THEME : Anneau (Principaux, factoriels, euclidiens, Idéal premier)

Plan

INTRODUCTION

I) Définition des anneaux
II) Anneaux principaux
III) Anneaux factoriel
IV) Anneaux euclidiens
V) Idéal premier

CONCLUSION

Introduction

Deux définitions différentes sont significativement représentées dans la littérature mathématique. La majorité des sources récentes définit un « anneau » comme un anneau unitaire, exigeant que la multiplication ait un élément neutre; Un nombre non négligeable d'ouvrages n'exige en revanche pas la présence d'une unité multiplicative. La structure qu'ils appellent alors « anneau » est ailleurs dénommée pseudo-anneau.

Toutefois, il faut noter que ces deux théories des anneaux sont à bien voisines, avec un nombre important d'énoncés communs. Mais dans la suite, notre travail portera généralement sur la première approche des anneaux.

I) Généralité sur les anneaux

1) Structure des anneaux

Soit A un ensemble muni de deux lois de composition internes notées + et $*$. On dit que le triplet (A,+, $*$) possède une structure d'anneau si :

i) (A, +) a une structure de groupe abélien. Le neutre de la loi + est noté 0.

ii) La loi $*$ est associative:

$\forall$ x, y, z $\in$ A, x$*$ (y$*$z) = (x$*$y) $*$z

iii) La loi $*$ est distributive par rapport à la loi + :

$\forall$ x, y, z $\in$ A, x$*$(y + z) = x$*$y + x$*$z

iv) Il existe un élément neutre dans A pour la loi $*$ noté 1. L'anneau A est dit unitaire.

Si de plus, la loi $*$ est commutatif, l'anneau est dit commutatif.

Exemples
(Z, +, $*$), (Q, +, $*$), (R, +, $*$), (C, +, $*$) sont des anneaux commutatifs. (N, +, $*$) n'est pas un anneau.

2) Définition et proposition :

Définition 1 :

Soit A un anneau et a, b $\in$A non nuls tels que a$*$b=0.

a et b sont des diviseurs de 0.

Exemple :

Dans $\mathcal{M}_2$(R), M=$\begin{pmatrix} 1 & -2 \\ 0 & 0 \end{pmatrix}$, N=$\begin{pmatrix} 2 & -4 \\ 1 & -2 \end{pmatrix}$, MN=0 donc M et N sont des diviseurs de zéro.

Définition 2 :

Un anneau $(A, +, *)$, est dit intègre si pour tout élément

$a, b \in A, a*b = 0 \Rightarrow a = 0$ ou $b = 0$.

Un anneau intègre est commutatif et ne possède pas de diviseur de zéro.

Divisibilité :

Soit $(A, +, *)$ un anneau intègre, a et $b \in A$ avec $a \neq 0$. On dit que a divise b et on note a/b s'il existe $q \in A$ tel que $b = a*q$

Définition 3 :

Soit A un anneau commutatif. On dit qu'un élément $a \in A$ non nul est nilpotent s'il existe un entier $n \in N^*$ tel que $a^n = 0$. Le plus petit entier n vérifiant $a^n = 0$ est appelé indice de nilpotence de a. Un anneau intègre n'a pas d'élément nilpotent.

Proposition : Propriétés arithmétiques sur les anneaux.

Soit $(A,+, *)$ un anneau.
Pour tout $x, y \in A$, on a :
1. $0.x = 0$
2. $(-1).x = -x$
3. $(-1).(-1) = 1$
4. $(-x).y = -x.y$

Démonstration
1. $0.x + x = 0.x + e.x = (0 + e).x = e.x = x$. Donc $0.x = 0$.
2. $0 = 0.x = (1 - 1).x = 1.x - 1.x = x - 1.x$ donc $-x = -1.x$.
3. On multiplie par -1 l'égalité $(-1)+1 = 0$. Cela donne $(-1).(-1)+(-1).(1) =$ 0 et donc $(-1).(-1) + (-1) = 0$ ce qui prouve que $(-1).(-1) = 1$.
4. $x.y + (-x).y = (x + (-x)).y = (x - x).y = 0.y = 0$ donc l'opposé de x.y qui est, par convention d'écriture, $-x.y$, est égal à $(-x).y$.

