– Chapitre 5 : Structure d'anneaux –

I. Rappels sur les anneaux.

I.1. Définition. Généralité.

Définition 1. On appelle *anneau* tout triplet $(A, +, \times)$ où A est un ensemble et $+$ et $\times$ sont deux lois de composition interne sur A vérifiant les propriétés suivantes :

1. $(A, +)$ est un *groupe abélien* (d'élément neutre noté 0 ou 0_A),

2. la loi $\times$ est *associative*,

3. la loi $\times$ admet un *élément neutre* (noté 1 ou 1_A),

4. $\times$ est distributive par rapport à $+$:

Si de plus, la loi $\times$ est commutative, on dit que $(A, +, \times)$ un *anneau commutatif*.

Exemple 1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ munis de l'addition et de la multiplication usuelles sont des anneaux commutatifs.

Exercice 1. Soit $(A, +, \times)$ un anneau.

1. Montrer que pour tout $a \in A, 0_A \times a = a \times 0_A = 0_A$.

2. Montrer que si A contient au moins deux éléments distincts, alors $0_A \neq 1_A$.

I.2. Notion d'intégrité.

Définition 2. Un anneau $(A, +, \times)$ est dit *intègre* s'il vérifie les trois propriétés suivantes :

1. l'anneau $(A, +, \times)$ est commutatif,

2. A contient au moins deux éléments,

3. $\forall (a, b) \in A^2,\ a \times b = 0 \Rightarrow (a = 0 \text{ ou } b = 0)$.

Exemple 2. Les anneaux $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont intègres.

Les anneaux $(\mathcal{F}(\mathbb{R}), +, \times)$, $(\mathbb{R}^{\mathbb{N}}, +, \times)$ et $(\mathcal{M}_n(\mathbb{R}), +, \times)$ avec $n \geqslant 2$ ne sont pas intègres.

Exercice 2. Montrer que dans un anneau intègre $(A,+,\times)$: $\forall (a,b,c)\in A^*\times A^2,\ ab=ac\Rightarrow b=c$.

I.3. Notion de sous-anneau.

Définition 3. On appelle *sous-anneau* d'un anneau $(A,+,\times)$ toute partie B de A telle que :

1. $1_A\in B$,

2. B est stable par la loi $+$,

3. B est stable par la loi $\times$,

4. B est stable par passage à l'opposé.

Exemple 3. $\mathbb{Z}$ est un sous-anneau de $(\mathbb{R},+,\times)$.

⚠ Le singleton $\{0\}$ est une partie de $\mathbb{R}$ stable par les deux lois $+$ et $\times$, stable par passage à l'opposé mais ce n'est pas un sous-anneau de $\mathbb{R}$ puisqu'il

Proposition 1. Une partie B de A est un sous-anneau de l'anneau $(A,+,\times)$ si, et seulement si, B est un sous-groupe de $(A,+)$ qui est stable par la loi $\times$ et qui contient 1_A.

Proposition 2. Tout sous-anneau muni des lois induites, est un anneau.

I.4. Morphisme d'anneaux.

Soit $(A,+,\times)$ et $(B,+,\times)$ deux anneaux (à au moins deux éléments).

Définition 4. On appelle *morphisme d'anneaux* de A dans B, toute application f de A dans B vérifiant :

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

2. $\forall (x,y)\in A^2, f(x+y)=f(x)+f(y)$

3. $\forall (x,y)\in A^2, f(x\times y)=f(x)\times f(y)$.

Remarque 1. Si f est un morphisme d'anneaux de $(A,+,\times)$ dans $(B,+,\times)$, alors f est en particulier un morphisme de groupe de $(A,+)$ dans $(B,+)$. Le vocabulaire des morphismes de groupes sera donc toujours utilisé pour des morphismes d'anneaux : endomorphisme, isomorphisme, automorphisme, noyau, et image. Le noyau de f est donc défini par : $\operatorname{Ker} f=\{x\in A\mid f(x)=0_B\}$.

