Les anneaux

Arithmétique dans $\mathbb{Z}$ et $\mathbb{K}[X]$

Pascal DELAHAYE - d'après le cours de David Delaunay

6 octobre 2024

Après la structure de groupe que nous venons de voir, vient la structure d'anneau $(A,\ +,\ \times)$.
La présence de deux lois de composition internes (notées en général + et $\times$) vérifiant des propriétés usuelles telles que la commutativité, l'associativité, la distributivité, la présence d'éléments neutres (...) rend cette structure extrêmement intéressante. En particulier, dans un anneau intègre, nous retrouvons la propriété de divisibilité sur laquelle repose toutes les propriétés d'arithmétique.

Ce chapitre sera donc l'occasion de revoir les notions d'arithmétique dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$ vues en MPSI (à réviser en autonomie) et d'étudier en détail la "fonction indicatrice" d'Euler rencontrée dans le chapitre sur les groupes.

Nous nous intéresserons également à la notion d'Idéal d'un anneau commutatif, notion qui sera utilisée pour :

- établir certaines propriétés usuelles d'arithmétique dans un anneau intègre
- étudier l'ensemble des polynômes annulateurs dans le chapitre sur la réduction algébrique des endomorphismes.

La structure de corps, indispensable à la définition des $\mathbb{K}$-espaces vectoriels et des $\mathbb{K}$-algèbres, sera très rapidement abordée.

Questions de cours à maîtriser pour les colles :

1. La formule de l'indicatrice d'Euler
2. Les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$
   Application à la résolution d'équations algébriques simples
3. Le théorème des restes chinois
   Application à la résolution d'un système de congruence
4. Définition et propriétés du PGCD et du PPCM de deux entiers
5. Théorème d'Euler et petit théorème de Fermat
   Application à la simplification de $a^n[p]$ lorsque $a \wedge p = 1$
6. Les idéaux de $\mathbb{Z}$ et de $\mathbb{K}[X]$

Table des matières

1 Structure d'anneau

Dans toute cette partie, A représente un anneau $(A,\ +,\ \times)$.

1. Définition :

Cf cours MPSI (à réviser en autonomie)

DÉFINITION : **Anneau**

$(A,\ +,\ \times)$ est un anneau lorsque $\begin{cases} (A,\ +) \text{ est une groupe abélien} \\ \times \text{ est une lci } \begin{cases} \text{associative} \\ \text{distributive à droite et à gauche} \\ \text{avec un élément neutre} \end{cases} \end{cases}$

⚠ *On remarquera en particulier que :*

- *les éléments d'un anneau n'ont pas nécessairement de symétrique pour la loi $\times$.*
- *Si la deuxième lci $\times$ est commutative, on dit que A est un anneau commutatif.*

Notations : les éléments neutres sont notés $\begin{cases} 0_A \\ 1_A \end{cases}$ et les symétriques $\begin{cases} -x \\ x^{-1} \text{ s'il existe} \end{cases}$.

Exemples : Anneaux stricts usuels (qui NE SONT PAS des corps)

- Nombres : $(\{0\},\ +,\ \times)$, $(\mathbb{Z},\ +,\ \times)$
- Fonctions : $(\mathcal{F}(X,\ \mathbb{K}),\ +,\ \times)$, $(\mathbb{K}^{\mathbb{N}},\ +,\ \times)$, $(\mathfrak{M}_n(\mathbb{K}),\ +,\ \times)$, $(\mathcal{L}(E),\ +,\ \circ)$
- Autres : $(\mathbb{K}[X],\ +,\ \times)$, $(\mathbb{Z}/n\mathbb{Z},\ +,\ \times)$ pour n non premier

2. Calculs complémentaires :

Cf cours MPSI (à réviser en autonomie)

- Formules de base : (« naturelles »)
  - ▷ $0_A \times a = a \times 0_A = 0_A$
  - ▷ $-(a \times b) = (-a) \times b = a \times (-b)$
  - ▷ $n(a \times b) = (na) \times b = a \times (nb)$ pour tout $n \in \mathbb{Z}$
- Lorsque $ab = ba$
  - ▷ Formule du binôme : $\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$
  - ▷ Formule de factorisation : $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b^1 + \cdots + a^1 b^{n-2} + b^{n-1})$
  - ▷ Formule de factorisation pour $b = 1_A$: $a^n - 1_A = (a - 1_A)(a^{n-1} + a^{n-2} + \cdots + a^1 + 1_A)$

Question : Que dire d'un anneau tel que $0_A = 1_A$?

3. Eléments remarquables d'un anneau :

Cf cours MPSI (à réviser en autonomie)

DÉFINITION : **Diviseur de zéro**
Soit $a \in A$ non nul.
On dit que a est un *diviseur de* 0 lorsque qu'il existe $b \in A$ $(b \neq 0)$ tel que $ab = 0_A$.

Remarques :

→ Les éléments inversibles d'un anneau ne sont pas des diviseurs de 0.

→ ⚠ On ne peut pas simplifier par $a \neq 0$ dans $ab = ac$ si a est un diviseur de 0.

Exemples d'anneaux qui admettent des diviseurs de 0 :

- Matrices
- Fonctions
- $\mathcal{L}(E)$
- $\mathbb{Z}/n\mathbb{Z}$ (avec n non premiers)
- Suites
- $\mathbb{R}^2$

Définition : **Elément idempotent**
Dans un anneau A.
Un élément $a \in A$ est dit *idempotent* lorsque $a^2 = a$

Exemples :

→ Cas d'un anneau intègre
→ Projecteurs de l'anneau $\mathcal{L}(E)$
→ $(0,\ 1)$ dans $\mathbb{R}^2$
→ $\bar{3}$ dans $\mathbb{Z}/6\mathbb{Z}$

Définition : **Elément nilpotent** :
Dans un anneau A.
Un élément $a \in A$ est dit *nilpotent* lorsqu'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0_A$.

Le plus petit $n \in \mathbb{N}^*$ tel que $a^n = 0_A$ est alors appelé l'*ordre de nilpotence* de a.

Exemples :

- 0_A dans A
- $\bar{2}$ dans $\mathbb{Z}/8\mathbb{Z}$,
- $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ dans $\mathfrak{M}_2(\mathbb{R})$

Propriété : ♡ Lorsque a est nilpotent, $1_A - a$ est inversible.

Exemple : Les matrices de $\mathfrak{M}_n(\mathbb{K})$ de la forme $A = \begin{pmatrix} 0 & \star & \dots & \star \\ \vdots & 0 & \star & \vdots \\ \vdots & & \ddots & \star \\ 0 & \dots & \dots & 0 \end{pmatrix}$ sont nilpotentes.

Preuve : Conséquence immédiate du théorème de Cayley-Hamilton (vu plus tard).

4. Groupes des inversibles : (ou des unités)

Cf cours MPSI (à réviser en autonomie)

Dans un anneau $(A,\ +,\ \times)$.

Eléments inversibles : Il s'agit des éléments de A qui admettent un symétrique pour $\times$

Lorsque x et y sont inversibles, on a : $\begin{cases} (x^{-1})^{-1} = x \\ (xy)^{-1} = y^{-1}x^{-1} \end{cases}$ (Attention à l'ordre)

Le groupe des inversibles :

- C'est l'ensemble des éléments inversibles de A muni de la loi $\times$
- On le note A^* ou $U(A)$

- $(A^*, \times)$ est un groupe

Le groupe des inversibles intervient dans la caractérisation des « éléments associés »d'un anneau.

Exemples :

- $U(\mathbb{Z}) = \{-1,\ 1\}$
- $U(\mathbb{R}) = \mathbb{R}^*$
- $U(\mathbb{K}[X]) = \mathbb{K}_0[X]\backslash\{0\}$
- $U(\mathfrak{M}_n(\mathbb{K})) = \mathrm{GL}_n(\mathbb{K})$
- $U(\mathcal{L}(E)) = \mathrm{GL}(\mathbb{E})$

Exemple : Quel est le groupe des inversibles de l'anneau $(\mathcal{F}(\mathbb{R},\ \mathbb{R}),\ +,\ \times)$?

5. Produit fini d'anneaux :

Cf cours MPSI (à réviser en autonomie)

- Définition : $A_1 \times A_2 \times \cdots \times A_m$ avec les lci produit $+$ et $\times$ usuelles
- Eléments neutres : $(0_1, \ldots,\ 0_m)$ et $(1_1,\ \ldots,\ 1_m)$
- Eléments opposés : $-x = (-x_1,\ \ldots,\ -x_m)$
- Eléments inversibles : $x^{-1} = (x_1^{-1},\ \ldots,\ x_m^{-1})$

Groupe des inversibles : $U(A) = U(A_1) \times \cdots \times U(A_m)$.

