrer que :

$$\forall n \in \mathbb{Z} \quad n\ \text{pair} \Rightarrow [n^2 - 6n + 5]\,\text{impair}$$

Soit $n \in \mathbb{Z}$

$$\begin{aligned} n\,\text{pair} \quad &\Rightarrow \quad n = 2k\ \text{avec}\ k \in \mathbb{Z} \\ &\Rightarrow \quad n^2 - 6n + 5 = (2k)^2 - 6(2k) + 5 \\ &= \quad 4k^2 - 12k + 5 = 2(2k^2 - 6k + 2) + 1 \\ &= \quad 2k' + 1 \end{aligned}$$

On en conclut que $n^2 - 6n + 5$ est impair

1.2.2 raisonnement par l'absurde

Pour montrer qu'une proposition P est vraie on suppose que sa négation $\overline{P}$ est vraie et on aboutit à une contradiction logique.

■ **Exemple 1.9** Montrons par l'absurde que $\sqrt{2}$ est irrationnel
On suppose que :

$$\sqrt{2} \in \mathbb{Q} \Rightarrow \sqrt{2} = \frac{a}{b}\ \text{avec}\ a \wedge b = 1 \Rightarrow 2 = \frac{a^2}{b^2} \Rightarrow a^2 = 2b^2$$

$$\text{D'après lemme d'Euclide}\ 2|a^2 \Rightarrow 2|a$$

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

$$2|b^2 \Rightarrow 2|b \Rightarrow 2|(a \wedge b) \Rightarrow 2|1\ \text{(contradiction logique)}$$

R Pour montrer que $P \Rightarrow Q$ on suppose que $\overline{Q}$ est vraie et on aboutit à une contradiction logique ou avec l'hypothèse P

■ **Exemple 1.10** Montrons par l'absurde que :

$$\left(\forall n \in \mathbb{N}\,\text{premier}, \sqrt{n}\ \text{irrationnel}\right) \Rightarrow \left(\sqrt{2} + \sqrt{5}\right)\ \text{irrationnel}$$

On suppose que $\left(\sqrt{2} + \sqrt{5}\right) \in \mathbb{Q} \Rightarrow \sqrt{2} + \sqrt{5} = \frac{a}{b}$ avec $a \wedge b = 1 \Rightarrow \sqrt{5} = \frac{a}{b} - \sqrt{2}$

$\Rightarrow 5 = \left(\frac{a}{b} - \sqrt{2}\right)^2 = \frac{a^2}{b^2} + 2 - 2\frac{a\sqrt{2}}{b} \Rightarrow \sqrt{2} = \left(3 - \frac{a^2}{b^2}\right) \times \frac{b}{-2a} = \frac{3b^2 - a^2}{-2ba} \Rightarrow \sqrt{2} \in \mathbb{Q}$

Ce qui contredit notre hypothèse

1.2.3 raisonnement par récurrence

Le principe du raisonnement par récurrence est comme suit :
On veut montrer que $\forall n \geq n_0 \quad P(n)$ est vrai (avec $n_0 \in \mathbb{N}$)

1. On montre que $P(n)$ est vrai pour $n = n_0$
2. On suppose que $P(n)$ est vrai pour un certain $n \geq n_0$ (hypothèse de récurrence)
3. On montre que $P(n+1)$ est vrai

■ **Exemple 1.11** Montrons par récurrence que :

$$\forall n \geq 1 \quad 1+2+3+\cdots+n = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

1. On montre que $P(n)$ est vraie pour $n = 1$
$$e\frac{1(1+1)}{2} = 1$$
2. On suppose que $P(n)$ est vraie pour un certain $n \geq 1$ (hypothèse de récurrence) cad
$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \qquad \text{pour}\, n\, \text{fixé}$$
3. On montre que $P(n+1)$ est vraie cad
$$\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}$$

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

1.2.4 raisonnement par contre exemple

On sait que $\overline{[\forall x\, P(x)]} \Leftrightarrow \exists x\, \overline{P(x)}$
Pour montrer que $\forall x\, P(x)$ est fausse on doit trouver x_0 qui ne vérifie pas $P(x_0)$.

■ **Exemple 1.12** Toute fonction $f : \mathbb{R} \to \mathbb{R}$ est soit paire soit impaire
Pour montrer que cette proposition est fausse on doit chercher un contre exemple
$f(x) = e^x$ n'est ni paire ni impaire

Définition 1.2.1 — Théorème, lemme, corollaire, axiome. Un théorème est un résultat mathématique important qui a été démontré. Un lemme est un résultat de moindre importance qu'un théorème. Un corollaire est la conséquence immédiate d'un théorème. Une conjecture est un résultat qui n'as pas encore été démontré. Un axiome est un résultat non démontré mais qui est supposé vrai.

1.3 Généralités sur les ensembles

Soit x un élément de E
On note $x \in E$ et on dit que x appartient à E
si x n'est pas un élément de E on note $x \notin E$ et on dit que x n'appartient pas à E
Un ensemble peut être défini de 2 manières : Soit en donnant la liste de ses éléments par ex :
$A = \{0,1,2,3\}$ soit en précisant les propriétés vérifiées par ses éléments par ex : $A = \{n \in \mathbb{N}\, n \leq 3\}$

Définition 1.3.1 Le cardinal d'un ensemble E noté $\mathrm{card}(E)$ est le nombre d'éléments de cet ensemble.
si $\mathrm{card}(E) < \infty$ alors l'ensemble E est dit fini, sinon on dit que E est infini. L'ensemble vide ne contient aucun élément, il est noté $\varnothing$

■ **Exemple 1.13** $\mathrm{card}(A) = 4 \quad \mathrm{card}(\varnothing) = 0 \quad \mathrm{card}(\mathbb{N}) = \infty$

1.3.1 Sous-ensemble et ensemble de parties

Définition 1.3.2 — Inclusion. Soient A et E deux ensembles.

1. On dit que A est inclus dans E et on note $A \subset E$ si et seulement si tout élément de A est aussi un élément de E i.e :
$$x \in A \Rightarrow x \in E$$
On dit aussi que A est un sous ensemble ou une partie de E
2. On dit que A et E sont égaux et on note $A = E$ si et seulement si $A \subset E$ et $E \subset A$

■ **Exemple 1.14** $E = \{0,1\} \quad A = \{1\} \Rightarrow A \subset E$

Définition 1.3.3 L'ensemble des parties de E noté $P(E)$ est l'ensemble dont les éléments sont tous les sous ensembles de E càd $P(E) = \{X \text{ tel que} X \subset E\}$

■ **Exemple 1.15** $E = \{0,1\} \Rightarrow \mathbb{P}(E) = \{\varnothing, \{0\}, \{1\}, \{0,1\}\}$

1.3.2 Opérations sur les ensembles

Soient A et B deux sous ensembles d'un ensemble E

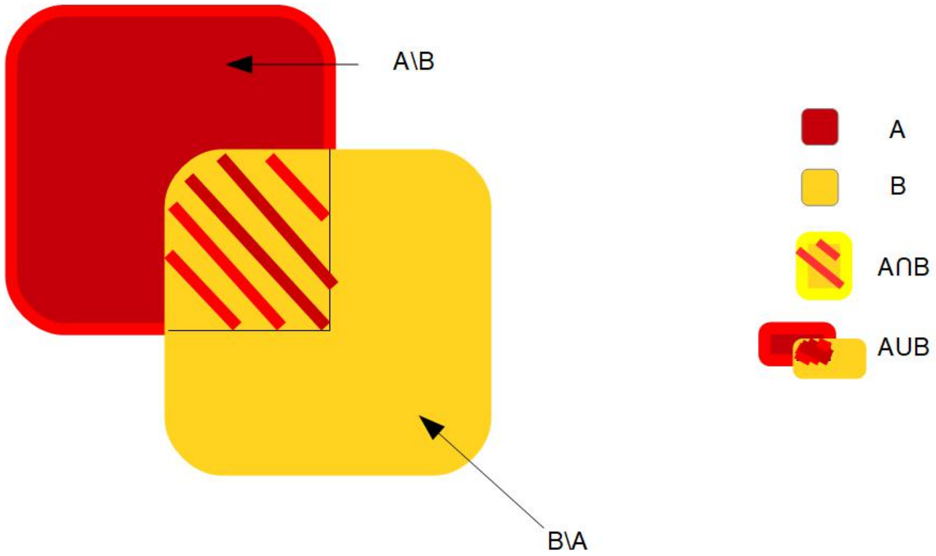
Définition 1.3.4 — Réunion. On appelle union des deux ensembles A et B et on note $A \cup B$ l'ensemble défini par :
$$A \cup B = \{x \in E / x \in A \text{ ou} x \in B\}$$

Définition 1.3.5 — intersection. On appelle intersection des deux ensembles A et B et on note $A \cap B$ l'ensemble défini par :
$$A \cap B = \{x \in E / x \in A \text{ et} x \in B\}$$
Si $A \cap B = \varnothing$ alors A et B sont dits disjoints

Définition 1.3.6 — différence. On appelle différence des deux ensembles A et B et on note $A \setminus B$ l'ensemble défini par :
$$A \setminus B = \{x \in E / x \in A \text{ et} x \notin B\}$$

Définition 1.3.7 — complémentaire. On appelle complémentaire de A noté C_E^A l'ensemble défini par :
$$C_E^A = \{x \in E / x \notin A\} = E \setminus A$$
C_E^A est souvent noté $\overline{A}$

Théorème 1.3.1 Soit E un ensemble et soient $A,\ B \in P(E)$
$$\overline{A} = B \Leftrightarrow (A \cap B = \emptyset) \wedge (A \cup B = E)$$
On dit que A et B sont complémentaires dans E



1.3.3 Propriétés des opérations sur les ensembles :

Commutativité

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

Associativité

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

Distributivité

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

Transitivité

$$(A \subset B) \wedge (B \subset C) \Rightarrow A \subset C$$

Idempotence :

$$\overline{\overline{A}} = A$$

Inclusion et complémentaire :

$$A \subset B \Rightarrow \overline{B} \subset \overline{A}$$

Lois de Morgan :

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

Définition 1.3.8 — Produit cartésien. Soient $E_1, E_2, \cdots, E_n$ des ensembles non vides.
Le produit cartésien des ensembles $E_1, E_2, \cdots, E_n$ noté $E_1 \times E_2 \times \cdots \times E_n$ est définie par l'ensemble :

$$E_1 \times E_2 \times \cdots \times E_n = \{(x_1, x_2, \cdots, x_n) \text{ avec} x_1 \in E_1,\ x_2 \in E_2,\ \cdots, x_n \in E_n$$

Les éléments du produit cartésien son appelés “n-uplets”, si $n = 2$ on les appelle “couple”

■ **Exemple 1.16**
1. $\mathbb{R}^2 = \{(x,y) \text{ tels que} x, y \in \mathbb{R}\} \quad (0,1) \in \mathbb{R}^2$
2. $D = J \times M \times A$ avec $J = \{1, 2, \cdots, 31\}$ $M = \{1, 2, \cdots, 12\}$ $A = \{1, 2, \cdots, 2019\}$
   $(5, 7, 1962) \in D$

R Attention, $E_1 \times E_2 \not\subset E_1 \times E_2 \times E_3$

Proposition 1.3.2 $Card(A \times B) = Card(A) \times Card(B)$

1.4 Applications

Définition 1.4.1 Une application f d'un ensemble E vers un ensemble F notée $f : E \to F$ est une relation qui à chaque élément x de E associe un et un seul élément y de F
On note

$$f : \begin{array}{l} E \to F \\ x \mapsto y = f(x) \end{array}$$

y est dite image de x et x est dit antécédent de y
On appelle E ensemble de départ et F ensemble d'arrivée.
L'ensemble $\Gamma = \{(x,y) \in E \times F / y = f(x)\}$ est appelé graphe de f
L'image de f notée Imf est définie par $Imf = \{y \in F / y = f(x)\}$

■ **Exemple 1.17** $f : \begin{array}{ccc} \mathbb{R}^+ & \to & \mathbb{R} \\ x & \mapsto & \sqrt{x} \end{array}$ est une application

$g : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \sqrt{x} \end{array}$ n'est pas une application

$Id_E : \begin{array}{ccc} E & \to & E \\ x & \mapsto & x \end{array}$ est appelée application identité

Définition 1.4.2 Soient $A \subset E$ et $f : \begin{array}{ccc} E & \to & F \\ x & \mapsto & f(x) \end{array}$ une application

L'application g définie par $g : \begin{array}{ccc} A & \to & F \\ x & \mapsto & f(x) \end{array}$ est dite restriction de f à une partie A de E

Elle est souvent notée par $f|_A$
f est alors dite prolongement de g sur l'ensemble E

■ **Exemple 1.18** $f : \begin{array}{ccc} \mathbb{R}^+ & \to & \mathbb{R} \\ x & \mapsto & \sqrt{x} \end{array}$ $\quad f|_{[0,1]} : \begin{array}{ccc} [0,1] & \to & \mathbb{R} \\ x & \mapsto & \sqrt{x} \end{array}$

Définition 1.4.3 — Composition d'applications. Soient $f : E \to F$ et $g : F \to G$ deux applications.
L'application composée de f et g notée $g \circ f$ est définie par : $g \circ f : \begin{array}{ccc} E & \to & G \\ x & \mapsto & g(f(x)) \end{array}$

R Attention, en général $g \circ f \neq f \circ g$

■ **Exemple 1.19** $f : \begin{array}{ccc} [1,+\infty) & \to & (0,1] \\ x & \mapsto & \dfrac{1}{x} \end{array}$ $\quad g : \begin{array}{ccc} (0,1] & \to & \mathbb{R}^+ \\ x & \mapsto & \sqrt{x} \end{array}$

$$g \circ f : \begin{array}{ccc} [1,+\infty) & \to & \mathbb{R}^+ \\ x & \mapsto & g(f(x)) = g\left(\dfrac{1}{x}\right) = \sqrt{\dfrac{1}{x}} \end{array}$$

1.4.1 Injectivité, Surjectivité, Bijectivité et application réciproque

Définition 1.4.4 — Injectivité. Une application $f : E \to F$ est dite injective si tout élément de F a au plus un antécédent dans E c.à.d $\forall x_1, x_2 \in E,\ x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

R En général, pour monter qu'une application est injective, on utlise plutot la contraposée : $\forall x_1, x_2 \in E,\ f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

■ **Exemple 1.20** $f : \begin{array}{ccc} \mathbb{R}_+ & \to & \mathbb{R}_+ \\ x & \mapsto & \sqrt{x} \end{array}$ est injective $\quad g : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^2 \end{array}$ n'est pas injective

Soient $x_1, x_2 \in \mathbb{R}_+$ tels que : $f(x_1) = f(x_2) \Rightarrow \sqrt{x_1} = \sqrt{x_2} \Rightarrow x_1 = x_2 \Rightarrow f$ est injective
Soient $x_1, x_2 \in \mathbb{R}$ tels que : $g(x_1) = g(x_2) \Rightarrow x_1^2 = x_2^2 \Rightarrow x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2) = 0$
$\Rightarrow (x_1 = x_2)$ ou $(x_1 = -x_2)$
Contre-exemple : $g(1) = g(-1) = 1 \Rightarrow g$ n'est pas injective

Définition 1.4.5 — Surjectivité. Une application $f : E \to F$ est dite surjective si tout élément de F a au moins un antécédent dans E c.à.d $\forall y \in F,\ \exists x \in \mathbb{E} / y = f(x)$

R Pour monter qu'une application est surjective, plutot que d'utiliser la définition il est preferable de s'aider du théorème suivant :

Théorème 1.4.1 f surjective $\Leftrightarrow Imf = F$

■ **Exemple 1.21** $f : \begin{array}{ccc} \mathbb{R}_+ & \to & \mathbb{R}_+ \\ x & \mapsto & \sqrt{x} \end{array}$ est surjective $\quad g : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^2 \end{array}$ n'est pas surjective

$0 \leq x < +\infty \Rightarrow 0 \leq \sqrt{x} < +\infty \Rightarrow 0 \leq f(x) < +\infty \Rightarrow Imf = F = \mathbb{R}_+$
Donc f est surjective.
$x \in \mathbb{R} \Rightarrow x^2 \geq 0 \Rightarrow g(x) \geq 0 \Rightarrow Img = \mathbb{R}_+ \neq F = \mathbb{R}$
Donc, g n'est pas surjective

Définition 1.4.6 — Bijectivité. Une application $f : E \to F$ injective et surjective est dite bijective :

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

■ **Exemple 1.22** $f:\begin{array}{ccc}\mathbb{R}_+ & \to & \mathbb{R}_+\\ x & \mapsto & \sqrt{x}\end{array}$ est bijective $\quad g:\begin{array}{ccc}\mathbb{R} & \to & \mathbb{R}\\ x & \mapsto & x^2\end{array}$ n'est pas bijective

Théorème 1.4.2 Soit $f:E\to F$ une application.

$$f \text{ bijective} \Leftrightarrow \exists ! g: F\to E \text{ telle que } f\circ g = Id_F \text{ et } g\circ f = Id_E$$

g est dite réciproque de f, elle est notée f^{-1}

■ **Exemple 1.23** $f:\begin{array}{ccc}\mathbb{R}_+ & \to & \mathbb{R}_+\\ x & \mapsto & \sqrt{x}\end{array}$ $\quad f^{-1}:\begin{array}{ccc}\mathbb{R}_+ & \to & \mathbb{R}_+\\ y & \mapsto & y^2\end{array}$

$y=\sqrt{x}\Rightarrow x=y^2$

1.4.2 Résultats fondamentaux

Théorème 1.4.3
1. La composée de deux applications injectives est injective.
2. La composée de deux applications surjectives est surjective.
3. La composée de deux applications bijectives est bijective.Sa réciproque est donnée par :

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

preuve
1. Soient $x_1,x_2\in E,\ (g\circ f)(x_1)=(g\circ f)(x_2)\Rightarrow g(f(x_1))=g(f(x_2))$
   $\Rightarrow f(x_1)=f(x_2)$ (car : g est injective)
   $\Rightarrow x_1=x_2$ (car : f est injective)
2.
$$\begin{aligned} g \text{ surjective} &\Rightarrow \forall z\in G,\exists y\in F, z=g(y)\\ &\Rightarrow \forall z\in G,\exists x\in E, z=g(f(x)) \text{ (car : } f \text{ est surjective)}\\ &\Rightarrow \forall z\in G,\exists x\in E, z=(g\circ f)(x)\\ &\Rightarrow g\circ f \text{ est surjective}\end{aligned}$$
3. $(g\circ f)\circ(g\circ f)^{-1}=Id_G\Rightarrow g^{-1}\circ(g\circ f)\circ(g\circ f)^{-1}=g^{-1}\circ Id_G\Rightarrow f\circ(g\circ f)^{-1}=g^{-1}$
   $\Rightarrow f^{-1}\circ f\circ(g\circ f)^{-1}=f^{-1}\circ g^{-1}\Rightarrow(g\circ f)^{-1}=f^{-1}\circ g^{-1}$

Théorème 1.4.4 Soient $f:E\to F$ et $g:F\to G$ deux applications
1. $(g\circ f)$ injective $\Rightarrow f$ injective
2. $(g\circ f)$ surjective $\Rightarrow g$ surjective

preuve
1. Soient $x_1,x_2\in E,\ f(x_1)=f(x_2)\Rightarrow g(f(x_1))=g(f(x_2))\Rightarrow(g\circ f)(x_1)=(g\circ f)(x_2)$
   $\Rightarrow x_1=x_2$ (car $g\circ f$ est injective)
2. $(g\circ f)$ surjective $\Rightarrow\forall z\in G,\exists x\in E,z=(g\circ f)(x)\Rightarrow\forall z\in G,\exists x\in E,z=g(f(x))$
   On pose $y=f(x)\Rightarrow y\in F\Rightarrow\forall z\in G,\exists y\in F,z=g(y)$
   Donc g est surjective