La caractérisation de l'injectivité par le noyau est donc toujours vraie pour un morphisme d'anneaux.

On remarque aussi que $f(0_A)=0_B$ puisque f est un morphisme de groupe de $(A,+)$ dans $(B,+)$.

Remarque 2. Pour n'importe quel anneau $(A,+,\times)$, Id_A est un endomorphisme d'anneau.
Si $(B,+,\times)$ possède au moins deux éléments l'application constante égale à 0_B n'est pas un endomorphisme d'anneau car :

Exercice 3. Déterminer tous les endomorphismes de l'anneau $(\mathbb{Z}, +, \times)$.

Proposition 3. Soit f un morphisme d'anneaux de A dans B. Alors, Im f est un sous-anneau de B, mais Ker f n'est pas un sous-anneau de A.

Démonstration.

□

I.5. Groupe des inversibles.

Proposition 4. L'ensemble des éléments inversibles pour $\times$ d'un anneau $(A, +, \times)$, muni de la loi $\times$ est un groupe, appelé *groupe des inversibles*. On note $A^\times$ cet ensemble.

Démonstration.

□

Exemples 4. $\mathbb{Z}^\times =$ $\mathbb{Q}^\times =$ $\mathbb{R}^\times =$ $\mathbb{C}^\times =$ $\mathcal{M}_n(\mathbb{K})^\times =$

I.6. Corps.

Définition 5. On appelle *corps* tout anneau commutatif $(\mathbb{K}, +, \times)$ contenant au moins deux éléments, et dont tout élément non nul est inversible (i.e. $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$).
Autrement-dit, un corps est un anneau $(\mathbb{K}, +, \times)$ tel que $(\mathbb{K} \setminus \{0\}, \times)$ soit un groupe abélien.

Exemples 5. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ munis des lois usuelles, sont des corps, mais pas $\mathbb{Z}$ puisque $\mathbb{Z}^\times \neq \mathbb{Z}^*$.

Remarque importante. Par définition, un corps contient toujours au moins deux éléments. On a déjà vu que dans ce cas : $0 \neq 1$.

Exercice 4. Montrer que tout corps est un anneau intègre.

Définition 6. On appelle *sous-corps* tout sous-anneau $\mathbb{L}$ d'un corps $(\mathbb{K}, +, \times)$ tel que pour tout élément non nul x de $\mathbb{L}$, $x^{-1} \in \mathbb{L}$.

Remarque 4. Un sous-corps, muni des lois induites, est lui-même un corps.

Exemples 6. $\mathbb{Q}$ et $\mathbb{R}$ sont deux sous-corps de $\mathbb{C}$.

II. Compléments sur les anneaux.

II.1. Produit fini d'anneaux.

Soit $n \in \mathbb{N}^*$. Pour tout $i \in [\![1, n]\!]$, $(A_i, +, \times)$ désigne un anneau.

Proposition 5. Les deux opérations internes $+$ et $\times$ définies pour tout $(a_1, \dots, a_n)$ et $(b_1, \dots, b_n)$ dans $A_1 \times \cdots \times A_n$ par :

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$$
$$(a_1, \dots, a_n) \times (b_1, \dots, b_n) = (a_1 \times b_1, \dots, a_n \times b_n)$$

munissent $A_1 \times \cdots \times A_n$ d'une structure d'anneau.

Démonstration.

□

Remarque 5. On en déduit que si $(A, +, \times)$ est un anneau, alors on peut définir l'anneau $(A^n, +, \times)$. Ceci permet notamment de définir les anneaux $(\mathbb{R}^n, +, \times)$ et $(\mathbb{C}^n, +, \times)$.

Exercice 5. Déterminer les éléments inversibles de l'anneau $A_1 \times \cdots \times A_n$.

II.2. Idéal d'un anneau commutatif.

Définition 7. On appelle *idéal* d'un anneau commutatif $(A, +, \times)$ tout sous-groupe I de $(A, +)$ qui vérifie de plus :

$$\forall a \in A, \forall x \in I, a \times x \in I.$$

Proposition 6. Soit A un anneau commutatif, et B un anneau quelconque.
Si f est un morphisme de l'anneau A dans l'anneau B, alors son noyau $\operatorname{Ker} f$ est un idéal de A.