Exemple : $(\mathbb{Z}^2,\ +,\ \times)$ est l'anneau produit $\mathbb{Z} \times \mathbb{Z}$.

---

6. Sous-anneau de $(A,\ +,\ \times)$:

Cf cours MPSI (à réviser en autonomie)

- Def° 1 : Partie stable de A par $\begin{cases} \text{les deux lci} \\ \text{la symétrisation pour } + \end{cases}$ et contenant 1_A (important).
- Def° 2 : Anneau inclus dans un anneau avec $\begin{cases} \text{les MEMES lci} \\ \text{les MEMES éléments neutres} \end{cases}$.

Remarque : Un sous-anneau de A est nécessairement un sous-groupe de $(A, +)$.

Méthode : Pour montrer que B est un sous-anneau de A

On vérifie que :

- $B \subset A$
- $0_A,\ 1_A \in B$ (on peut se dispenser de $0_A \in B$)
- B est stable pour $+$ et $\times$
- B est stable par passage à l'opposé

Exemples : Sous-anneaux

- $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$.
- L'ensemble des suites réelles convergentes est un sous-anneau de $\mathbb{R}^{\mathbb{N}}$.
- L'ensemble des polynômes pairs est un sous-anneau de l'anneau $\mathbb{R}[X]$
- $\mathbb{Z}[\sqrt{3}] = \{x + y\sqrt{3} \mid x,\ y \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{R}$
- $\mathbb{Z}[i] = \{x + iy \mid x,\ y \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$.

Exemples : Ne sont pas des sous-anneaux

- $2\mathbb{Z}$ n'est pas un sous-anneau de l'anneau $\mathbb{Z}$
- L'ensemble des suites convergentes vers 0 n'est pas un sous-anneau de l'anneau $\mathbb{R}^{\mathbb{N}}$
- L'ensemble des polynômes impairs n'est pas un sous-anneau de l'anneau $\mathbb{R}[X]$

7. Anneaux intègres :

Cf cours MPSI (à réviser en autonomie)

DÉFINITION : **Anneau intègre**

Un anneau intègre est un anneau $\begin{cases} \text{non réduit à } \{0\} \quad (\text{on dit aussi } \ll \text{ non trivial } \gg) \\ \text{commutatif} \\ \text{sans diviseur de 0} \end{cases}$

Exemples usuels : $\mathbb{R}[X]$, $\mathbb{Z}$.

PROPOSITION : **Les bonnes propriétés d'un anneau intègre**

Les anneaux intègres sont nommés ainsi car ils possèdent les "bonnes propriétés" suivantes :

- Commutativité de $\times$
- Pas de diviseur de zéro
- 0_A est le seul élément nilpotent
- Simplification par $a \neq 0_A$ de $ab = ac$ et de $ba = ca$
- Notion de divisibilité (vue plus tard)

♡ *Il ne manque plus que la division pour pouvoir travailler comme on le fait habituellement dans* $\mathbb{R}$.

Preuve :

Exercice : 1

1. Montrer que un anneau intègre, $x^2 = 1$ n'a que 2 solutions.

♡ *Si dans un anneau, l'équation* $x^2 = 1$ *admet plus de deux solutions, c'est qu'il n'est pas intègre.*

2. Montrer en utilisant la méthode précédente que l'anneau $\mathfrak{M}_2(\mathbb{R})$ n'est pas intègre.

2 L'anneau : $(\mathbb{Z}/n\mathbb{Z},\ +,\ \times)$

DÉFINITION : **Multiplication sur** $\mathbb{Z}/n\mathbb{Z}$

On définit la loi $\times$ sur $\mathbb{Z}/n\mathbb{Z}$ par : $\quad \bar{x} \times \bar{y} = \overline{x \times y}$

Remarque : Cette définition a bien un sens car $\overline{x \times y}$ *est bien indépendant des représentants* x *et* y *choisis.*

PROPOSITION : **L'anneau** $(\mathbb{Z}/n\mathbb{Z},\ +,\ \times)$

$(\mathbb{Z}/n\mathbb{Z},\ +,\ \times)$ est un anneau dont les éléments inversibles sont $\bar{p}$ tels que $p \wedge n = 1$.

Les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ *sont également les éléments générateurs du groupe* $(\mathbb{Z}/n\mathbb{Z},\ +)$.

Preuve :

- On montre facilement que c'est un anneau.
- Recherche des éléments inversibles par équivalences.

Remarque : Lorsque p est premier, on remarque que tous les éléments non nuls de $\mathbb{Z}/n\mathbb{Z}$ sont inversibles.

Exemple : Déterminer les éléments inversibles de $\mathbb{Z}/14\mathbb{Z}$.

Méthode pour déterminer l'inverse d'un élément $\bar{p}$ de $\mathbb{Z}/n\mathbb{Z}$

- Méthode 1 : Comme $p \wedge n = 1$, on peut déterminer une relation de Bezout : $pa + nb = 1$.
  On obtient alors $\bar{p}.\bar{a} = \bar{1}$ et donc $(\bar{p})^{-1} = \bar{a}$
- Méthode 2 : L'inverse d'un élément inversible est lui-même inversible.
  Si n est petit, on peut donc tester tous les éléments de $U(\mathbb{Z}/n\mathbb{Z})$.
- Méthode 3 : On remarque que $\overline{n+1} = \bar{1}$, $\overline{2n+1} = \bar{1}$, $\overline{3n+1} = \bar{1}$... que l'on factorise.

Remarque : On obtient facilement une relation de Bezout en écrivant les premiers multiples de p et n et en s'arrêtant dès qu'il existe une différence de 1 entre 2 multiples.

Exemple : Déterminer les inverses des éléments inversibles de $\mathbb{Z}/14\mathbb{Z}$.

Avec Bezout	En testant les éléments de $U(\mathbb{Z}/14\mathbb{Z})$	En factorisant $\overline{15}$, $\overline{29}$, $\overline{43}$

Méthode de résolution de $ax \equiv b\ [c]$

$$ax \equiv b\ [c] \iff \bar{a}\bar{x} = \bar{b} \quad \text{dans } \mathbb{Z}/c\mathbb{Z}$$

- Si $a \wedge c = 1$: cad si $\bar{a}$ est inversible dans $\mathbb{Z}/c\mathbb{Z}$.

  On obtient alors les solutions en cherchant l'inverse de $\bar{a}$ dans $\mathbb{Z}/c\mathbb{Z}$.

  $$\bar{a}\bar{x} = \bar{b} \iff \bar{x} = (\bar{a})^{-1}\bar{b}$$

- Si $a \wedge c = \delta \neq 1$: cad si $\bar{a}$ n'est inversible dans $\mathbb{Z}/c\mathbb{Z}$.

  $\rightarrow$ Si $\delta \mid b$ on simplifie l'équation et on se ramène au cas précédent.
  $\rightarrow$ Sinon, l'équation n'a pas de solution.

Exemples :

- $4x + 2 \equiv 0\ [11]$
- $4x \equiv 6\ [10]$
- $4x \equiv 7\ [10]$

Méthode générale pour résoudre une équation dans $\mathbb{Z}/n\mathbb{Z}$

- Si n est premier : on a intérêt à se ramener à $\boxed{a(\bar{x})b(\bar{x}) = 0}$ avec $a(\bar{x}), b(\bar{x}) \in \mathbb{Z}/n\mathbb{Z}$.

  Nous pouvons alors affirmer que $a(\bar{x}) = 0$ ou $b(\bar{x}) = 0$.

- Si n n'est pas premier : on a intérêt à se ramener à $\boxed{a(\bar{x})b(\bar{x}) = 1}$ avec $a(\bar{x}), b(\bar{x}) \in \mathbb{Z}/n\mathbb{Z}$.

  Nous pouvons alors affirmer que $a(\bar{x})$ est un élément inversible ce qui limite les sol° possibles.

⚠ A partir de maintenant, les éléments de $\mathbb{Z}/n\mathbb{Z}$ seront souvent notés sans la barre. $(\bar{x} \to x)$

Exercice : 2

(∗) Résoudre :

- $x^2 = 1$ dans $\mathbb{Z}/8\mathbb{Z}$.
- $x^2 + 2x + 2 = 0$ dans $\mathbb{Z}/5\mathbb{Z}$.