Proposition Voici quelques formules algébriques dans un anneau A commutatif :

si $x,y \in A$, $n,m \in N$:
- $x^{m+n} = x^{mxn}$
- $(x^m)^n = x^{mxn}$
- $(xy)^n = x^n y^n$

3) Idéal d'un anneau commutatif

Soit $(A, +, *)$ un anneau commutatif et I une parte non vide de A. On dit que I est un idéal de A si :

i. (I, +) est un sous-groupe de (A, +).

ii. Pour tout x ∈ I et a ∈ A, ax ∈ I.

Si x ∈ A, l'ensemble xA = { ax / a ∈ A } est un idéal de A. Il est l'ensemble des multiple de x.

II) ANNEAU PRINCIPAL

a. Définition

Soit (A, +, ∗) un anneau commutatif, on a :

i. Un idéal I est dit principal s'il existe xϵA tel que I = xA
xA est dit idéal engendré par x.
ii. L'anneau A est dit principal si tous ses idéaux sont principaux.
Exemple : Cas de Z

Nous savons que les seuls sous-groupe de (Z, +) sont les nZ. Un idéal de Z est donc de la forme nZ.

a. Théorème

Les idéaux de Z sont les nZ. En conséquence, (Z, +, ∗) est un anneau principal.

L'anneau (Z/nZ, +, ∗)

Z/nZ = { $\overline{0}, \overline{1}, \dots, \overline{n-1}$ }

Sur Z/nZ, on définit l'addition et la multiplication en posant

$\overline{a} + \overline{b} := \overline{a+b}, \qquad \overline{a} * \overline{b} := \overline{ab},$

Du fait de la compatibilité de la relation de congruence avec l'addition et le produit c'est à dire :

$$\begin{cases} a \equiv b\ [n] \\ a' \equiv b [n] \end{cases} \Rightarrow \begin{cases} a + a' \equiv b + b'\ [n] \\ aa' \equiv bb' [n] \end{cases}$$

Alors on a les théorèmes suivent :

Théorème 1

Pour n≥2, (Z/nZ, +, ∗) est un anneau commutatif.

Théorème 2

Les inversibles de l'anneau (Z/nZ, +, ∗) est un corps si et seulement si n est premier.

Preuve

Soit k ϵ [|1, n-1|]. Si n est premier, k et n sont premiers entre eux d'ou $\overline{k}$ est inversible. Z/nZ est donc un corps.

Théorème 3

Pour n≥2, Z/nZ est un anneau intègre si n est premier.

Théorème 4 : Théorème chinois.

Soit m et n des entiers premiers entre eux, l'application

f: $(Z/nmZ, +, *) \to (Z/nZ \times Z/mZ, +, *)$

$\bar{a} \quad \mapsto \quad (\hat{a}, \dot{a})$

est un isomorphisme.

Preuve :

Soit (a, a') ϵ Z^2 tel que $\bar{a} = \bar{a'}$. Alors $a \equiv a'[nm]$. En particulier $a \equiv a'[n]$ et $a \equiv a'[m]$. Donc $\hat{a} = \widehat{a'}$ et $\dot{a} = \dot{a'}$. f est bien une application.

f ($\bar{a} + \bar{b}$) = f ($\overline{a+b}$) = ($\widehat{a+b}$, $\dot{a+b}$)

= ($\hat{a} + \hat{b}$, $\dot{a} + \dot{b}$)

= ($\hat{a}$, $\dot{a}$) + ($\hat{b}$, $\dot{b}$)

= f ($\bar{a}$) + f ($\bar{b}$) .

f ($\bar{a} * \bar{b}$) = f ($\overline{ab}$) = ($\widehat{ab}$, $\dot{ab}$)

= ($\hat{a} * \hat{b}$, $\dot{a} * \dot{b}$)

= ($\hat{a}$, $\dot{a}$) $*$ ($\hat{b}$, $\dot{b}$)

= f ($\bar{a}$) $*$ f ($\bar{b}$)

- Application du théorème chinois aux système de congruence.

Théorème 1

Soit m et n deux entiers premier entre eux. Soit a et b deux entier relatif et (S) le système :

(S) : $\begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases}$

Alors

i. (S) admet au moins une solution x_0 ϵ Z

ii) Les solutions de (S) dans Z sont les nombres de la forme x_0 + knm, k ϵ Z.

