Introduction aux structures algébriques

Manon Chouët

Juin 2023

Table des matières

1 Introduction **5**

2 Notion de groupe **5**

3 Théorie des anneaux **6**
3.1 Premières définitions 6
3.2 Idéaux 7
3.3 Anneau quotient 8
3.4 L'anneau $\mathbb{Z}/n\mathbb{Z}$ 12

4 Polynôme **13**
4.1 Définitions 13
4.2 $\mathbb{R}[X]/(X^2+1)$ 16
4.3 Racine de polynôme dans un anneau quotient 18
4.4 Polynôme irréductible 19

1 Introduction

Ce document est une introduction à l'algèbre et plus particulièrement à certaines structures algébriques. Une structure algébrique est un ensemble muni d'une ou plusieurs lois de composition, externes ou internes, vérifiant certains axiomes. Dans la suite, nous nous intéresserons aux groupes et aux anneaux. Un groupe est une notion mathématique qui décrit naturellement les symétries des objets de la nature. Cette notion trouve son origine dans le problème de résolubilité des équations polynomiales par radicaux, via une théorie développée par Évariste Galois (voir par exemple [G97] pour plus d'informations). De plus, les groupes et les anneaux sont des notions qui apparaissent dans divers domaines des mathématiques tels que la géométrie, la théorie des nombres (nous pouvons par exemple penser à son implication dans les théorèmes de Fermat) ou encore l'analyse. C'est la mathématicienne Emmy Noether qui a établi les fondements de la théorie des anneaux commutatifs unitaires.

Les corps, dont les plus connus sont les réels $\mathbb{R}$ ou encore les complexes $\mathbb{C}$, sont des cas particuliers d'anneaux très importants. Une différence notable entre $\mathbb{R}$ et $\mathbb{C}$ est que $\mathbb{C}$ contrairement à $\mathbb{R}$ est algébriquement clos. Cela signifie que tout polynôme à coefficients dans $\mathbb{C}$ admet une racine dans $\mathbb{C}$. Ainsi dans ce document nous allons voir que lorsqu'un polynôme n'a pas de racine dans $\mathbb{R}$, on peut construire un corps plus grand dans lequel il en possède.

2 Notion de groupe

Pour arriver à la notion d'anneaux, nous avons tout d'abord besoin d'une notion plus faible, celle de groupe. Nous verrons plus tard qu'un anneau est un groupe muni d'une loi supplémentaire.

Définition 2.0.1. *Un **groupe** est un ensemble G muni d'une loi interne que l'on note $\star$ qui vérifie :*

— *(Associativité) :*
$$\forall a, b, c \in G,\ a \star (b \star c) = (a \star b) \star c,$$

— *(Existence du neutre) :*
$$\exists e_G \in G,\ \forall a \in G,\ a \star e_G = e_G \star a = a,$$

— *(Existence du symétrique) :*
$$\forall a \in G,\ \exists b \in G \text{ tel que } a \star b = b \star a = e_G.$$
*On appelle b le **symétrique** de a, et on le note a^{-1}.*

*Un groupe est dit **abélien** si la loi $\star$ est commutative, c'est-à-dire si elle vérifie :*
$$\forall a, b \in G, a \star b = b \star a.$$

Exemple 2.0.1. *L'ensemble des entiers relatifs $\mathbb{Z}$ muni de l'addition classique forme un groupe, avec 0 comme élément neutre et l'opposé comme symétrique. Ainsi, l'ensemble des entiers naturels $\mathbb{N}$ muni de l'addition ne forme pas un groupe puisque par exemple, 2 n'a pas de symétrique.*

Définition 2.0.2. *:*
Un ***sous-groupe*** *H d'un groupe $(G, \star)$ est une partie de G qui vérifie les propriétés suivantes :*

— $e_G \in H$
— $\forall x \in H, x^{-1} \in H$
— $\forall x, y \in H, x \star y \in H$.

Exemple 2.0.2. *L'ensemble $H = \{0\}$ est un sous-groupe de $\mathbb{Z}$ alors que $G = \{0, 1\}$ n'est pas un sous-groupe de $\mathbb{Z}$ car $-1 \notin G$.*

3 Théorie des anneaux

3.1 Premières définitions

Cette section est dédiée aux anneaux et aux corps.

⚠ Les lois que l'on va noter dans la suite $+$ et $\times$, que l'on appelle loi additive et loi multiplicative, sont des lois internes quelconques. C'est-à-dire ce ne sont ni l'addition que l'on connaît ni la multiplication que l'on connaît.

Définition 3.1.1. *Un* ***anneau*** *est un ensemble A muni de deux lois internes que l'on notera $+$ et $\times$, telles que $(A, +)$ forme un groupe abélien et A muni de $\times$ vérifie les propriétés de l'associativité, de l'existence d'un neutre et de distributivité avec $+$:*

$$\forall a, b, c \in A, a \times (b + c) = (a \times b) + (a \times c).$$

Un anneau est dit ***commutatif*** *si la loi $\times$ est commutative.*

Remarque 3.1.1. *Soit $(A, +, \times)$ un anneau. Dans la suite, on notera en général 0_A le neutre de la loi additive et 1_A le neutre de la loi multiplicative dans l'ensemble A.*

Exemple 3.1.1. *L'ensemble des matrices carrées de taille n à coefficients dans $\mathbb{R}$ muni de l'addition et de la multiplication de matrices est un anneau. De plus, $(\mathbb{R}, +, \times)$ est un anneau commutatif.*

Définition 3.1.2. *Soient $(A, +, \times)$ un anneau et $x \in A$. On dit que x est un* ***élément inversible*** *si il existe $y \in A$ tel que*

$$x \times y = y \times x = 1_A.$$

On note $A^\times$ l'ensemble des éléments inversibles d'un anneau $(A, +, \times)$.

