Anneaux-Arithmétique-Polynômes

I Généralités sur les anneaux

I.1 Définition

Définition

On dit que $(A, +, \cdot)$ est un anneau lorsque :

i. $(A, +)$ est un groupe abélien.

ii. $\cdot : A \times A \longrightarrow A$ est un loi de composition interne associative ayant un neutre.

iii. $\cdot$ est distributive à droite et à gauche par rapport à $+$.

Remarque. Lorsque $\cdot$ est commutative, on dit que A est un anneau commutatif. L'anneau $A = \{0\}$ est appelé l'anneau nul.

I.2 Éléments remarquables

- Le neutre de $+$, noté 0, ainsi que le neutre de $\cdot$, noté 1, sont des éléments remarquables :
  — $\forall x \in A,\ 0 \cdot x = x \cdot 0 = 0$.
  — Si A possède deux éléments ou plus, on a $0 \neq 1$.
  — Si $x \neq 0$, $x \cdot 1 = 1 \cdot x = x$.

- Si $(x, y) \in A^2$, on dit que x et y sont **permutables** lorsque $xy = yx$. Les éléments permutables vérifient la formule du binôme du Newton.

On dit que x divise 0 à gauche lorsque $x \neq 0$ et qu'il existe $y \neq 0$ tel que $x \cdot y = 0$. On définit la notion analogue de diviseur à droite.

- On dit que x est simplifiable à gauche si pour tout $(y, z) \in A^2$, l'égalité $x \cdot y = x \cdot z$ implique l'égalité $y = z$.

Les deux notions précédentes sont synonymes : Un élément est simplifiable à gauche si et seulement si il n'est pas diviseur de 0.

- On dit que $x \in A$ est inversible lorsqu'il existe $y \in A$ tel que $x \cdot y = y \cdot x = 1$.

On note x^{-1} l'inverse de x. **La notation $\frac{1}{x}$ est autorisée seulement dans le cas commutatif.**

0 n'est jamais inversible. Les inversibles ne divisent pas zéro et sont simplifiables. Les éléments inversibles de A **forment un groupe, noté A^* et appelé groupe des unités de l'anneau A.**

- On dit que $x \in A$ est nilpotent s'il existe $n \in \mathbb{N}$ tel que $x^n = 0$.

Les nilpotents ne sont pas inversibles (ils divisent 0).

Définition

On dit qu'un anneau est intègre lorsqu'il n'admet pas de diviseur de 0.

Intérêt de l'intégrité : simplification des équations :
Par exemple :Dans un anneau commutatif intégre, un polynôme n'a pas plus de racines que son degré.

Définition

Un corps est un anneau **commutatif** dans lequel tous les éléments non nuls sont inversibles.

Remarque. Comme un élément inversible n'est pas diviseur de 0, les corps sont intègres.

I.3 Exemples : anneaux de référence

- $(\mathbb{Z}, +, \times)$ est un anneau intègre commutatif, et $\mathbb{Z}^* = \{-1, 1\}$.

- Les corps usuels $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$et $(\mathbb{C}, +, \times)$ sont bien entendu des anneaux.

- $(\mathbb{K}[X], +, \cdot)$ est un anneau commutatif intègre. $\mathbb{K}[X]^*$ est l'ensemble des polynômes constants non nuls(on l'identifie à $\mathbb{K}^*$).

- $(\mathcal{M}_n(\mathbb{K}), +, \cdot)$ et $(\mathcal{L}(E), +, \circ)$ sont des anneaux non commutatifs et non intègres.

Remarque. Dans $\mathcal{M}_n(\mathbb{K})$, les diviseurs de 0 sont exactement les matrices non inversibles.

- Anneau des fonctions :
Si A est un ensemble, $(\mathbb{R}^A, +, \cdot)$ est un anneau, avec $f+g : x \longmapsto f(x)+g(x)$ et $f \cdot g : x \longmapsto f(x) \cdot g(x)$.
Cet anneau n'est pas intègre.

- Si A est un anneau, on peut munir $A[X]$ et $\mathcal{M}_n(A)$ de structures d'anneaux.

On verra des exemples d'utilisation de $\mathbb{Z}[X]$ (polynômes à coefficients entiers) et des exemples d'utilisation de $\mathcal{M}_n(\mathbb{Z})$. Un exercice classique consiste à déterminer les inversibles de ces anneaux.

- Nous verrons bientôt que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau.