Démonstration.

□

Proposition 7. Intersection et somme d'idéaux.
Soit I et J deux idéaux d'un anneau commutatif A. Alors :
- $I \cap J$ est un idéal de A,
- $I + J = \{x + y \mid (x, y) \in I \times J\}$ est un idéal de A.

Démonstration.

□

Remarque 6. On peut généraliser cette proposition au cas d'une intersection quelconque d'idéaux, et au cas d'une somme finie d'idéaux.

II.3. Idéal engendré par un élément.

Soit $(A, +, \times)$ un anneau commutatif et soit $a \in A$. On définit une partie de A, notée aA par :

$$aA = \{a \times x \mid x \in A\}.$$

Proposition 8. Pour tout $a \in A$, aA est un idéal de l'anneau A. C'est même le plus petit idéal (au sens de l'inclusion) de A contenant a i.e. que pour tout idéal I de A :

$$a \in I \Rightarrow aA \subset I.$$

On l'appelle l'idéal *engendré* par a.

Démonstration.

□

Remarque 7. Un idéal de A qui peut s'écrire sous la forme aA i.e. qui est engendré par un seul élément est appelé *idéal principal*.
Un anneau commutatif et intègre dont tous les idéaux sont principaux est appelé *anneau principal*.

II.4. Divisibilité dans un anneau commutatif intègre.

Nous allons ici généraliser la notion de divisibilité déjà rencontrée dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$ au cas d'un anneau commutatif intègre $(A, +, \times)$.

Définition 8. Soit a et b deux éléments d'un anneau commutatif intègre $(A, +, \times)$.
On dit que a *divise* de b, s'il existe $k \in A$ tel que $b = ka$.
On le note $a \mid b$. Sa négation sera notée : $a \nmid b$.

Remarque 8. S'il existe $k \in A$ tel que $b = ka$ et si $a \neq 0$ alors l'élément k est unique En effet:

Proposition 9. Interprétation en termes d'idéaux.
Soit a et b deux éléments de l'anneau A. On a :

$$a \mid b \Leftrightarrow bA \subset aA.$$

Démonstration.

□

II.5. Idéaux de l'anneau $(\mathbb{Z}, +, \times)$.

Pour tout $a \in \mathbb{Z}$ la partie de $\mathbb{Z}$, notée $a\mathbb{Z}$ et définie par :

$$a\mathbb{Z} = \{ak \mid k \in \mathbb{Z}\}$$

est, comme nous l'avons vu précédemment, un idéal de l'anneau $\mathbb{Z}$ appelé idéal engendré par a.

Proposition 10. Réciproquement, tout idéal de $\mathbb{Z}$ peut s'écrire sous la forme $a\mathbb{Z}$ pour un unique $a \in \mathbb{N}$.

Démonstration.

□

Remarque 9. Cette proposition peut se reformuler en disant que tout idéal de $\mathbb{Z}$ est un idéal principal ou encore que l'anneau $\mathbb{Z}$ est un anneau principal.

Définition du PGCD et du PPCM de $n \geqslant 2$ entiers relatifs.

Soit $n \geqslant 2$ et soit $a_1, \dots, a_n$ des entiers relatifs.

Proposition 11.

1. Il existe un unique entier naturel d tel que :

$$d\,\mathbb{Z} = a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}.$$

2. On a existence d'une relation de Bézout :

$$\exists (u_1, \dots, u_n) \in \mathbb{Z}^n,\ d = a_1u_1 + \cdots + a_nu_n.$$

3. Cet entier vérifie, pour tout $k \in \mathbb{Z}$,

$$k \mid d \ \Leftrightarrow\ (\forall i \in [\![1, n]\!],\ k \mid a_i)\,.$$

Cet entier d est appelé le PGCD de $a_1, \dots, a_n$.