Définition 3.1.3. *Un* ***corps*** *est un anneau commutatif $(A, +, \times)$ où $(A)^\times = A \setminus \{0_A\}$.*

Exemple 3.1.2.
— *$(\mathbb{Z}, +, \times)$ n'est pas un corps. En effet 2 n'a pas d'inverse dans $\mathbb{Z}$.*
— *$(\mathbb{R}, +, \times)$, $(\mathbb{Q}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des corps.*

Définition 3.1.4. *Soit $(A, +, \times)$ un anneau. Soit $x \in A$ non nul. On dit que x est un* ***diviseur de zéro*** *s'il existe $y \in A$ non nul tel que*

$$x \times y = 0_A.$$

Définition 3.1.5. *Soit $(A, +, \times)$ un anneau. On dit que $(A, +, \times)$ est un* ***anneau intègre*** *si il n'admet pas de diviseur de zéro.*

Exemple 3.1.3. *L'anneau $(\mathbb{R}, +, \times)$ est un anneau intègre : en effet, dans $\mathbb{R}$ un produit de facteur est nul si et seulement si l'un des facteurs est nul. Au contraire, l'anneau $(\mathrm{M}_4(\mathbb{R}, +, \times))$ n'est pas un anneau intègre. Par exemple soient*

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

et

$$B = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Ainsi, en notant 0_4 la matrice nulle de taille 4, on a :

$$A \times B = 0_4$$

alors que $A \neq 0_4$ et $B \neq 0_4$. Ainsi A et B sont des diviseurs de zéros, donc $(M_4(\mathbb{R}), +, \times)$ n'est pas un anneau intègre.

3.2 Idéaux

Dans cette section, nous allons voir la définition d'un idéal ainsi que des définitions d'idéaux particuliers. Cette notion nous permettra par la suite de créer de nouveaux anneaux.

Définition 3.2.1. *Soit $(A, +, \times)$ un anneau. Et soit I un sous-groupe de $(A, +)$. On dit que I est un* ***idéal à gauche (resp. : à droite)*** *si*

$$\forall a \in A, \forall x \in I, a \times x \in I \text{ (resp. : } x \times a \in I).$$

On dit que I est un ***idéal bilatère*** *si c'est à la fois un idéal à gaucche et un idéal à droite.*

Remarque 3.2.1. *Dans la suite, nous utiliserons seulement des idéaux bilatères.*

Exemple 3.2.1. *Les ensembles $I = \{0_A\}$ et $J = A$ sont des idéaux triviaux de n'importe quel anneau $(A, +, \times)$. Et l'ensemble $I = \{2, 0, -2\}$ n'est pas un idéal de $(\mathbb{Z}, +, \times)$ car $4 \in \mathbb{Z}$ or $4 \times 2 = 8 \notin I$.*

Définition 3.2.2. *Soit I un idéal de $(A, +, \times)$ un anneau. I est dit* ***premier*** *si pour tout $a, b \in A$,*

$$a \times b \in I \Rightarrow (a \in I \text{ ou } b \in I).$$

Définition 3.2.3. *Soit $(A, +, \times)$ un anneau et I un idéal de $(A, +, \times)$. Alors l'idéal I est dit* ***maximal*** *dans A si et seulement si $I \neq A$ et pour tout J un autre idéal de A, si J contient strictement I, alors $J = A$.*

Définition 3.2.4. *Soient $(A, +, \times)$ un anneau et $a \in A$. On appelle* ***idéal engendré par a*** *l'idéal le plus petit (au sens de l'inclusion) contenant a. Autrement dit, pour tout idéal J de A contenant a, on a $I \subset J$.*

Exemple 3.2.2. *L'idéal $I = \{2k, k \in \mathbb{Z}\}$ est l'idéal engendré par 2 dans $\mathbb{Z}$.*

Proposition 3.2.1. *Soit $(A, +, \times)$ un anneau, et $a \in A$. L'idéal engendré par a est :*

$$I = \{x \times a, x \in A\}.$$

Démonstration.
— $0_A = 0_A \times a$ donc $0_A \in I$.
— Soit $y \in I$, soit $x \in A$ tels que $y = a \times x$. Alors $-y = -a \times x = a \times (-x)$ or $-x \in A$ car A est un anneau, donc $-y \in I$.
— Soient $y, z \in I$, soient $k, l \in A$ tels que $y = a \times k$ et $z = a \times l$. Ainsi, on obtient :

$$y + z = a \times k + a \times l = a \times (k + l)$$

car A est un anneau donc vérifie la propriété de distributivité. Or, $k + l \in A$ alors $y + z \in I$.
Ainsi, on voit que $(I, +)$ est un sous groupe de $(A, +)$.
— Soient $y \in A$ et $j \in I$. Soit alors $k \in A$ tel que $j = a \times k$.
Alors,

$$j \times y = a \times k \times y = a \times (k \times y).$$

Or $k \times y \in A$ donc $j \times y \in I$.
Donc I est un idéal. De plus, comme $a = 1_A \times a$ alors $a \in I$ donc I est un idéal contenant a.

Montrons maintenant que I est l'idéal engendré par a. Soit J un idéal de A qui contient a. Comme J est un idéal, on sait que $\forall x, y \in A \times J, x \times y \in J$. Or comme J contient a, $\forall x \in A, x \times a \in J$. On obtient donc :

$$\{a \times x, x \in A\} \subseteq J$$

or

$$\{a \times x, x \in A\} = I$$

ainsi I est le plus petit idéal contenant a, donc c'est l'idéal engendré par a. □

Proposition 3.2.2. *L'idéal I engendré par 1 de l'anneau $(A, +, \times)$ où 1 est le neutre de la loi $\times$ est $I = A$.*

Démonstration. D'après la proposition précédente, l'idéal I engendré par 1 est

$$I = \{x \times 1, x \in A\}.$$

Or 1 est le neutre de A donc

$$I = \{x \times 1, x \in A\} = \{x, x \in A\} = A.$$

□

3.3 Anneau quotient

Dans cette sous-section, nous allons construire de nouveaux anneaux, en considérant de bonnes relations d'équivalences. Nous allons voir par la suite que cette construction nous permettra de créer des anneaux « plus grands » dans lesquels on a « ajouté » des racines de certains polynômes.
Par la suite, tout anneau considéré est un anneau commutatif.

Définition 3.3.1. *Une **relation d'équivalence** $\mathcal{R}$ sur un ensemble E est une relation binaire qui vérifie les propriétés :*

— *reflexivité :*

$$\forall x \in E, x\mathcal{R}x$$

— *symétrique :*

$$\forall x, y \in E, x\mathcal{R}y \iff y\mathcal{R}x$$

— *transitivité :*

$$\forall x, y, z \in E, x\mathcal{R}y \text{ et } y\mathcal{R}z \Rightarrow x\mathcal{R}z.$$

Définition 3.3.2. *Soit E un ensemble et $x \in E$. On appelle* ***classe d'équivalence de*** *x et on note $\overline{x}$, l'ensemble des $y \in E$ tels que $y\mathcal{R}x$. Ainsi, on a :*

$$\overline{x} = \{y\mathcal{R}x, y \in E\}.$$

Définition 3.3.3. *On appelle* ***ensemble quotient*** *de E par la relation d'équivalence $\mathcal{R}$ l'ensemble des classes d'équivalences de E.*

Définition 3.3.4. *Soit $(A, +, \times)$ un anneau et I un idéal de cet anneau. Soit la relation suivante :*
$\forall x, y \in A$,

$$\overline{x} = \overline{y} \iff x - y \in I.$$

Proposition 3.3.1. *Cette relation est une relation d'équivalence. On note A/I l'ensemble quotient de l'anneau $(A, +, \times)$ par cette relation d'équivalence.*

Démonstration. — Soit $x \in A$,

$$x - x = 0_A \in I$$

car $(I, +)$ est un sous-groupe de $(A, +)$ donc contient l'élément neutre.