- **Produit de deux anneaux :**
$(A_1, +_1, \cdot_1)$ et $(A_2, +_2, \cdot_2)$ peut être muni d'une structure d'anneau : $(A_1 \times A_2, +, \cdot)$ avec $(x_1, x_2) + (y_1, y_2) = (x_1 +_1 y_1, x_2 +_2 y_2)$ et $(x_1, x_2) \cdot (y_1, y_2) = (x_1 \cdot_1 y_1, x_2 \cdot_2 y_2)$.
Les neutres sont $(0_A, 0_B)$ et $(1_A, 1_B)$. Cet anneau n'est jamais intègre comme le prouve le produit $(1, 0) \cdot (0, 1) = (0, 0)$

Dans cette catégorie se trouve par exemple l'anneau produit $\mathbb{Z}^2$ ou les anneaux $\mathbb{K}^n$ lorsque $\mathbb{K}$ est un corps.

I.4 Morphismes d'anneaux

Définition

Soient $(A, +\cdot)$ et $(B, +, \cdot)$ deux anneaux et $\phi : A \longrightarrow B$. On dit que ϕ est un morphisme d'anneau lorsque :

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

ii. $\forall\, (x, y) \in A^2,\ \phi(x \cdot y) = \phi(x) \cdot \phi(y)$

iii. $\phi(1_A) = 1_B$

Proposition

Les images directes et les images réciproques de sous-anneaux par un morphisme sont des sous-anneaux.

Attention !Le noyau d'un morphisme d'anneaux n'est jamais un sous-anneau, puisque $\phi(1) = 1 \neq 0$. C'est en partie ce qui justifie l'introduction de la nouvelle structure ci dessous, qui est fondamentale dans la théorie des anneaux et l'arithmétique.

II Idéaux d'un anneau commutatifs

Dans cette section, on ne considère que des anneaux commutatifs.

II.1 Définition

Définition

Soit $(A, +, \cdot)$ un anneau, et soit I un partie de A. On dit que I est un idéal de A lorsque :

i. $(I, +)$ est un sous-groupe additif.

ii. I est multiplicativement permis :

$$\forall\, x \in I,\ \forall\, a \in A,\ a \cdot x \in I$$

II.2 Propriétés

• $\{0\}$ et A sont des idéaux.

On les appelle les idéaux triviaux . Les autres idéaux de A sont dits "propres".

• Idéaux et inversibilité :

Proposition

Soit I un idéal contenant un élément inversible x. Alors $I = A$.

Démonstration à connaitre

• Idéaux des corps :
Les idéaux d'un corps sont $\{0\}$ et lui-même.

Exercice de cours : réciproquement, un anneau dont les seuls idéaux sont les idéaux triviaux est un corps.

II.3 Idéaux et morphismes d'anneaux

Proposition

Soit $\phi : A \longrightarrow B$ un morphisme d'anneaux. Pour tout J idéal de B, $\phi^{-1}(J)$ est un idéal de A.

En particulier :
Le noyau d'un morphisme d'anneaux est un idéal.

Démonstration

Corollaire

Soit $\phi : K \longrightarrow B$ un morphisme d'anneaux, avec de plus K un corps. Alors ϕ est injectif.

II.4 Opérations

Intersection d'ideaux

Proposition

Toute intersection d'idéaux est un idéal.

Somme de deux idéaux

Proposition

Si I et J sont deux idéaux, on pose $I + J = \{x + y, x \in I, y \in J\}$

$I + J$ est un idéal.

II.5 Idéal engendré par un élément

Proposition

Soit a un élément de A. L'ensemble

$$aA = \{ax, x \in A\}$$

est un idéal. C'est le plus petit idéal contenant a. On l'appelle idéal engendré par a

Vocabulaire : Un idéal de la forme précédente est appelé un idéal principal.

II.6 Idéaux de $\mathbb{Z}$ et de $\mathbb{K}[X]$

Définition

Un anneau intègre et dont tous les idéaux sont principaux s'appelle un anneau principal.

La proosition qui suit précise un important résultat sur les idéaux :

Proposition

$\mathbb{Z}$ et de $\mathbb{K}[X]$ sont des anneaux principaux.

Démonstration.

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

Cette section revisite les propriétés de divisibilité dans les deux anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ et explique leur similarité grace à la théorie des anneaux.

Tous les anneaux considérés sont commutatifs et intègres.

III.1 Divisibilité et idéaux.