<u>Preuve</u>

Adoptons les notations du théorème chinois. On a :

$\begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases}$ devient $\begin{cases} \hat{a} = \hat{b} \\ \dot{a} = \dot{b} \end{cases}$

f ($\bar{x}$) = ($\hat{b}$, $\dot{a}$) => $\bar{x}$ = f^{-1} ($\hat{b}$, $\dot{a}$)

Désignons par x_0 un représentant de $f^{-1}(\hat{b}, \dot{a})$

$\bar{x} = \bar{x}_0 \Leftrightarrow x \equiv x_0 [nm] \Leftrightarrow x = x_0 + knm, k \in Z.$

- Méthode de résolution de Bézout

$$(S) : \begin{cases} x \equiv a\,[m] \\ x \equiv b\,[n] \end{cases}$$

Puisque m et n sont premier entre eux, d'après Bézout

Il existe u et v ϵ Z tel que mu + nv = 1.

Posons $x_0 = bmu + anv \Rightarrow x_0 \equiv anv \equiv a[m]$

$$\Rightarrow x_0 \equiv bmu \equiv b[n]$$

Si x' est une autre solution de (S) alors $x_0 \equiv x'[m]$ et $x_0 \equiv x'[n]$. Donc $x_0 - x'$ est divisible par n et m. Comme m et n sont premier entre eux d'après Gauss $x_0 - x'$ est divisible par mn d'où $x' \equiv x_0[mn]$.

- L'indicatrice d'Euler

Pour n≥2, on note **φ** (n) le nombre dentier d'élément de [|1, n-1|] premier avec l'entier n.

Définition 1

On appelle indicatrice d'Euler la fonction **φ** qui à n≥2 associe

φ (n) = card { k ϵ [|1, n-1|], pgcd (k, n) = 1}

= card { $\bar{k}$ inversible, $\bar{k}$ ϵ Z/ nZ }

= card ((Z/nZ)^x)

φ (n) = card { k ϵ Z/ $\bar{k}$ est un générateur de (Z/nZ, +) }

Exemple : **φ** (2) =1, **φ** (4) =2.

III) Anneau factoriel

Définition

Soit A un anneau. A est dit factoriel s'il vérifie chacune des trois propriétés suivantes :

i. A est intègre.
ii. Tout élément x non nul de A s'écrit $x = u.p_1. \dots . p_n$ avec $u \in A^*$ et p_i irréductibles dans A pour i=1,...,n.
iii. La décomposition précédente, à permutation près des éléments irréductibles et à produit par un inversible près, est unique.

Proposition :

Si a et b sont des éléments d'un même anneau factoriel alors a/b est équivalent à $v_p(a) \leq v_p(b)\ \forall\ p \in P$.

Théorème :

Soit A un anneau intègre et vérifiant la propriété ii. On a équivalence entre:
1. A vérifie iii.
2. Le lemme d'Euclide: Si p est irréductible et si p divise ab alors p divise a ou p divise b.
3. p irréductible $\Leftrightarrow$ (p) est premier.
4. Le lemme de Gauss :

Si c est premier avec a et que c divise ab alors c divise b.

Démonstration

Commençons par rappeler que dans un anneau intègre, il est toujours vrai que si (p) est un idéal premier alors p est irréductible. Supposons alors que 2. est vrai et démontrons que p irréductible $\Rightarrow$ (p) est premier. Soit a et b des éléments de A tels que $ab \in (p)$. On sait donc que p/ab. Le lemme d'Euclide permet d'affirmer que p divise a ou que p divise b. Donc que a ou b est élément de (p).

Montrons aussi que 3. $\Rightarrow$2.

Supposons que 3. est vrai. Soit p un élément irréductible de A et soient a et $b \in A$ tels que p/ab. ab est alors élément de (p). Cet idéal étant premier, a ou b, est nécessairement élément de (p). Donc p/a ou p/b. Cela implique le lemme d'Euclide.

Proposition

Soit A un anneau intègre et unitaire, soient deux éléments a et b de cet anneau. On a : $(a) = (b) \Leftrightarrow \exists u \in A^*\ a = ub$.