— Soient $x, y \in A$ tels que $x - y \in I$. Alors comme I est un idéal,

$$-(x - y) = -x + y = y - x \in I.$$

— Soient $x, y, z \in A$ tels que $x - y \in A$ et $y - z \in A$. Alors on a

$$x - y + y - z = x - z \in I$$

car I est stable par somme.

Donc $\mathcal{R}$ est bien une relation d'équivalence. □

Proposition 3.3.2. *On peut munir l'ensemble A/I des deux lois internes provenant des lois de A, qui en font un anneau.*

Démonstration. Soit $(A, +, \times)$ un anneau et I un idéal de A . On munit A/I de deux lois, que l'on notera toujours $+$ et $\times$, définies ainsi :

— $\forall x, y \in A$, on pose $\overline{x} + \overline{y} := \overline{x + y}$ où $+$ est la loi additive de $(A, +, \times)$.

— $\forall x, y \in A$, on pose $\overline{x} \times \overline{y} := \overline{x \times y}$ où $\times$ est la loi multiplicative de $(A, +, \times)$.

Montrons dans un premier temps que $+$ et $\times$ sont bien définies.
Soient $\overline{x}, \overline{y} \in A/I$ et soient $x' \in \overline{x}$ et $y' \in \overline{y}$ alors $\overline{x'} = \overline{x}$ et $\overline{y'} = \overline{y}$. Ainsi, $x - x' \in I$ et $y - y' \in I$. Comme I est un idéal, $x - x' + y - y' \in I$ donc $\overline{x + y} = \overline{x' + y'}$.
Et soient $\overline{x}, \overline{y} \in A/I$. Soient $x' \in \overline{x}$ et $y' \in \overline{y}$. Alors, on a : $x - x' \in I$ et $y - y' \in I$. Comme I est un idéal, $y' \times (x - x') \in I$ et $x \times (y - y') \in I$. Et, ainsi $y' \times (x - x') + x \times (y - y') = y' \times x - y' \times x' + x \times y - x \times y' = x \times y - x' \times y' \in I$, et donc $\overline{x \times y} = \overline{x' \times y'}$.
Par conséquent, les lois $+$ et $\times$ sont bien définies.

Associativité de $+$:
Soient $\overline{a}, \overline{b}, \overline{c} \in A/I$,

$$\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{b+c} = \overline{a+b+c} = \overline{a+b} + \overline{c} = (\overline{a} + \overline{b}) + \overline{c}.$$

Commutativité de $+$:
Soient $\overline{x}, \overline{y} \in A/I$,

$$\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a}$$

par commutativité de $(A, +)$,

$$\overline{b+a} = \overline{b} + \overline{a}.$$

Neutre de $+$:
On peut trouver un élément neutre dans A/I qui est la classe d'équivalence de l'élément neutre de $(A, +\times)$. En effet, soit $\overline{x} \in A/I$,

$$\overline{0_A} + \overline{x} = \overline{0_A + x} = \overline{x + 0_A} = \overline{x}$$

car 0_A est le neutre de $(A, +)$.

Symétrique de $+$:
Soit $\overline{x} \in A/I$, alors soit $(-x) \in A$ tel que $(-x)$ est le symétrique de x dans A. Alors,

$$\overline{x} + \overline{-x} = \overline{x - x} = \overline{0_A}.$$

Donc le symétrique de $\overline{x}$ est la classe d'équivalence du symétrique de x.
Donc $(A/I, +)$ est un groupe abélien.

Associativité de $\times$:
Soient $\overline{x}, \overline{y}, \overline{z} \in A/I$,

$$\overline{x} \times (\overline{y} \times \overline{z}) = \overline{x} \times \overline{y \times z} = \overline{x \times y \times z} = \overline{x \times y} \times \overline{z} = (\overline{x} \times \overline{y}) \times \overline{z}.$$

Neutre de $\times$:
Soit $\overline{x} \in A/I$. Alors, on a :

$$\overline{1_A} \times \overline{x} = \overline{1_A \times x} = \overline{x \times 1_A} = \overline{x}$$

car 1_A est le neutre de $(A, \times)$. Ainsi, $\overline{1_A}$ est le neutre pour la multiplication.

Distributivité de $\times$ par rapport à $+$:
Soient $\overline{x}, \overline{y}, \overline{z} \in A/I$,

$$\overline{x} \times (\overline{y} + \overline{z}) = \overline{x} \times \overline{y+z} = \overline{x \times (y+z)} = \overline{x \times y + x \times z}$$

par distributivité de (A,+,×),

$$\overline{x \times y + x \times z} = \overline{x \times y} + \overline{x \times z} = \overline{x} \times \overline{y} + \overline{x} \times \overline{z}$$

Donc $(A/I, +, \times)$ est un anneau. □

On dit que $(A/I, +, \times)$ est un ***anneau quotient****.*

Remarque 3.3.1. *Lorsque l'on crée un anneau quotient, on quotiente un anneau par l'un de ses idéaux. Mais on peut quotienter un anneau par autre chose qu'un idéal comme par exemple par un sous-groupe, cependant, le résultat ne sera pas un anneau.*

Proposition 3.3.3. *Soit $(A, +, \times)$ un anneau et I un idéal de A. L'anneau quotient A/I est un anneau intègre si et seulement si I est premier.*

Démonstration. On va procéder par double implication :
($\Rightarrow$) Supposons que A/I est un anneau intègre. Alors, soient $x, y \in A$. Supposons $x \times y \in I$. Alors :

$$\overline{x} \times \overline{y} = \overline{0_A}$$

donc

$$\overline{x} = \overline{0_A} \text{ ou } \overline{y} = \overline{0_A}$$

donc $x \in I$ ou $y \in I$ donc I est premier.