Définition

Soit $(a, b) \in A^2$. On dit que a divise b (on note $a|b$) lorsqu'il existe $x \in A$ tel que $b = a \cdot x$.

Interpétation en termes d'idéaux : a divise b équivaut à $b \in aA$ qui équivaut à $bA \subset aA$.

Définition

On dit que a et b sont associés lorsque a divise b et que b divise a.
(a et b sont associés si et seulement si ils engendrent le même idéal)

Proposition

a et b sont associés si et seulement si $a = ub$, avec $u \in A^*$.

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

- Dans $\mathbb{Z}$, comme $\mathbb{Z}^* = \{-1, 1\}$, le seul associé de n est $-n$.
- Dans $\mathbb{K}[X]$, P et Q sont associés lorsqu'il sont égaux à une constante multiplicative non nulle près.

III.2 Décomposition en facteurs irréductibles

Définition

Soit $a \in A$ un élément non nul et non inversible. On dit que a est irréductible lorsque :

$$b|a \quad \Longrightarrow \quad b \text{ inversible ou } a \text{ et } b \text{ sont associés}$$

Remarque. En termes d'idéaux, a est irréductible si le seul idéal contenant strictement aA est A.

Cas des entiers

Les entiers (positifs) irréductibles **sont les nombres premiers.**

Tout entier naturel n s'écrit de façon unique sous la forme

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

Cas des polynômes

Les polynômes irréductibles de $\mathbb{K}[X]$ dépendent du corps de base. Au programme de classes prépas, seuls les deux cas suivants doivent être connus :

• **Cas où** $\mathbb{K} = \mathbb{C}$

Les polynômes irréductibles de $\mathbb{C}$ sont les polynômes de degré 1.

Tout polynôme P non nul possède une unique décomposition sous la forme

$$P = c(X - a_1)^{\alpha_1} \cdots (X - a_r)^{\alpha_r}$$

où c est une constante non nulle et $a_1, \ldots, a_r$ sont les racines de P.

• **Cas où** $\mathbb{K} = \mathbb{R}$

Les polynômes irréductibles de $\mathbb{C}$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle.

Les polynômes irréductibles unitaires de degré 2 s'écrivent au choix sous l'une des deux formes suivantes :

-$P = X^2 + bX + c$ avec $b^2 - 4c < 0$
ou $P = (X - \lambda)(X - \overline{\lambda})$ avec λ non réel.

Tout polynôme P non nul possède une unique décomposition sous la forme

$$P = cP_1^{\alpha_1} \cdots P_r^{\alpha_r} \qquad (1)$$

où c est une constante non nulle et $P_1, \ldots, P_r$ sont irréductibles et unitaires.

• **Remarque dans le cas d'un corps quelconque :**

La forme de la décomposition (1) est valable dans n'importe quel corps.

Cependant, les irréductibles dépendent du corps de base.

Par exemple, examinons la décomposition en facteurs irréductibles du polynôme $P = X^3 + 2$:

Si $\mathbb{K} = \mathbb{C}$

Si $\mathbb{K} = \mathbb{R}$

Si $\mathbb{K} = \mathbb{Q}$

III.3 PGCD

Le but de cette section est de redéfinir le PGCD en termes d'idéaux. A est l'anneau $\mathbb{Z}$ ou $\mathbb{K}[X]$.
On rappelle que**ces deux anneaux sont principaux**. C'est cette propriété qui va être utilisée.

Définition (PGCD de deux entiers)

Soient a, b dans $\mathbb{Z}$ non nuls
le pgcd de a et b est le plus grand entier positif d tel que $d|a$ et $d|b$
C'est aussi le seul entier vérifiant :
pour tout x, $x|a$ et $x|b$ si et seulement si $x|d$.

il y a deux façons en général de trouver le pgcd :

• Par l'algorithme d'Euclide (c'est le dernier reste non nul) : c'est la méthode à privilégier pour les algorithmes de calcul.

• A l'aide de la décomposition en facteurs premiers : c'est l'entier

$$d = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$$

Avec les idéaux on dispose en plus de la caractérisation suivante :

Proposition

Soit $(a, b) \in \mathbb{Z}^2$ et d leur pgcd. On a l'égalité d'idéaux

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$$

Entiers premiers entre eux

Deux entiers sont premiers entre eux si et seulement si leur pgcd vaut 1. Ceci équivaut au fait qu'ils n'ont pas de facteur premier en commum.