⚠ On retrouve le théorème de Bézout.

Démonstration.

□

On a de manière évidente :

Proposition 12.

1. Il existe un unique entier naturel m tel que :

$$m\,\mathbb{Z} = a_1\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z}.$$

2. Cet entier vérifie, pour tout $k \in \mathbb{Z}$,

$$m \mid k \ \Leftrightarrow\ (\forall i \in [\![1, n]\!],\ a_i \mid k)\,.$$

Cet entier m est appelé le PPCM de $a_1, \dots, a_n$.

III. Anneaux $\mathbb{Z}/n\mathbb{Z}$.

Soit n entier naturel vérifiant $\boxed{n \geqslant 2}$.

Le but de cette partie est de définir les anneaux $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$; anneaux qui jouent un rôle important en arithmétique dans $\mathbb{Z}$.

Lemme. Soit $(a, b, a', b') \in \mathbb{Z}^4$. Si $a \equiv a'\ [n]$ et si $b \equiv b'\ [n]$, alors : $a \cdot b \equiv a' \cdot b'\ [n]$.

Démonstration.

□

Proposition 13. On définit une loi de multiplication sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$ en posant :

$$\forall (a, b) \in \mathbb{Z}^2, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Démonstration.

⚠ Il est important de prouver que le résultat ne dépend pas des représentants a et b choisis pour les classes d'équivalence $\overline{a}$ et $\overline{b}$.

Soit un élément quelconque a' de $\overline{a}$ et un élément b' de $\overline{b}$. Montrons que $\overline{a \cdot b} = \overline{a' \cdot b'}$

□

Proposition 14. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif.

Démonstration. On vérifie facilement les différents points de la définition d'un anneau.

Bien noter que le neutre de l'addition est $\overline{0}$ et le neutre de la multiplication est $\overline{1}$. □

Exemple 7. Posons $n = 6$. On a donc : $\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$.
$\overline{2} + \overline{4} =$ et $\overline{5} \cdot \overline{5} =$

L'opposé de $\overline{2}$ est et l'opposé de $\overline{5}$ est
L'élément $\overline{5}$ est-il inversible ? Et l'élément $\overline{2}$? On rappelle que le terme "inversible" signifie symétrisable pour la loi $\cdot$.

L'anneau $(\mathbb{Z}/6\mathbb{Z}, +, \cdot)$ est-il intègre ?

Proposition 15. La projection canonique, notée π_n et définie par :

$$\begin{array}{rccc} \pi_n & : & \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & & x & \mapsto & \overline{x} \end{array}$$

est un morphisme d'anneaux.

Théorème 1. Soit $a \in \mathbb{Z}$. Alors, $\overline{a}$ est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ si, et seulement si, $a \wedge n = 1$.

Démonstration.

□

Théorème 2. Les affirmations suivantes sont équivalentes :

1. l'entier n est un nombre premier,

2. l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps,

3. l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un intègre.

Démonstration.

□

Notation. Lorsque p est premier on note $\mathbb{F}_p$, le corps $\mathbb{Z}/p\mathbb{Z}$.

Rappel. $\pi_n(k)$ désigne la classe d'équivalence de k pour la relation de congruence modulo n.

Théorème 3. Théorème chinois.
Soit $(n,m) \in (\mathbb{N}^*)^2$. Si $n \wedge m = 1$, alors l'application :

$$\begin{array}{rccc} \psi & : & \mathbb{Z}/(nm)\mathbb{Z} & \to & (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \\ & & \pi_{nm}(k) & \mapsto & (\pi_n(k), \pi_m(k)) \end{array}$$

est un isomorphisme d'anneaux.

L'application ψ ci-dessus est qualifiée d'*isomorphisme naturel* de $\mathbb{Z}/(nm)\mathbb{Z}$ sur $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$.

Démonstration.

□

Remarque importante. La réciproque est vraie puisque si les anneaux $\mathbb{Z}/(nm)\mathbb{Z}$ sur $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ sont isomorphes alors il en est de même des groupes additifs. Et on a déjà prouvé que dans ce cas $n \wedge m = 1$.