($\Leftarrow$) Supposons que I est premier. Soient $\overline{x}, \overline{y} \in A/I$. Supposons

$$\overline{x} \times \overline{y} = \overline{x \times y} = \overline{0}.$$

Ainsi, $x \times y \in I$. Or comme I est premier, $x \in I$ ou $y \in I$ donc $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$. Par conséquent, A/I est intègre. □

Proposition 3.3.4. *Soit $(A, +, \times)$ un anneau et I un idéal de A. Alors, A/I est un corps si et seulement si I est un idéal maximal de A.*

Démonstration. On va procéder par double implication :

($\Rightarrow$) On suppose que A/I est un corps. Soit J un idéal de $(A, +, \times)$ tel que $I \subset J$, soit $x \in J$ et $x \notin I$. Comme I est un idéal alors $0_A \in I$ ainsi $\overline{x} \neq \overline{0_A}$. Comme A/I est un corps, $\exists \overline{y} \in A/I$ tel que

$$\overline{x} \times \overline{y} = \overline{1}$$

or

$$A/I = \{\overline{x}, x \in A\}$$

et

$$\overline{x} = \{x + u, u \in I\}$$

donc $x \times y = 1 + u$ avec $u \in I$ donc

$$1 = x \times y - u \in J = A$$

car le seul idéal contenant 1 est A donc I est maximal.

($\Leftarrow$) Supposons maintenant que I est maximal. Soit $\overline{x} \in A/I$ tel que $\overline{x} \neq \overline{0}$. Ainsi, $x \notin I$. Soit J le plus petit idéal contenant x et I donc

$$J = \{a \times x + m, a \in A, m \in I\}.$$

Ainsi, $I \subset J$ or I est maximal donc $J = A$. Or $1 \in A$ donc il existe $b \in A$ et $m \in I$ tel que $1 = b \times x + m$ donc $\overline{1} = \overline{b \times x} + \overline{m}$ or $m \in I$ donc $\overline{m} = \overline{0}$ donc $\overline{1} = \overline{b} \times \overline{x}$ donc $\overline{x}$ est inversible donc A/I est un corps.

□

3.4 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Nous allons à présent voir un exemple très intéressant.

Définition 3.4.1. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est le quotient de l'anneau $\mathbb{Z}$ par l'idéal engendré par l'entier n dans $\mathbb{Z}$. Ainsi, $\mathbb{Z}/n\mathbb{Z} = \{\overline{a}, a \in \mathbb{Z}\}$ où $\overline{a}$ est l'ensemble des entiers congrus à a modulo n, donc c'est l'ensemble des entiers qui ont pour reste a dans la division euclidienne par n.*

Exemple 3.4.1. *Dans $\mathbb{Z}/6\mathbb{Z}, \overline{0}$ est l'ensemble des multiples de 6.*
Et on peut calculer :
$\overline{1} + \overline{5} = \overline{6} = \overline{0}; \overline{2} + \overline{5} = \overline{7} = \overline{1}$ *;* $\overline{3} \times \overline{4} = \overline{12} = \overline{0}$ *;* $\overline{3} \times \overline{3} = \overline{9} = \overline{3}$.

Théorème 3.4.1. *Lemme de Bezout*
Soient $(a, b) \in \mathbb{Z}^2$. Si $a \wedge b = 1$ alors il existe $(u, v) \in \mathbb{Z}^2$ tel que

$$a \times u + b \times v = 1.$$

Démonstration. On peut trouver la démonstration dans [L19], Chapitre 2, partie 3, sous-partie 2.3.2. □

Proposition 3.4.1. *L'ensemble des éléments inversibles de l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ est :*

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{k}, k \wedge n = 1\}.$$

Démonstration. Montrons d'abord que l'ensemble $\{\overline{k}, k \wedge n = 1\}$ est bien défini. Ainsi, soient $k \in \mathbb{Z}$ et $p \in \overline{k}$. Comme $p \in \overline{k}$, il existe $l \in \mathbb{Z}$ tel que $p = ln + k$ donc en particulier $k = p - ln$. De plus, $k \wedge n = 1$ donc d'après le lemme de Bezout 3.4.1, il existe $(u, v) \in \mathbb{Z}^2$ tel que $ku + nv = 1$ donc

$$u(p - ln) + nv = up - uln + nv = up + n(v - lu) = 1$$

et ainsi $p \wedge n = 1$.
Montrons que $\{\overline{k}, k \wedge n = 1\} \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$.
Soit $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ tel que $k \wedge n = 1$ donc par le lemme de Bezout 3.4.1, il existe un couple $(u, v) \in \mathbb{Z}$ tel que

$$ku + nv = 1 \text{ donc } \overline{ku + nv} = \overline{1} \text{ donc } \overline{ku} + \overline{nv} = \overline{1}.$$

or

$$\overline{nv} = \overline{0} \text{ donc } \overline{ku} = \overline{k} \times \overline{u} = \overline{1}.$$

Ainsi, $\overline{k}$ est inversible.

Montrons maintenant que $(\mathbb{Z}/n\mathbb{Z})^\times \subseteq \{\overline{k}, k \wedge n = 1\}$.
On va le montrer par contraposée.
Soit $\overline{p} \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que $p \wedge n = k$ avec $k \in \mathbb{Z} \setminus \{1\}$. Ainsi, $p = ak$ et $n = bk$ avec $(a, b) \in \mathbb{Z}^2$. Or comme b est un diviseur strict de n, $|b| < n$. De plus $bp = bak$ ainsi

$$\overline{bp} = \overline{bak} = \overline{b} \times \overline{p} = \overline{0}$$

donc $\overline{p}$ n'est pas inversible car $\overline{b} \neq 0$.
Donc, on a

$$(\mathbb{Z}/n\mathbb{Z})^\times \subseteq \{\overline{k}, k \wedge n = 1\}.$$

et

$$\{\overline{k}, k \wedge n = 1\} \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$$

ainsi

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{k}, k \wedge n = 1\}.$$

□

Proposition 3.4.2. *:*
Soit $n \in \mathbb{N}$. Les propriétés suivantes sont équivalentes :

1. *$(\mathbb{Z}/n\mathbb{Z})$ est un anneau intègre,*
2. *$(\mathbb{Z}/n\mathbb{Z})$ est un corps,*
3. *Le nombre n est premier.*

Démonstration. :
Montrons (3) ⇒ (2), donc que si n est premier alors $\mathbb{Z}/n\mathbb{Z}$ est un corps.
Soit $\overline{p} \in \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{1}\}$, comme n est premier et que p n'est pas un multiple de n, $p \wedge n = 1$. Or d'après la proposition précédente, $\overline{p} \in (\mathbb{Z}/n\mathbb{Z})^\times$ donc $\overline{p}$ est inversible, ainsi $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Montrons à présent (2) ⇒ (1), donc que si $\mathbb{Z}/n\mathbb{Z}$ est un corps, $\mathbb{Z}/n\mathbb{Z}$ est aussi un anneau intègre.
Nous allons le démontrer par contraposée.
Supposons donc que $\mathbb{Z}/n\mathbb{Z}$ n'est pas un anneau intègre. Donc soit $\overline{q} \in \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$, soit $\overline{u} \in \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$ tel que $\overline{q} \times \overline{u} = \overline{0}$. Supposons maintenant que $\overline{q}$ est inversible. Soit $\overline{v} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{q} \times \overline{v} = \overline{1}$. Ainsi, on a

$$\overline{v} \times \overline{q} \times \overline{u} = \overline{1} \times \overline{u} = \overline{u} = \overline{0}$$

c'est absurde car on a supposé $\overline{u} \neq \overline{0}$. Ainsi, $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps.