Théorème de Bézout

Soit $(a, b) \in \mathbb{Z}^2$.

$$a \wedge b = 1 \iff \exists\, (u, v) \in \mathbb{Z}^2,\ au + bv = 1$$

On a également la généralisation suivante au cas de n entiers

Définition

On appelle pgcd de $a_1, ..., a_n$ tout générateur de $a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$.

Définition

Soit $(a_1, ..., a_n) \in \mathbb{Z}^n$. On dit que $a_1, ..., a_n$ sont premiers entre eux dans leur ensemble lorsque $\mathbb{Z} = a_1\mathbb{Z} + \cdots a_n\mathbb{Z}$.

Attention : il ne faut pas confondre : "premier entre eux deux à deux" et "premiers entre eux dans leur ensemble"

Définition (PGCD de deux polynômes)

Soient P, Q dans $\mathbb{K}[X]$ non nuls
Il existe un unique polynôme unitaire R de degré maximal tel que R divise P et Q : on l'appelle le PGCD de P, Q.
pour tout polynome T on a , $T|P$ et $T|Q$ si et seulement si $T|R$.

il y a deux façons en général de trouver le pgcd :

• Par l'algorithme d'Euclide (c'est le dernier reste non nul) : c'est la méthode à privilégier pour les algorithmes de calcul.

• A l'aide de la décomposition en facteurs irréductibles : c'est l'entier

$$R = \prod_{S\text{irréductible}} S^{\min(v_S(P), v_S(Q))}$$

Quand $\mathbb{K} = \mathbb{C}$, le PGCD est donc le polynôme unitaire ayant pour racines les racines communes à P et Q avec à chaque fois la plus petite multiplicité des deux.

Comme précédemment on a la même caractérisation avec les idéaux :

Proposition

Soit $(P, Q) \in \mathbb{K}[X]$ et R leur pgcd. On a l'égalité d'idéaux

$$P\mathbb{K}[X] + Q\mathbb{K}[X] = R\mathbb{K}[X]$$

Polynômes premiers entre eux

Deux polynômes sont premiers entre eux si et seulement si leur pgcd vaut 1.
Ceci équivaut au fait qu'ils n'ont pas de racine réelle ou complexe en commun

Théorème de Bézout

Soit $(P,Q) \in \mathbb{K}[X]^2$.

$$P \wedge Q = 1 \iff \exists\,(U,V) \in \mathbb{K}[X]^2,\ UP + VQ = 1$$

Ce théorème est souvent utilisé en algèbre linéaire avec des polynômes annulateurs. En voici un exemple.

Exercice de cours : soit M une matrice carrée de polynôme minimal P. Montrer que si Q est premier avec P alors la matrice $Q(M)$ est inversible. On utilisera deux méthodes différentes.

Il n'échappe à personne que les situations des entiers et des polynômes sont totalement similaires. Pourquoi ? Ceci vient du fait que les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ **sont tous les deux principaux** : tous leurs idéaux sont principaux. Afin d'illustrer ce fait, nous allons terminer ce paragraphe en démontrant quelques résultats classiques d'arithémtique dans un anneau principal A (commutatif et intègre) quelconque : ils seront donc en particulier vrais pour les entiers et les polynômes.

Définition (PPCM)

Soit $(a,b) \in A^2$. L'idéal $aA \cap bA$ est principal, donc il existe $c \in A$ tel que $aA \cap bA = cA$. On dit que c est un plus petit commun multiple (ppcm) de a et b.

Proposition

Les ppcm vérifie la propriété suivante :

$$\forall\, x \in A,\ (a|x \text{ et } b|x) \Longrightarrow ppcm(a,b)|x$$

Théorème de Gauss

Soient $(a,b,c) \in A^3$ tels que $a|bc$ et $a \wedge b = 1$. Alors $a|c$.

Démonstration. $a \wedge b = 1 \iff \exists\,(u,v) \in A^2,\ au + bv = 1$. Ainsi $acu + bcv = c$. Comme $c|acu$, $a|bc$ $\Longrightarrow a|c$.

Proposition

Soit a un élément irréductible. Soit $(b,c) \in A^2$. Si $a|bc$, alors $a|b$ ou $a|c$.

Démonstration.

IV L'anneau $\mathbb{Z}/n\mathbb{Z}$. Introduction à l'arithmétique modulaire.

IV.1 Définition de la multiplication

Proposition (compatibilité du produit avec l'égalité modulo n)

Soit $n \in \mathbb{N}^* \backslash \{1\}$. La relation d'égalité modulo n est compatible avec le produit. En posant sur $\mathbb{Z}/n\mathbb{Z}$ par définition $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$, on définit une multiplication "$\cdot$", et $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau.