■ **Exemple 1.24** $f:\begin{array}{ccc}[-1,+\infty[& \to & \mathbb{R}\\ x & \mapsto & \sqrt{x+1}\end{array}$ est injective $\quad g:\begin{array}{ccc}\mathbb{R} & \to & \mathbb{R}\\ x & \mapsto & x^2\end{array}$ n'est pas injective

$g\circ f:\begin{array}{ccc}[-1,+\infty[& \to & \mathbb{R}\\ x & \mapsto & x+1\end{array}$ est injective

■ **Exemple 1.25** $f:\begin{array}{ccc}[-1,+\infty[& \to & \mathbb{R}\\ x & \mapsto & \sqrt{x+1}\end{array}$ n'est pas surjective $\quad g:\begin{array}{ccc}\mathbb{R} & \to & \mathbb{R}_+\\ x & \mapsto & x^2\end{array}$ est surjective

$$g\circ f:\begin{array}{ccc}[-1,+\infty[& \to & \mathbb{R}_+\\ x & \mapsto & x+1\end{array}\quad \text{est surjective}$$

1.4.3 Image directe et image réciproque

Définition 1.4.7 Soient $f:E\to F$ une application et soient $A\subset E$ et $B\subset F$

1. L'image directe d'une partie A de E notée $f(A)$ est définie par :

$$f(A)=\{y\in F/y=f(a)\quad a\in A\}$$

2. L'image réciproque d'une partie B de F notée $f^{-1}(B)$ est définie par :

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

R $f(A)\subset F$ et $f^{-1}(B)\subset E$
$f^{-1}(F)=E$
$f(E)=Im(f)$

■ **Exemple 1.26** $f:\begin{array}{ccc}\mathbb{R} & \to & \mathbb{R}\\ x & \mapsto & x^2+1\end{array}$

On pose $A=[-3,3]$ et $B=[1,2]$ calculons $f(A)$ et $f^{-1}(B)$
$-3\leq x\leq 3\Rightarrow 0\leq x^2\leq 3^2\Rightarrow 0+1\leq x^2+1\leq 3^2+1\Rightarrow 1\leq f(x)\leq 10\Rightarrow f(A)=[1,10]$

$1\leq f(x)\leq 2\Rightarrow 1\leq x^2+1\leq 2\Rightarrow 0\leq x^2\leq 1\Rightarrow 0\leq |x|\leq 1\Rightarrow -1\leq x\leq 1\Rightarrow f^{-1}(B)=[-1,1]$

Théorème 1.4.5 1. $f(E)=F\Leftrightarrow f$ est surjective
2. $\forall A\in P(E),\ f(A)\cap f(\overline{A})=\emptyset\Leftrightarrow f$ injective

preuve

1. $f(E)=F\Leftrightarrow f$ est surjective
   $\Rightarrow$:
   $y\in F\Rightarrow y\in f(E)\Rightarrow y=f(x)$ avec : $x\in E\Rightarrow f$ est surjective
   $\Leftarrow$:
   $\subset$:
   $f(E)\subset F$ (par définition)
   $\supset$:
   $y\in F\Rightarrow \exists x\in E, y=f(x)$ (car f est surjective)
   $\Rightarrow y\in f(E)\Rightarrow F\subset f(E)$
2. $\forall A\in P(E),\ f(A)\cap f(\overline{A})=\emptyset\Leftrightarrow f$ injective
   $\Rightarrow$:
   Soient $x_1,x_2\in E, x_1\neq x_2$
   On pose $A=\{x_1\}\Rightarrow f(x_1)\in f(A)$
   $x_1\neq x_2\Rightarrow x_2\in\overline{A}\Rightarrow f(x_2)\in f(\overline{A})$
   $f(A)\cap f(\overline{A})=\emptyset\Rightarrow f(x_1)\neq f(x_2)$
   Donc f est injective
   $\Leftarrow$:Montrons par l'absurde que : $f(A)\cap f(\overline{A})=\emptyset$
   $f(A)\cap f(\overline{A})\neq\emptyset\Rightarrow \exists y\in f(A)\cap f(\overline{A})\Rightarrow y\in f(A)$ et $y\in f(\overline{A})$
   $\Rightarrow [y=f(a)\ \ ,a\in A]$ et $[y=f(x)\ \ ,x\in\overline{A}]$
   $\Rightarrow f(a)=f(x)\Rightarrow a=x$ (car f est injective) $\Rightarrow a\in\overline{A}$
   contradiction avec $a\in A$
   Donc $f(A)\cap f(\overline{A})=\emptyset$

1.5 Série d'exercices

Exercice 1 Établir les équivalences suivantes en utilisant les tables de vérité :

$$\neg(P \wedge Q) \Leftrightarrow (\neg P) \vee (\neg Q)$$
$$\neg(P \vee Q) \Leftrightarrow (\neg P) \wedge (\neg Q)$$
$$\neg(P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q)$$
$$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$$

■

Exercice 2
1. Les propositions suivantes sont elles vraies ?
   (a) $\exists x \in \mathbb{R},\ \forall y \in \mathbb{R},\ x+y>0$
   (b) $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\ x+y>0$
   (c) $\exists x \in \mathbb{R},\ \forall y \in \mathbb{R},\ y^2>x$
2. Donner leur négation

■

Exercice 3 Soit $n \in \mathbb{N}$, montrer par contraposée que :

$$2^n - 1 \text{ premier} \Rightarrow n \text{ premier}$$

■

Exercice 4 Soit $x \in \mathbb{R}$ tq $\forall \varepsilon > 0, x \leq \varepsilon$ Montrer par l'absurde que : $x \leq 0$ ■

Exercice 5
1. Montrer que la proposition suivante est vraie :

$$\forall q > 0,\ \exists N \in \mathbb{N} \text{ tel que } n \geq N \Rightarrow 2-q < \frac{2n+1}{n+2} < 2+q$$

2. Donner sa négation puis sa contraposée

■

Exercice 6 On définit pour tout entier $n \in \mathbb{N}$, $\quad A_n = 3^{2n+2} - 2^{n+1}$
1. Calculer $A_{n+1} - 2A_n$
2. Montrer par récurrence que $\forall n \in \mathbb{N} \quad A_n$ est divisible par 7

■

Exercice 7 Soit $E = \{a, b\}$
1. Donner l'ensemble $\mathbb{P}(E)$
2. A quel ensemble appartiennent (a,b) , $\{a\},(a,\{b\}),(\{a\},\{b\}),\{\{a\},\{b\}\},(a,E)$

■

Exercice 8 Soit E un ensemble et soient $A, B \in \mathbb{P}(E)$
résoudre dans $\mathbb{P}(E)$ les équations suivantes :

1. $X \cap A = B$
2. $X \setminus A = B$

Exercice 9 Soit E un ensemble et soient $A, B, C \in \mathbb{P}(E)$
On définit la différence symétrique des ensembles A et B par :

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

1. Montrer que $A \Delta B = (A \setminus B) \cup (B \setminus A)$
2. Calculer $A \Delta A, \quad A \Delta \overline{A}, \quad A \Delta E, \quad A \Delta \emptyset$
3. En supposant que $A \Delta B = A \Delta C$ démontrer que $B = C$

Exercice 10 On définit l'application caractéristique

$$\begin{array}{rccl} \varphi_A : & E & \to & \{0,1\} \\ & x & \mapsto & \varphi_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases} \end{array}$$

1. Montrer que $\varphi_A = \varphi_B \Leftrightarrow A = B$
2. Vérifier les propriétés suivantes :
   (a) $\varphi_{\overline{A}} = 1 - \varphi_A$
   (b) $\varphi_{A \cap B} = \varphi_A \varphi_B$
   (c) $\varphi_{A \cup B} = \varphi_A + \varphi_B - \varphi_A \varphi_B$
3. En déduire que $(A \cup B = A \cup C) \wedge (A \cap B = A \cap C) \Rightarrow (B = C)$

Exercice 11 1. Sachant que $E = F = \mathbb{R}$, les fonctions suivantes sont elles des applications ?

$$f : \begin{array}{ccc} E & \to & F \\ x & \mapsto & x^2 + 1 \end{array} \qquad g : \begin{array}{ccc} E & \to & F \\ x & \mapsto & exp\,(x+2) \end{array} \qquad h : \begin{array}{ccc} E & \to & F \\ x & \mapsto & \sqrt{1 - x^2} \end{array}$$

2. sont-elles injectives, surjectives, bijectives ?
3. Déterminer dans chaque càs E et F les plus grands possibles pour que f, g et h soient bijectives, puis donner leur réciproque

Exercice 12 Établir les propriétés suivantes :

1. f injective $\Leftrightarrow \forall A \in P(E),\ f^{-1}(f(A)) = A$
2. f surjective $\Leftrightarrow \forall B \in P(F),\ f(f^{-1}(B)) = B$

1.6 corrigé de la série d'exercices

Exercice 1 A l'aide de la table de vérité, montrer les propriétés suivantes :

$$\neg(P \wedge Q) \Leftrightarrow (\neg P) \vee (\neg Q)$$
$$\neg(P \vee Q) \Leftrightarrow (\neg P) \wedge (\neg Q)$$
$$\neg(P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q)$$
$$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$$

P	1	1	0	0
Q	1	0	0	1
$\neg P$	0	0	1	1
$\neg Q$	0	1	1	0
$P \wedge Q$	1	0	0	0
$P \vee Q$	1	1	0	1
$\neg(P \wedge Q)$	0	1	1	1
$(\neg P) \vee (\neg Q)$	0	1	1	1
$\neg(P \vee Q)$	0	0	1	0
$(\neg P) \wedge (\neg Q)$	0	0	1	0
$P \Rightarrow Q$	1	0	1	1
$\neg Q \Rightarrow \neg P$	1	0	1	1
$\neg(P \Rightarrow Q)$	0	1	0	0
$P \wedge \neg Q$	0	1	0	0

■

Exercice 2

1. Les propositions suivantes sont elles vraies ?
   (a) $\exists x \in \mathbb{R}\ \forall y \in \mathbb{R};\ x+y>0$ est fausse car on peut trouver un contre exemple :
   $$y=-x-1 \Rightarrow x+y=x+(-x-1)=-1<0$$
   (b) $\forall x \in \mathbb{R}\ \exists y \in \mathbb{R};\ x+y>0$ est vraie car :
   $$\forall x \in \mathbb{R}\ \exists y=(-x+2) \in \mathbb{R};\ x+y=x+(-x+2)=2>0$$
   (c) $\exists x \in \mathbb{R}\ \forall y \in \mathbb{R};\ y^2>x$ est vraie car :
   $$\exists x=-1 \in \mathbb{R}\ \forall y \in \mathbb{R};\ y^2>x$$
2. Donner leur négation

$(\neg a)$ $\quad \forall x \in \mathbb{R}\ \exists y \in \mathbb{R};\ x+y \leq 0$

$(\neg b)$ $\quad \exists x \in \mathbb{R}\ \forall y \in \mathbb{R};\ x+y \leq 0$

$(\neg c)$ $\quad \forall x \in \mathbb{R}\ \exists y \in \mathbb{R};\ y^2 \leq x$

■

Exercice 3 Soit $n \in \mathbb{N}$, montrer par contraposée que : $2^n - 1$ premier $\Rightarrow n$ premier

Contraposée : n n'est pas premier $\Rightarrow 2^n - 1$ n'est pas premier
n n'est pas premier $\Rightarrow n = pq$ avec $p \neq 1$ et $p \neq n \Rightarrow 2^n - 1 = 2^{pq} - 1 = (2^p)^q - 1$
On pose $P(X) = X^q - 1$
$P(1) = 0 \Rightarrow P(X) = (X-1)S(X) \Rightarrow P(2^p) = (2^p)^q - 1 = (2^p - 1)S(2^p)$
$\Rightarrow (2^p - 1)$ divise $(2^n - 1)$
$p \neq 1$ et $p \neq n \Rightarrow 2^p - 1 \neq 1$ et $2^p - 1 \neq 2^n - 1$
Donc $2^n - 1$ n'est pas premier ■

Exercice 4 Soit $x \in \mathbb{R}$ tq $\forall \varepsilon > 0, x \leq \varepsilon$ Montrer par l'absurde que : $x \leq 0$
Supposons que $x > 0 \Rightarrow \exists \varepsilon = \dfrac{x}{2} > 0$ On remarque que : $x > \varepsilon$ ce qui contredit notre hypothèse.
Donc $x \leq 0$

■

Exercice 5

1. Montrer que la proposition suivante est vraie :

$$(P) \quad \forall \varepsilon > 0 \; \exists N \in \mathbb{N} \text{ tel que } n \geq N \Rightarrow 2 - \varepsilon < \frac{2n+1}{n+2} < 2 + \varepsilon$$

$$\frac{2n+1}{n+2} < 2 + \varepsilon \text{ est toujours vraie car :}$$

$$\frac{2n+1}{n+2} = \frac{2n+4-3}{n+2} = \frac{2(n+2)-3}{n+2} = 2 - \frac{3}{n+2} < 2 < 2 + \varepsilon$$

$$2 - \varepsilon < \frac{2n+1}{n+2} \Leftrightarrow (2-\varepsilon)(n+2) < 2n+1 \Leftrightarrow 2n+4-\varepsilon n - 2\varepsilon < 2n+1 \Leftrightarrow 3 - 2\varepsilon < \varepsilon n$$

$$\Leftrightarrow \frac{3-2\varepsilon}{\varepsilon} < n$$

Il suffit de choisir $N > \dfrac{3}{\varepsilon} - 2$ par exemple $N = E\left(\dfrac{3}{\varepsilon}\right)$

2. Donner sa négation puis sa contraposée
Négation :

$$(\neg P) \quad \exists \varepsilon > 0 \; \forall N \in \mathbb{N} \text{ tel que } (n \geq N) \wedge \left[\left(2 - \varepsilon \geq \frac{2n+1}{n+2}\right) \vee \left(\frac{2n+1}{n+2} \geq 2 + \varepsilon\right)\right]$$

Contraposée : $\forall \varepsilon > 0 \; \exists N \in \mathbb{N}$ tel que $\left[\left(2 - \varepsilon \geq \dfrac{2n+1}{n+2}\right) \vee \left(\dfrac{2n+1}{n+2} \geq 2 + \varepsilon\right)\right] \Rightarrow n < N$

■

Exercice 6 On définit pour tout entier $n \in \mathbb{N}$ $\quad A_n = 3^{2n+2} - 2^{n+1}$

1. Calculer $A_{n+1} - 2A_n$

$$\begin{aligned} A_{n+1} - 2A_n &= 3^{2(n+1)+2} - 2^{(n+1)+1} - 2(3^{2n+2} - 2^{n+1}) \\ &= 3^{2n+4} - 2^{n+2} - 2(3^{2n+2}) + 2^{n+2} \\ &= 3^2(3^{2n+2}) - 2(3^{2n+2}) \\ &= 7\left(3^{2n+2}\right) \end{aligned}$$

2. Montrer par récurrence que $\forall n \in \mathbb{N} \quad A_n$ est divisible par 7

Pour $n = 0$ on a $A_0 = 7$
Hypothèse de récurrence : Soit $n \in \mathbb{N}$
On suppose que A_n est divisible par 7 et on montre que A_{n+1} est divisible par 7

$$A_{n+1} - 2A_n = 7\left(3^{2n+2}\right) \Rightarrow A_{n+1} = 2A_n + 7\left(3^{2n+2}\right)$$

A_n est divisible par 7 $\Rightarrow A_n = 7k$ avec $k \in \mathbb{Z}$ ce qui implique que :

$$A_{n+1} = 2A_n + 7\left(3^{2n+2}\right) = 2(7k) + 7\left(3^{2n+2}\right) = 7(2k + 3^{2n+2}) = 7k'$$

Coclusion : $\forall n \in \mathbb{N}$ A_n est divisible par 7

■

Exercice 7 Soit $E = \{a, b\}$

1. $\mathbb{P}(E) = \{\{a\}, \{b\}, E, \emptyset\}$
2. A quel ensemble appartiennent (a, b) , $\{a\}, (a, \{b\}), (\{a\}, \{b\}), \{\{a\}, \{b\}\}, (a, E)$

$$(a, b) \in E \times E \qquad \{a\} \in \mathbb{P}(E) \qquad (a, \{b\}) \in E \times \mathbb{P}(E) \qquad (\{a\}, \{b\}) \in \mathbb{P}(E) \times \mathbb{P}(E)$$

$$\{\{a\}, \{b\}\} \in \mathbb{P}\big(\mathbb{P}(E)\big) \qquad (a, E) \in E \times \mathbb{P}(E)$$

■

Exercice 8 Soit E un ensemble et soient $A, B \in \mathbb{P}(E)$
résoudre dans $\mathbb{P}(E)$ les équations suivantes :

1. $X \cap A = B$

$$x \in B \Rightarrow x \in (X \cap A) \Rightarrow x \in X \text{ et } x \in A \Rightarrow B \subset X \text{ et } B \subset A$$

$$B \subset X \Rightarrow X = B \cup C \text{ avec } C = C_X^B$$

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

$$B \cap C = \emptyset \Rightarrow C \cap A = \emptyset \Rightarrow C \subset \overline{A}$$

$$\boxed{X = B \cup C \text{ avec } C \subset \overline{A}}$$

2. $X \setminus A = B$

$$x \in B \Rightarrow x \in (X \setminus A) \Rightarrow x \in X \text{ et } x \notin A \Rightarrow B \subset X \text{ et } A \cap B = \emptyset$$

$$B \subset X \Rightarrow X = B \cup C \text{ avec } C = C_X^B$$

$$X \setminus A = B \Rightarrow (B \cup C) \setminus A = B \Rightarrow (B \cup C) \cap \overline{A} = B \Rightarrow (B \cap \overline{A}) \cup (C \cap \overline{A}) = B \Rightarrow B \cup (C \cap \overline{A}) = B$$

$$B \cap C = \emptyset \Rightarrow C \cap \overline{A} = \emptyset \Rightarrow C \subset A$$

$$\boxed{X = B \cup C \text{ avec } C \subset A}$$

<u>deuxième méthode :</u>

$X \setminus A = B \Leftrightarrow X \cap \overline{A} = B$ en posant $\overline{A} = F$ et $B = G$ on aura $X \cap F = G$
D'après la premiere question $X = G \cup C$ avec $C \subset \overline{F} \Rightarrow X = B \cup C$ avec $C \subset \overline{\overline{A}} = A$

■

Exercice 9 Soit E un ensemble et soient $A, B, C \in \mathbb{P}(E)$
On définit la différence symétrique des ensembles A et B par :

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

1. Montrer que $A \Delta B = (A \setminus B) \cup (B \setminus A)$

$$\begin{array}{rcl}
(A \setminus B) \cup (B \setminus A) & = & (A \cap \overline{B}) \cup (B \cap \overline{A}) \\
& = & ((A \cap \overline{B}) \cup B) \cap ((A \cap \overline{B}) \cup \overline{A}) \\
& = & (A \cup B) \cap (\overline{B} \cup B) \cap (A \cup \overline{A}) \cap (\overline{B} \cup \overline{A}) \\
& = & (A \cup B) \cap E \cap E \cap (\overline{B} \cup \overline{A}) \\
& = & (A \cup B) \cap (\overline{B} \cup \overline{A}) \\
& = & (A \cup B) \cap (\overline{A \cap B}) \\
& = & (A \cup B) \setminus (A \cap B) \\
& = & A \Delta B
\end{array}$$