Pour finir, montrons (1) ⇒ (3), donc que si $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre alors n est premier.
On va également le montrer par contraposée.
Ainsi, soient n un nombre non premier, et $\overline{p} \in \mathbb{Z}/n\mathbb{Z}$ tel que p est un diviseur strict de n non égal à 1. Alors, on a : $p \wedge n = k$ avec $k \in \mathbb{Z} \setminus \{0\}$. Soit $(a, b) \in \mathbb{Z}^2$ tel que $p = a \times k$ et $n = b \times k$ alors on a que $|b| < n$ car b est un diviseur strict de n. On obtient alors :

$$\overline{bp} = \overline{b} \times \overline{p} = \overline{b} \times \overline{ak} = \overline{a} \times \overline{bk} = \overline{a} \times \overline{n} = \overline{a} \times \overline{0} = \overline{0}.$$

Or $\overline{b}$ et $\overline{p}$ sont non nuls donc ce sont des diviseurs de zéros. Par conséquent, $\mathbb{Z}/n\mathbb{Z}$ n'est pas un anneau intègre. □

4 Polynôme

4.1 Définitions

Définition 4.1.1. *Soit $\mathbb{K}$ un corps.*
*On appelle **polynôme à coefficients dans** $\mathbb{K}$ toute somme formelle :*

$$\sum_{i=0}^{n} a_i X^i$$

avec $n \in \mathbb{N}$ et $(a_i)_{i \in [0,n]} \in \mathbb{K}^n$.

On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.

Exemple 4.1.1. *La somme formelle $X^3 + 4X + 5$ est un polynôme de $\mathbb{R}[X]$.*

Définition 4.1.2. *Soit $m \in \mathbb{N}$, on dit que m est le **degré du polynôme** $P = \sum_{i=0}^{n} a_i X^i$ si et seulement si m est le plus grand i tel que $a_i \neq 0$. On le note $deg(P)$. Par convention, on va dire que le degré du polynôme nul est $-\infty$.*

Proposition 4.1.1. *Soit $\mathbb{K}$ un corps. Alors, $(\mathbb{K}[X], +, \times)$ est un anneau où la loi $+$ et la loi $\times$ sont définies ainsi :*

soient $n, m \in \mathbb{N}$ et $(a_i)_{i\in[0,n]} \in \mathbb{K}^n, (b_i)_{i\in[0,m]} \in \mathbb{K}^m$. On suppose $n \geq m$ et on définit :

$$\sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{m} b_i X^i = \sum_{i=0}^{m} (a_i + b_i) X^i + \sum_{i=m+1}^{n} a_i X^i,$$

$$\sum_{i=0}^{n} a_i X^i \times \sum_{j=0}^{m} b_j X^j = \sum_{k=0}^{n+m} X^k \Big(\sum_{i+j=k} a_i \times b_j \Big).$$

Démonstration. Associativité de $+$:
Soient $n, m, p \in \mathbb{N}$ et $(a_i)_{i\in[0,n]} \in \mathbb{K}^n, (b_i)_{i\in[0,m]} \in \mathbb{K}^m, (c_i)_{i\in[0,p)]} \in \mathbb{K}^p$.
On suppose $n \geq m \geq p$. Et $\forall i > p$, on pose $c_i = 0$ et $\forall i > m$, on pose $b_i = 0$.

$$\bullet \sum_{i=0}^{n} a_i X^i + \Big(\sum_{i=0}^{n} b_i X^i + \sum_{i=0}^{n} c_i X^i\Big) = \sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{n} (b_i + c_i) X^i = \sum_{i=0}^{n} (a_i + b_i + c_i) X^i.$$

$$\bullet \Big(\sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{n} b_i X^i\Big) + \sum_{i=0}^{n} c_i X^i = \sum_{i=0}^{n} (a_i + b_i) X^i + \sum_{i=0}^{n} c_i X^i = \sum_{i=0}^{n} (a_i + b_i + c_i) X^i$$

$$= \sum_{i=0}^{n} a_i X^i + \Big(\sum_{i=0}^{n} b_i X^i + \sum_{i=0}^{n} c_i X^i\Big).$$

On voit donc que l'associativité de l'addition de polynômes provient de celle de l'addition dans $\mathbb{K}$. De même, on montre que $+$ est commutative.

Commutativité de $+$:
Soient $n, m \in \mathbb{N}$ et $(a_i)_{i\in[0;n]} \in \mathbb{K}^n, (b_i)_{i\in[0;m]} \in \mathbb{K}^m$.Et,$\forall i > m$, on pose $b_i = 0$,

$$\sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{n} b_i X^i = \sum_{i=0}^{n} (a_i + b_i) X^i = \sum_{i=0}^{n} (b_i + a_i) X^i$$

car $(\mathbb{K}, +)$ est un groupe abélien donc est commutatif. Et, on a

$$\sum_{i=0}^{n} (b_i + a_i) X^i = \sum_{i=0}^{n} (b_i X^i + a_i X^i) = \sum_{i=0}^{n} b_i X^i + \sum_{i=0}^{n} a_i X^i.$$

Existence du neutre de $+$:
Soit le polynôme constant égal à 0 et $n \in \mathbb{N}$ et soit $(a_i)_{i\in[0,n]} \in \mathbb{K}^n$.