Démonstration

Supposons que (a) = (b). Si a est nul, b aussi est nul et la propriété est démontrée. Supposons donc que a n'est pas nul. Alors il existe $u \in A$ tel que a = u.b et $u' \in A$ tel que b = u'.a. En particulier a = u.u'.a, ou encore: a(1-u.u') = 0. Comme a n'est pas nul et que l'anneau est intègre, cela implique que 1-u.u' = 0 ou encore que u.u' = 1. u est donc élément de A^*. Supposons maintenant qu'il existe un élément u de A^* tel que a = ub. Cette égalité permet d'affirmer que b divise a et donc que $(a) \subset (b)$. Comme u est inversible, on a : $b = u^{-1}.a$ ce qui signifie que a divise b et que $(b) \subset (a)$.

Définition

Dans le cas ou a et b sont éléments d'un anneau unitaire A et qu'il existe un élément u de A^* tel que a = u.b, on dira que a et b sont des éléments associés de l'anneau.

Proposition Soit A un anneau intègre et soit p un élément de A. Supposons que l'idéal (p) est un idéal premier de A. Alors p est un élément irréductible de A.

Démonstration Soient a et b dans A tels que p= a.b. Alors a.b est élément de (p).

IV) ANNEAU EUCLIDIEN

Définition

Soit A un anneau. On dit que A est muni d'une division Euclidienne s'il existe une application $u : A \setminus 0 \rightarrow N$ telle que si a et b sont éléments de $A \setminus 0$ alors il existe q et $r \in A$ vérifiant a = bq+r et r = 0 ou u(r) < u(b). Remarquons que cette application u est dans le cas des anneaux polynômiaux l'application qui à un polynôme associe son degré.

Définition

Un anneau A est Euclidien si :
– A est intègre.
– A possède une division Euclidienne.

Proposition : Un anneau Euclidien est principal.

Démonstration

Soit A un anneau Euclidien. A est par définition intègre. Soit I un idéal de A et soit u l'application de A dans N permettant de définir une division euclidienne sur A. Soit x un élément de I tel que u(x) soit minimal. Alors pour tout a dans I, il existe q et r dans A tels que a = xq+r. De plus soit r est nul soit il vérifie u(r) < u(x). Remarquons que x étant élément de I, il en est de même de xq. De plus, comme a-xq est aussi élément de I, r est élément de I. L'inégalité u(r) < u(b) est donc, par choix de x, impossible. Nécessairement, r=0 et a = qx. Comme a est quelconque dans I, I=(x). A est par conséquent principal.

V) IDEAL PREMIER

Soit A un anneau commutatif unitaire, a ϵ A et I un idéal de A.

▪Un idéal I de A est dit premier si le quotient de A par I est intègre.

▪Un élément a de A est dit premier si et seulement si l'idéal a.A est premier.

Propriétés

Lemme d'Euclide

▪Un idéal I est premier si et seulement si c'est un idéal propre tel que pour tout a,b ϵ A{a ;b ϵ I=> (a ϵI ou b ϵ I)}

De manière équivalente.

▪Un idéal propre est premier si et seulement si chaque fois qu'il contient le produit de deux idéaux il contient l'un ou l'autre. (La contraposée est vrai).

Caractérisation

Soit I un idéale propre distinct de A.

▪ I premier équivaut à A/I intègre

En effet pour tout a;b ϵ A ; $\bar{a}.\ \bar{b} = \bar{0}$ ou $\bar{b} = \bar{0}$ qui appartient a A/I revient a dire que a.b ϵ I.

- Si I est premier et ne contient ni idéal J ni idéal K alors il ne contient pas leur produit. En effet il existe a ϵ J, b ϵ K tel que a.b ϵ J.K qui appartient I car I est premier.
- Si I n'est pas premier alors il existe deux idéaux J et K tel que J.K inclus dans I. Mais soit strictement dans J et K (donc ne contient ni l'un ni l'autre)

  En effet, Il existe a, b ϵ A tel que a, b n'appartenant pas a I, on ait a.b ϵ I.

  Les idéaux J = I + (a) et K = I + (b) contiennent I tandis que J.K inclus dans I.

  Par conséquent tout idéal premier est irréductible s'il est égal à l'intersection de deux idéaux alors il est égal à l'un ou l'autre (car il contient leur produit et il est premier).