<u>deuxième méthode :</u> On peut montrer le même résultat en utilisant les propositions logiques
On pose $(P) : x \in A$ et $(Q) : x \in B$
Notre but est de montrer que $A \Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$

$$\begin{array}{rcl}
A \cup B & = & \{x \in E / (x \in A) \,\text{ou}\, (x \in B)\} \\
& = & \{x \in E / P \vee Q\} \\
A \cap B & = & \{x \in E / (x \in A) \,\text{et}\, (x \in B)\} \\
& = & \{x \in E / P \wedge Q\} \\
(A \cup B) \setminus (A \cap B) & = & \{x \in E / (x \in A \cup B) \,\text{et}\, (x \notin A \cap B)\} \\
& = & \{x \in E / (P \vee Q) \wedge \neg (P \wedge Q)\} \\
& = & \{x \in E / (P \vee Q) \wedge [\neg P \vee \neg Q]\} \\
& = & \{x \in E / (P \wedge \neg P) \vee (Q \wedge \neg P) \vee (P \wedge \neg Q) \vee (Q \wedge \neg Q)\} \\
& = & \{x \in E / (Q \wedge \neg P) \vee (P \wedge \neg Q)\} \\
A \setminus B & = & \{x \in E / (x \in A) \,\text{et}\, (x \notin B)\} \\
& = & \{x \in E / P \wedge \neg Q\} \\
B \setminus A & = & \{x \in E / Q \wedge \neg P\} \\
(A \setminus B) \cup (B \setminus A) & = & \{x \in E / (x \in A \setminus B) \,\text{ou}\, (x \in B \setminus A)\} \\
& = & \{x \in E / (P \wedge \neg Q) \vee (Q \wedge \neg P)\} \\
& = & (A \cup B) \setminus (A \cap B) \\
& = & A \Delta B
\end{array}$$

2.

$$\begin{array}{rclclcl}
A \Delta A & = & (A \setminus A) \cup (A \setminus A) & = & (A \cap \overline{A}) \cup (A \cap \overline{A}) & = & \emptyset \\
A \Delta \overline{A} & = & (A \setminus \overline{A}) \cup (\overline{A} \setminus A) & = & (A \cap \overline{\overline{A}}) \cup (\overline{A} \cap \overline{A}) & = & A \cup \overline{A} = E \\
A \Delta E & = & (A \setminus E) \cup (E \setminus A) & = & (A \cap \overline{E}) \cup (E \cap \overline{A}) & = & (A \cap \emptyset) \cup (E \cap \overline{A}) \\
& = & \emptyset \cup \overline{A} & = & \overline{A} & & \\
A \Delta \emptyset & = & (A \setminus \emptyset) \cup (\emptyset \setminus A) & = & (A \cap \overline{\emptyset}) \cup (\emptyset \cap \overline{A}) & = & (A \cap E) \cup (\emptyset \cap \overline{A}) \\
& = & A \cup \emptyset & = & A & &
\end{array}$$

3. En supposant que $A\Delta B = A\Delta C$ démontrer que $B = C$
Commençons par montrer que $B \subset C$
Soit $x \in B$ on distingue 2 cas
Si $x \in A \Rightarrow x \in A \cap B \Rightarrow x \notin A\Delta B \Rightarrow x \notin A\Delta C \Rightarrow x \notin (A \cup C) \setminus (A \cap C)$
$x \in A \cup C \Rightarrow x \in A \cap C \Rightarrow x \in C$
Si $x \notin A \Rightarrow x \notin A \cap B \Rightarrow x \in A\Delta B \Rightarrow x \in A\Delta C \Rightarrow x \in (A \cup C) \setminus (A \cap C) \Rightarrow x \in A \cup C \Rightarrow x \in C$
De la même manière, on montre que $C \subset B$

■

Exercice 10 On définit l'application caractéristique

$$\begin{array}{rccl} \varphi_A : & E & \to & \{0,1\} \\ & x & \mapsto & \varphi_A(x) = \left\{ \begin{array}{ll} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{array} \right. \end{array}$$

1. Montrer que $\varphi_A = \varphi_B \Leftrightarrow A = B$
$\underline{\Rightarrow}$
$\underline{\subseteq}$
$x \in A \Rightarrow \varphi_A(x) = 1 \Rightarrow \varphi_B(x) = 1 \Rightarrow x \in B$
$\underline{\subseteq}$
$x \in B \Rightarrow \varphi_B(x) = 1 \Rightarrow \varphi_A(x) = 1 \Rightarrow x \in A$
$\underline{\Leftarrow}$ il suffit de remplacer A par B
2. Vérifier les propriétés suivantes :
   (a) $\varphi_{\overline{A}} = 1 - \varphi_A$
   $x \in A \Rightarrow x \notin \overline{A} \Rightarrow \varphi_A(x) = 1$ et $\varphi_{\overline{A}}(x) = 0$
   $x \notin A \Rightarrow x \in \overline{A} \Rightarrow \varphi_A(x) = 0$ et $\varphi_{\overline{A}}(x) = 1$
   Donc, $\forall x \in E, \varphi_{\overline{A}}(x) = 1 - \varphi_A(x)$
   (b) $\varphi_{A\cap B} = \varphi_A \varphi_B$
   $x \in A \cap B \Rightarrow x \in A$ et $x \in B \Rightarrow \varphi_{A\cap B}(x) = \varphi_A(x) = \varphi_B(x) = 1$
   $x \notin A \cap B \Rightarrow x \in \overline{A \cap B} \Rightarrow x \notin A$ ou $x \notin B \Rightarrow \varphi_{A\cap B}(x) = 0$ et
   $\varphi_A(x) = 0$ ou $\varphi_B(x) = 0$
   Donc, $\forall x \in E, \varphi_{A\cap B}(x) = \varphi_A(x)\varphi_B(x)$
   (c) $\varphi_{A\cup B} = \varphi_A + \varphi_B - \varphi_A \varphi_B$
   $x \in A \cup B \Rightarrow x \in A$ ou $x \in B \Rightarrow \varphi_{A\cup B}(x) = 1$ et
   $\varphi_A(x) = 1$ ou $\varphi_B(x) = 1$
   $x \notin A \cup B \Rightarrow x \in \overline{A \cup B} \Rightarrow x \notin A$ et $x \notin B \Rightarrow \varphi_{A\cup B}(x) = \varphi_A(x) = \varphi_B(x) = 0$
   Donc, $\forall x \in E, \varphi_{A\cup B}(x) = \varphi_A(x) + \varphi_B(x) - \varphi_A(x)\varphi_B(x)$
3. En déduire que $(A \cup B = A \cup C) \wedge (A \cap B = A \cap C) \Rightarrow (B = C)$
$(A \cup B = A \cup C) \wedge (A \cap B = A \cap C) \Rightarrow \varphi_{A\cup B} = \varphi_{A\cup C}$ et $\varphi_{A\cap B} = \varphi_{A\cap C}$
d'ou, $\varphi_A + \varphi_B - \varphi_A \varphi_B = \varphi_A + \varphi_C - \varphi_A \varphi_C$ et $\varphi_A \varphi_B = \varphi_A \varphi_C \Rightarrow \varphi_B = \varphi_C \Rightarrow B = C$

■

Exercice 11 1. Sachant que $E = F = \mathbb{R}$, les fonctions suivantes sont elles des applications ?

$$f: \begin{array}{ccc} E & \rightarrow & F \\ x & \mapsto & x^2+1 \end{array} \qquad g: \begin{array}{ccc} E & \rightarrow & F \\ x & \mapsto & exp\,(x+2) \end{array} \qquad h: \begin{array}{ccc} E & \rightarrow & F \\ x & \mapsto & \sqrt{1-x^2} \end{array}$$

$\forall x \in \mathbb{R},\ f(x) \in \mathbb{R} \Rightarrow f$ est une application
$\forall x \in \mathbb{R},\ g(x) \in \mathbb{R} \Rightarrow g$ est une application
Pour $x = -2\,; h(-2) = \sqrt{-3}$ n'est pas définie $\Rightarrow h$ n'est pas une application
Pour que h soit une application , on chosiit $E = D_h = [-1,1]$

2. sont-elles injectives, surjectives, bijectives ?
$f(-1) = f(1) = 2 \Rightarrow f$ n'est pas injective
$\forall x \in \mathbb{R},\ x^2 \geq 0 \Rightarrow x^2+1 \geq 1 \Rightarrow f(x) \geq 1 \Rightarrow Im\,f = [1,+\infty[\neq F \Rightarrow f$ n'est pas surjective

g est injective car :
Soient $x_1, x_2 \in \mathbb{R}$ tels que $g(x_1) = f(x_2)$
$\Rightarrow exp(x_1+2) = exp(x_2+2) \Rightarrow x_1+2 = x_2+2 \Rightarrow \boxed{x_1 = x_2}$
$\forall x \in \mathbb{R},\ x+2 \in \mathbb{R} \Rightarrow \exp(x+2) > 0 \Rightarrow g(x) > 0 \Rightarrow Im\,g = \mathbb{R}_+^* \neq F \Rightarrow g$ n'est pas surjective

$h(-1) = h(1) = 0 \Rightarrow h$ n'est pas injective
$\forall x \in [-1,1],\ 0 \leq x^2 \leq 1 \Rightarrow -1 \leq -x^2 \leq 0 \Rightarrow 0 \leq 1-x^2 \leq 1 \Rightarrow 0 \leq \sqrt{1-x^2} \leq 1$
$\Rightarrow 0 \leq h(x) \leq 1 \Rightarrow Im\,h = [0,1] \neq F \Rightarrow h$ n'est pas surjective

3. Déterminer dans chaque càs E et F pour que f, g et h soient bijectives, puis donner leur réciproque

Déterminons E pour que f soit injective
Soient $x_1, x_2 \in \mathbb{R}$ tels que $f(x_1) = f(x_2) \Rightarrow x_1^2+1 = x_2^2+1$
$\Rightarrow x_1^2 - x_2^2 = (x_1-x_2)(x_1+x_2) = 0 \Rightarrow (x_1 = x_2)$ ou $(x_1 = -x_2)$
Pour que f soit injective, on choisit $E = \mathbb{R}_+$
Pour que f soit surjective, il suffit de choisir $F = Im\,f = [1,\infty[$
$y = x^2+1 \Rightarrow x^2 = y-1 \Rightarrow x = \sqrt{y-1}$

$$f: \begin{array}{ccc} \mathbb{R}_+ & \rightarrow & [1,\infty[\\ x & \mapsto & x^2+1 \end{array} \text{ est bijective et } \quad f^{-1}: \begin{array}{ccc} [1,\infty[& \rightarrow & \mathbb{R}_+ \\ y & \mapsto & \sqrt{y-1} \end{array}$$

On a deja montré que g est injective pour $E = \mathbb{R}$
Pour que g soit surjective, on choisit $F = Im\,g = \mathbb{R}_+^*$
$y = \exp(x+2) \Rightarrow x+2 = \ln y \Rightarrow x = \ln y - 2$

$$g: \begin{array}{ccc} \mathbb{R} & \rightarrow & \mathbb{R}_+^* \\ x & \mapsto & \exp(x+2) \end{array} \text{ est bijective et } \quad g^{-1}: \begin{array}{ccc} \mathbb{R}_+^* & \rightarrow & \mathbb{R} \\ y & \mapsto & \ln y - 2 \end{array}$$

Déterminons E pour que h soit injective
Soient $x_1, x_2 \in [-1,1]$ tels que $h(x_1) = h(x_2) \Rightarrow \sqrt{1-x_1^2} = \sqrt{1-x_2^2} \Rightarrow 1-x_1^2 = 1-x_2^2$
$\Rightarrow x_1^2 - x_2^2 = (x_1-x_2)(x_1+x_2) = 0 \Rightarrow (x_1 = x_2)$ ou $(x_1 = -x_2)$
Pour que h soit injective, on choisit $E = [0,1]$

Pour que h soit surjective, il suffit de choisir $F = Im\,h = [0,1]$
$y = \sqrt{1-x^2} \Rightarrow 1-x^2 = y^2 \Rightarrow x^2 = 1-y^2 \Rightarrow x = \pm\sqrt{1-y^2}$
Comme on a deja choisi $E = [0,1]$ alors x doit etre positif ($x = \sqrt{1-y^2}$)

$h : \begin{array}{ccc} [0,1] & \rightarrow & [0,1] \\ x & \mapsto & \sqrt{1-x^2} \end{array}$ est bijective et $\quad h^{-1} : \begin{array}{ccc} [0,1] & \rightarrow & [0,1] \\ y & \mapsto & \sqrt{1-y^2} \end{array}$

R On remarque que $h = h^{-1}$ $\qquad h$ est dite involution

Exercice 12 Établir les propriétés suivantes :

1. f injective $\Leftrightarrow \forall A \in P(E),\ f^{-1}(f(A)) = A$

   <u>$\Rightarrow$:</u>
   Soit $A \in P(E)$
   Supposons que f est injective et montrons que $f^{-1}(f(A)) = A$

   $$f(A) = \{y \in F / y = f(a) \text{ avec } a \in A\}$$

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

   <u>$\subseteq$:</u>
   $x \in f^{-1}(f(A)) \Rightarrow f(x) \in f(A) \Rightarrow f(x) = f(a)$ avec $a \in A \Rightarrow x = a$ (car f est injective)
   <u>$\supseteq$:</u>
   $x \in A \Rightarrow f(x) \in f(A) \Rightarrow x \in f^{-1}(f(A))$ par définition de $f^{-1}(f(A))$
   <u>$\Leftarrow$:</u>
   Supposons que $\forall A \in P(E),\ f^{-1}(f(A)) = A$ et montrons que f est injective
   Soient $x_1, x_2 \in E / f(x_1) = f(x_2)$ $\qquad$ Montrons que $x_1 = x_2$
   Posons $A = \{x_1\} \Rightarrow f(x_1) \in f(A) \Rightarrow f(x_2) \in f(A) \Rightarrow x_2 \in f^{-1}(f(A)) \Rightarrow x_2 \in A \Rightarrow x_1 = x_2$
2. f surjective $\Leftrightarrow \forall B \in P(F),\ f(f^{-1}(B)) = B$

   <u>$\Rightarrow$:</u>
   Soit $B \in P(F)$
   Supposons que f est surjective et montrons que $f(f^{-1}(B)) = B$

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

   $$f(f^{-1}(B)) = \{y \in F / y = f(x) \text{ avec } x \in f^{-1}(B)\}$$

   <u>$\subseteq$:</u>
   $y \in f(f^{-1}(B)) \Rightarrow y = f(x)$ avec $x \in f^{-1}(B) \Rightarrow f(x) = y \in B$ par définition de $f^{-1}(B)$
   <u>$\supseteq$:</u>
   $y \in B \Rightarrow \exists x \in E / y = f(x)$ (par surjectivité de f)
   $f(x) \in B \Rightarrow x \in f^{-1}(B) \Rightarrow f(x) = y \in f(f^{-1}(B))$ par définition de $f(f^{-1}(B))$
   <u>$\Leftarrow$:</u>
   Supposons que $\forall B \in P(F),\ f(f^{-1}(B)) = B$ et montrons que f est surjective
   On chosit $B = F \Rightarrow f(f^{-1}(F)) = f(E) = F \Rightarrow f$ surjective

2. Structures algébriques

2.1 Groupes

2.1.1 Loi de composition interne

Définition 2.1.1 Soit E un ensemble non vide. On appelle loi de composition interne (L.c.i) dans E toute application $* : \begin{array}{ccc} E \times E & \to & E \\ (x,y) & \mapsto & *(x,y) = x*y \end{array}$

■ **Exemple 2.1**

$+$ est une L.c.i sur $\mathbb{N}$

$-$ n'est pas une L.c.i sur $\mathbb{N}$, par exemple $1-5=-4 \notin \mathbb{N}$

$*$ est une L.c.i sur $\mathbb{N}$ avec $x*y = x^2+y^2$ ■

R Si $*$ est une L.c.i sur un ensemble E on dit que E est muni de la loi $*$ et on note $(E,*)$

2.1.2 Groupe, sous-groupe, morphisme

Définition 2.1.2 — Groupe. Soit $(E,*)$ un ensemble muni d'une L.c.i $*$.
On dit que $(E,*)$ est un groupe si et seulement si :

1. $*$ est associative i.e : $\forall x,y,z \in E,\ (x*y)*z = x*(y*z)$
2. E admet un élément neutre pour $*$ i.e : $\exists e \in E,\ \forall x \in E / x*e = e*x = x$
3. Tout élément de E admet un symétrique i.e : $\forall x \in E,\ \exists x' \in E / x*x' = x'*x = e$

R Si $\forall x,y \in E,\ x*y = y*x$ on dit que $(E,*)$ est un groupe commutatif ou abélien
le symétrique de x est souvent noté x^{-1} ou x'

■ **Exemple 2.2**

$(\mathbb{Z},+), (\mathbb{Q},\times)$ sont des groupes abéliens.

$(\mathbb{Z},\times),(\mathbb{N},+)$ ne sont pas des groupes car : le symétrique de x par rapport à la loi $\times$ n'existe pas toujours par exemple pour $x=2\Rightarrow x'=1/2\notin\mathbb{Z}$

On peut dire la même chose pour $(\mathbb{N},+)$, en effet $x=2\Rightarrow x'=-2\notin\mathbb{N}$ ■

■ **Exemple 2.3** On définit sur $\mathbb{R}$ la loi $*$ par : $a*b=a+b-ab$

$(\mathbb{R},*)$ est-il un groupe ?

Soient $a,b\in\mathbb{R}$

1. Loi de composition interne : $a*b=(a+b-ab)\in\mathbb{R}\Rightarrow *$ est une Lci dans $\mathbb{R}$
2. Asociativité :
   $(a*b)*c=(a+b-ab)*c=(a+b-ab)+c-(a+b-ab)c=a+b+c-ab-ac-bc-abc$
   $a*(b*c)=a*(b+c-bc)=a+(b+c-bc)-a(b+c-bc)=a+b+c-bc-ab-ac-abc$
   $\Rightarrow (a*b)*c=a*(b*c)\Rightarrow *$ est associative
3. Commutativité : $a*b=a+b-ab=b+a-ba=b*a$
4. Élément neutre : $a*e=a+e-ae=a\Rightarrow e(1-a)=0\Rightarrow \boxed{e=0}$
5. symétrique : $a*a'=e\Rightarrow a+a'-aa'=0\Rightarrow a+a'(1-a)=0\Rightarrow \boxed{a'=\frac{a}{a-1}}$

Pour $a=1,\ a'$ n'existe pas $\Rightarrow(\mathbb{R},*)$ n'est pas un groupe. Par contre, $(\mathbb{R}\setminus\{1\},*)$ est un groupe. ■

Théorème 2.1.1 Soit $(E,*)$ un groupe et soient $x,y\in E$

$$\boxed{(x*y)'=y'*x'}$$

<u>preuve</u>

$$\begin{aligned}\text{On pose } (x*y)'=s \quad &\Rightarrow \quad s*(x*y)=e\\ &\Rightarrow \quad s*x*y*y'=e*y'\\ &\Rightarrow \quad s*x=y'\\ &\Rightarrow \quad s*x*x'=y'*x'\\ &\Rightarrow \quad s=y'*x'\end{aligned}$$

Définition 2.1.3 — Sous-groupe. Soit $(E,*)$ un groupe et soit $A\in P(E)$, on dit que $(A,*)$ est un sous-groupe de $(E,*)$ si et seulement si :

1. $e\in A$ (A est non vide)
2. $\forall x,y\in A,\ (x*y)\in A$ (stabilité)
3. $\forall x\in A,\ x'\in A$ (symétrie)

■ **Exemple 2.4**

$(2\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{Z},+)$ avec $2\mathbb{Z}$ l'ensemble des entiers paires.