Corollaire 1. Théorème chinois.
Soit $(n,m) \in (\mathbb{N}^*)^2$ tel que $n \wedge m = 1$. Pour tout $(a,b) \in \mathbb{Z}^2$,

- il existe au moins une solution $k \in \mathbb{Z}$ au système :

$$(S) \quad \begin{cases} k & \equiv & a & [n] \\ k & \equiv & b & [m] \end{cases}$$

- L'ensemble des solutions de (S) est l'ensemble des entiers ℓ tels que $\ell \equiv k\ [nm]$

Exercice 6. Résoudre le système :

$$(S) \quad \begin{cases} x & \equiv & 2 & [10] \\ x & \equiv & 5 & [13] \end{cases}$$

Par récurrence sur r, on obtient :

Corollaire 2. Si $n_1, \dots, n_r$ sont des entiers naturels premiers entre eux deux à deux, alors les anneaux $\mathbb{Z}/(n_1 \cdots n_r)\mathbb{Z}$ et $(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})$ sont isomorphes.

IV. Indicatrice d'Euler φ.

Définition 9. On appelle *indicatrice d'Euler* l'application φ définie pour tout $n \in \mathbb{N}^*$ par :

$$\varphi(n) = \text{Card } \{k \in [\![1, n]\!] \mid k \wedge n = 1\}.$$

Proposition 16. Pour tout $n \geqslant 2$ on a : $\varphi(n) \leqslant n-1$ avec égalité si, et seulement si, n est premier.

Démonstration.

□

Quelques valeurs de $\varphi(n)$:

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$\varphi(n)$													

Proposition 17. Pour tout $n \in \mathbb{N}^*$, $\varphi(n)$ est égal :
- au nombre d'éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$;
- au nombre de générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$;
- au nombre de racines primitives n-ièmes de l'unité ;
- et plus généralement au nombre de générateurs de n'importe quel groupe cyclique d'ordre n.

Proposition 18. Soit p un nombre premier. Pour tout $k \in \mathbb{N}^*$, on a $\varphi(p^k) = p^k - p^{k-1}$.

Démonstration.

□

Proposition 19. Si n et m sont deux entiers naturels premiers entre eux, alors $\varphi(nm) = \varphi(n)\varphi(m)$.
Plus généralement, si $n_1, \ldots, n_r$ sont des entiers naturels premiers entre eux deux à deux, alors $\varphi(n_1 \cdots n_r) = \varphi(n_1) \cdots \varphi(n_r)$.

⚠ Ne pas oublier l'hypothèse $n \wedge m = 1$. Par exemple, $\varphi(2 \times 4) = 4$ alors que $\varphi(2) \times \varphi(4) = 2$.

Démonstration.

□

Proposition 20. Pour tout $n \in \mathbb{N}^*$ de décomposition en produit de facteurs premiers $n = p_1^{k_1} \cdots p_r^{k_r}$, où les k_i sont des entiers naturels non nuls, on a :

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Démonstration.

□

Théorème 4. Théorème d'Euler.
Soit $n \in \mathbb{N}^*$. Pour tout $a \in \mathbb{Z}$, si $a \wedge n = 1$, alors : $a^{\varphi(n)} \equiv 1\ [n]$.

Démonstration.

□

Corollaire 3. Le petit théorème de Fermat.
Soit p un nombre premier.

- Pour tout $a \in \mathbb{Z}$, si $a \wedge p = 1$, alors : $a^{p-1} \equiv 1\ [p]$.
- Pour tout $a \in \mathbb{Z}$, $a^p \equiv a\ [p]$.

⚠ Dans le petit théorème de Fermat p est premier. Donc, l'hypothèse $a \wedge p = 1$ équivaut à dire :

V. Anneaux $\mathbb{K}[X]$.

Dans ce paragraphe, $\mathbb{K}$ est un sous-corps de $\mathbb{C}$.

V.1. Rappels sur les polynômes.