Exercice : 3

(∗) Le groupe des inversibles de $\mathbb{Z}/8\mathbb{Z}$ est-il cyclique ? Et le groupe des inversibles de $\mathbb{Z}/9\mathbb{Z}$?

Pensez à déterminer les ordres des éléments !

$U\ (\mathbb{Z}/8\mathbb{Z})$	$U\ (\mathbb{Z}/9\mathbb{Z})$

3 Les Corps et $\mathbb{K}$-algèbres

1. Les corps :

Cf cours MPSI (à réviser en autonomie)

DÉFINITION : **Corps**

Anneau $\begin{cases} \text{commutatif} \\ \text{non réduit à } \{0_A\} \end{cases}$ où tous les éléments NON NULS sont inversibles (pour $\times$).

Dans un corps $\mathbb{K}$, nous avons donc $0_{\mathbb{K}} \neq 1_{\mathbb{K}}$.

Exemples usuels : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{K}(X)$ et $\mathbb{Z}/p\mathbb{Z}$ lorsque p est premier.

Remarque : Un corps étant un anneau commutatif, nous retrouvons toutes les propriétés calculatoires des anneaux, y compris la formule de factorisation et la formule du binôme.

PROPOSITION :
- Tout corps est intègre (non trivial, commutatif et sans diviseur de 0)
- Dans un corps, l'équation $ax = b$ (où $a \neq 0_{\mathbb{K}}$) admet une unique solution $x = a^{-1}b$

2. Sous-corps :

Cf cours MPSI (à réviser en autonomie)

DÉFINITION : **Sous-corps** : Les deux définitions suivantes sont équivalentes.
- Sous-anneau non trivial stable par symétrisation pour $\times$.
- C'est un corps inclus dans un autre corps avec $\begin{cases} \text{les mêmes lci} \\ \text{les mêmes éléments neutres} \end{cases}$.

Méthode pour montrer que L est un sous-corps de K

On vérifie que :
- $L \subset K$
- $0_K,\ 1_K \in L$
- L est stable pour $+$ et $\times$
- L est stable pour les 2 symétrisations

Exemples : $\mathbb{Q}$ et $\mathbb{Q}[\sqrt{2}]$ sont des sous-corps de $\mathbb{R}$.

3. Les corps : $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ lorsque p premier.

THÉORÈME : $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p premier.

Notation : $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Preuve : On constate que $\mathbb{F}_p$ est un anneau non trivial et commutatif.
De plus, tous les éléments non nuls sont inversibles si et seulement si p est premier.

Remarque : Les corps $\mathbb{F}_p$ sont des exemples de corps FINIS.

Exemples : $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/23\mathbb{Z}$ ... sont des corps finis.

Voir l'exercice 66 de la banque CCINP.

---

4. Les $\mathbb{K}$-algèbres :

DÉFINITION : **$\mathbb{K}$-Algèbre**

Soit A un ensemble muni de deux lci $\left\{ \begin{array}{l} + \\ \times \end{array} \right.$ et d'une lce $''.''$.

- On dit que A est une $\mathbb{K}$-*algèbre* lorsque : $\left\{ \begin{array}{l} (A, +, \times) \text{ est un anneau} \\ (A, +, .) \text{ est un } \mathbb{K}\text{-ev} \\ \lambda.(x \times y) = (\lambda.x) \times y = x \times (\lambda.y) \end{array} \right.$
- On appelle *Dimension* de la $\mathbb{K}$-algèbre A la dimension de l'espace vectoriel $(A, +, .)$.

Exemples : $\mathbb{K}[X]$, $\mathcal{L}(E)$, $\mathfrak{M}_n(\mathbb{K})$, $\mathbb{K}^{\mathbb{N}}$ et $(\mathcal{F}(X, \mathbb{K}), +, \times, .)$ sont des $\mathbb{K}$-algèbres usuelles.

DÉFINITION : **Sous-algèbre**

Soit B une partie de A une $\mathbb{K}$-algèbre.
On dit que B est une sous-algèbre de A lorsque :

- Définition 1 : B est une $\mathbb{K}$-algèbre incluse dans A avec $\left\{ \begin{array}{l} \text{les mêmes lci et lce} \\ \text{les mêmes éléments neutres} \end{array} \right.$.
- Définition 2 : Utilisée en pratique !

  $\rightarrow$ $B \subset A$
  $\rightarrow$ B contient les deux éléments neutres 0_A et 1_A
  $\rightarrow$ B est table par combinaison linéaire
  $\rightarrow$ B est stable par la loi $\times$

Exemples : Les ensembles des matrices scalaires et des matrices diagonales sont des sous-algèbres de $\mathfrak{M}_n(\mathbb{K})$.

Exercice : 4

$(*)$ Montrer que $E = \{ \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \mid a,\ b,\ c \in \mathbb{R}^3 \}$ est une sous-algèbre de $\mathfrak{M}_3(\mathbb{R})$.
Préciser sa dimension.

4 Les morphismes d'anneau

Comme pour les groupes, pour identifier les anneaux de même nature, nous commençons par introduire la notion de morphisme d'anneau, puis celle d'isomorphisme d'anneau.

1. Morphismes d'anneaux : A et B représentent des anneaux $(A, +, \times)$ et $(B, +, \times)$.

Cf cours MPSI (à réviser en autonomie)

Il est usuel d'utiliser abusivement les mêmes notations pour les lci des 2 anneaux.

DÉFINITION : **Morphisme d'anneau** :

$\varphi : A \to B$ est un morphisme d'anneau lorsque $\begin{cases} A \text{ et } B \text{ sont des annneaux} \\ \varphi(x+y) = \varphi(x) + \varphi(y) \\ \varphi(x \times y) = \varphi(x) \times \varphi(y) \\ \varphi(1_A) = 1_B \end{cases}$.

On remarque qu'un morphisme d'anneau est également un morphisme de groupe.

Exemples :

- id_A
- $\varphi(u_n) = \lim u_n$ de l'anneau des suites convergentes dans $\mathbb{R}$
- $\varphi(k) = k.1_A$ de $\mathbb{Z}$ dans A.
- $\varphi(k) = \bar{k}$ de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.
- $\tau_a(x) = axa^{-1}$ de A dans A où a est un élément inversible de A.

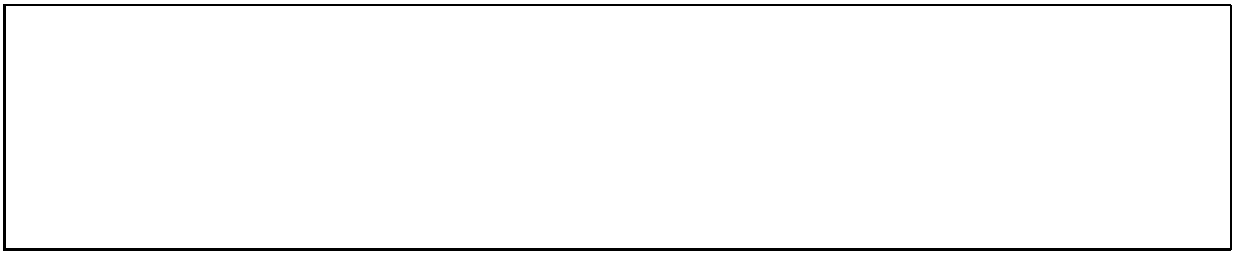
DÉFINITION : **Morphisme d'algèbre**

Soit $\varphi : A \to B$.

On dit que φ est un morphisme d'algèbre lorsque : $\begin{cases} \varphi \text{ est un morphisme d'anneau} \\ \varphi \text{ est une application linéaire} \end{cases}$.

Exemples :

- $z \mapsto \bar{z}$ est un automorphisme de la $\mathbb{R}$-algèbre $\mathbb{C}$.
- $M \mapsto PMP^{-1}$ est un automorphisme de la $\mathbb{K}$-algèbre $\mathfrak{M}_n(\mathbb{K})$.



Retenir et savoir démontrer...