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

car 0 est le neutre de l'addition. On obtient donc :

$$a_0X^0 + \sum_{i=1}^{n} a_iX^i = \sum_{i=0}^{n} a_iX^i.$$

Symétrique de $+$:
Soient $n \in \mathbb{N}$ et $(a_i)_{i\in[0,n]} \in \mathbb{K}^n$ donc $(-a_i)_{i\in[0,n]} \in \mathbb{K}^n$ car $(\mathbb{K}, +)$ est un groupe. Et, de plus, on a :

$$\sum_{i=0}^{n} a_iX^i + \sum_{i=0}^{n} -a_iX^i = \sum_{i=0}^{n} (a_i - a_i)X^i = \sum_{i=0}^{n} 0 \times X^i = 0$$

car le neutre de $(\mathbb{K}, +)$ est 0. Ainsi,

$$\sum_{i=0}^{n} 0 \times X^i = \sum_{i=0}^{0} 0$$

donc $\sum_{i=0}^{n} -a_iX^i$ est le symétrique de $\sum_{i=0}^{n} a_iX^i$.

Associativité de $\times$:
On peut voir de la même façon que l'associativité de $\times$ provient de celle du corps $\mathbb{K}$.
Existence du neutre de $\times$:
On peut voir que le neutre de $\times$ provient du neutre de la loi multiplicative du corps $\mathbb{K}$. En effet, le neutre de $\times$ est égal au polynôme constant égal au neutre de $\times$ dans $\mathbb{K}$.
Distributivité de $\times$ par $+$:
Soient $n, m, p \in \mathbb{N}$, on suppose $n \geq m \geq p$. Et $(a_i)_{i\in[0,n]} \in \mathbb{K}^n, (b_i)_{i\in[0,m]} \in \mathbb{K}^m, (c_i)_{i\in\mathbb{N}} \in \mathbb{K}^p$. De plus, $\forall i > p$, on pose $c_i = 0$, $\forall i > m$, on pose $b_i = 0$. Ainsi :

$$\sum_{i=0}^{n} a_iX^i \times (\sum_{j=0}^{m} b_jX^j + \sum_{j=0}^{p} c_jX^j) = \sum_{i=0}^{n} a_iX^i \times (\sum_{j=0}^{n} b_jX^j + \sum_{j=0}^{n} c_jX^j) = \sum_{i=0}^{n} a_iX^i \times (\sum_{j=0}^{n} (b_j + c_j)X^j)$$

$$= \sum_{k=0}^{2n} X^k (\sum_{i+j=k} a_i(b_j + c_j)) = \sum_{k=0}^{2n} X^k (\sum_{i+j=k} (a_ib_j + a_ic_j))$$

car $(\mathbb{K}, +, \times)$ est un corps donc vérifie la propriété de distributivité.

$$\sum_{k=0}^{n} X^k (\sum_{i+j=k} (a_ib_j + a_ic_j)) = \sum_{k=0}^{n} X^k (\sum_{i+j=k} a_ib_j + \sum_{i+j=k} a_ic_j) = \sum_{k=0}^{2n} (X^k \sum_{i+j=k} a_ib_j + X^k \sum_{k=i+j} (a_ic_j))$$

$$= \sum_{k=0}^{2n} X^k (\sum_{i+j=k} a_ib_j) + \sum_{k=0}^{2n} X^k (\sum_{i+j=k} a_ic_j) = \sum_{i=0}^{n} a_iX^i \times \sum_{j=0}^{n} b_jX^j + \sum_{i=0}^{n} a_iX^i \times \sum_{j=0}^{n} c_jX^j.$$

□

Définition 4.1.3. *Soit $P \in \mathbb{K}[X]$ et $x \in \mathbb{K}$. On dit que x est une **racine** de P dans $\mathbb{K}$ si $P(x) = 0$.*

Exemple 4.1.2. *:*
Les polynômes $X^2 + X$ et $X^2 + 1$ sont des polynômes de $\mathbb{R}[X]$ et 0 et -1 sont des racines de $X^2 + X$. Tandis que, $X^2 + 1$ n'a pas de racines dans $\mathbb{R}$.

Définition 4.1.4. *Un corps $\mathbb{K}$ est dit* ***algébriquement clos*** *si tout polynôme de $\mathbb{K}[X]$ possède une racine dans $\mathbb{K}$.*

Exemple 4.1.3. *Ainsi, comme dit précédemment dans l'introduction, $\mathbb{R}$ n'est pas un corps algébriquement clos car X^2+1 n'a pas de racine dans $\mathbb{R}$. Mais $\mathbb{C}$ lui est algébriquement clos.*

Proposition 4.1.2. *:(division euclidienne dans $\mathbb{K}[X]$)*
Soit $\mathbb{K}$ un corps. Soient $A, B \in \mathbb{K}[X]$ avec B non nul. Alors, il existe un unique couple $(Q,R) \in \mathbb{K}[X]^2$ tel que $A = B \times Q + R$ avec $deg(R) < deg(B)$.

Démonstration. Admis, preuve dans le livre [B18]. □

Exemple 4.1.4. *:*
Si on fait la division euclidienne de $3X^3+7X^2+13X+12$ par X^2+1,
on obtient :

$$3X^3+7X^2+13X+12 = (3X+7)(X^2+1)+10X+5$$

Ainsi,

$$Q = (3X+7) \text{ et } R = 10X+5.$$

4.2 $\mathbb{R}[X]/(X^2+1)$

Dans cette partie, nous allons voir un exemple très intéressant d'anneau quotient. Mais avant cela, nous auront besoin de définir quelques notions.

Définition 4.2.1. *Un* ***morphisme d'anneaux*** *φ d'un anneau $(A,+,\times)$ vers un anneau $(B,\star,\square)$ est une application $\varphi : A \to B$ qui vérifie les propriétés suivantes :*
$\forall x, y \in A$
- $\varphi(x+y) = \varphi(x) \star \varphi(y)$
- $\varphi(x \times y) = \varphi(x) \square \varphi(y)$
- $\varphi(1_A) = 1_B$.

Exemple 4.2.1. *Soit $x \in \mathbb{R}$, alors l'application :*

$$\begin{aligned} \varphi : \mathbb{R}[X] &\to \mathbb{R} \\ P &\mapsto P(0) \end{aligned}$$

est un morphisme d'anneau, c'est d'ailleurs le morphisme d'évaluation en 0.
Au contraire, l'application

$$\begin{aligned} \phi : \mathbb{R} &\to \mathbb{C} \\ x &\mapsto xi \end{aligned}$$

n'est pas un morphisme d'anneaux car $\phi(1) = i$ or i n'est pas le neutre de la loi multiplicative de $\mathbb{C}$.