$(2\mathbb{Z}+1,+)$ n'est pas un sous-groupe de $(\mathbb{Z},+)$ avec $2\mathbb{Z}+1$ l'ensemble des entiers impaires ■

Définition 2.1.4 — Morphisme. Soient $(E,*)$ et (F,Δ) deux groupes et soit $f:E\to F$ une application.
On dit que f est un morphisme de groupe ssi : $\forall x,y\in E,\ f(x*y)=f(x)\Delta f(y)$

R

un morphisme bijectif est dit isomorphisme.
un endomorphisme est un morphisme de E vers E
un automorphisme est un endomorphisme bijectif.

Théorème 2.1.2 Soient $(E,*)$ et (F,Δ) deux groupes dont l'élément neutre est noté respectivement e_1, e_2 et soit $f : E \to F$ un morphisme de groupe, alors :
1. $f(e_1) = e_2$
2. $\forall x \in E,\ [f(x)]^{-1} = f(x^{-1})$

Preuve :
1. Montrons que $f(e_1) = e_2$
$$\begin{aligned} f(e_1 * e_1) = f(e_1)\Delta f(e_1) = f(e_1) \quad &\Rightarrow \quad f(e_1)\Delta f(e_1)\Delta[f(e_1)]^{-1} = f(e_1)\Delta[f(e_1)]^{-1} \\ &\Rightarrow \quad f(e_1)\Delta e_2 = e_2 \\ &\Rightarrow \quad f(e_1) = e_2 \end{aligned}$$
2. Soit $x \in E$ Montrons que $[f(x)]^{-1} = f(x^{-1})$
$$\begin{aligned} f(x * x^{-1}) = f(x)\Delta f(x^{-1}) = f(e_1) = e_2 \quad &\Rightarrow \quad [f(x)]^{-1}\Delta f(x)\Delta f(x^{-1}) = [f(x)]^{-1}\Delta e_2 \\ &\Rightarrow \quad e_2\Delta f(x^{-1}) = [f(x)]^{-1}\Delta e_2 \\ &\Rightarrow \quad [f(x)]^{-1} = f(x^{-1}) \end{aligned}$$

■ **Exemple 2.5** $f : \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C}^* \\ z & \mapsto & e^z \end{array}$ est un morphisme de groupe de $(\mathbb{C},+)$ vers $(\mathbb{C}^*,\times)$. En effet,
$\forall z_1, z_2 \in \mathbb{C},\ f(z_1+z_2) = e^{z_1+z_2} = e^{z_1} \times e^{z_2} = f(z_1)f(z_2)$
On remarque que $f(0) = 1$ et $f(1) = e \Rightarrow [f(1)]^{-1} = \dfrac{1}{e}$
Or, $f(-1) = e^{-1} = \dfrac{1}{e} \Rightarrow [f(1)]^{-1} = f(-1)$ ■

2.2 Anneau, sous anneau, corps

Soit E un ensemble et soient $+$ et $\times$ deux L.c.i sur E

Définition 2.2.1 — Anneau. On dit que $(E,+,\times)$ est un anneau ssi :
1. $(E,+)$ est un groupe abélien, son élément neutre est noté 0_E
2. $\times$ est associative.
3. $\forall x,y,z \in E,\ x \times (y+z) = (x \times y) + (x \times z)$ (on dit que $\times$ est distributive sur $+$)
$(y+z) \times x = (y \times x) + (z \times x)$
4. E admet un élément neutre pour $\times$ noté 1_E

R

Attention, la loi $(+)$ n'est pas l'addition et la loi $(\times)$ n'est pas la multiplication, ce sont des notations.

$x \times y$ est souvent notée xy

le symétrique de x par rapport à la loi $(+)$ est dit opposé de x, il est noté $-x$

le symétrique de x par rapport à la loi $(\times)$ est dit inverse de x, il est noté x^{-1} s'il existe on dit que x est inversible.

■ **Exemple 2.6**

$(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$ sont des anneaux.

$(\mathbb{N},+,\times)$ n'est pas un anneau. ■

Notations

Soit $n \in \mathbb{N}^*$ et soient $x,y \in (E,+,\times)$
1. $nx = x + x + \cdots + x$ (n fois)
2. $x^n = x \times x \times \cdots \times x$ (n fois) Attention, en général $(xy)^n \neq x^n y^n$

2.2.1 Propriétés

Soient $x, y \in (E, +, \times)$

1. $x0 = 0x = 0$
2. $(-x)y = -xy = x(-y)$

<u>Preuve :</u>

1. Montrons que $x0 = 0$

$$\begin{aligned} x0 = x(0+0) = x0 + x0 &\Rightarrow x0 + (-x0) = x0 + x0 + (-x0) \\ &\Rightarrow 0 = x0 + 0 \\ &\Rightarrow 0 = x0 \end{aligned}$$

2. Montrons que $(-x)y = -xy$

$$\begin{aligned} (-x)y + xy = [(-x) + x]y = 0 &\Rightarrow (-x)y + xy + (-xy) = 0 + (-xy) \\ &\Rightarrow (-x)y + 0 = 0 + (-xy) \\ &\Rightarrow (-x)y = -xy \end{aligned}$$

Soit $(E, +, \times)$ un anneau et soit $A \in P(E)$

Définition 2.2.2 — Sous anneau. On dit que $(A, +, \times)$ est un sous anneau de E ssi :

1. $(A, +)$ est un sous-groupe de $(E, +)$.
2. $\forall x, y \in A,\ xy \in A$
3. $1_E \in A$

■ **Exemple 2.7**

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

$(2\mathbb{Z}, +, \times)$ n'est pas un sous-anneau de $(\mathbb{Z}, +, \times)$ avec $2\mathbb{Z}$ l'ensemble des entiers paires car $1 \notin 2\mathbb{Z}$
■

2.2.2 Corps

Soit E un ensemble et soient $+$ et $\times$ deux L.c.i sur E

Définition 2.2.3 On dit que $(E, +, \times)$ est un corps ssi :

1. $(E, +, \times)$ un anneau
2. $0_E \neq 1_E$
3. Tout élément x de $E \setminus \{0_E\}$ admet un symétrique par rapport à $\times$ noté x^{-1}

■ **Exemple 2.8**

$(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des corps.

$(\mathbb{Z}, +, \times)$ n'est pas un corps. ■

2.3 série d'exercices

Exercice 1 Soit $n \in \mathbb{N}^*$ On définit sur $\mathbb{R}$ la loi $*$ par :

$$a * b = a + b - nab$$

1. $(\mathbb{R}, *)$ est-il un groupe ?
2. Trouver $E \subset \mathbb{R}$ tel que $(E, *)$ soit un groupe.

■

Exercice 2 Soient A et B deux sous-groupes de $(E,*)$

1. Montrer que $A\cap B$ est un sous-groupe de E.
2. Soit $n\in\mathbb{N}^*$ on définit $n\mathbb{Z}$ par :

$$n\mathbb{Z}=\{nx/x\in\mathbb{Z}\}$$

   (a) Montrer que $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$
   (b) $2\mathbb{Z}\cup3\mathbb{Z}$ est-il un sous-groupe ?

■

Exercice 3 Soit $(E,*)$ un groupe. On définit le centre de E par :

$$Z(E)=\{x\in E/\forall y\in E,\ x*y=y*x\}$$

1. Montrer que $Z(E)$ est un sous-groupe de $(E,*)$
2. $Z(E)$ est il un groupe abélien ?

■

Exercice 4 Soit $(E,*)$ un groupe et soient A,B deux sous-groupes de E, on définit les ensembles :

$$AB=\{x\in E/x=a*b \text{ avec } a\in A,\ b\in B\} \qquad BA=\{x\in E/x=b*a \text{ avec } b\in B,\ a\in A\}$$

Montrer que : AB sous-groupe de $E\Leftrightarrow AB=BA$

■

Exercice 5 Soit $(\mathbb{R}\setminus\{-3\},*)$ un groupe dont la loi $*$ est définie par : $a*b=ab+3(a+b+2)$
Et soit l'application $f:(\mathbb{R}\setminus\{-3\},*)\to(\mathbb{R}^*,.)$

$$x\mapsto x+3$$

1. Montrer que f est un morphisme de groupes
2. Calculer de deux manières differentes l'élément neutre e puis le symétrique x^{-1}

■

Exercice 6 Soit $f:(E,*)\to(F,\Delta)$ un morphisme de groupes.

1. Soit B sous-groupe de F, Montrer que : $f^{-1}(B)$ sous groupe de E
2. on définit le noyau de f par : $ker(f)=\{x\in E/f(x)=e_2\}$ avec e_2 : élément neutre de (F,Δ)
   (a) Déduire que $ker(f)$ est un sous-groupe de $(E,*)$
   (b) Montrer que : f injective $\Leftrightarrow ker(f)=\{e_1\}$ avec e_1 : élément neutre de $(E,*)$

■

Exercice 7 — Anneau de Boole. Soit $(E,+,\times)$ un anneau tel que $\forall x\in E/x\times x=x^2=x$

1. Montrer que $\forall x\in E,\ x+x=0$
2. En déduire que $(E,+,\times)$ est un anneau commutatif

■

Exercice 8 Soit $(E,+,\times)$ un anneau et soit $x \in E$
On dit que x est un élément nilpotent ssi $\exists n \in \mathbb{N}^*$ tel que $x^n = 0$
Montrer que :
1. $(x \text{ nilpotent}) \wedge (xy = yx) \Rightarrow xy$ nilpotent
2. xy nilpotent $\Rightarrow yx$ nilpotent

Exercice 9 $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}/a, b \in \mathbb{Q}\}$
1. Montrer que $\left(\mathbb{Q}[\sqrt{2}],+,\times\right)$ est un sous-anneau de $(\mathbb{R},+,\times)$.
2. En déduire que $\left(\mathbb{Q}[\sqrt{2}],+,\times\right)$ est un corps.

Exercice 10 Soit $(A,+,.)$ un anneau. On dit que A est intègre ssi :

$$\forall a,b \in A,\ ab = 0 \Rightarrow (a = 0) \text{ ou } (b = 0)$$

1. Donner deux exemples d'anneaux intègres.
2. Soit $(\mathscr{F},+,.)$ l'anneau des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$ On pose :

$$\begin{array}{lcl} f:\mathbb{R} & \to & \mathbb{R} \\ x & \to & f(x) = \begin{cases} x & \text{si } x \geq 0 \\ 0 & \text{si } x < 0 \end{cases} \end{array} \qquad \begin{array}{lcl} g:\mathbb{R} & \to & \mathbb{R} \\ x & \to & g(x) = \begin{cases} 0 & \text{si } x \geq 0 \\ x & \text{si } x < 0 \end{cases} \end{array}$$

Calculer fg puis en déduire que l'anneau $(\mathscr{F},+,.)$ n'est pas intègre.

Exercice 11 Soit $(A,+,.)$ un anneau et soit I une partie non vide de A
On dit que I est un idéal de A ssi :
1. $(I,+)$ sous groupe de A
2. $\forall (a,x) \in A \times I,\ ax \in I$

1. Montrer que pour tout $n \in \mathbb{N}^*$ $n\mathbb{Z}$ est un idéal de $(\mathbb{Z},+,.)$
(On rappelle que $n\mathbb{Z} = \{nx/x \in \mathbb{Z}\}$)
2. Soient I et J deux idéaux de A
   (a) Montrer que $I \cap J$ est aussi un idéal de A
   (b) $I \cup J$ est-il toujours un idéal de A ?

2.4 Corrigé de la serie d'exercices

Exercice 1 Soit $n \in \mathbb{N}^*$ On définit sur $\mathbb{R}$ la loi $*$ par :

$$a * b = a + b - nab$$

1. $(\mathbb{R}, *)$ est-il un groupe ?
   Soient $a, b \in \mathbb{R}$
   (a) Loi de composition interne : $a * b = (a + b - nab) \in \mathbb{R} \Rightarrow *$ est une Lci dans $\mathbb{R}$
   (b) Asociativité :
   $(a * b) * c = (a + b - nab) * c = (a + b - nab) + c - n(a + b - nab)c = a + b + c - nab - nac - nbc - n^2abc$
   $a * (b * c) = a * (b + c - nbc) = a + (b + c - nbc) - na(b + c - nbc) = a + b + c - nbc - nab - nac - n^2abc$
   $\Rightarrow (a * b) * c = a * (b * c) \Rightarrow *$ est associative
   (c) Commutativité : $a * b = a + b - nab = b + a - nba = b * a$
   (d) Élément neutre : $a * e = a + e - nae = a \Rightarrow e(1 - na) = 0 \Rightarrow \boxed{e = 0}$
   (e) symétrique : $a * a' = e \Rightarrow a + a' - naa' = 0 \Rightarrow a + a'(1 - na) = 0 \Rightarrow \boxed{a' = \dfrac{a}{na - 1}}$
   Pour $a = \dfrac{1}{n}$, a' n'existe pas $\Rightarrow (\mathbb{R}, *)$ n'est pas un groupe.
2. Trouver $E \subset \mathbb{R}$ tel que $(E, *)$ soit un groupe.
   $\left(\mathbb{R} \setminus \{\frac{1}{n}\}, *\right)$ est un groupe.

■

Exercice 2 Soient A et B deux sous-groupes de $(E, *)$
1. Montrer que $A \cap B$ est un sous-groupe de E.
   (a) Élément neutre : $e \in A$ car A sous-groupe et $e \in B$ car B sous-groupe $\Rightarrow e \in A \cap B$
   (b) Stabilité : Soit $x, y \in A \cap B \Rightarrow x, y \in A$ et $x, y \in B$
   $(x * y) \in A$ et $(x * y) \in B$ car A et B sous-groupes $\Rightarrow (x * y) \in A \cap B$
   (c) Symétrique : $x \in A \cap B \Rightarrow x \in A$ et $x \in B$
   A et B sous groupes $\Rightarrow x' \in A$ et $x' \in B \Rightarrow x' \in A \cap B$
2. Soit $n \in \mathbb{N}^*$ on définit $n\mathbb{Z}$ par :

$$n\mathbb{Z} = \{nx / x \in \mathbb{Z}\}$$

   (a) Montrer que $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$
      i. Élément neutre : $0 = n0 \Rightarrow 0 \in n\mathbb{Z}$
      ii. Stabilité : Soit $a, b \in n\mathbb{Z} \Rightarrow a = nx,\ b = ny \Rightarrow a + b = nx + ny = n(x + y) \Rightarrow (a + b) \in n\mathbb{Z}$
      iii. Symétrique : $a \in n\mathbb{Z} \Rightarrow a = nx \Rightarrow a' = -nx = n(-x) \Rightarrow a' \in n\mathbb{Z}$
   (b) $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe car :
   2 et $3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ mais $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$

■

Exercice 3 Soit $(E, *)$ un groupe. On définit le centre de E par :

$$Z(E) = \{x \in E / \forall y \in E,\ x * y = y * x\}$$

1. Montrer que $Z(E)$ est un sous-groupe de $(E,*)$
   (a) Élément neutre : $\forall y \in E,\ e*y = y*e = y \Rightarrow e \in Z(E)$
   (b) Stabilité : Soient $a,b \in Z(E) \Rightarrow \forall y \in E,\ (a*b)*y = a*b*y = a*y*b = y*a*b = y*(a*b)$
   (c) Symétrique : $a \in Z(E) \Rightarrow \forall y \in E,\ a'*y = a'*y*a*a' = a'*a*y*a' = y*a' \Rightarrow a' \in Z(E)$
2. $Z(E)$ est il un groupe abélien ?
   Soient $a,b \in Z(E) \Rightarrow \forall y \in E,\ a*y = y*a$,en particulier pour $y=b$ on aura $a*b = b*a$
   Donc, $Z(E)$ est un groupe abélien.

■

Exercice 4 Soit $(E,*)$ un groupe et soient A,B deux sous-groupes de E, on définit les ensembles :

$$AB = \{x \in E / x = a*b \text{ avec } a \in A,\ b \in B\} \qquad BA = \{x \in E / x = b*a \text{ avec } b \in B,\ a \in A\}$$

Montrer que : AB sous-groupe de $E \Leftrightarrow AB = BA$

$\Rightarrow$:

$\subset$:

$x \in AB \Rightarrow x' \in AB$ (car AB sous-groupe) $\Rightarrow x' = a*b$ avec $a \in A,\ b \in B$

$\Rightarrow (x')' = (a*b)' \Rightarrow x = b'*a' \Rightarrow x \in BA$ (car $b' \in B$ et $a' \in A$)

$\supset$:

$x \in BA \Rightarrow x = b*a \Rightarrow x' = a'*b' \Rightarrow x' \in AB \Rightarrow x \in AB$ (car AB sous-groupe)

$\Leftarrow$: Montrons que AB sous-groupe de E

1. Élément neutre : $e = e*e$ (avec $e \in A$ et $e \in B$) $\Rightarrow e \in AB$
2. Stabilité : Soient $x,y \in AB \Rightarrow x*y = (a_1*b_1)*(a_2*b_2) = a_1*(b_1*a_2)*b_2$
   $c = b_1*a_2 \in BA \Rightarrow c \in AB$ (car $AB = BA$) $\Rightarrow c = a_3*b_3$
   Donc, $x*y = a_1*(a_3*b_3)*b_2 = (a_1*a_3)*(b_3*b_2) \Rightarrow x*y \in AB$
3. Symétrique : $x \in AB \Rightarrow x = a*b \Rightarrow x' = b'*a' \Rightarrow x' \in BA \Rightarrow x' \in AB$ (car $AB = BA$)

■

Exercice 5 Soit $(\mathbb{R}\setminus\{-3\},*)$ un groupe dont la loi $*$ est définie par : $a*b = ab + 3(a+b+2)$

Et soit l'application $f : (\mathbb{R}\setminus\{-3\},*) \to (\mathbb{R}^*,.)$

$$x \mapsto x+3$$

1. Montrer que f est un morphisme de groupes
   On montre que $f(x*y) = f(x)f(y)$
2. Calculer de deux manières differentes l'élément neutre e puis le symétrique x^{-1}
   $a*e = a \Rightarrow ae + 3(a+e+2) = a \Rightarrow e(a+3) + 3a + 6 = a \Rightarrow e = -\frac{2a+6}{a+3} \Rightarrow e = -2$
   $f(e) = 1 \Rightarrow e+3 = 1 \Rightarrow e = -2$

   $x*x^{-1} = e \Rightarrow xx^{-1} + 3(x + x^{-1} + 2) = -2 \Rightarrow x^{-1}(x+3) + 3x + 6 = -2$
   $\Rightarrow x^{-1} = \dfrac{-3x-8}{x+3} = \dfrac{1-3(x+3)}{x+3} = \dfrac{1}{x+3} - 3$
   $f(x^{-1}) = [f(x)]^{-1} \Rightarrow x^{-1} + 3 = \dfrac{1}{x+3} \Rightarrow x^{-1} = \dfrac{1}{x+3} - 3$

■

Exercice 6 Soit $f:(E,*)\to(F,\Delta)$ un morphisme de groupes.