- ... que la composée de 2 morphismes d'algèbre est un morphisme d'algèbre
- ... que la bijection réciproque d'un isomorphisme d'algèbre est un morphisme d'algèbre
- ... que les images directes et réciproques d'une sous-algèbre par un morphisme d'algèbre est une sous-algèbre

---

2. Propriétés : Soit $\varphi : A \to B$ un morphisme d'anneau.

Cf cours MPSI (à réviser en autonomie)

PROPOSITION : **Propriétés d'un morphisme d'anneau**

- Image d'un sous-anneau : $\begin{cases} \text{l'image} \\ \text{l'image réciproque} \end{cases}$ d'un sous-anneau par φ est un sous-anneau.
- Calculs : Lorsque φ est un morphisme d'anneau, outre les 3 propriétés de définition on a :

$$\begin{cases} \varphi(0) = 0 \\ \varphi(-x) = -\varphi(x) \\ \varphi(x^{-1}) = (\varphi(x))^{-1} \quad \text{si } x \in U(A) \end{cases} \qquad \text{et } \forall n \in \mathbb{Z} : \quad \begin{cases} \varphi(nx) = n\varphi(x) \\ \varphi(x^n) = \varphi(x)^n \end{cases}$$

- Inversibles : $x \in U(A) \Rightarrow \varphi(x) \in U(B)$
- Stabilité : La composition de deux morphismes d'anneau est un morphisme d'anneau

D/ Facile

3. Image et noyau : Soit $\varphi : A \to B$ un morphisme d'anneau.

Cf cours MPSI (à réviser en autonomie)

DÉFINITION : **Usuelles !**

$$\operatorname{Im}\varphi = \{\varphi(a) \mid a \in A\} \quad \text{et} \quad \ker\varphi = \varphi^{-1}(\{0_B\})$$

Remarques : $\begin{cases} \operatorname{Im}\varphi \text{ est un sous-anneau de } B \\ \text{⚠ } \ker\varphi \text{ n'est pas un sous-anneau de } A \quad (1_A \notin \ker\varphi \text{ car } \varphi(1_A) = 1_B \neq 0_A) \end{cases}$.

Exemple : Déterminer le noyau du morphisme d'anneau $\varphi : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} \\ k & \mapsto & \bar{k} \end{array}$.

Caractérisations : Injectivité et Surjectivité. (comme dans le cas des groupes)

Exemple : Montrer que φ définie par $\varphi(a+ib) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ sur $\mathbb{C}$ est un morphisme d'anneau injectif !

4. Isomorphisme d'anneau ou d'algèbre :

Cf cours MPSI (à réviser en autonomie)

DÉFINITION : **Isomorphisme d'anneau ou d'algèbre**

- Un morphisme d'anneau bijectif est appelé un *isomorphisme d'anneau*
- Deux anneaux sont *isomorphes* lorsqu'il existe un isomorphisme de l'un vers l'autre

Définition analogue pour les isomorphismes d'algèbre.

Propriété : L'ensemble des isomorphismes d'anneau (ou d'algèbre) est stable par $\begin{cases} \text{par composition} \\ \text{par inversion} \end{cases}$

Exemples :

- Soit $a \in A$ non nul.
  φ définie sur A par $\varphi(x) = axa^{-1}$ est un automorphisme d'anneau (ou d'algèbre).

- $\left(\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a,\ b \in \mathbb{C}\right\},\ +,\ \times\right)$ est une algèbre isomorphe à la $\mathbb{R}$-algèbre $\mathbb{C}$.

PROPOSITION : **Correspondance des éléments inversibles**

Lorsque $\varphi : A \to B$ est un isomorphisme d'anneau, on a :

$$\varphi_{|U(A)} : \begin{array}{ccc} U(A) & \longrightarrow & U(B) \\ a & \mapsto & \varphi(a) \end{array} \quad \text{est une bijection}$$

A et B contiennent donc "le même nombre" d'éléments inversibles qui se correspondent via φ

Preuve : On remarque que :

- L'image d'un élément inversible par un isomorphisme est un élément inversible
- $\varphi_{|U(A)}$ est injective var φ l'est.
- On montre facilement que $\varphi_{|U(A)}$ est surjective.

5. Théorème des restes chinois :

THÉORÈME FONDAMENTAL : **Restes chinois**

Lorsque $p \wedge q = 1$: $\varphi : \begin{array}{ccc} \mathbb{Z}/(pq\mathbb{Z}) & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ \bar{k} & \mapsto & (\hat{k},\ \tilde{k}) \end{array}$ est un isomorphisme d'anneau.

Ce théorème se généralise à n entiers $p_1, \ldots, p_n$, premiers entre eux deux à deux.

Preuve : On s'assure de la définition de φ en montrant que $\varphi(\bar{k})$ est indépendante du représentant choisi.
Puis on montre que φ est un morphisme d'anneau.
Puis on montre la bijectivité en montrant l'injectivité et l'égalité des cardinaux.

Remarque : Ce théorème sera utilisé pour établir la formule donnant l'expression de l'indicatrice d'Euler.

COROLLAIRE : **Application 1 : Solutions d'un système de congruences**

Soit $p,\ q \in \mathbb{N}$ tels que $p \wedge q = 1$ et $a,\ b \in \mathbb{Z}$.

L'ensemble des solutions de (S) $\begin{cases} x \equiv a\ [p] \\ x \equiv b\ [q] \end{cases}$ est : $\mathcal{S} = x_0 + pq\mathbb{Z}$

Où x_0 est une solution particulière qui existe bien.

Preuve : En notant $\hat{x}$ et $\tilde{x}$ les classes d'équivalence dans $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$.

$$\begin{cases} x \equiv a\ [p] \\ x \equiv b\ [q] \end{cases} \iff \begin{cases} \hat{x} \equiv \hat{a} \\ \tilde{x} \equiv \tilde{b} \end{cases} \iff \varphi(x) = (\hat{a},\ \tilde{b}) \iff \bar{x} = \varphi^{-1}(\hat{a},\ \tilde{b})$$

Méthode de résolution d'un système de congruence

Il s'agit de résoudre (S) $\begin{cases} x \equiv a\ [p] \\ x \equiv b\ [q] \end{cases}$ lorsque $p \wedge q = 1$.

- Pour trouver une solution particulière :
  On détermine une relation de Bezout $pu + qv = 1$ reliant p et q.
  On remarque alors que l'entier $x_0 = pub + qva$ est une solution particulière.
- Les solutions sont alors les valeurs $x \equiv x_0\ [pq]$.

Exemples :

- $\begin{cases} x \equiv 1\ [5] \\ x \equiv 7\ [9] \end{cases}$
- $\begin{cases} 3x \equiv 1\ [7] \\ 5x \equiv 2\ [8] \end{cases}$
- $\begin{cases} x \equiv 3\ [21] \\ x \equiv 5\ [14] \end{cases}$
- CCINP n° 94

COROLLAIRE : **Application 2 : Indicatrice d'Euler**

Lorsque $n \wedge m = 1$, on a $\varphi(nm) = \varphi(n)\varphi(m)$.

Par récurrence, on généralise cette propriété à un produit de nombres premiers entre eux deux à deux.

Preuve : Comme $\mathbb{Z}/mn\mathbb{Z}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, ils ont le même nombre d'éléments inversibles. Or, les éléments inversibles de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont... et il y en a donc...

La suite du chapitre porte sur les notions d'arithmétique dans un anneau.

5 Idéal d'un anneau commutatif (Préliminaire d'arithmétique)

Nous sommes ici dans un anneau A COMMUTATIF.

1. Définition :

DÉFINITION : **Idéal d'un anneau commutatif** :

$I \subset A$ est un idéal de A lorsque : $\begin{cases} I \text{ un sous-groupe additif de } A \\ I \text{ est absorbant c'est à dire : } \begin{cases} a \in A \\ x \in I \end{cases} \Rightarrow ax \in I \end{cases}$.

On dit qu'un idéal de A est « un sous-groupe additif absorbant » de $(A, +)$.

Remarque : La stabilité par symétrisation pour $+$ est une conséquence de l'absorption.

THÉORÈME : **Caractérisation des idéaux**

$I \subset A$ est un idéal de A si et seulement si $\begin{cases} 0_A \in I \\ I \text{ est stable par l'addition} \\ I \text{ est absorbant} \end{cases}$

Preuve : Facile.