Proposition (structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$)

En posant sur $\mathbb{Z}/n\mathbb{Z}$ par définition $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$, on définit une multiplication "$\cdot$", et $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau.

Démonstration

IV.2 Exemples

Dressons les tables de multiplication de $\mathbb{Z}/n\mathbb{Z}$ pour quelques valeurs de n.

IV.3 Caractérisation des éléments inversibles

Le résultat suivant est sans doute le plus important des résultats concernant l'anneau $\mathbb{Z}/n\mathbb{Z}$

Théorème

Soit $x \in \mathbb{Z}$. Les propriétés suivantes sont équivalentes :

i. $\overline{x}$ ne divise pas $\overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$

ii. $\overline{x}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$

iii. $x \wedge n = 1$

iv. $\overline{x}$ est générateur pour $+$ du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$

Corollaire

Il est équivalent de dire :

i. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est intègre

ii. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps

iii. n est premier

Remarque. On note en général $n = p$ lorsque n est premier, et le corps $\mathbb{Z}/p\mathbb{Z}$ est noté F_p.

Corollaire

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

Exemple : examinons le groupe des inversibles lorsque $n = 5$ et $n = 6$.

Exemples

Résoudre les équations modulaires $12x = 5[17]$ et étudier l'existence de solution à l'équation $12x = a[15]$ lorsque a est un entier.

IV.4 Le théorème de restes chinois

Le théorème qui suit est le second résultat important de cette section.

Théorème (des restes chinois)

Si n et m sont premiers entre eux, alors iles deux anneaux $(\mathbb{Z}/nm\mathbb{Z}, +, \cdot)$ et $(\mathbb{Z}/m\mathbb{Z}, +, \cdot) \times (\mathbb{Z}/n\mathbb{Z}, +, \cdot)$
sont isomorphes.

Démonstration

Première application : systèmes de congruences

Voici quelques exemples de problèmes qu'on peut résoudre avec le théorème des restes chinois
Résoudre l'équation $x^2 = 4[77]$ (ou plus généralement modulo pq lorsque p et q sont deux nombres premiers.)

Existe t'il des entiers n tels que $2^n = 2n + 5[31]$?

IV.5 L'indicateur d'Euler

Définition

On note $\varphi(n)$ le nombre d'entiers k, $1 \leq k \leq n$ tels que $k \wedge n = 1$.
la fonction φ s'appelle **l'indicateur d'Euler**

D'après ce que nous avons vu précédemment, la fonction φ compte beaucoup d'objets différents :

Proposition

$\varphi(n)$ est aussi :

-Le nombre d'éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$
-Le nombre de générateurs du groupe additif cyclique $\mathbb{Z}/n\mathbb{Z}$
-Le nombre de générateurs de n'importe quel groupe cyclique
-Le nombre de racines primitives $n$ièmes de l'unité.

Exemple : regardons le cas $n = 6$.

Multiplicativité de l'indicateur d'Euler

Proposition

Soient m et n deux entiers **premiers entre eux**.
On a l'égalité

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Noter que cette égalité n'a pas du tout lieu lorsque m et n sont quelconques. On dit que l'indicateur d'Euler est une fonction arithmétique multiplicative.
Démonstration

Grace à cette propriété, disposons d'une formule explicite pour le calcul de $\varphi(n)$

Proposition

Soit n un entier et $p_1, \ldots, p_r$ ses diviseurs premiers : on a l'égalité :

$$\varphi(n) = n \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right)$$

IV.6 Théorèmes de Fermat et Euler

Théorème (Petit théorème de Fermat)

Si p est premier, alors pour tout $a \in \mathbb{N}$, $a^p \equiv a\ [p]$.

Démonstration.

En fait, le petit théorème de Fermat est un cas particulier du théorème suivant :

Théorème (Théorème d'Euler)

Soit $n \in \mathbb{N}^*$. Si $a \wedge n = 1$, alors $a^{\varphi(n)} \equiv 1\ [n]$.

Exemple
Voici un petit exercice illustrant la façon d'utiliser ces théorèmes (on peut aussi reprendre l'exercice de congruences $2^n = 2n + 5[31]$ vue plus haut).

Soit p, q des entiers premiers impairs. On suppose que $2^q \equiv 1\ [p]$. Montrer que $p \equiv 1\ [2q]$.