1. Soit B sous-groupe de F, Montrer que : $f^{-1}(B)$ sous groupe de E
   (a) Élément neutre : $f^{-1}(B)=\{x\in E/f(x)\in B\}$
   $f(e_1)=e_2\in B$ car B sous-groupe $\Rightarrow e_1\in f^{-1}(B)$
   (b) Stabilité : Soient $x,y\in f^{-1}(B)\Rightarrow f(x)$ et $f(y)\in B$
   $\Rightarrow f(x)\Delta f(y)\in B$ (car : B est un sous-groupe)
   Or, f est un morphisme de groupe $\Rightarrow f(x)\Delta f(y)=f(x*y)\Rightarrow f(x*y)\in B$
   $\Rightarrow (x*y)\in f^{-1}(B)$
   (c) Symétrique : Soit $x\in f^{-1}(B)\Rightarrow f(x)\in B\Rightarrow [f(x)]^{-1}\in B$ (car : B est un sous-groupe)
   Or, f est un morphisme de groupe $\Rightarrow [f(x)]^{-1}=f(x^{-1})$
   $\Rightarrow f(x^{-1})\in B\Rightarrow x^{-1}\in f^{-1}(B)$
2. on définit le noyau de f par : $ker(f)=\{x\in E/f(x)=e_2\}$
   avec e_2 : élément neutre de (F,Δ)
   (a) Déduire que $ker(f)$ est un sous-groupe de $(E,*)$
   $ker(f)=\{x\in E/f(x)=e_2\}=\{x\in E/f(x)\in\{e_2\}\}=f^{-1}(\{e_2\})$
   Or, $\{e_2\}$ sous-groupe de $F\Rightarrow f^{-1}(\{e_2\})=ker(f)$ sous-groupe de E
   (b) Montrer que : f injective $\Leftrightarrow ker(f)=\{e_1\}$ avec e_1 : élément neutre de $(E,*)$
   $\underline{\Rightarrow :}$
   $\underline{\supset :}$ $\{e_1\}\subset ker(f)$ car : $ker(f)$ est un sous-groupe de E
   $\underline{\subset :}$
   $x\in ker(f)\Rightarrow f(x)=e_2$,
   Or : $f(e_1)=e_2\Rightarrow f(x)=f(e_1)\Rightarrow x=e_1$ (car : f est injective)
   $\underline{\Leftarrow :}$
   Soient $x_1,x_2\in E$ tels que $f(x_1)=f(x_2)$
   $f(x_1)\Delta[f(x_1)]^{-1}=e_2\Rightarrow f(x_2)\Delta[f(x_1)]^{-1}=e_2$
   $\Rightarrow f(x_2)\Delta f(x_1^{-1})=e_2\Rightarrow f(x_2*x_1^{-1})=e_2$
   $\Rightarrow (x_2*x_1^{-1})\in ker(f)\Rightarrow (x_2*x_1^{-1})\in\{e_1\}\Rightarrow x_2*x_1^{-1}=e_1$
   $\Rightarrow x_2*x_1^{-1}*x_1=e_1*x_1\Rightarrow x_2=x_1$

■

Exercice 7 — Anneau de Boole. Soit $(E,+,\times)$ un anneau tel que $\forall x\in E/x\times x=x^2=x$

1. Montrer que $\forall x\in E,\ x+x=0$
   $(x+x)^2=x^2+x^2+x^2+x^2=x+x+x+x=x+x\Rightarrow x+x=0$
2. En déduire que $(E,+,\times)$ est un anneau commutatif
   $(x+y)^2=x+y\Rightarrow x^2+xy+yx+y^2=x+y\Rightarrow x+xy+yx+y=x+y\Rightarrow xy+yx=0\Rightarrow$
   $xy+yx+yx=0+yx\Rightarrow xy=yx$

■

Exercice 8 Soit $(E,+,\times)$ un anneau et soit $x\in E$
On dit que x est un élément nilpotent ssi $\exists n\in\mathbb{N}^*$ tel que $x^n=0$
Montrer que :

1. $(x$ nilpotent$)\wedge(xy=yx)\Rightarrow xy$ nilpotent
   x nilpotent $\Rightarrow \exists n\in\mathbb{N}^*$ tel que $x^n=0\Rightarrow (xy)^n=xyxy\cdots xy=(x)^n(y)^n$ (car : $xy=yx$)
   $\Rightarrow (xy)^n=0(y)^n=0\Rightarrow xy$ nilpotent
2. xy nilpotent $\Rightarrow yx$ nilpotent
   xy nilpotent $\Rightarrow \exists n\in\mathbb{N}^*$ tel que $(xy)^n=0\Rightarrow xyxy\cdots xyxy=0\Rightarrow y(xyxy\cdots xy)x=0$
   $\Rightarrow (yx)^{n+1}=0\Rightarrow yx$ nilpotent

■

Exercice 9 $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}/a, b \in \mathbb{Q}\}$

1. Montrer que $\left(\mathbb{Q}[\sqrt{2}], +, \times\right)$ est un sous-anneau de $(\mathbb{R}, +, \times)$.
   (a) Montrons que $\left(\mathbb{Q}[\sqrt{2}], +\right)$ est un sous-groupe de $(\mathbb{R}, +)$
      i. Élément neutre : $0 = 0 + 0\sqrt{2} \Rightarrow 0 \in \mathbb{Q}[\sqrt{2}]$
      ii. Stabilité :
      Soient $x, y \in \mathbb{Q}[\sqrt{2}] \Rightarrow x = a_1 + b_1\sqrt{2}$ et $y = a_2 + b_2\sqrt{2}$
      $\Rightarrow x + y = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \Rightarrow x + y \in \mathbb{Q}[\sqrt{2}]$
      iii. Symétrie : Soit $x \in \mathbb{Q}[\sqrt{2}] \Rightarrow x = a + b\sqrt{2}$
      $\Rightarrow -x = -a - b\sqrt{2} = (-a) + (-b)\sqrt{2} \Rightarrow -x \in \mathbb{Q}[\sqrt{2}]$
   (b) Stabilité : Soient $x, y \in \mathbb{Q}[\sqrt{2}] \Rightarrow x = a_1 + b_1\sqrt{2}$ et $y = a_2 + b_2\sqrt{2}$
   $\Rightarrow xy = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}$
   $\Rightarrow xy \in \mathbb{Q}[\sqrt{2}]$
   (c) Élément neutre : $1 = 1 + 0\sqrt{2} \Rightarrow 1 \in \mathbb{Q}[\sqrt{2}]$
2. En déduire que $\left(\mathbb{Q}[\sqrt{2}], +, \times\right)$ est un corps.
   $x \in \mathbb{Q}[\sqrt{2}] \Rightarrow x = a + b\sqrt{2}$
   $\Rightarrow \frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \left(\frac{-b}{a^2 - 2b^2}\right)\sqrt{2}$
   $\Rightarrow \frac{1}{x} \in \mathbb{Q}[\sqrt{2}]$

■

Exercice 10 Soit $(A, +, .)$ un anneau. On dit que A est intègre ssi :

$$\forall a, b \in A,\ ab = 0 \Rightarrow (a = 0) \text{ ou } (b = 0)$$

1. Donner deux exemples d'anneaux intègres.
   (a) L'anneau des entiers $(\mathbb{Z}, +, .)$ est un anneau intègre car :

$$\forall a, b \in \mathbb{Z},\ ab = 0 \Rightarrow (a = 0) \text{ ou } (b = 0)$$

   (b) L'anneau des polynômes $(\mathbb{R}[X], +, .)$ est un anneau intègre car :

$$\forall P, Q \in \mathbb{R}[X],\ PQ = 0 \Rightarrow (P = 0) \text{ ou } (Q = 0)$$

2. Soit $(\mathscr{F}, +, .)$ l'anneau des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$ On pose :

$$\begin{array}{lcl} f : \mathbb{R} & \to & \mathbb{R} \\ x & \to & f(x) = \left\{ \begin{array}{ll} x & \text{si } x \geq 0 \\ 0 & \text{si } x < 0 \end{array} \right. \end{array} \qquad \begin{array}{lcl} g : \mathbb{R} & \to & \mathbb{R} \\ x & \to & g(x) = \left\{ \begin{array}{ll} 0 & \text{si } x \geq 0 \\ x & \text{si } x < 0 \end{array} \right. \end{array}$$

   Calculer fg puis en déduire que l'anneau $(\mathscr{F}, +, .)$ n'est pas intègre.

$$x \geq 0 \Rightarrow \left\{ \begin{array}{l} f(x) = x \\ g(x) = 0 \end{array} \right. \Rightarrow f(x)g(x) = x.0 = 0$$

$$x < 0 \Rightarrow \left\{ \begin{array}{l} f(x) = 0 \\ g(x) = x \end{array} \right. \Rightarrow f(x)g(x) = 0.x = 0$$

Donc, $\forall x \in \mathbb{R},\ (fg)(x) = 0$
On en conclut que $(\mathscr{F},+,.)$ n'est pas un anneau intègre car :

$$\exists f,g \in \mathscr{F} \text{ tels que } (fg = 0) \text{ et } (f \neq 0 \text{ et } g \neq 0)$$

■

Exercice 11 Soit $(A,+,.)$ un anneau et soit I une partie non vide de A
On dit que I est un idéal de A ssi :
1. $(I,+)$ sous groupe de A
2. $\forall (a,x) \in A \times I,\ ax \in I$

1. Montrer que pour tout $n \in \mathbb{N}^*$ $n\mathbb{Z}$ est un idéal de $(\mathbb{Z},+,.)$
(On rappelle que $n\mathbb{Z} = \{nx / x \in \mathbb{Z}\}$)
Soit $y \in n\mathbb{Z} \Rightarrow y = nx$ avec $x \in \mathbb{Z}$
Soit $a \in \mathbb{Z} \Rightarrow ay = a(nx) = n(ax) \Rightarrow ay \in n\mathbb{Z}$
On a déjà vu que $n\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$
Donc $n\mathbb{Z}$ est un idéal de $(\mathbb{Z},+,.)$
2. Soient I et J deux idéaux de A
   (a) Montrer que $I \cap J$ est aussi un idéal de A
   Soit $x \in I \cap J$ et $a \in A \Rightarrow (x \in I)$ et $(x \in J)$
   $\Rightarrow (ax \in I)$ et $(ax \in J)$ car I et J sont des idéaux
   $\Rightarrow ax \in I \cap J$
   On a déjà vu que l'intersection de deux sous groupes est un sous groupe
   On en conclut que $I \cap J$ est un idéal de A
   (b) $I \cup J$ est-il un idéal de A ?
   Soit $x \in I \cup J$ et $a \in A \Rightarrow (x \in I)$ ou $(x \in J)$
   $\Rightarrow (ax \in I)$ ou $(ax \in J)$ car I et J sont des idéaux
   $\Rightarrow ax \in I \cup J$
   On a déjà vu que la réunion de deux sous groupes n'est pas toujours un sous groupe
   On en conclut que $I \cup J$ n'est pas toujours un idéal de A

■

3. Polynômes

3.1 Généralités

Définition 3.1.1 Soit $\mathbb{K}$ un corps commutatif. On appelle polynôme à une indéterminée à coefficients dans $\mathbb{K}$ toute expression de la forme :

$$P(X) = \sum_{i=0}^{n} a_i X^i = a_0 X^0 + a_1 X^1 + \cdots + a_n X^n \quad \text{avec } a_i \in \mathbb{K} \text{ et } n \in \mathbb{N}$$

R

L'ensemble de tous les polynômes est noté $\mathbb{K}[X]$
X est dite indéterminée.
Ne pas confondre Polynôme et fonction polynomiale.
$P(X) = a_p X_p$ est dit monôme.
Dans la suite de ce chapitre on prendra ($\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$)

Définition 3.1.2 Soit $P \in \mathbb{K}[X]$ On appelle degré de P et on note $degP$ le plus grand entier naturel i tel que $a_i \neq 0$

R

a_{degP} s'appelle coefficient dominant de P
Si $a_{degP} = 1$, P est dit unitaire.
L'ensemble des polynômes de degré inférieur ou égal à n est noté $\mathbb{K}_n[X]$

■ **Exemple 3.1** $deg(X^3 - 1) = 3 \quad deg(5) = 0 \quad deg(0) = -\infty($ par convention $)$

Définition 3.1.3 Soit $P \in \mathbb{K}[X]$ avec :

$$P(X) = \sum_{i=0}^{n} a_i X^i = a_0 X^0 + a_1 X^1 + \cdots + a_n X^n$$

Le polynôme $P^{(1)}$ tel que
$P^{(1)}(X) = \sum_{i=1}^{n} ia_i X^{i-1} = a_1 X^0 + 2a_2 X^1 + \cdots + na_n X^{n-1}$ est dit dérivée de P

Proposition 3.1.1 Soit $k \in \mathbb{N}^*$ $\quad degP^{(k)} = degP - k$

3.2 Opérations sur les polynômes

3.2.1 Addition

Définition 3.2.1 Soient $P, Q \in \mathbb{K}[X]$ avec : $P(X) = \sum_{i \geq 0} a_i X^i$ et $Q(X) = \sum_{i \geq 0} b_i X^i$

La somme de P et de Q notée $P+Q$ est définie par :

$$(P+Q)(X) = \sum_{i \geq 0} c_i X^i \text{ avec } c_i = a_i + b_i$$

Proposition 3.2.1

1. $deg(P+Q) \leq Max(degP, degQ)$
2. $degP \neq degQ \Rightarrow deg(P+Q) = Max(degP, degQ)$

■ **Exemple 3.2** $P(X) = -3X^2 + X + 1 \quad Q(X) = 3X^2 - X + 3 \quad (P+Q)(X) = 4$

3.2.2 Multiplication

Définition 3.2.2 Soient $P, Q \in \mathbb{K}[X]$ avec : $P(X) = \sum_{i \geq 0} a_i X^i$ et $Q(X) = \sum_{i \geq 0} b_i X^i$

Le produit de P et de Q notée PQ est définie par :

$$(PQ)(X) = \sum_{i \geq 0} c_i X^i \text{ avec } c_i = \sum_{k=0}^{i} a_k b_{i-k}$$

Proposition 3.2.2 deg PQ=deg P+ deg Q

3.2.3 Division euclidienne

Définition 3.2.3 Soient $P \in \mathbb{K}[X]$ et , $S \in \mathbb{K}[X] \setminus \{0\}$

$$\boxed{\exists !(Q,R) \in \mathbb{K}[X]^2, P = QS + R \quad \text{avec } degR < degS}$$

On appelle Q le quotient de la division euclidienne de P par S
On appelle R le reste de la division euclidienne de P par S
Si $R = 0$ on dit que S divise P ou que P est un multiple de S

■ **Exemple 3.3** $X^3 + X^2 + 3X - 2 = (X+1)(X^2+3) - 5$

$$\begin{array}{rrrr|l}
X^3 & +X^2 & +3X & -2 & X+1 \\ \cline{5-5}
X^3 & +X^2 & & & X^2+3 \\ \cline{1-4}
 & & 3X & -2 & \\
 & & 3X & +3 & \\ \cline{3-4}
 & & & -5 &
\end{array}$$

3.3 Racines d'un polynômes

Définition 3.3.1 Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$

$$\alpha \text{ racine de } P \Leftrightarrow (X-\alpha) \text{ divise } P$$

Proposition 3.3.1 α racine de $P \Leftrightarrow P(\alpha) = 0$

3.3.1 Multiplicité d'une racine

Définition 3.3.2 Soit $P \in \mathbb{K}[X]$ $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$
Si $(X-\alpha)^m$ divise P et $(X-\alpha)^{m+1}$ ne divise pas P alors on dit que α est une racine d'ordre de multiplicité m et on note $mult(\alpha) = m$

Proposition 3.3.2 $(X-\alpha)^m$ divise $P \Leftrightarrow \left[P(\alpha) = P^{(1)}(\alpha) = P^{(2)}(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0\right]$

Théorème 3.3.3 $mult(\alpha) = m \Leftrightarrow P(\alpha) = P^{(1)}(\alpha) = P^{(2)}(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0$ et $P^{(m)}(\alpha) \neq 0$

■ **Exemple 3.4** $P(X) = (X+1)^2(X-2) = X^3 - 3X - 2$ $\quad mult(-1) = 2 \quad mult(2) = 1$
$P(-1) = 0 \quad P'(-1) = 3(-1)^2 - 3 = 0 \quad P''(-1) = 6(-1) \neq 0$
On en conclut que $\alpha = -1$ est d'ordre de multiplicité 2

Théorème 3.3.4 Soit $P \in \mathbb{K}_n[X]$ avec $P(X) = a_0X^0 + a_1X^1 + \cdots + a_nX^n$
et soit $\alpha = \dfrac{a}{b} \in \mathbb{Q}$ avec $a \wedge b = 1$

$$P(\alpha) = 0 \Rightarrow a|a_0 \text{ et } b|a_n$$

■ **Exemple 3.5** $P(X) = X^4 + X^3 - X^2 + X - 2$ On doit choisir $a|a_0 = -2 \quad b|a_4 = 1$
On choisit $a = 1$ et $b = 1 \Rightarrow \alpha = 1$
On choisit $a = -2$ et $b = 1 \Rightarrow \alpha = -2$
$P(1) = P(-2) = 0$

$Q(X) = 2X^3 - 3X^2 + 3X - 1$ On doit choisir $a|a_0 = -1 \quad b|a_3 = 2$
On choisit $a = 1$ et $b = 2 \Rightarrow \alpha = \dfrac{1}{2}$
$P\left(\dfrac{1}{2}\right) = 0$

Théorème 3.3.5 Toutes les racines de Q
(considérées avec leur multiplicité) sont aussi des racines de $P \Leftrightarrow Q|P$

■ **Exemple 3.6** Soient $P(X) = X^{2n+1} + 1 \quad Q(X) = X + 1 \quad S(X) = (X+1)^2$
$Q(-1) = 0 \quad P(-1) = 0 \Rightarrow Q|P$
$P'(X) = (2n+1)X^{2n} \Rightarrow P'(-1) = (2n+1)(-1)^{2n} = 2n+1 \neq 0 \Rightarrow S$ ne divise pas P

3.4 Polynome irréductible - PGCD - PPCM

Définition 3.4.1 Soit $P \in \mathbb{K}[X]$
On dit que P est irréductible ssi tous ses diviseurs sont de la forme α ou αP

R

1. Dans $\mathbb{R}[X]$ Les polynômes irréductibles sont les polynômes de degré 1 et les polynômes de degré 2 avec $\Delta < 0$
2. Dans $\mathbb{C}[X]$ Les seuls polynômes irréductibles sont les polynômes de degré 1

■ **Exemple 3.7** $P(X) = X^2 + 1$ $\quad P$ est irreductible dans $\mathbb{R}$ $\quad P$ n'est pas irreductible dans $\mathbb{C}$

Définition 3.4.2 — PGCD-PPCM. Soient $P_1, P_2, \cdots, P_n$ n polynômes dans $\mathbb{K}[X] \setminus \{0\}$ et soit D, M deux polynômes dans $\mathbb{K}[X] \setminus \{0\}$
On dit que D est le plus grand commun diviseur de $P_1, P_2, \cdots, P_n$ et on note $D = pgcd(P_1, P_2, \cdots, P_n)$ ssi :

1. D est un polynôme unitaire.
2. $\forall i \in \{0, \cdots, n\}$ D divise P_i
3. $\forall i \in \{0, \cdots, n\}$ P divise $P_i \Rightarrow degP \leq degD$

On dit que M est le plus petit commun multiple de $P_1, P_2, \cdots, P_n$ et on note $M = ppcm(P_1, P_2, \cdots, P_n)$ ssi :