Exemples d'idéaux dans un anneau A quelconque :

- $\{0_A\}$ et A sont toujours des idéaux de A
- Lorsque $a \in A$, aA est un idéal de A.
- Le noyau d'un morphisme d'anneau $\varphi : A \to B$ est un idéal de A.
- L'ensemble des éléments nilpotents de A est un idéal appelé le *nilradical*. (cf exo de TD)

Remarque : Un idéal I de A est un sous-groupe de A mais pas un sous-anneau de A. (Expl : $2\mathbb{Z}$)

PROPOSITION : **2 Conditions Suffisantes pour que $I = A$:**

$$\text{Si} \quad \begin{cases} I \text{ contient } 1_A \\ \text{ou} \\ I \text{ contient un élément inversible} \end{cases} \quad \text{alors} \quad I = A.$$

Preuve : Facile.

Conséquence : les seuls idéaux d'un corps sont donc $\{0\}$ et lui-même.

---

2. Opérations :

PROPOSITION : Si I et J sont des idéaux de A, alors

- $I \cap J$ est un idéal - c'est même le plus grand idéal inclus dans I et dans J.
- $I + J$ est un idéal - c'est même le plus petit idéal contenant I et J.

Preuve : Facile.

3. Idéal principal (engendré par un élément) :

DÉFINITION : **Idéal principal**

On dit qu'un idéal I de A est *engendré* par $a \in A$ lorsque : $I = aA$

On dit alors que :

$\rightarrow$ I est un idéal *principal*
$\rightarrow$ a est un *élément générateur* de I.

Remarques :

- aA est le plus petit des idéaux contenant a.
- Il peut exister plusieurs éléments générateurs : $\begin{cases} 2\mathbb{Z} = -2\mathbb{Z} \\ X\mathbb{R}[X] = 2X\mathbb{R}[X] \end{cases}$.

Vocabulaire : Si dans un anneau INTEGRE tous les idéaux sont principaux, on dit que l'*anneau est principal.*

---

4. Idéaux de $\mathbb{Z}$ et de $\mathbb{K}[X]$:

THÉORÈME : **Idéaux de $\mathbb{Z}$ et de $\mathbb{K}[X]$**

- Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$.
- Les idéaux de $\mathbb{K}[X]$ sont les $P\mathbb{K}[X]$ avec $P \in \mathbb{K}[X]$.

Preuve :

Vocabulaire : Comme $\mathbb{Z}$ et $\mathbb{K}[X]$ sont aussi intègres, alors $\mathbb{Z}$ et $\mathbb{K}[X]$ sont des anneaux principaux.

6 Divisibilité dans un anneau intègre

On se place ici dans un anneau $(A, +, \times)$ INTEGRE.

Puisque A est en particuler commutatif, on pourra s'intéresser aux idéaux de A.

1. Divisibilité :

DÉFINITION : **Divisibilité dans un anneau intègre**

Soit $a,\ b \in A$.
On dit que a *divise* b lorsqu'il existe $c \in A$ tel que $b = ac$.

Exemples :

- 1_A divise tout $b \in A$,
- tout élément a divise au moins a et 0_A,
- 0_A ne divise que 0_A.

THÉORÈME : **Caractérisation de la divisibilité avec les idéaux**

$$a \mid b \iff bA \subset aA$$

Preuve : Facile.

Cette caractérisation est souvent utilisée dans les démonstrations faisant intervenir la divisibilité.
On passe alors d'un problème d'arithmétique à un problème algébrique (« principe du parapluie »)

PROPOSITION :

- $\left\{ \begin{array}{l} a \mid b \\ b \mid c \end{array} \right. \Rightarrow a \mid c$ (Transitivité)
- $\left\{ \begin{array}{l} a \mid b \\ a \mid c \end{array} \right. \Rightarrow a \mid (b + c)$.

Preuve : Avec les idéaux.

2. Association :

DÉFINITION : **Eléments associés**

Soit $a,\ b \in A$.
On dit que a et b non nuls *sont associés* s'ils se divisent mutuellement c'est à dire lorsque :

$$aA = bA$$

Autrement dit : deux éléments sont associés si et seulement si ils engendrent le même idéal.

Propriétés :

- 0_A n'est associé qu'à 0_A.
- L'association est une relation d'équivalence sur l'anneau A

THÉORÈME : **Caractérisations** :

$$a \text{ et } b \text{ associés} \iff \exists u \in U(A) \text{ tel que } b = au.$$

Preuve : On a facilement $a = a(uv)$ et on utilise l'intégrité.

COROLLAIRE : **Eléments associés dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$** :

- Dans $\mathbb{Z}$: a et b associés ssi $|a| = |b|$
- Dans $\mathbb{K}[X]$: A et B associés ssi ils diffèrent d'une constante non nulle.

  Tout polynôme non nul est ainsi associé à un unique polynôme unitaire.

Preuve : Pas de difficulté lorsqu'on sait que $U(\mathbb{Z}) = \{-1,\ 1\}$ et $U(\mathbb{K}[X]) = \mathbb{K}_0[X]$.

Ce corollaire sera utilisé lors de la définition du PPCM et du PGCD de 2 entiers ou de 2 polynômes.

7 Arithmétique dans $\mathbb{Z}$

1. Les bases :

   Rappel : $a \mid b \iff b\mathbb{Z} \subset a\mathbb{Z}$

   Théorème : Division euclidienne de deux entiers. (connu !)

   PGCD et PPCM : Ici $a,\ b \in \mathbb{Z}$ avec l'un des deux non nul.

THÉORÈME : **PGCD**

Il existe un unique $\delta \in \mathbb{N}^*$ tel que $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$.

→ on montre que δ est un diviseur commun à a et b.
→ on obtient la relation de Bezout
→ on montre que les diviseurs communs à a et b sont les diviseurs de δ.

δ est donc le plus grand diviseur commun à a et b et est noté : $\delta = a \wedge b$.

Preuve : $a\mathbb{Z} + b\mathbb{Z}$ est un idéal de $\mathbb{Z}$

Théorème : **PPCM**

Il existe un unique $\mu \in \mathbb{N}^*$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$.

→ on montre que μ est un multiple commun à a et b.
→ on montre que les multiples communs à a et b sont les multiples de μ.

μ est alors le plus petit multiple commun positif à a et b et est noté : $\mu = a \vee b$.

Preuve : $a\mathbb{Z} \cap b\mathbb{Z}$ est un idéal de $\mathbb{Z}$

Remarque : On généralise les notions de PPCM et de PGCD à n entiers a_1, ..., a_n.

Cf cours MPSI (à réviser en autonomie)

Définition : **Entiers premiers entre eux**
On dit que deux entiers a et b sont premiers entre eux lorsque $a \wedge b = 1$.

Théorème : **Bezout (bis)** $a \wedge b = 1 \iff \exists u, v \in \mathbb{Z},\ au + bv = 1$

Preuve :

3 corollaires indispensables :

Corollaire : $\begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \Rightarrow a \wedge bc = 1$ et les 3 généralisations : $\begin{cases} \forall k \in [\![1, n]\!], a \wedge a_k = 1 \Rightarrow \dots \\ a \wedge b = 1 \Rightarrow a \wedge b^p = 1 \\ a \wedge b = 1 \Rightarrow a^q \wedge b^p = 1 \end{cases}$

Preuve : En effectuant le produit des deux relations de bezout.

Corollaire : $\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \Rightarrow a \mid c$ (**Gauss**)

Preuve : Quasi-immédiat avec Bezout.

Corollaire : $\begin{cases} a \mid c \\ b \mid c \\ a \wedge b = 1 \end{cases} \Rightarrow ab \mid c.$

Preuve : En traduisant les hypothèses et en appliquant Gauss.

Les 3 relations utiles dans les raisonnements d'arithmétique

- $ab = c$ permet d'affirmer que a divise c et donc d'obtenir de précieuses informations sur a
- $au + bv = d$ permet d'affirmer que le PGCD de a et b divise d.
- $ab = cd$ permet de dire que $a \mid d$ lorsque $a \wedge c = 1$.

2. Nombres premiers

Cf cours MPSI (à réviser en autonomie)

Définition : **Nombre premier**

Soit $p \in \mathbb{N}^*$ avec $p \geq 2$.
On dit que p est un *nombre premier* lorsque ses seuls diviseurs positifs sont 1 et lui-même.

Théorème : Décomposition unique d'un entier $n \in \mathbb{N}^*$ en produit de facteurs premiers.

$$n = p_1^{\alpha_1} \dots p_q^{\alpha_q}$$

Exemple : $n = 3300$

Corollaire :

- Caractérisation des diviseurs
- Formules PPCM et PGCD
- Caractérisation du caractère "premiers entre eux"

Exemple : $a = 2^2.5^4.7^2.13$ et $b = 2^3.3^4.7.11^2$

- Diviseurs de $a = \{$
- $a \wedge b =$
- $a \vee b =$
- a et b ne sont pas premiers entre eux car

3. Fonction indicatrice d'Euler :

Définition : **Indicatrice d'Euler**

Il s'agit de $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ définie par :

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

Remarque : $\varphi(n)$ est également...