Définition 4.2.2. *Soit $(A,+,\times)$ et $(B,\star,\square)$ deux anneaux. Alors, l'anneau $(A,+,\times)$ est dit* ***isomorphe*** *à $(B,\star,\square)$ si et seulement si il existe un morphisme d'anneaux bijectif entre $(A,+,\times)$ et $(B,\star,\square)$. On dit que cette fonction est un* ***isomorphisme d'anneaux****.*

Définition 4.2.3. *Soit l'anneau quotient $(\mathbb{R}[X]/(X^2+1),+,\times)$, alors*

$$\mathbb{R}[X]/(X^2+1) = \{\overline{P}, P \in \mathbb{R}[X]\}.$$

Pour tout polynôme $P \in \mathbb{R}[X]$, $\overline{P}$ est l'ensemble des polynômes ayant le même reste dans la division euclidienne par (X^2+1).

Proposition 4.2.1. *On a l'égalité d'ensembles suivante :*

$$\mathbb{R}[X]/(X^2+1) = \{\overline{\alpha X+\beta}, (\alpha,\beta)\in\mathbb{R}^2\}.$$

Démonstration. Posons $A = \{\overline{\alpha X+\beta}, (\alpha,\beta)\in\mathbb{R}^2\}$ et $B = \{\overline{P}, P\in\mathbb{R}[X]\}$.
Montrons que $A = B$.
Montrons d'abord que $A\subseteq B$. Soit $a\in A$, $a = \overline{\alpha X+\beta}$. Or, puisque $\alpha X+\beta\in\mathbb{R}[X]$ on a : $a\in B$ donc $A\subseteq B$.

Montrons maintenant que $B\subseteq A$. Soit $a\in B$ donc $a = \overline{P}$ avec $P\in\mathbb{R}[X]$. On fait la division euclidienne de P par X^2+1. Soient alors Q et $R\in\mathbb{R}[X]$ tels que

$$P(X) = Q(X)(X^2+1)+R(X).$$

Or, on sait que

$$R(X) = cX+d$$

avec $c,d\in\mathbb{R}$ car quelque soit le polynôme, son reste dans la division euclidienne par X^2+1 est un polynôme de degré au plus 1. Ainsi,

$$a = \overline{Q(X)(X^2+1)+cX+d} = \overline{Q(X)}\times\overline{X^2+1}+\overline{cX+d} = \overline{Q(X)}\times\overline{0}+\overline{cX+d} = \overline{cX+d}\in A$$

donc $B\subseteq A$ donc $A = B$. □

Proposition 4.2.2. *Soit*

$$\begin{aligned}\varphi : \mathbb{R}[X] &\to \mathbb{C}\\ \overline{\alpha X+\beta} &\mapsto \alpha i+\beta.\end{aligned}$$

L'application φ est un morphisme d'anneaux bijectif entre $\mathbb{R}[X]/(X^2+1)$ et $\mathbb{C}$. Ainsi, $\mathbb{R}[X]/(X^2+1)$ et $\mathbb{C}$ sont isomorphes.

Démonstration. :
Montrons d'abord que φ est bien définie.
Soient $\overline{\alpha X+\beta}$ et $\overline{\alpha' X+\beta'}$ tels que $\overline{\alpha X+\beta} = \overline{\alpha' X+\beta'}$.

$$\alpha X+\beta-\alpha' X-\beta' = P(X)(X^2+1)$$

avec $P(X)\in\mathbb{R}[X]$.

Montrons que $\varphi(\overline{\alpha X+\beta}) = \varphi(\overline{\alpha' X+\beta'})$, c'est à dire que $\alpha i+\beta = \alpha' i+\beta'$ donc que $i(\alpha-\alpha')+\beta-\beta' = 0$. Or

$$(\alpha-\alpha')X+\beta-\beta' = P(X)(X^2+1)$$

donc

$$(\alpha-\alpha')i+\beta-\beta' = P(i)(i^2+1) = P(i)\times 0 = P(0)$$

donc $(\alpha-\alpha')i+\beta-\beta' = 0$ donc φ est bien définie car tout élément d'une même classe d'équivalence a la même image.

Montrons maintenant que φ est un morphisme d'anneaux.
Soient $\overline{aX+b}, \overline{cX+d}\in\mathbb{R}[X]/(X^2+1)$,

$$\varphi(\overline{aX+b}+\overline{cX+d}) = \varphi(\overline{aX+b+cX+d}) = ai+b+ci+d = \varphi(\overline{aX+b})+\varphi(\overline{cX+d}).$$

$$\varphi(\overline{aX+b}\times\overline{cX+d})=\varphi(\overline{acX^2+bcX+adX+bd})$$

or

$$acX^2+bcX+adX+bd=ac(X^2+1)+X(bc+ad)+bd-ac$$

donc

$$\varphi(\overline{acX^2+bcX+adX+bd})=\varphi(\overline{X(bc+ad)+bd-ac})=i(bc+ad)+bd-ac.$$

Ainsi,

$$\varphi(\overline{aX+b})\times\varphi(\overline{cX+d})=(ai+b)(ci+d)=-ac+bci+adi+bd=\varphi(\overline{aX+b}\times\overline{cX+d}).$$

$\varphi(\overline{1})=1$
donc φ est un morphisme d'anneaux.

Enfin, montrons qu'elle est bijective donc qu'elle est injective et surjective.
Soient $\overline{aX+b},\overline{cX+d}\in\mathbb{R}[X]/(X^2+1)$ tels que

$$\varphi(\overline{aX+b})=\varphi(\overline{cX+d}).$$

Donc $ai+b=ci+d$ et ainsi $i(a-c)=b-d$.
Par identification : $a=c$ et $b=d$ donc $aX=cX$ donc $aX+b=cX+b=cX+d$ car $b=d$ donc $\overline{aX+b}=\overline{cX+d}$ donc φ est injective.

Soit $c\in\mathbb{C}$, soient $a,b\in\mathbb{R}$ tel que $c=ai+b$, soit alors $P=aX+b$, $P\in\mathbb{R}[X]$ donc $\overline{P}\in\mathbb{R}[X]/(X^2+1)$,

$$\varphi(\overline{P})=\varphi(\overline{aX+b})=ai+b=c$$

donc $\forall c\in\mathbb{C}$,
$\exists\overline{P}\in\mathbb{R}[X]/(X^2+1)$ tel que $c=\varphi(\overline{P})$ donc φ est surjective.

Ainsi, φ est injective et surjective donc elle est bijective.