Proposition 21. L'anneau $(\mathbb{K}[X], +, \times)$ est intègre.

Démonstration.

□

Proposition 22. L'ensemble $\mathbb{K}[X]^\times$ des éléments inversibles de $\mathbb{K}[X]$ est l'ensemble des polynômes de degré 0. On peut donc écrire : $\mathbb{K}[X]^\times = \mathbb{K}_0[X] \setminus \{0\} = \mathbb{K} \setminus \{0\}$.

Démonstration.

□

Proposition 23. On a : $(P \mid Q \text{ et } Q \mid P) \Leftrightarrow (\exists \alpha \in \mathbb{K}^*,\ P = \alpha Q)$.
Dans ce cas, on dit que P et Q sont *associés*.

Démonstration.

□

Théorème 5. Division euclidienne.
Soit $(A, B) \in \mathbb{K}[X]^2$ avec $B \neq 0$. Il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que :

$$A = BQ + R, \qquad \text{avec} \qquad \deg R < \deg B.$$

Q est appelé le *quotient* et R le *reste* de la division euclidienne de A par B.

V.2. Idéaux de $\mathbb{K}[X]$.

Théorème 6. L'anneau $(\mathbb{K}[X], +, \times)$ est principal, i.e. que tout idéal de $\mathbb{K}[X]$ est engendré par un polynôme. Autrement-dit, pour tout idéal I de $\mathbb{K}[X]$ il existe au moins un polynôme M tel que :

$$I = M\mathbb{K}[X] = \{M \times P \mid P \in \mathbb{K}[X]\}.$$

Si on suppose de plus que le polynôme M est unitaire ou nul, il est alors unique et appelé *le générateur normalisé* de I.

Démonstration.

□

V.3. PGCD et PPCM.

Soit $n \geqslant 2$ et soit $A_1, \dots, A_n$ des éléments de $\mathbb{K}[X]$.

Proposition 24.

1. Il existe un unique polynôme D unitaire ou nul tel que :

$$D\mathbb{K}[X] = A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X].$$

2. On a existence d'une relation de Bézout :

$$\exists (U_1, \dots, U_n) \in \mathbb{K}[X]^n,\ D = A_1U_1 + \cdots + A_nU_n.$$

3. Ce polynôme vérifie, pour tout $P \in \mathbb{K}[X]$,

$$P \mid D \ \Leftrightarrow\ (\forall i \in [\![1, n]\!],\ P \mid A_i)\,.$$

Cet polynôme D est appelé le PGCD de $A_1, \dots, A_n$.

Démonstration.

□

⚠ Un polynôme associé au PGCD est parfois appelé un PGCD.

Proposition 25.

1. Il existe un unique polynôme M unitaire ou nul tel que :

$$M\mathbb{K}[X] = A_1\mathbb{K}[X] \cap \cdots \cap A_n\mathbb{K}[X].$$

2. Cet polynôme vérifie, pour tout $P \in \mathbb{K}[X]$,

$$M \mid P \ \Leftrightarrow\ (\forall i \in [\![1, n]\!],\ A_i \mid P)\,.$$

Cet polynôme M est appelé le PPCM de $A_1, \dots, A_n$.

⚠ Un polynôme associé au PPCM est parfois appelé un PPCM.

V.4. Polynômes irréductibles.

Définition 10. On appelle *polynôme irréductible* de $\mathbb{K}[X]$ tout polynôme P vérifiant :
- $\deg P \geqslant 1$ i.e. P est non constant,
- les seuls diviseurs de P sont les constantes non nulles et les polynômes associés à P, i.e. :

$$\forall (A,B) \in \mathbb{K}[X]^2,\ P = AB \ \Rightarrow\ (\deg A = 0 \quad \text{ou} \quad \deg B = 0).$$

Remarque 11. Pour rappel, on dit qu'un polynôme est associé à P s'il s'écrit αP avec $\alpha \in \mathbb{K}^*$. Concrètement, la deuxième condition dit qu'on ne peut pas trouver de factorisation de P autre que celles de la forme $P = \alpha^{-1} \times (\alpha P)$ avec $\alpha \in \mathbb{K}^*$, ou encore on ne peut pas écrire P comme un produit de deux polynômes non constants.