- le nombre de générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$ *(plus généralement de tout groupe cyclique de cardinal n)*
- le cardinal de $U(\mathbb{Z}/n\mathbb{Z})$, c'est à dire le nombre d'éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

LEMME : Calcul de $\varphi(p^\alpha)$ avec p premier : $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Preuve : On commence par remarquer que $k \wedge p^\alpha \neq 1 \iff p \mid k$.
On décide donc de dénombrer le nombre de $k \in [\![1, p^\alpha]\!]$ divisibles par p.

Rappel : Lorsque $n \wedge m = 1$, on a $\varphi(nm) = \varphi(n)\varphi(m)$.

THÉORÈME : **Formule** :

Lorsque $n = \prod_{k=1}^{N} p_k^{\alpha_k}$ est la décomposition de n en facteurs premiers, on a :

$$\varphi(n) = \prod_{k=1}^{N} (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) \quad \text{ou encore} \quad \boxed{\varphi(n) = n \prod_{k=1}^{N} (1 - \frac{1}{p_k})}$$

Preuve : Simple calcul utilisant les deux lemmes précédents.

Exemples :

- $\varphi(12)$: $12 = 2^2 \times 3$ donc $\varphi(12) = 12(1 - \frac{1}{2})(1 - \frac{1}{3}) = 12.\frac{1}{2}.\frac{2}{3} = 4$
- Combien y-a-t-il d'éléments inversibles dans $\mathbb{Z}/78\mathbb{Z}$?

Khûbes

Exercice : 5

$(***)$ Montrer que $n = \sum_{d \mid n} \varphi(d)$ pour $n \in \mathbb{N}^*$.

Preuve : Méthode classique par dénombrement.

On introduit $\Delta = \{\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}\}$ dont le cardinal vaut $\text{Card}(\Delta) = n$.

Ces nombres s'écrivent de façon irréductible unique sous la forme $\frac{k}{d}$ avec $d \mid n$ et $\begin{cases} 1 \leq k < d \\ k \wedge d = 1 \end{cases}$.

On partitionne alors Δ en $\bigcup_{d \mid n} \{\frac{k}{d} \mid \text{irréductibles}\}$.

4. Théorème d'Euler :

THÉORÈME : **Théorème d'Euler**

Lorsque $a \wedge n = 1$ alors on a : $a^{\varphi(n)} \equiv 1\ [n]$

Preuve : Le groupe $U(\mathbb{Z}/n\mathbb{Z})$ contient $\varphi(n)$ éléments.
Puisque $a \wedge n = 1$, on a $\bar{a} \in U(\mathbb{Z}/n\mathbb{Z})$ et le théorème de Lagrange nous donne directement : $\bar{a}^{\varphi(n)} = \bar{1}$.

Exercice : 6

Application à la réduction des puissances modulo n

On souhaite déterminer le chiffre des unités de 7^{222}.
En d'autres termes, il s'agit de simplifier ce nombre modulo 10.

1. Justifier que $7^4 \equiv 1\ [10]$
2. Conclure.

COROLLAIRE : **Petit théorème de Fermat**

Lorsque p est premier, on a :
- Pour tout $a \in \mathbb{Z}$ non divisible par p : $a^{p-1} = 1\ [p]$.
- Pour a un entier quelconque : $a^p \equiv a\ [p]$.

Preuve :
- Comme a n'est pas divisible par p, alors $a \wedge p = 1$ et $\varphi(p) = p - 1$.
- $\rightarrow$ Si a n'est pas divisible par p alors $a^{p-1} = 1\ [p]$ et donc $a^p \equiv a\ [p]$.
  $\rightarrow$ Si a est divisible par p alors $a = 0\ [p]$ et $a^p = 0\ [p]$ d'où $a^p = a\ [p]$.

Voir l'exercice 86 de la banque CCINP pour une démonstration niveau MPSI de ce théorème.

Exercice : codage RSA

Khûbes

- MISE en OEUVRE : Alice souhaite qu'on lui envoie des messages confidentiels.

  Elle définit une Clé PUBLIQUE pour chiffrer et Clé PRIVEE pour déchiffrer (secrête).
  Pour cela :

  $\rightarrow$ 1ère partie de la Clé PUBLIQUE et de la Clé PRIVEE :
  Elle choisit p et q deux nombres premiers distincts et on calcule $\boxed{n = pq}$

  $\rightarrow$ On a alors $\varphi(n) = (p-1)(q-1)$

  $\rightarrow$ 2ème partie de la Clé PUBLIQUE :
  Elle choisit un entier naturel $\boxed{e}$ premier avec $\varphi(n)$ et tel que $e < \varphi(n)$.
  e est appelé : "l'exposant de chiffrement".

  $\rightarrow$ 2ème partie de la Clé PRIVEE :
  On calcule un entier $\boxed{d}$ inverse de e modulo $\varphi(n)$ $\quad (ed = 1\ [\varphi(n)])$.
  Par exemple par l'algorithme de Bezout.

  Le couple (n, e) est la Clé PUBLIQUE et (n, d) est la Clé PRIVEE.

- CHIFFREMENT :

  Si M est le "message" envoyé ($< n$), le message codé sera $C = M^e\ [n]$.
  C est donc le reste de la DE de M^e par n.

- DECODAGE :

  On retrouve M grâce à la formule $M = C^d\ [n]$ (reste de la DE de C^d par n.)

Preuve : Nous savons que $C = M^e\ [n]$
- Si $M \wedge p = 1$ alors $M^{ed} \equiv M\ [p]$ (calcul simple sachant que $M^{p-1} \equiv 1\ [p]$).
- Si $M \wedge p \neq 1$ alors M et donc M^{ed} sont multiples de p et donc $M^{ed} \equiv M\ [p]$.

Finalement, nous avons toujours $\begin{cases} M^{ed} - M \equiv 0\ [p] \\ M^{ed} - M \equiv 0\ [q] \end{cases}$ et comme $p \wedge q = 1$ alors $M^{ed} \equiv M\ [pq]$

8 Arithmétique dans $\mathbb{K}[X]$

$\mathbb{K}$ désigne ici un sous-corps de $\mathbb{C}$: généralement $\mathbb{R}$ ou $\mathbb{C}$.

1. L'algèbre : $\mathbb{K}[X]$

Cf cours MPSI (à réviser en autonomie)

DÉFINITION : **Polynôme**

Un polynôme P à coefficients dans $\mathbb{K}$ est :

$$P = \sum_{k=0}^{+\infty} a_k X^k \quad \text{où} \quad (a_k) \in \mathbb{K}^{(\mathbb{N})} \quad (\textit{une suite presque nulle d'éléments de } \mathbb{K})$$

Le polynôme X est appelé l'*indéterminée*.

Vocabulaire :

- Le degré est l'indice du dernier terme non nul de la suite (a_k).
- Par convention on dit que $\deg 0 = -\infty$.

Lois : 2 lci "+", "$\times$" et 1 lce "." définies de façon "usuelle".

Formules sur le degré :

- $\deg(P+Q) \leq \max(\deg P,\ \deg Q)$ avec égalité lorsque $\deg P \neq \deg Q$
- $\deg(PQ) = \deg P + \deg Q$ lorsque P et Q sont non nuls.

THÉORÈME : **Structure de $\mathbb{K}[X]$.**

$\mathbb{K}[X]$:

- est un anneau (commutatif) intègre
  - $\rightarrow$ d'éléments neutres les polynômes constants 0 et 1
  - $\rightarrow$ dont les éléments inversibles sont les polynômes constants non nuls.
- est un $\mathbb{K}$-ev de base canonique $(X^k)_{k\in\mathbb{N}}$.
- vérifie : $\lambda.(PQ) = (\lambda.P)Q = P(\lambda.Q)$

$(\mathbb{K},\ +,\ \times,\ .)$ est donc une $\mathbb{K}$-algèbre.

PROPOSITION : **Idéaux de $\mathbb{K}[X]$**

Les idéaux de $\mathbb{K}[X]$ sont les ensembles $P.\mathbb{K}[X]$ où $P \in \mathbb{K}[X]$.