Par conséquent, φ est un morphisme d'anneaux bijectif entre $\mathbb{R}[X]/(X^2+1)$ et $\mathbb{C}$ donc $\mathbb{R}[X]/(X^2+1)$ est isomorphe à $\mathbb{C}$. □

Remarque 4.2.1. *Ainsi, on peut construire le corps des complexes $\mathbb{C}$ à l'aide de polynômes. Et $\mathbb{R}[X]/(X^2+1)\simeq\mathbb{C}$.*

4.3 Racine de polynôme dans un anneau quotient

Certains polynômes tel que X^2+1 n'admettent pas de racine dans le corps dans lequel ils sont définis, ici dans $\mathbb{R}$, mais en quotientant l'anneau des polynômes on peut lui trouver une racine.

Proposition 4.3.1. *:*
L'anneau quotient $\mathbb{R}[X]/(X^2+X+1)$ *est un anneau dans lequel le polynôme* X^2+X+1 *admet une racine.*

Démonstration. :

$$\overline{X^2+X+1} = \overline{X} \times \overline{X} + \overline{X} + \overline{1} = \overline{0}$$

donc $\overline{X}$ est une racine de X^2+X+1 dans $\mathbb{R}[X]/(X^2+X+1)$. □

En réalité, on peut montrer que cet exemple se généralise avec n'importe quel polynôme.

Proposition 4.3.2. *Soit* $P \in \mathbb{R}[X]$ *un polynôme sans racine dans* $\mathbb{R}$*. L'anneau quotient* $\mathbb{R}[X]/(P)$ *est un anneau où* P *admet une racine.*

Démonstration. :
Soit $P \in \mathbb{R}[X]$ donc soient $n \in \mathbb{N}$ et $(a_i)_{i\in[0;n]} \in \mathbb{R}$ tels que $P = \sum_{i=0}^{n} a_i X^i$.

$$\overline{P} = \overline{\sum_{i=0}^{n} a_i X^i} = \sum_{i=0}^{n} \overline{a_i} \times \overline{X^i} = \sum_{i=0}^{n} \overline{a_i} \times \overline{X}^i = \overline{0}$$

donc $\overline{X}$ est une racine de P dans $\mathbb{R}[X]/(P)$. □

Remarque 4.3.1. *L'anneau quotient* $\mathbb{R}[X]/(X^2+X+1)$ *est également isomorphe à* $\mathbb{C}$*. On pose* $j := \frac{1+i\sqrt{3}}{2}$ *donc* j *est une racine de* X^2+X+1*. Le morphisme d'anneaux bijectif entre* $\mathbb{R}[X]/(X^2+X+1)$ *et* $\mathbb{C}$ *est l'application suivante :*

$$\begin{aligned} \phi : \mathbb{R}[X]/(X^2+X+1) &\to \mathbb{C} \\ \overline{\alpha X+\beta} &\to \alpha j + \beta. \end{aligned}$$

On peut montrer comme avec φ *l'isomorphisme entre* $\mathbb{R}[X]/(X^2+1)$ *et* $\mathbb{C}$ *que* ϕ *est bien définie et que c'est bien un morphisme d'anneaux bijectif. Ainsi,* $\mathbb{R}[X]/(X^2+X+1) \simeq \mathbb{C}$*. Ainsi, on a construit* $\mathbb{C}$ *à partir d'une nouvelle base, en effet, on l'a construit à partir de* j *et non de* i*.*

4.4 Polynôme irréductible

Définition 4.4.1. *Soit* $P \in \mathbb{R}[X]$*. On dit que* P *est* ***irreductible*** *si* P *est non constant, et que toute décomposition de la forme* $P = Q \times R$ *avec* $Q, R \in \mathbb{R}[X]$ *implique que* Q *ou* R *est constant.*

Proposition 4.4.1. *Tout idéal de* $\mathbb{R}[X]$ *est un idéal engendré par un polynôme de* $\mathbb{R}[X]$*.*

Démonstration. Admis, preuve [P96],Chapitre II, Corollaire 3.32 et théorème 3.29. □

Proposition 4.4.2. *Soit* $P \in \mathbb{R}[X]$*. L'idéal engendré par* P *est maximal si et seulement si* P *est un polynôme irréductible.*

Démonstration. On va le démontrer par double implication.
($\Rightarrow$) Soit $P \in \mathbb{R}[X]$. Soit I l'idéal engendré par P alors $I = \{P \times Q, Q \in \mathbb{R}[X]\}$. Supposons que I est un idéal maximal. On va montrer que P est irréductible par l'absurde, donc on va supposer qu'il est réductible. Ainsi, soient $L, R \in \mathbb{R}[X]$ avec L et R des polynômes non constants tels que $P = L \times R$. Soit J l'idéal engendré par L. Alors $P \in J$ car P est un multiple de L donc $I \subseteq J$. Or, I est un idéal maximal, donc $J = I$ ou $J = A$.
On va procéder par disjonction des cas :

— si $J = I$ alors $L \in I$ or L est un diviseur de P. Mais comme P est un multiple de L alors $L = cP$ avec c une constante, donc R est un polynôme constant ainsi P est irréductible.
— si $J = A$ alors J est l'idéal engendré par le polynôme constant égal à 1 d'après les propositions 3.2.2 et 4.4.1. Ainsi, L est un polynôme constant donc P est irréductible.

Ainsi, dans tous les cas, P est irréductible.
($\Leftarrow$) Supposons que P est irréductible. Montrons alors que I l'idéal engendré par P est maximal. Ainsi, $I = \{PQ, Q \in \mathbb{R}[X]\}$. Soit J un ideal de A tel que $I \subseteq J$, comme J est un idéal de $\mathbb{R}[X]$ alors d'après la proposition 4.4.1 on a un $L \in \mathbb{R}[X]$ tel que $J = \{L \times D, D \in \mathbb{R}[X]\}$. Or comme $I \subseteq J$, on a $P \in J$ donc $P = L \times D$. Comme P est irréductible L est constant ou D est constant.
On va procéder par disjonction des cas :

— si L est un polynôme constant alors d'après la Proposition 3.2.2, $J = \mathbb{R}[X]$.
— si D est un polynôme constant alors $J \subseteq I$. Or, on a supposé $I \subseteq J$ donc $J = I$.

Ainsi, le seul ideal contenant strictement I est $\mathbb{R}[X]$. Par conséquent, l'idéal engendré par P est maximal. □

Références

[B18] G. Berhuy, *Algèbre, le grand combat.* , Calvage et Mounet, 2018.

[G97] I. Gozard, *Théorie de Galois.* Ellipses, 1997.

[L19] F. Liret, *Arithmétique : Cours et exercices corrigés.* Dunod, 2019.

[P96] D. Perrin, *Cours d'algèbre.* Ellipses, 1996.