1. M est un polynôme unitaire.
2. $\forall i \in \{0, \cdots, n\}$ P_i divise M
3. $\forall i \in \{0, \cdots, n\}$ P_i divise $P \Rightarrow degP \geq degM$

■ **Exemple 3.8** $P(X) = 5(X-3)^2(X^2+1)$ $\quad Q(X) = -(X+1)^2(X-3)^3$
$R(X) = -(X-1)(X-3)^4$
$pgcd(P, Q, R) = (X-3)^2$ $\quad ppcm(P, Q, R) = (X-1)(X+1)^2(X-3)^4(X^2+1)$

R pgcd(P_1, P_2) est souvent noté $P_1 \wedge P_2$ de même que ppcm(P_1, P_2) est noté $P_1 \vee P_2$

■ **Exemple 3.9 — Algorithme d'Euclide.** $P(X) = X^2 - X - 2$ $\quad Q(X) = X^2 + 2X + 1$

$$\begin{array}{rrr|l}
X^2 & -X & -2 & X^2+2X+1 \\ \cline{4-4}
X^2 & +2X & 1 & \hfill 1 \\ \hline
 & -3X & -3 &
\end{array}
\qquad
\begin{array}{rrr|l}
X^2 & +2X & +1 & -3X-3 \\ \cline{4-4}
X^2 & +X & & -\frac{1}{3}X - \frac{1}{3} \\ \hline
 & X & +1 & \\
 & X & +1 & \\ \cline{2-3}
 & & \boxed{0} &
\end{array}$$

$$P \wedge Q = \frac{-3X-3}{-3} = X + 1$$

Théorème 3.4.1 Soient P et Q deux polynômes dans $\mathbb{K}[X] \setminus \{0\}$

$$(P \wedge Q)(P \vee Q) = N_{PQ} \text{ avec } N_{PQ} \text{ le polynôme normalisé de } PQ$$

■ **Exemple 3.10** $P(X) = X^2 - X - 2$ $\quad Q(X) = X^2 + 2X + 1$ $\quad P \wedge Q = X + 1$

$$\Rightarrow \frac{P(X)Q(X)}{P(X) \wedge Q(X)} = \frac{(X^2 - X - 2)(X^2 + 2X + 1)}{X + 1} = X^3 - 3X - 2$$
$$\Rightarrow P \vee Q = X^3 - 3X - 2$$

Définition 3.4.3 Soient $P_1, P_2, \cdots, P_n$ n polynômes dans $\mathbb{K}[X] \setminus \{0\}$ On dit que $P_1, P_2, \cdots, P_n$ sont premiers entre eux ssi $pgcd(P_1, P_2, \cdots, P_n) = 1$

Théorème 3.4.2 — Bézout. Soient $P_1, P_2, \cdots, P_n$ n polynômes dans $\mathbb{K}[X] \setminus \{0\}$

$$P_1, P_2, \cdots, P_n \text{ premiers entre eux} \Leftrightarrow \exists Q_1, Q_2, \cdots, Q_n \in \mathbb{K}[X] \text{ tel que } \sum_{i=1}^{n} P_i Q_i = 1$$

Théorème 3.4.3 — Gauss. Soient $P, Q, R \in \mathbb{K}[X] \setminus \{0\}$

$$(P \text{ divise } QR) \text{ et } (pgcd(P, Q) = 1) \Rightarrow (P \text{ divise } R)$$

3.5 Factorisation d'un polynôme dans $\mathbb{K}[X]$

Théorème 3.5.1 Tout polynôme P de $\mathbb{K}[X]$ se décompose en produit de polynômes irréductibles de $\mathbb{K}[X]$
Une telle décomposition s'appelle *factorisation* de P

R

$$P \in \mathbb{C}[X] \Rightarrow P(X) = \lambda (X - a_1)^{n_1} (X - a_2)^{n_2} \cdots (X - a_k)^{n_p}$$

$$P \in \mathbb{R}[X] \Rightarrow P(X) = \lambda (X - a_1)^{n_1} (X - a_2)^{n_2} \cdots (X - a_k)^{n_p} (X^2 + b_1 X + c_1)^{k_1}$$
$$(X^2 + b_2 X + c_2)^{k_2} \cdots (X^2 + b_q X + c_q)^{k_q} \text{ avec } \Delta_i = b_i^2 - 4c_i < 0$$

■ **Exemple 3.11** $P(X) = X^3 - X^2 + X - 1$
On commence par factoriser P sur $\mathbb{R}[X]$
$P(1) = 0 \Rightarrow X - 1$ divise P

$$\begin{array}{rrrr|l} X^3 & -X^2 & +X & -1 & X-1 \\ \cline{5-5} X^3 & -X^2 & & & X^2+1 \\ \hline & & X & -1 & \\ & & X & -1 & \\ \cline{3-4} & & & 0 & \end{array}$$

$P(X) = (X - 1)(X^2 + 1)$
P n'as pas la même factorisation sur $\mathbb{C}[X]$, en effet il reste à décomposer $X^2 + 1$
$X^2 + 1 = 0 \Rightarrow X^2 = -1 \Rightarrow X = i$ ou $X = -i \Rightarrow X^2 + 1 = (X + i)(X - i)$
$P(X) = (X - 1)(X + i)(X - i)$

■ **Exemple 3.12** $P(X) = X^4 + 1$
On commence par factoriser P sur $\mathbb{R}[X]$
$P(X) = X^4 + 1 = (X^4 + 2X^2 + 1) - 2X^2 = (X^2 + 1)^2 - 2X^2$
$\boxed{P(X) = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)}$
Ensuite, on factorise P sur $\mathbb{C}[X]$

$\Delta_1 = 2 - 4 = 2i^2 \Rightarrow \alpha_1 = \dfrac{-\sqrt{2} + \sqrt{2}i}{2} \qquad \alpha_2 = \dfrac{-\sqrt{2} - \sqrt{2}i}{2}$

$\Delta_2 = 2 - 4 = 2i^2 \Rightarrow \alpha_3 = \dfrac{\sqrt{2} + \sqrt{2}i}{2} \qquad \alpha_4 = \dfrac{\sqrt{2} - \sqrt{2}i}{2}$

$$P(X) = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4)$$

$$P(X)=\left(X+\frac{\sqrt{2}-\sqrt{2}i}{2}\right)\left(X+\frac{\sqrt{2}+\sqrt{2}i}{2}\right)\left(X-\frac{\sqrt{2}+\sqrt{2}i}{2}\right)\left(X-\frac{\sqrt{2}-\sqrt{2}i}{2}\right)$$

Définition 3.5.1 Un polynôme est dit scindé dans $\mathbb{K}[X]$ s'il peut s'écrire comme produit de polynômes de degré 1

■ **Exemple 3.13** X^4+1 est scindé dans $\mathbb{C}[X]$ mais n'est pas scindé dans $\mathbb{R}[X]$

Théorème 3.5.2 Tout polynôme est scindé dans $\mathbb{C}[X]$

3.6 Fractions rationnelles

Définition 3.6.1 On appelle fraction rationnelle toute expression de la forme :

$F=\frac{P}{Q}$ avec $P\in K[X]$ et $Q\in K[X]\setminus\{0\}$

L'ensemble des fractions rationnelles est noté $K(X)$

$deg(F)=deg(P)-deg(Q)$

■ **Exemple 3.14** $F(X)=\frac{X^2-3X+2}{X^3-2X+1}\Rightarrow deg(F)=2-3=-1$ ■

Définition 3.6.2 Soit $F\in K(X)$ une fraction rationnelle

On appelle forme irréductible de F le couple (A,B) avec $F=\frac{A}{B}$ et $A\wedge B=1$

■ **Exemple 3.15** $F(X)=\frac{X^2-3X+2}{X^3-2X+1}=\frac{P(X)}{Q(X)}$

On cherche les racines communes : $\alpha^2-3\alpha+2=0\Rightarrow\alpha_1=1$ et $\alpha_2=2$

$Q(1)=0$ et $Q(2)\neq 0\Rightarrow(X-1)$ divise P et Q

$\Rightarrow F(X)=\frac{(X-1)(X-2)}{(X-1)(X^2+X-1)}=\frac{X-2}{X^2+X-1}=\frac{A(X)}{B(X)}$ avec $A\wedge B=1$ ■

Définition 3.6.3 Soit $F=\frac{P}{Q}$ une fraction rationnelle avec $P\wedge Q=1$ et soit

α une racine de multiplicité n de Q alors, α est dite pôle de F de multiplicité n

■ **Exemple 3.16** $F(X)=\frac{X^2+1}{(X-2)^3}\Rightarrow\alpha=2$ est un pôle de F de multiplicité 3 ■

Définition 3.6.4 Soit $F=\frac{P}{Q}$ une fraction rationnelle avec $P\wedge Q=1$

On appelle partie entière de F le quotient de la division de P par Q

$$P=QE+R\Rightarrow\frac{P}{Q}=\frac{QE+R}{Q}=E+\frac{R}{Q}\text{ avec } degR<degQ$$

Si $degP<degQ$ alors $E(X)=0$

■ **Exemple 3.17** $F(X)=\frac{X^2+2X-1}{X+1}=\frac{(X+1)(X+1)-2}{X+1}=X+1-\frac{2}{X+1}$

La partie entière de F est donc $E(X)=X+1$ ■

3.6.1 Décomposition en éléments simples dans $\mathbb{R}(X)$

Définition 3.6.5 On appelle élément simple de $\mathbb{R}(X)$:

— Tous monôme de $\mathbb{R}[X]$

— Toute fraction rationnelle de la forme :

$$\frac{k}{(X-\alpha)^p} \text{ avec } k,\alpha \in \mathbb{R} \text{ et } p \in \mathbb{N}^* \quad \text{(élément simple de première espèce)}$$

— Toute fraction rationnelle de la forme :

$$\frac{aX+b}{(X^2+cX+d)^p} \text{ avec } k,\alpha \in \mathbb{R}, p \in \mathbb{N}^* \text{ et } c^2-4d<0 \quad \text{(élément simple de seconde espèce)}$$

Théorème 3.6.1 Toute fraction rationnelle s'écrit de manière unique comme la somme d'éléments simples de $\mathbb{R}(X)$

preuve :

Soit $F \in \mathbb{R}(X) \Rightarrow F(X) = \dfrac{P(X)}{Q(X)}$ $\quad P \wedge Q = 1$ avec :

$$Q(X) = \lambda(X-a_1)^{n_1}(X-a_2)^{n_2}\cdots(X-a_k)^{n_p}(X^2+b_1X+c_1)^{k_1}(X^2+b_2X+c_2)^{k_2}\cdots(X^2+b_qX+c_q)^{k_q}$$

avec $b_i^2-4c_i<0$

$$\frac{P(X)}{Q(X)} = E(X) + \left[\frac{\alpha_1}{X-a_1}+\frac{\alpha_2}{(X-a_1)^2}+\cdots+\frac{\alpha_{n_1}}{(X-a_1)^{n_1}}\right]+\cdots+\left[\frac{\beta_1}{X-a_k}+\frac{\beta_2}{(X-a_k)^2}+\cdots+\frac{\beta_{n_k}}{(X-a_k)^{n_p}}\right]$$
$$+\left[\frac{u_1X+v_1}{X^2+b_1X+c_1}+\frac{u_2X+v_2}{(X^2+b_1X+c_1)^2}+\cdots+\frac{u_{k_1}X+v_{k_1}}{(X^2+b_1X+c_1)^{k_1}}\right]+\cdots$$
$$+\left[\frac{s_1X+t_1}{X^2+b_qX+c_q}+\frac{s_2X+t_2}{(X^2+b_qX+c_q)^2}+\cdots+\frac{s_{k_q}X+t_{k_q}}{(X^2+b_qX+c_q)^{k_q}}\right]$$

■ **Exemple 3.18** Décomposer $F(X) = \dfrac{X^3}{X^2-X-2}$ en éléments simples dans $\mathbb{R}(X)$

$$\begin{array}{rrr|l}
X^3 & & & X^2-X-2 \\ \cline{4-4}
X^3 & -X^2 & -2X & X+1 \\ \cline{1-3}
 & X^2 & +2X & \\
 & X^2 & -X \quad -2 & \\ \cline{2-3}
 & & 3X \quad +2 &
\end{array}$$

$$X^3 = (X+1)(X^2-X-2)+(3X+2) \Rightarrow \frac{X^3}{X^2-X-2} = \frac{(X+1)(X^2-X-2)+3X+2}{X^2-X-2}$$
$$= X+1+\frac{3X+2}{X^2-X-2}$$

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

$$\Rightarrow \frac{3X+2}{X^2-X-2} = \frac{3X+2}{(X+1)(X-2)} = \frac{k_1}{X+1}+\frac{k_2}{X-2}$$

Calcul de k_1

$$\frac{3X+2}{(X+1)(X-2)}(X+1) = \frac{k_1}{X+1}(X+1)+\frac{k_2}{X-2}(X+1)$$
$$\Rightarrow \frac{3X+2}{X-2} = k_1+\frac{k_2(X+1)}{X-2}$$

$X=-1 \Rightarrow \dfrac{3(-1)+2}{(-1)-2}=k_1+\dfrac{k_2((-1)+1)}{(-1)-2} \Rightarrow \boxed{k_1=\dfrac{1}{3}}$

<u>Calcul de k_2</u>

$\dfrac{3X+2}{(X+1)(X-2)}(X-2)=\dfrac{k_1}{X+1}(X-2)+\dfrac{k_2}{X-2}(X-2)$

$\Rightarrow \dfrac{3X+2}{X+1}=\dfrac{k_1(X-2)}{X+1}+k_2$

$X=2 \Rightarrow \dfrac{3(2)+2}{2+1}=\dfrac{k_1(2-2)}{2+1}+k_2 \Rightarrow \boxed{k_2=\dfrac{8}{3}}$

Conclusion :

$$\boxed{\frac{X^3}{X^2-X-2}=X+1+\frac{1}{3(X+1)}+\frac{8}{3(X-2)}}$$

■ **Exemple 3.19** Décomposer $F(X)=\dfrac{X^2}{X^3-X^2+X-1}$ en éléments simples dans $\mathbb{R}(X)$

$X^3-X^2+X-1=(X^2+1)(X-1) \Rightarrow F=\dfrac{X^2}{(X^2+1)(X-1)}=\dfrac{aX+b}{X^2+1}+\dfrac{k_1}{X-1}$

<u>Calcul de k_1</u>

$\dfrac{X^2}{(X^2+1)(X-1)}(X-1)=\dfrac{aX+b}{X^2+1}(X-1)+\dfrac{k_1}{X-1}(X-1)$

$\Rightarrow \dfrac{X^2}{X^2+1}=\dfrac{aX+b}{X^2+1}(X-1)+k_1$

$X=1 \Rightarrow \dfrac{1^2}{1^2+1}=\dfrac{a+b}{1^2+1}(1-1)+k_1 \Rightarrow \boxed{k_1=\dfrac{1}{2}}$

<u>Calcul de a,b</u>

$\dfrac{X^2}{(X^2+1)(X-1)}(X^2+1)=\dfrac{aX+b}{X^2+1}(X^2+1)+\dfrac{k_1}{X-1}(X^2+1)$

$\Rightarrow \dfrac{X^2}{X-1}=(aX+b)+\dfrac{k_1}{X-1}(X^2+1)$

$X=i \Rightarrow \dfrac{i^2}{i-1}=(ai+b)+\dfrac{k_1}{i-1}(i^2+1) \Rightarrow \dfrac{1}{2}+\dfrac{1}{2}i=ai+b \Rightarrow a=b=\dfrac{1}{2}$

Conclusion :

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

■ **Exemple 3.20** Décomposer $F(X)=\dfrac{X^4+2}{X^2(X^2+1)^2}$ en éléments simples dans $\mathbb{R}(X)$

$F(X)=\dfrac{X^4+2}{X^2(X^2+1)^2}=\dfrac{k_1}{X}+\dfrac{k_2}{X^2}+\dfrac{a_1X+b_1}{X^2+1}+\dfrac{a_2X+b_2}{(X^2+1)^2}$

On remarque que $F(X)=F(-X)$ avec :

$F(-X)=\dfrac{-k_1}{X}+\dfrac{k_2}{X^2}+\dfrac{-a_1X+b_1}{X^2+1}+\dfrac{-a_2X+b_2}{(X^2+1)^2}$

Par identification, $k_1=-k_1 \quad a_1=-a_1 \quad a_2=-a_2 \Rightarrow k_1=a_1=a_2=0$

$$F(X) = \frac{k_2}{X^2} + \frac{b_1}{X^2+1} + \frac{b_2}{(X^2+1)^2}$$

Calcul de k_2

$$\frac{X^4+2}{X^2(X^2+1)^2}X^2 = \frac{k_2}{X^2}X^2 + \frac{b_1}{X^2+1}X^2 + \frac{b_2}{(X^2+1)^2}X^2$$

$$\Rightarrow \frac{X^4+2}{(X^2+1)^2} = k_2 + \frac{b_1}{X^2+1}X^2 + \frac{b_2}{(X^2+1)^2}X^2$$

$$X = 0 \Rightarrow \boxed{k_2 = 2}$$

Calcul de b_2

$$\frac{X^4+2}{X^2(X^2+1)^2}(X^2+1)^2 = \frac{k_2}{X^2}(X^2+1)^2 + \frac{b_1}{X^2+1}(X^2+1)^2 + \frac{b_2}{(X^2+1)^2}(X^2+1)^2$$

$$\Rightarrow \frac{X^4+2}{X^2} = \frac{k_2}{X^2}(X^2+1)^2 + b_1(X^2+1) + b_2$$

$$X = i \Rightarrow \frac{i^4+2}{i^2} = b_2 \Rightarrow \boxed{b_2 = -3}$$

$$\frac{X^4+2}{X^2(X^2+1)^2} = \frac{2}{X^2} + \frac{b_1}{X^2+1} - \frac{3}{(X^2+1)^2}$$

Calcul de b_1

$$X = 1 \Rightarrow \frac{1^4+2}{1^2(1^2+1)^2} = \frac{2}{1^2} + \frac{b_1}{1^2+1} - \frac{3}{(1^2+1)^2} \Rightarrow \frac{3}{4} = 2 + \frac{b_1}{2} - \frac{3}{4}$$

$$\Rightarrow b_1 = 2\left(\frac{3}{4} - 2 + \frac{3}{4}\right) \Rightarrow \boxed{b_1 = -1}$$

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

3.7 série d'exercices

Exercice 1 Résoudre dans $\mathbb{R}[X]$ l'équation suivante :

$$P(X^2) = (X^2+1)P(X)$$

Exercice 2 Trouver le reste de la division du polynôme P par Q

$$P(X) = X^n + (X-1)^n + 1 \qquad Q(X) = X^2 - X$$

$$P(X) = (X sin\theta + cos\theta)^n \text{ avec } n \in \mathbb{N}, \theta \in \mathbb{R} \qquad Q(X) = Q(X) = X^2+1$$