Preuve : Vu précédemment.

Comme l'anneau $\mathbb{K}[X]$ est intègre, $\mathbb{K}[X]$ est un anneau principal.

Vocabulaire :

- Valeur de P en $x \in \mathbb{K}$: $P(x) = \sum_{k=0}^{+\infty} a_k x^k$. *(« On parle d'expression polynômiale »)*
- Racines $P \in \mathbb{K}[X]$: les solutions dans $\mathbb{K}$ de $P(x) = 0$

Nous verrons dans le chapitre "réduction algébrique" les notions de $\left\{ \begin{array}{l} \text{"polynôme matriciel"} \\ \text{"polynôme en un endomorphisme"} \end{array} \right.$.

---

2. Divisibilité dans : $\mathbb{K}[X]$

$\mathbb{K}[X]$ est un anneau intègre, on peut donc s'intéresser à la notion de divisibilité.

PROPOSITION : **Divisibilité et polynômes associés**

- $A \mid B \iff B.\mathbb{K}[X] \subset A.\mathbb{K}[X]$.
- A et B associés ssi $A = \lambda B$ avec $\lambda \in \mathbb{K}^*$

Tout polynôme non nul est donc associé à un unique polynôme unitaire.

Théorème : Division euclidienne d'un polynôme par un polynôme non nul. (cf MPSI)

Corollaire : $a \in \mathbb{K}$ racine de P ssi $(X - a) \mid P$.

---

3. PGCD et PPCM :

- PGCD : Pour $A,\ B \in \mathbb{K}[X]$ non tous les deux nuls

LEMME : Il existe un unique polynôme unitaire (ou nul) D tel que $A.\mathbb{K}[X] + B.\mathbb{K}[X] = D.\mathbb{K}[X]$.

Preuve :
→ Existence : La somme de deux idéaux est un idéal et $\mathbb{K}[X]$ est principal.
→ Unicité : 2 polynômes qui conviennent sont associés et unitaires !

COROLLAIRE : **PGCD**

→ D est le plus grand (au sens du degré) diviseur unitaire commun à A et B.
On l'appelle le PGCD de A et B et il est noté $D = A \wedge B$.

→ Les diviseurs communs à A et B sont les diviseurs de D.

→ Théorème de Bezout : $A \wedge B = D \Rightarrow \exists U,\ V \in \mathbb{K}[X],\ AU + BV = D$

- PPCM : Pour $A,\ B \in \mathbb{K}[X]$ non tous les deux nuls

LEMME : Il existe un unique polynôme unitaire (ou nul) M tel que $A.\mathbb{K}[X] \cap B.\mathbb{K}[X] = M.\mathbb{K}[X]$.

Preuve : OK pour l'existence.
Unicité en remarquant que 2 polynômes qui conviennent sont associés et unitaires !

COROLLAIRE : **PPCM**

→ M est le plus petit (au sens du degré) multiple unitaire commun à A et B.
On l'appelle le PPCM de A et B et il est noté $M = A \vee B$.

→ Les multiples communs à A et B sont les multiples de M.

Ces deux notions se généralisent à n polynômes...

---

4. Polynômes premiers entre eux

Cf cours MPSI (à réviser en autonomie)

Définition : Deux polynômes A et B sont premiers entre eux lorsque $A \wedge B = 1$

THÉORÈME : **Caractérisation avec les racines** :

$$A \wedge B = 1 \iff A \text{ et } B \text{ n'ont aucune racine complexe en commun}$$

Preuve : Par double contraposée en admettant D'Alembert-Gauss qui dit que tout polynôme à coefficients complexes non constant admet une racine complexe.

Exemple : $P = X^2 + X + 1$ et $Q = X^2 + 1$ sont premiers entre eux.

THÉORÈME : **Bezout (bis)** : $A \wedge B = 1 \iff \exists\ U,\ V \in \mathbb{K}[X],\ AU + BV = 1$

Exemple : Pour tout $X - a \wedge X - b = 1$ lorsque $a \neq b$.

COROLLAIRE : $\begin{cases} A \wedge C = 1 \\ B \wedge C = 1 \end{cases} \Rightarrow AB \wedge C = 1.$

Preuve : Avec le produit des deux relations de bezout ou en utilisant la caractérisation avec les racines.

Exemple : Pour tout $p,\ q \in \mathbb{N}$, $(X-a)^p \wedge (X-b)^q = 1$ lorsque $a \neq b$.

Corollaire : **(Gauss)** $\begin{cases} A \mid BC \\ A \wedge B = 1 \end{cases} \Rightarrow A \mid C$

Preuve : Quasi-immédiat avec Bezout.

Corollaire : $\begin{cases} A \mid C \\ B \mid C \\ A \wedge B = 1 \end{cases} \Rightarrow AB \mid C.$

Preuve : En traduisant les hypothèses et en appliquant Gauss.

Corollaire : Si $a_1, \ldots,\ a_n$ sont des racines distinctes de P alors $(X-a_1)\ldots(X-a_n) \mid P$

Preuve : Simple généralisation par récurrence.

Méthode pour montrer qu'un polynôme est nul

On montre qu'il admet plus de racines que son degré.
Par exemple :

- un polynôme qui admet une infinité de racines est nul.
- un polynôme de $\mathbb{K}_n[X]$ qui admet $n+1$ racines est nul

Corollaire : $P \in \mathbb{C}[X]$ est à racines simples ssi $P \wedge P' = 1$.

Preuve : Par double contraposée.

Exemple : Le polynôme $P = X^3 - X^2 + 1$ admet-il une racine multiple ?

5. Polynômes irréductibles :

La notion de polynôme irrédctible dans $\mathbb{K}[X]$ est analogue à la notion de nombre premier dans $\mathbb{Z}$.
Il s'agit des briques élémentaires à partir desquelles on peut construire tous les polynômes.

Définition : **Polynômes irréductibles de $\mathbb{K}[X]$**

Ce sont les polynômes P non constants de $\mathbb{K}[X]$ uniquement divisibles par :

$$\begin{cases} \text{les polynômes constants non nuls : } \lambda \\ \text{les polynômes associés : } \lambda P \end{cases}$$

Exemples : $X - a$ et $X^2 + 1$ sont irréductibles dans $\mathbb{R}[X]$

Théorème : **Les polynômes irréductibles de $\mathbb{R}[X]$ et $\mathbb{C}[X]$**

- de $\mathbb{C}[X]$ sont les polynômes de degré 1
- de $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 à discriminant strictement négatif.

Proposition : Tout polynôme réel de degré impair possède au moins une racine réelle.

Preuve :

- D1 : Avec les polynômes irréductibles

- D2 : Avec le TVI

Exemple : Dans $\mathbb{Q}[X]$: X^3+X+1 est irréductible.

Preuve :

- D1 : Par l'arithmétique des entiers

- D2 : En recherchant qualitativement les racines

THÉORÈME FONDAMENTAL : Il y a unicité (à l'ordre près) de la décomposition d'un polynôme unitaire en produit de polynômes irréductibles unitaires.

$$P=\prod_{k=1}^{q} P_1^{\alpha_1}\dots P_q^{\alpha_q}$$

Preuve : Par récurrence sur le degré.

Méthode pour décomposer un polynôme à racines SIMPLES

Soit P un polynôme de dégré n de coefficient dominant a_n.

- Dans $\mathbb{C}[X]$: On recherche les racines x_k de P et on a alors : $P=a_n.\prod_{k=1}^{n}(X-x_k)$

- Dans $\mathbb{R}[X]$: On décompose P dans $\mathbb{C}[X]$: $P=a_n.\prod_{k=1}^{n}(X-x_k)$, puis :

  → On isole les facteurs réels : $P=a_n.(X-\alpha_1)\dots(X-\alpha_p).\prod_{k=1}^{q}(X-\beta_k)$.

  → On regroupe deux à deux les facteurs complexes et on développe :

  $$(X-\beta_k)(X-\bar{\beta_k})=X^2-(\beta_k+\bar{\beta_k})X+\beta_k\bar{\beta_k}\in\mathbb{R}[X]$$

  Ceci est possible car si a est une racine complexe non réelle de $P\in\mathbb{R}[X]$ alors $\bar{a}$ est aussi racine de P avec le même ordre de multiplicité.

Lorsque P admet des racines multiples, on procède de la même manière mais il faut commencer par déterminer les ordres de multiplicité.