Remarque 12. Les polynômes de degré 1 sont irréductibles quel que soit le corps $\mathbb{K}$. En effet :

Théorème 7. Tout polynôme non constant de $\mathbb{K}[X]$ se décompose en un produit de polynômes irréductibles.

Si l'on écrit cette décomposition sous la forme d'un élément de $\mathbb{K}$ et d'un produit de polynômes irréductibles unitaires, elle est alors unique à l'ordre près des facteurs.

Démonstration. On démontre facilement la partie existence en procédant par récurrence forte sur le degré du polynôme à décomposer. □

Remarque importante. On va voir que la forme des polynômes irréductibles dépend fortement du corps $\mathbb{K}$ sur lequel on travaille. D'ailleurs, si l'on travaillait sur un autre corps que $\mathbb{R}$ ou $\mathbb{C}$ les polynômes irréductibles seraient encore différents.

Théorème 8. Théorème de d'Alembert-Gauss.

Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine complexe.

Démonstration. Admis. □

Irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$.

Proposition 26. Les polynômes irréductibles de $\mathbb{C}[X]$ sont

Démonstration.

□

Remarque importante. Ainsi tout polynôme non constant de $\mathbb{C}[X]$ est *scindé* i.e. admet une factorisation de la forme :

$$P = \lambda \prod_{i=1}^{p} (X - \alpha_i)^{r_i},$$

où $\lambda \in \mathbb{C}^*$ et $\alpha_1, \alpha_2, \ldots, \alpha_p$ sont les racines complexes distinctes de P, et $r_1, r_2, \ldots, r_p$ leur multiplicité respective.

Proposition 27. Les polynômes irréductibles de $\mathbb{R}[X]$ sont :

-
-

Démonstration.

□

VI. Algèbres.

Définition 11. On appelle $\mathbb{K}$-*algèbre*, ou *algèbre sur le corps* $\mathbb{K}$ tout quadruplet $(E, +, \times, \cdot)$ tel que :

1. $(E, +, \times)$ est un anneau,

2. $(E, +, \cdot)$ est un $\mathbb{K}$-espace-vectoriel,

3. $\forall \alpha \in \mathbb{K},\ \forall (x, y) \in E^2,\ (\alpha \cdot x) \times y = \alpha \cdot (x \times y) = x \times (\alpha \cdot y)$.

Remarque 15. La multiplication interne $\times$ est bilinéaire. En effet :

Exemple 8. $\mathbb{K}[X], \mathcal{L}(E), \mathcal{M}_n(\mathbb{K}), \mathcal{F}(X, K)$ sont des $\mathbb{K}$-algèbres (où X est un ensemble quelconque).
Préciser les lois : $(\mathbb{K}[X],\quad)$, $(\mathcal{L}(E),\quad)$, $(\mathcal{M}_n(\mathbb{K}),\quad)$, $(\mathcal{F}(X, \mathbb{K})\quad)$

Définition 12. On appelle *sous-algèbre* d'une $\mathbb{K}$-algèbre E tout sous-espace vectoriel de E, stable pour le produit et contenant 1_E.
Autrement-dit, une sous-algèbre de E est une partie de E qui est à la fois un sous-espace vectoriel de E et un sous-anneau de E.

Définition 13. On appelle *morphisme* d'une $\mathbb{K}$-algèbre E dans une $\mathbb{K}$-algèbre F, toute application de E dans F qui est à la fois un morphisme d'anneau et une application linéaire.

Remarque 16. Le noyau d'un morphisme d'algèbre est donc à la fois un idéal de E et un sous-espace vectoriel de E.

Soit $a \in \mathbb{K}$. Le morphisme d'évaluation $P \mapsto P(a)$ est un morphisme de $\mathbb{K}$-algèbres.