Exercice 3 Soient $\alpha, \beta, \gamma, \delta \in \mathbb{N}$ et $n \in \mathbb{N}^*$ Montrer que Q divise P

$$P(X) = X^{4\alpha+3} + X^{4\beta+2} + X^{4\gamma+1} + X^{4\delta} \qquad Q(X) = X^3 + X^2 + X + 1$$

$$P(X) = nX^{n+1} - (n+1)X^n + 1 \qquad Q(X) = (X-1)^2$$

Exercice 4 Soit $P_n(X) = (X^4+1)^n - X^n$ et soit $Q(X) = X^2 + X + 1$

Pour quelles valeurs de $n \in \mathbb{N}$ $\quad P_n$ est-il divisible par Q

Exercice 5 Pour $n \in \mathbb{N}^*$ quel est l'ordre de multiplicité de 2 comme racine du polynôme :

$$P(X) = nX^{n+2} - (4n+1)X^{n+1} + 4(n+1)X^n - 4X^{n-1}$$

Exercice 6 Déterminer $P \wedge Q$ et $P \vee Q$

$$P(X) = -2X^4 + 2X^3 + 2X - 2 \qquad Q(X) = 3X^3 + 9X^2 + 9X + 6$$

$$P(X) = X^3 + X^2 - 5X + 3 \qquad Q(X) = 2X^3 - 3X^2 + 1$$

$$P(X) = X^n - 1 \qquad Q(X) = (X-1)^n \quad n \geq 1$$

Exercice 7 Soient $P(X) = X^4 + 1$ et $Q(X) = X^3 + 1$

1. Déterminer $U, V \in \mathbb{R}[X]$ tels que : $UP + VQ = 1$
2. En déduire que $U \wedge V = 1$

Exercice 8 Factoriser les polynômes suivants dans $\mathbb{R}[X]$ puis dans $\mathbb{C}[X]$

1. $P_1(X) = X^3 + 4X^2 + 4X + 3$
2. $P_2(X) = X^3 - X^2 - 8X + 12$
3. $P_3(X) = (X^2 - X + 2)^2 + (X - 2)^2$

En déduire $P_1 \wedge P_2$ et $P_1 \vee P_2$ puis $pgcd(P_1, P_2, P_3)$ et $ppcm(P_1, P_2, P_3)$

Exercice 9 Soient $P_a(X) = X(X+a)(X+2a)(X+3a) + a^4$ avec $a \in \mathbb{R}$

1. Montrer que P_a est le carré d'un polynôme
2. En déduire la factorisation du polynôme $Q(X) = X(X+1)(X+2)(X+3) - 8$ dans $\mathbb{R}[X]$ puis dans $\mathbb{C}[X]$

Exercice 10 Décomposer les fractions rationnelles suivantes dans $\mathbb{R}(X)$

$$A = \frac{X^3+1}{(X-1)^3} \qquad B = \frac{3}{(X^3-1)^2} \qquad C = \frac{1}{X^3(X-2)^3} \qquad D = \frac{X^3}{X^4+X^2+1}$$

3.8 Corrigé de la série d'exercices

Exercice 1 Résoudre dans $\mathbb{R}[X]$ l'équation suivante :

$$P(X^2) = (X^2+1)P(X)$$

$deg(P) = k \Rightarrow P(X) = a_kX^k + a_{k-1}X^{k-1} + \cdots + a_0$ avec $a_k \neq 0$
$\Rightarrow P(X^2) = a_kX^{2k} + a_{k-1}X^{2k-2} + \cdots + a_0 \Rightarrow deg(P(X^2)) = 2k$
$deg[(X^2+1)P(X)] = k+2$
$P(X^2) = (X^2+1)P(X) \Rightarrow 2k = k+2 \Rightarrow k = 2$
$P(X) = a_0 + a_1X + a_2X^2 \Rightarrow P(X^2) = a_0 + a_1X^2 + a_2X^4$

$$\begin{aligned} P(X^2) = (X^2+1)P(X) \Rightarrow a_0 + a_1X^2 + a_2X^4 &= (X^2+1)(a_0 + a_1X + a_2X^2) \\ &= a_0X^2 + a_1X^3 + a_2X^4 + a_0 + a_1X + a_2X^2 \end{aligned}$$

$\Rightarrow a_1X^3 + (a_0 - a_1 + a_2)X^2 + a_1X = 0$
$\Rightarrow (a_1 = 0)$ et $(a_0 - a_1 + a_2 = 0)$
$\Rightarrow (a_1 = 0)$ et $(a_0 = -a_2)$
$P(X) = a_0 + a_1X + a_2X^2 \Rightarrow P(X) = -a_2 + a_2X^2 = a_2(-1+X^2)$ avec $a_2 \in \mathbb{R}$

■

Exercice 2 Trouver le reste de la division du polynôme A par B

1) $A(X) = (X sin\theta + cos\theta)^n$ avec $n \geq 2, \theta \in \mathbb{R}$ $\qquad B(X) = X^2+1$

2) $A(X) = X^n + (X-1)^n + 1$ $\qquad B(X) = X^2 - X$

1. $A(X) = Q(X)B(X) + R(X)$ avec $deg(R) < 2 \Rightarrow R(X) = a_0 + a_1X$
   $B(X) = X^2 + 1 = 0 \Rightarrow X^2 = -1 \Rightarrow X = i$ ou $X = -i$
   $A(i) = Q(i)B(i) + R(i) \Rightarrow A(i) = R(i)$
   $A(i) = (isin\theta + cos\theta)^n = cos n\theta + i sin n\theta$
   $\Rightarrow cos n\theta + i sin n\theta = a_0 + a_1 i \Rightarrow a_0 = cos n\theta$ et $a_1 = sin n\theta$
   $\Rightarrow R(X) = cos n\theta + sin n\theta X$
2. $A(X) = Q(X)B(X) + R(X)$ avec $deg(R) < 2 \Rightarrow R(X) = a_0 + a_1X$
   $B(X) = X^2 - X = 0 \Rightarrow X(X-1) = 0 \Rightarrow X = 0$ ou $X = 1$
   $A(0) = Q(0)B(0) + R(0) \Rightarrow A(0) = R(0)$
   $A(0) = 0^n + (0-1)^n + 1 = (-1)^n + 1 = a_0 \Rightarrow R(X) = ((-1)^n + 1) + a_1X$
   $A(1) = Q(1)B(1) + R(1) \Rightarrow A(1) = R(1)$
   $A(1) = 1^n + (1-1)^n + 1 = 2 = ((-1)^n + 1) + a_1 \Rightarrow a_1 = 2 - ((-1)^n + 1) = 1 - (-1)^n$
   $R(X) = ((-1)^n + 1) + (1 - (-1)^n)X$
   n pair $\Rightarrow n = 2k \Rightarrow R(X) = 2$
   n impair $\Rightarrow n = 2k+1 \Rightarrow R(X) = 2X$

■

Exercice 3 Soient $\alpha, \beta, \gamma, \delta \in \mathbb{N}$ et $n \in \mathbb{N}^*$ Montrer que Q divise P

1) $P(X) = X^{4\alpha+3} + X^{4\beta+2} + X^{4\gamma+1} + X^{4\delta}$ $\qquad Q(X) = X^3 + X^2 + X + 1$

2) $P(X) = nX^{n+1} - (n+1)X^n + 1$ $\qquad Q(X) = (X-1)^2$

1. $Q(X) = X^3 + X^2 + X + 1$
   Cherchons les racines de Q

$Q(-1) = 0 \Rightarrow Q(X) = (X+1)(X^2+1)$

$$\begin{array}{cccc|c} X^3 & +X^2 & +X & +1 & X+1 \\ \cline{5-5} X^3 & +X^2 & & & X^2+1 \\ \cline{1-4} & & X & +1 & \\ & & X & +1 & \\ \cline{3-4} & & & 0 & \end{array}$$

$X^2+1 = 0 \Rightarrow X^2 = -1 \Rightarrow X = i$ ou $X = -i$
Donc Q possède trois racines $-i, 0, i$
Pour que Q divise P il faut que $P(-i) = P(0) = P(i) = 0$
$P(0) = 0^{4\alpha+3} + 0^{4\beta+2} + 0^{4\gamma+1} + 0^{4\delta} = 0$
$P(i) = i^{4\alpha+3} + i^{4\beta+2} + i^{4\gamma+1} + i^{4\delta} = -i - 1 + i + 1 = 0$
$P \in \mathbb{R}[X] \Rightarrow P(-i) = 0$
Donc Q divise P

2. $Q(X) = (X-1)^2 = 0 \Rightarrow X = 1$
Pour que Q divise P il faut que 1 soit une racine double de P
$P(1) = n - (n+1) + 1 = 0$
$P'(X) = n(n+1)X^n - n(n+1)X^{n-1} \Rightarrow P'(1) = 0$
Donc Q divise P

■

Exercice 4 Soit $P_n(X) = (X^4+1)^n - X^n$ et soit $Q(X) = X^2+X+1$

Pour quelles valeurs de $n \in \mathbb{N}$ $\quad P_n$ est-il divisible par Q
Cherchons les racines de Q
$X^2+X+1 = 0 \quad \Delta = 1-4 = 3i^2 \Rightarrow \alpha_1 = \dfrac{-1+\sqrt{3}i}{2} = e^{i\frac{2\pi}{3}}$ et $\alpha_2 = \dfrac{-1-\sqrt{3}i}{2} = -e^{i\frac{\pi}{3}}$

$$\begin{aligned} P_n(e^{i\frac{2\pi}{3}}) &= ([e^{i\frac{2\pi}{3}}]^4+1)^n - [e^{i\frac{2\pi}{3}}]^n \\ &= ([e^{i\frac{8\pi}{3}}]+1)^n - [e^{i\frac{2n\pi}{3}}] \\ &= ([e^{i\frac{\pi}{3}}])^n - [e^{i\frac{2n\pi}{3}}] \\ &= [e^{i\frac{n\pi}{3}}] - [e^{i\frac{2n\pi}{3}}] \\ &= e^{i\frac{n\pi}{3}}(1 - e^{i\frac{n\pi}{3}}) \end{aligned}$$

$P_n(e^{i\frac{2\pi}{3}}) = 0 \Rightarrow (e^{i\frac{n\pi}{3}} = 0)$ ou $(1 - e^{i\frac{n\pi}{3}} = 0)$

$e^{i\frac{n\pi}{3}} = 0 \Rightarrow cos\dfrac{n\pi}{3} + i\,sin\dfrac{n\pi}{3} = 0 \Rightarrow cos\dfrac{n\pi}{3} = 0$ et $sin\dfrac{n\pi}{3} = 0$
$cos\dfrac{n\pi}{3} = 0 \Rightarrow cos\dfrac{n\pi}{3} = cos(\dfrac{\pi}{2}+k\pi) \Rightarrow \dfrac{n\pi}{3} = \dfrac{\pi}{2}+k\pi \Rightarrow n = \dfrac{3}{2}+3k \Rightarrow n \notin \mathbb{N}$
Donc, $e^{i\frac{n\pi}{3}} \neq 0$
$1 - e^{i\frac{n\pi}{3}} = 0 \Rightarrow 1 - \left(cos\dfrac{n\pi}{3} + i\,sin\dfrac{n\pi}{3}\right) = 0 \Rightarrow \left[1 - cos\dfrac{n\pi}{3} = 0\right]$ et $\left[sin\dfrac{n\pi}{3} = 0\right]$
$1 - cos\dfrac{n\pi}{3} = 0 \Rightarrow cos\dfrac{n\pi}{3} = 1 \Rightarrow cos\dfrac{n\pi}{3} = cos(2k\pi) \Rightarrow \dfrac{n\pi}{3} = 2k\pi \Rightarrow \boxed{n = 6k \text{ avec } k \in \mathbb{Z}}$
$sin\dfrac{n\pi}{3} = 0 \Rightarrow sin\dfrac{n\pi}{3} = sin(k\pi) \Rightarrow \dfrac{n\pi}{3} = k\pi \Rightarrow \boxed{n = 3k \text{ avec } k \in \mathbb{Z}}$
$S_1 = \{n = 6k \text{ avec } k \in \mathbb{Z}\} = \{\cdots, -12, -6, 0, 6, 12, \cdots\}$
$S_2 = \{n = 3k \text{ avec } k \in \mathbb{Z}\} = \{\cdots, -6, -3, 0, 3, 6, \cdots\}$

$S = S_1 \cap S_2 = \{n = 6k \text{ avec } k \in \mathbb{Z}\}$
$P_n(\alpha_1) = 0 \Leftrightarrow n = 6k \text{ avec } k \in \mathbb{Z}$
$P_n(\alpha_2) = P_n(\overline{\alpha_1}) = P_n(\alpha_1) = 0$
Conclusion :

$$P_n \text{ est divisible par } Q \Leftrightarrow n = 6k \text{ avec } k \in \mathbb{Z}$$

■

Exercice 5 Pour $n \in \mathbb{N}^*$ quel est l'ordre de multiplicité de 2 comme racine du polynôme :

$$P(X) = nX^{n+2} - (4n+1)X^{n+1} + 4(n+1)X^n - 4X^{n-1}$$

$$\begin{array}{rcl}
P(2) & = & n2^{n+2} - (4n+1)2^{n+1} + 4(n+1)2^n - 4(2^{n-1}) \\
 & = & 4n2^n - 2(4n+1)2^n + 4(n+1)2^n - 2(2^n) = 0 \\
P'(X) & = & n(n+2)X^{n+1} - (4n+1)(n+1)X^n + 4n(n+1)X^{n-1} - 4(n-1)X^{n-2} \\
P'(2) & = & n(n+2)2^{n+1} - (4n+1)(n+1)2^n + 4n(n+1)2^{n-1} - 4(n-1)2^{n-2} \\
 & = & 2n(n+2)2^n - (4n+1)(n+1)2^n + 2n(n+1)2^n - (n-1)2^n = 0 \\
P^{(2)}(X) & = & n(n+1)(n+2)X^n - (4n+1)(n+1)nX^{n-1} + 4n(n+1)(n-1)X^{n-2} \\
 & & -4(n-1)(n-2)X^{n-3} \\
P^{(2)}(2) & = & n(n+1)(n+2)2^n - (4n+1)(n+1)n2^{n-1} + 4n(n+1)(n-1)2^{n-2} \\
 & & -4(n-1)(n-2)2^{n-3} \\
 & = & 8n(n+1)(n+2)2^{n-3} - 4(4n+1)(n+1)n2^{n-3} + 8n(n+1)(n-1)2^{n-3} \\
 & & -4(n-1)(n-2)2^{n-3} \\
 & = & [8n(n+1)(n+2) - 4(4n+1)(n+1)n + 8n(n+1)(n-1) - 4(n-1)(n-2)]\,2^{n-3} \\
 & \neq & 0
\end{array}$$

$P^{(2)}(2) \neq 0 \Rightarrow mult(2) = 2$ ■

Exercice 6 Déterminer $P \wedge Q$ et $P \vee Q$

$$P(X) = -2X^4 + 2X^3 + 2X - 2 \qquad Q(X) = 3X^3 + 9X^2 + 9X + 6$$

$$\begin{array}{rrrrr|l}
X^4 & -X^3 & & -X & +1 & X^3+3X^2+3X+2 \\ \cline{6-6}
X^4 & +3X^3 & +3X^2 & +2X & & \qquad\qquad X-4 \\ \cline{1-5}
 & -4X^3 & -3X^2 & -3X & +1 & \\
 & -4X^3 & -12X^2 & -12X & -8 & \\ \cline{3-5}
 & & 9X^2 & +9X & +9 &
\end{array}$$

$$\begin{array}{rrrr|l}
X^3 & +3X^2 & +3X & +2 & X^2+X+1 \\ \cline{5-5}
X^3 & +X^2 & +X & & \qquad X+2 \\ \cline{1-4}
 & 2X^2 & +2X & +2 & \\
 & 2X^2 & +2X & +2 & \\ \cline{2-4}
 & & & 0 &
\end{array}$$

Le pgcd est le polynôme normalisé du dernier reste non nul.
Donc, $P \wedge Q = X^2 + X + 1$

$$\begin{aligned}
\frac{P(X)Q(X)}{P \wedge Q} &= \frac{(-2X^4+2X^3+2X-2)(3X^3+9X^2+9X+6)}{X^2+X+1}\\
&= 3(-2X^4+2X^3+2X-2)(X+2)\\
&= -6(X^4+X^3+X-1)(X+2)
\end{aligned}$$

$\Rightarrow P \vee Q = (X^4+X^3+X-1)(X+2)$

$$P(X) = X^3 + X^2 - 5X + 3 \qquad Q(X) = 2X^3 - 3X^2 + 1$$

$$\begin{array}{rrrr|l}
X^3 & +X^2 & -5X & +3 & 2X^3-3X^2+1\\
\cline{5-5}
X^3 & -\frac{3}{2}X^2 & & +\frac{1}{2} & \frac{1}{2}\\
\hline
& \frac{5}{2}X^2 & -5X & +\frac{5}{2} &
\end{array}
\qquad
\begin{array}{rrrr|l}
2X^3 & -3X^2 & & +1 & X^2-2X+1\\
\cline{5-5}
2X^3 & -4X^2 & +2X & & 2X+1\\
\hline
& X^2 & -2X & +1 &\\
& X^2 & -2X & +1 &\\
\cline{2-4}
& & & 0 &
\end{array}$$

Le pgcd est le polynôme normalisé du dernier reste non nul.
Donc, $P \wedge Q = X^2 - 2X + 1$

$$\begin{aligned}
\frac{P(X)Q(X)}{P \wedge Q} &= \frac{(X^3+X^2-5X+3)(2X^3-3X^2+1)}{X^2-2X+1}\\
&= (X^3+X^2-5X+3)(2X+1)\\
&= 2(X+\frac{1}{2})(X^3+X^2-5X+3)
\end{aligned}$$

$\Rightarrow P \vee Q = \left(X + \frac{1}{2}\right)(X^3+X^2-5X+3)$

$$P(X) = X^n - 1 \qquad Q(X) = (X-1)^n \quad n \geq 1$$

Tout les diviseurs de Q sont de la forme $k(X-1)^p$ avec $p \leq n$
$P(1) = 0 \Rightarrow (X-1)$ divise P
$P'(X) = nX^{n-1} \Rightarrow P'(1) = n \neq 0 \Rightarrow (X-1)^2$ ne divise pas P
On en conclut que $P \wedge Q = X - 1$

$$P \vee Q = \frac{P(X)Q(X)}{P \wedge Q} = \frac{(X^n-1)(X-1)^n}{X-1} = (X^n-1)(X-1)^{n-1}$$ ■

Exercice 7 Soient $P(X) = X^4 + 1$ et $Q(X) = X^3 + 1$

1. Déterminer $U, V \in \mathbb{R}[X]$ tels que : $UP + VQ = 1$

$$
\begin{array}{ccc|c}
X^4 & & +1 & X^3+1 \\ \cline{4-4}
X^4 & +X & & X \\ \cline{1-3}
 & -X & +1 &
\end{array}
\qquad
\begin{array}{cccc|c}
X^3 & & & +1 & -X+1 \\ \cline{5-5}
X^3 & -X^2 & & & -X^2-X-1 \\ \cline{1-4}
 & X^2 & & +1 & \\
 & X^2 & -X & & \\ \cline{2-4}
 & & X & +1 & \\
 & & X & -1 & \\ \cline{2-4}
 & & & 2 &
\end{array}
$$

$$
\begin{array}{cc|c}
-X & +1 & 2 \\ \cline{3-3}
-X & +1 & \frac{-1}{2}(X-1) \\ \hline
 & 0 &
\end{array}
$$

$$
\begin{array}{rcl}
X^3+1=(-X+1)(-X^2-X-1)+2 \Rightarrow\ 2 & = & (X^3+1)-(-X+1)(-X^2-X-1) \\
 & = & (X^3+1)+(-X+1)(X^2+X+1) \quad (*) \\
X^4+1=(X^3+1)X+(-X+1) \Rightarrow\ -X+1 & = & (X^4+1)-(X^3+1)X
\end{array}
$$