Exercice : 7

$(*-**)$ Soit $n\in\mathbb{N}^*$.
Savoir décomposer dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$ les polynômes suivants :

- $P=X^n-1$ lorsque n est pair et impair
- $P=(X-1)^n-(X+1)^n$

- $P = X^8 + X^4 + 1$
- $P = X^{2n} - 2\cos 2a X^n + 1$ pour $a \in]0, \frac{\pi}{2}[$.

COROLLAIRE : Comme dans le cas des entiers, on en déduit alors :
- L'expression des diviseurs d'un polynôme
- Les expressions du PGCD et du PPCM de deux polynômes
- Une caractérisation de $A \wedge B = 1$.

6. A revoir dans le cours de MPSI :

Cf cours MPSI (à réviser en autonomie)

RAPPEL 1 : Lien coefficients-racines pour un polynôme scindé

Pour $P = \sum_{k=0}^{n} a_k X^k$ scindé de racines $a_1, \ldots, a_n \in \mathbb{K}$ comptées avec leur ordre de multiplicité :

- $P = \prod_{k=1}^{n} (X - a_k)$.
- Les fonctions symétriques élémentaires des racines sont définies par :

$$\begin{cases} \sigma_1 = a_1 + a_2 + \cdots + a_n \\ \sigma_2 = a_1a_2 + a_1a_3 + \cdots + a_{n-1}a_n \\ \cdots \\ \sigma_n = a_1a_2 \ldots a_n \end{cases}$$

- Les valeurs des σ_k sont données par la formule : $\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$.

Méthode pour déterminer les valeurs des σ_k

On identifie les coefficients : $\begin{cases} P = a_n(X^n + \frac{a_{n-1}}{a_n} X^{n-1} + \frac{a_{n-2}}{a_n} X^{n-1} + \cdots + \frac{a_0}{a_n}) \\ P = a_n(X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-1} + \cdots + \cdots + (-1)^n \sigma_n) \end{cases}$

Exemple :

1. Déterminer les valeurs de fonctions symétriques élementaires des racines de $P = 2X^5 + 4X^2 - X + 8$.
2. En déduire la valeur de $S_2 = a^2 + b^2 + c^2 + d^2 + e^2$ où a, b, c, d et e sont les racines de P.

RAPPEL 2 : Formules de Taylor pour les polynômes

Lorsque $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, on a :

$$P = \sum_{n=0}^{+\infty} \frac{P^{(n)}(a)}{n!}(X-a)^n$$

En prenant $a = 0$, on obtient la formule de Taylor-Mac Laurin.

Exemples :

- Déterminer les coordonnées de $P = X^4 - 2X^2 + X + 1$ dans la base de Taylor associée à $a = 1$.
- Déterminer le développement limité de $P = X^4 - 2X^2 + X + 1$ au voisinage de 2.

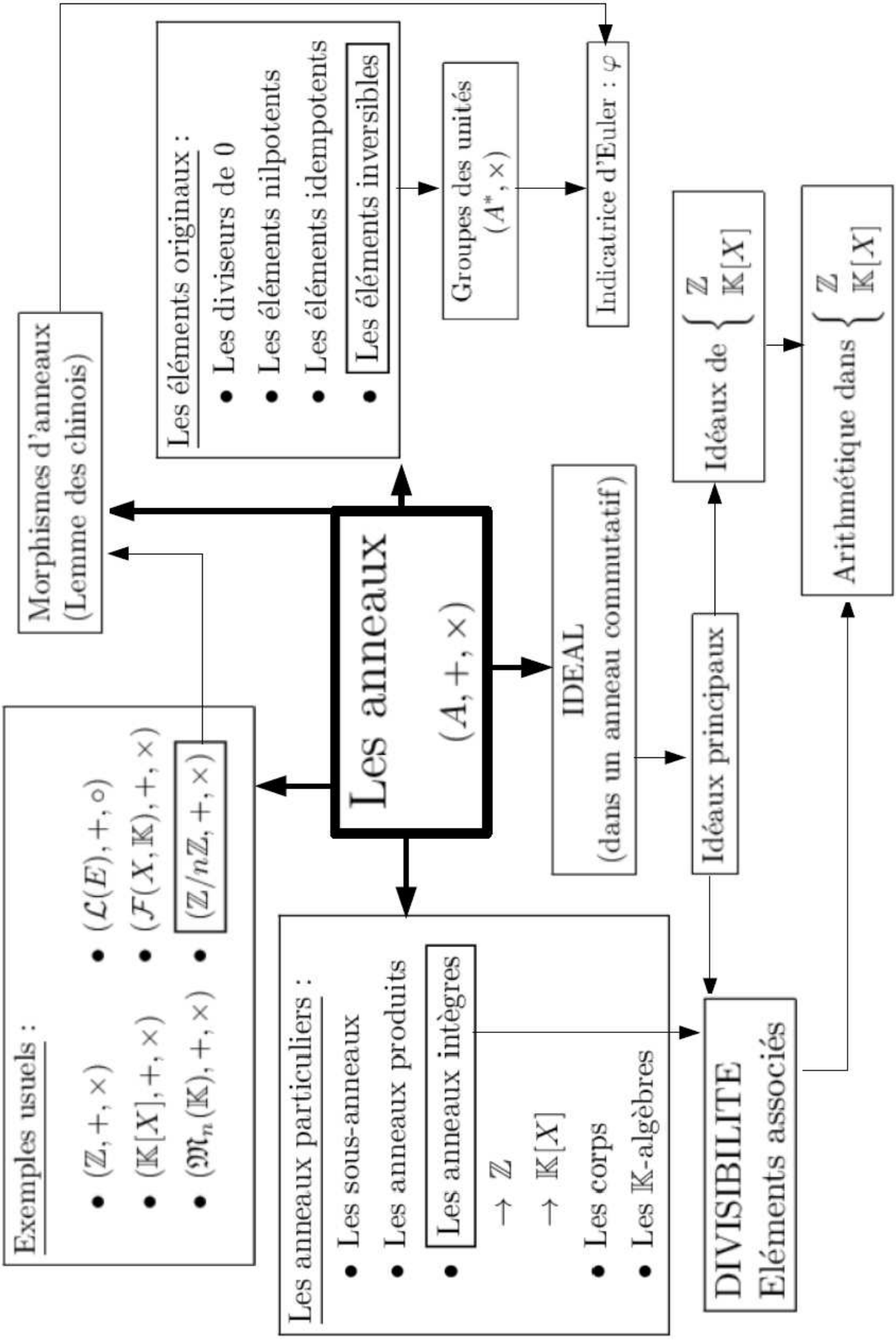
RAPPEL 3 : Notion et caractérisation des racines multiples

Lorsque $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, on a :

- a est racine d'ordre au moins k de P lorsque $(X-a)^k$ divise P.
- a est racine d'ordre au moins k de $P \iff P(a) = P'(a) = \dots P^{(k-1)}(a) = 0$.
- P admet une racine multiple $\iff \exists a \in \mathbb{K},\ P(a) = P'(a) = 0$.

Exemples :

- Le polynôme $P = X^3 - X + 2$ admet-il des racines multiples ?
- Déterminer l'ordre de la racine $a = 1$ de $P = X^4 - 3X^3 + X^2 + 3X - 2$.


Les anneaux
$(A, +, \times)$
Exemples usuels :
$(\mathbb{Z}, +, \times)$
$(\mathbb{K}[X], +, \times)$
$(\mathfrak{M}_n(\mathbb{K}), +, \times)$
$(\mathcal{L}(E), +, \circ)$
$(\mathcal{F}(X, \mathbb{K}), +, \times)$
$(\mathbb{Z}/n\mathbb{Z}, +, \times)$
Morphismes d'anneaux
(Lemme des chinois)
Les éléments originaux :
Les diviseurs de 0
Les éléments nilpotents
Les éléments idempotents
Les éléments inversibles
Groupes des unités
$(A^*, \times)$
Indicatrice d'Euler : φ
IDEAL
(dans un anneau commutatif)
Idéaux principaux
Idéaux de $\mathbb{Z}$ $\mathbb{K}[X]$
Arithmétique dans $\mathbb{Z}$ $\mathbb{K}[X]$
Les anneaux particuliers :
Les sous-anneaux
Les anneaux produits
Les anneaux intègres
$\to \mathbb{Z}$
$\to \mathbb{K}[X]$
Les corps
Les $\mathbb{K}$-algèbres
DIVISIBILITE
Eléments associés