En remplaçant $-X+1$ dans $(*)$ on obtient :

$$
\begin{array}{rcl}
2 & = & (X^3+1)+[(X^4+1)-(X^3+1)X](X^2+X+1) \\
\Rightarrow 2 & = & (X^2+X+1)(X^4+1)+[1-X(X^2+X+1)](X^3+1) \\
\Rightarrow 1 & = & \dfrac{1}{2}(X^2+X+1)(X^4+1)+\dfrac{1}{2}(1-X^3-X^2-X)(X^3+1) \\
\Rightarrow 1 & = & UP+VQ \qquad \text{avec :}
\end{array}
$$

$U(X)=\dfrac{1}{2}(X^2+X+1)$ et $V(X)=\dfrac{1}{2}(1-X^3-X^2-X)$

2. En déduire que $P\wedge Q=1$
   D'après le lemme de Bézout, $P\wedge Q=1$

■

Exercice 8 Factoriser les polynômes suivants dans $\mathbb{R}[X]$ puis dans $\mathbb{C}[X]$

$P_1(X)=X^3+4X^2+4X+3$

$P_1(-3)=0 \Rightarrow X+3$ divise P_1

$$
\begin{array}{cccc|c}
X^3 & +4X^2 & +4X & +3 & X+3 \\ \cline{5-5}
X^3 & +3X^2 & & & X^2+X+1 \\ \cline{1-4}
 & X^2 & +4X & +3 & \\
 & X^2 & +3X & & \\ \cline{2-4}
 & & X & +3 & \\
 & & X & +3 & \\ \cline{3-4}
 & & & 0 &
\end{array}
$$

$P_1(X)=(X+3)(X^2+X+1)$

$\Delta=1-4(1)=-3<0 \Rightarrow X^2+X+1$ est irreductible dans $\mathbb{R}[X]$

Donc la factorisation de P_1 sur $\mathbb{R}[X]$ donne $P_1(X)=(X+3)(X^2+X+1)$

Il reste à décomposer X^2+X+1 sur $\mathbb{C}[X]$

$\Delta=1-4(1)=-3=3i^2 \Rightarrow X^2+X+1=(X+\frac{1+\sqrt{3}i}{2})(X+\frac{1-\sqrt{3}i}{2})$

$P_1(X)=(X+3)(X+\frac{1+\sqrt{3}i}{2})(X+\frac{1-\sqrt{3}i}{2})$

$P_2(X) = X^3 - X^2 - 8X + 12$

$P_2(2) = 0 \Rightarrow X - 2$ divise P_2

$$\begin{array}{rrrr|l} X^3 & -X^2 & -8X & +12 & \quad X-2 \\ \cline{5-5} X^3 & -2X^2 & & & X^2+X-6 \\ \cline{1-4} & X^2 & -8X & +12 & \\ & X^2 & -2X & & \\ \cline{2-4} & & -6X & +12 & \\ & & -6X & +12 & \\ \cline{3-4} & & & 0 & \end{array}$$

$P_2(X) = (X-2)(X^2+X-6)$

$\Delta = 1 - 4(-6) = 25 \Rightarrow X^2+X-6 = (X-2)(X+3)$

$P_2(X) = (X-2)^2(X+3)$

$$\begin{aligned} P_3(X) &= (X^2-X+2)^2 + (X-2)^2 \\ &= (X^2-X+2)^2 - i^2(X-2)^2 \\ &= (X^2-X+2+(X-2)i)(X^2-X+2-(X-2)i) \\ &= (X^2+(-1+i)X+2-2i)(X^2-(1+i)X+2+2i) \end{aligned}$$

$\Delta_1 = (-1+i)^2 - 4(2-2i) = -8+6i = (1+3i)^2$

$\alpha_1 = \dfrac{1}{2}(1-i+1+3i) = 1+i \quad \alpha_2 = \dfrac{1}{2}(1-i-(1+3i)) = -2i$

$X^2 + (-1+i)X + (2-2i) = [X-(1+i)]\,(X+2i) = (X-1-i)(X+2i)$

Comme les coefficients des deux polynômes sont conjugués alors les racines de $X^2-(1+i)X+(2+2i)$ sont $\overline{\alpha_1}$ et $\overline{\alpha_2}$ d'où :

$X^2-(1+i)X+(2+2i) = (X-1+i)(X-2i)$

Donc, la factorisation de P_3 sur $\mathbb{C}[X]$ donne :

$P_3(X) = (X-1-i)(X+2i)(X-1+i)(X-2i)$

Pour trouver la factorisation de P_3 sur $\mathbb{R}[X]$ il suffit de multiplier les polynômes dont les coefficients sont conjugués :

$(X-1-i)(X-1+i) = X^2-2X+2$ et $(X+2i)(X-2i) = X^2+4$ ce qui donne :

$P_3(X) = (X^2-2X+2)(X^2+4)$

En déduire $P_1 \wedge P_2$ et $P_1 \vee P_2$ puis $pgcd(P_1,P_2,P_3)$ et $ppcm(P_1,P_2,P_3)$

$P_1 \wedge P_2 = X+3 \qquad P_1 \vee P_2 = (X^2+X+1)(X-2)^2(X+3)$

$pgcd(P_1,P_2,P_3) = 1$

$ppcm(P_1,P_2,P_3) = (X^2+X+1)(X-2)^2(X+3)(X^2-2X+2)(X^2+4)$

■

Exercice 9 Soient $P_a(X) = X(X+a)(X+2a)(X+3a) + a^4$ avec $a \in \mathbb{R}$

1. Montrer que P_a est le carré d'un polynôme

$$\begin{aligned} P_a(X) = X(X+a)(X+2a)(X+3a)+a^4 &= (X+a)(X+2a)X(X+3a)+a^4 \\ &= (X^2+3aX+2a^2)(X^2+3aX)+a^4 \\ &= (X^2+3aX)^2+2a^2(X^2+3aX)+(a^2)^2 \\ &= (X^2+3aX+a^2)^2 \end{aligned}$$

2. En déduire la factorisation du polynôme $Q(X) = X(X+1)(X+2)(X+3) - 8$ dans $\mathbb{R}[X]$ puis dans $\mathbb{C}[X]$

   $a = 1 \Rightarrow P_1(X) = X(X+1)(X+2)(X+3)+1 = (X^2+3X+1)^2$

$$\begin{aligned} Q(X)=X(X+1)(X+2)(X+3)-8 &= [X(X+1)(X+2)(X+3)+1]-9\\ &= (X^2+3X+1)^2-9\\ &= (X^2+3X+1+3)(X^2+3X+1-3)\\ &= (X^2+3X+4)(X^2+3X-2)\end{aligned}$$

$\Delta_1 = 3^2-4(4) = -7<0 \Rightarrow X^2+3X+4$ est irréductible dans $\mathbb{R}[X]$

$$\begin{aligned}\Delta_2 = 3^2-4(-2)=17 \Rightarrow X^2+3X-2 &= \left(X-\left(\tfrac{-3+\sqrt{17}}{2}\right)\right)\left(X-\left(\tfrac{-3-\sqrt{17}}{2}\right)\right)\\ &= \left(X+\tfrac{3-\sqrt{17}}{2}\right)\left(X+\tfrac{3+\sqrt{17}}{2}\right)\end{aligned}$$

Donc, $Q(X) = (X^2+3X+4)\left(X+\tfrac{3-\sqrt{17}}{2}\right)\left(X+\tfrac{3+\sqrt{17}}{2}\right)$

Il reste à factoriser X^2+3X+4 dans dans $\mathbb{C}[X]$

$$\begin{aligned}\Delta_1 = 3^2-4(4) = -7 = 7i^2 \Rightarrow X^2+3X+4 &= \left(X-\left(\tfrac{-3+\sqrt{7}i}{2}\right)\right)\left(X-\left(\tfrac{-3-\sqrt{7}i}{2}\right)\right)\\ &= \left(X+\tfrac{3-\sqrt{7}i}{2}\right)\left(X+\tfrac{3+\sqrt{7}i}{2}\right)\end{aligned}$$

$$Q(X) = \left(X+\tfrac{3-\sqrt{7}i}{2}\right)\left(X+\tfrac{3+\sqrt{7}i}{2}\right)\left(X+\tfrac{3-\sqrt{17}}{2}\right)\left(X+\tfrac{3+\sqrt{17}}{2}\right)$$

■

Exercice 10 Décomposer les fractions rationnelles suivantes dans $\mathbb{R}(X)$

$$A=\frac{X^3+1}{(X-1)^3} \qquad B=\frac{3}{(X^3-1)^2} \qquad C=\frac{1}{X^3(X-2)^3} \qquad D=\frac{X^3}{X^4+X^2+1}$$

■

$$A(X)=\frac{X^3+1}{(X-1)^3}$$

$$\begin{array}{rrrr|l} X^3 & & & +1 & X-1 \\ \cline{5-5} X^3 & -X^2 & & & X^2+X+1 \\ \hline & X^2 & & +1 & \\ & X^2 & -X & & \\ \cline{2-4} & & X & +1 & \\ & & X & -1 & \\ \cline{3-4} & & & 2 & \end{array}$$

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

$$\begin{array}{rrr|l} X^2 & +X & +1 & X-1 \\ \cline{4-4} X^2 & -X & & X+2 \\ \hline & 2X & +1 & \\ & 2X & -2 & \\ \hline & & 3 & \end{array}$$

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

$$\begin{array}{rr|l} X & +2 & X-1 \\ \cline{3-3} X & -1 & 1 \\ \hline & 3 & \end{array}$$

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

$$\boxed{A(X)=\frac{X^3+1}{(X-1)^3} = 1+\frac{3}{X-1}+\frac{3}{(X-1)^2}+\frac{2}{(X-1)^3}}$$

$B(X) = \dfrac{3}{(X^3-1)^2}$

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

$$\begin{aligned} B(X) &= \frac{3}{(X-1)^2(X^2+X+1)^2} \\ &= \frac{k_1}{(X-1)} + \frac{k_2}{(X-1)^2} + \frac{aX+b}{(X^2+X+1)} + \frac{cX+d}{(X^2+X+1)^2} \end{aligned}$$

<u>Calcul de k_2</u>

$$(X-1)^2 B(X) = \frac{3}{(X^2+X+1)^2} = k_1(X-1) + k_2 + (X-1)^2 \left[\frac{aX+b}{(X^2+X+1)} + \frac{cX+d}{(X^2+X+1)^2}\right] \quad (*)$$

$X = 1 \Rightarrow \boxed{k_2 = \dfrac{1}{3}}$

Calcul de k_1

On dérive $(*)$

$$\begin{aligned}
\left[\frac{3}{(X^2+X+1)^2}\right]' &= \frac{-6(2X+1)}{(X^2+X+1)^3} \\
&= k_1+(X-1)^2\left[\frac{aX+b}{(X^2+X+1)}+\frac{cX+d}{(X^2+X+1)^2}\right]' \\
&\quad +2(X-1)\left[\frac{aX+b}{(X^2+X+1)}+\frac{cX+d}{(X^2+X+1)^2}\right]
\end{aligned}$$

$X=1 \Rightarrow \boxed{k_1=\dfrac{-2}{3}}$

Calcul de c et d

$$\begin{aligned}
(X^2+X+1)^2B(X) &= \frac{3}{(X-1)^2} \\
&= (X^2+X+1)^2\left[\frac{k_1}{(X-1)}+\frac{k_2}{(X-1)^2}\right]+(aX+b)(X^2+X+1)+cX+d
\end{aligned}$$

$a^2+a+1=0 \Rightarrow a_1=\frac{-1}{2}+\frac{\sqrt{3}}{2}i$

$X=a_1 \Rightarrow \dfrac{3}{(\frac{-1}{2}+\frac{\sqrt{3}}{2}i-1)^2}=c(\frac{-1}{2}+\frac{\sqrt{3}}{2}i)+d$

$\Rightarrow \dfrac{3}{\frac{3}{2}-\frac{3\sqrt{3}}{2}i}=\dfrac{1}{\frac{1}{2}-\frac{\sqrt{3}}{2}i}=\dfrac{2}{1-\sqrt{3}i}=\dfrac{2(1+\sqrt{3}i)}{(1-\sqrt{3}i)(1+\sqrt{3}i)}=\dfrac{1}{2}+\dfrac{\sqrt{3}}{2}i=\left(\frac{-1}{2}c+d\right)+c\frac{\sqrt{3}}{2}i$

Donc $\boxed{c=d=1}$

Calcul de a

$$\begin{aligned}
\lim_{X\to+\infty} XB(X) &= \lim_{X\to+\infty}\frac{3X}{(X-1)^2(X^2+X+1)^2} \\
&= \lim_{X\to+\infty}\left[\frac{k_1X}{(X-1)}+\frac{k_2X}{(X-1)^2}+X\frac{aX+b}{(X^2+X+1)}+X\frac{cX+d}{(X^2+X+1)^2}\right]
\end{aligned}$$

$\Rightarrow 0=k_1+a \Rightarrow a=-k_1 \Rightarrow \boxed{a=\dfrac{2}{3}}$

Calcul de b

$$\begin{aligned}
B(0) &= 3 \\
&= -k_1+k_2+b+d
\end{aligned}$$

$\Rightarrow b=3+k_1-k_2-d=3-\dfrac{2}{3}-\dfrac{1}{3}-1 \Rightarrow \boxed{b=1}$

$$\boxed{B(X)=\frac{-2}{3(X-1)}+\frac{1}{3(X-1)^2}+\frac{2X+3}{3(X^2+X+1)}+\frac{X+1}{(X^2+X+1)^2}}$$

$$C(X) = \frac{1}{X^3(X-2)^3} = \frac{k_1}{X} + \frac{k_2}{X^2} + \frac{k_3}{X^3} + \frac{k_4}{(X-2)} + \frac{k_5}{(X-2)^2} + \frac{k_6}{(X-2)^3}$$

<u>Calcul de k_3</u>

$$X^3C(X) = \frac{1}{(X-2)^3} = X^2k_1 + Xk_2 + k_3 + X^3\left(\frac{k_4}{(X-2)} + \frac{k_5}{(X-2)^2} + \frac{k_6}{(X-2)^3}\right)$$

$$X = 0 \Rightarrow \boxed{k_3 = \frac{-1}{8}}$$

<u>Calcul de k_2</u>

En dérivant $X^3C(X)$,on obtient :

$$\frac{-3}{(X-2)^4} = 2Xk_1 + k_2 + \left[X^3\left(\frac{k_4}{(X-2)} + \frac{k_5}{(X-2)^2} + \frac{k_6}{(X-2)^3}\right)\right]'$$

$$X = 0 \Rightarrow \boxed{k_2 = \frac{-3}{16}}$$

<u>Calcul de k_1</u>

En dérivant une deuxième fois,on obtient :

$$\frac{12}{(X-2)^5} = 2k_1 + \left[X^3\left(\frac{k_4}{(X-2)} + \frac{k_5}{(X-2)^2} + \frac{k_6}{(X-2)^3}\right)\right]''$$

$$X = 0 \Rightarrow \frac{12}{-32} = 2k_1 \Rightarrow \boxed{k_1 = \frac{-3}{4}}$$

<u>Calcul de k_6</u>

$$(X-2)^3C(X) = \frac{1}{X^3} = (X-2)^3\left(\frac{k_1}{X} + \frac{k_2}{X^2} + \frac{k_3}{X^3}\right) + (X-2)^2k_4 + (X-2)k_5 + k_6$$

$$X = 2 \Rightarrow \boxed{k_6 = \frac{1}{8}}$$

<u>Calcul de k_5</u>

En dérivant $(X-2)^3C(X)$, on obtient :

$$\frac{-3}{X^4} = \left[(X-2)^3\left(\frac{k_1}{X} + \frac{k_2}{X^2} + \frac{k_3}{X^3}\right)\right]' + 2(X-2)k_4 + k_5$$

$$X = 2 \Rightarrow \boxed{k_5 = \frac{-3}{16}}$$

<u>Calcul de k_4</u>

En dérivant une deuxieme fois, on obtient :

$$\frac{12}{X^5} = \left[(X-2)^3\left(\frac{k_1}{X} + \frac{k_2}{X^2} + \frac{k_3}{X^3}\right)\right]'' + 2k_4$$

$$X = 2 \Rightarrow \frac{12}{32} = 2k_4 \Rightarrow \boxed{k_4 = \frac{3}{4}}$$

$$\boxed{C(X)=\frac{1}{X^3(X-2)^3}=\frac{-3}{4X}-\frac{3}{16X^2}-\frac{1}{8X^3}+\frac{3}{4(X-2)}-\frac{3}{16(X-2)^2}+\frac{1}{8(X-2)^3}}$$

$D(X)=\dfrac{X^3}{X^4+X^2+1}$

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

$D(X)=\dfrac{X^3}{(X^2+X+1)(X^2-X+1)}=\dfrac{a_1X+b_1}{X^2+X+1}+\dfrac{a_2X+b_2}{X^2-X+1}$

On remarque que : $D(-X)=-D(X)\Rightarrow \dfrac{-a_1X+b_1}{X^2-X+1}+\dfrac{-a_2X+b_2}{X^2+X+1}=\dfrac{-a_1X-b_1}{X^2+X+1}+\dfrac{-a_2X-b_2}{X^2-X+1}$

Par identification, on obtient : $a_1=a_2 \qquad b_1=-b_2 \qquad$ d'où :

$D(X)=\dfrac{X^3}{(X^2+X+1)(X^2-X+1)}=\dfrac{a_1X+b_1}{X^2+X+1}+\dfrac{a_1X-b_1}{X^2-X+1}$

Calcul de a_1

$\lim\limits_{x\to+\infty} XD(X)=\lim\limits_{x\to+\infty}\dfrac{X^4}{(X^2+X+1)(X^2-X+1)}=\lim\limits_{x\to+\infty} X\dfrac{a_1X+b_1}{X^2+X+1}+\lim\limits_{x\to+\infty} X\dfrac{a_1X-b_1}{X^2-X+1}$

$\Rightarrow 1=2a_1\Rightarrow \boxed{a_1=\dfrac{1}{2}}$

Calcul de b_1

$D(X)=\dfrac{X^3}{(X^2+X+1)(X^2-X+1)}=\dfrac{a_1X+b_1}{X^2+X+1}+\dfrac{a_1X-b_1}{X^2-X+1}$

$X=1\Rightarrow \dfrac{1}{3}=\dfrac{a_1+b_1}{3}+a_1-b_1\Rightarrow 1=a_1+b_1+3a_1-3b_1\Rightarrow -2b_1=1-4a_1\Rightarrow b_1=\dfrac{4a_1-1}{2}$

$\boxed{b_1=\dfrac{1}{2}}$

$$\boxed{D(X)=\frac{X^3}{(X^2+X+1)(X^2-X+1)}=\frac{X+1}{2(X^2+X+1)}+\frac{X-1}{2(X^2-X+1)}}$$

Bibliographie

[1] JEAN M. MONIER : *Les méthodes et exercices de mathematiques MPSI*, Dunod (2008), 423 pages.

[2] MARIE ALLANO-CHEVALIER , XAVIER OUDOT : *Maths MPSI 1e année*, Hachette (2008), 672 pages.

[3] HERVÉ GIANELLA, FRANCK TAIEB : *Maths MPSI : tests de cours*, Dunod (2011), 313 pages.

[4] DANIEL FREDON : *Mathématiques : résumé du cours en fiches MPSI.MP*, Dunod (2010), 268 pages.

[5] JEAN M. ARNAUDIÈS, HENRI FRAYSSE : *Cours de mathématiques-1 : Algèbre*, Dunod Université (1992), 680 pages.