Chapitre 17

Anneaux et corps

Résumé -

Après les groupes, deux nouvelles structures jouent un rôle important en mathématiques : les anneaux et les corps. Ils possèdent chacun deux lois internes et quelques régularités.
L'exemple type d'anneau est l'ensemble $\mathbb{Z}$. Nous baserons notre étude des anneaux sur ce que l'on a pu faire en arithmétique. En retour, nous verrons que le second exemple de l'année $\mathbb{K}[X]$ (anneau intégre des polynômes) possède beaucoup de points commun (notion de PGCD, primamlité...).
Les corps sont des anneaux où tous les éléments sont inversibles pour la seconde loi. C'est un ensemble fréquent : $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, et il sera important pour l'étude des espaces vectoriels...

Sommaire

1. Problèmes

? Problème 75 - Structures fondamentales associées à $\mathbb{Z}$

Les deux chapitres précédents nous ont prouvé qu'il est possible de faire beaucoup de chose avec une structure aussi limitée que $\mathbb{Z}$.
Pouvons-nous généraliser? Quelles sont les propriétés fondamentales vérifiées par $\mathbb{Z}$?
Rappelons que $\mathbb{Z}$ est créé par addition $+1$. Mais que très vite, c'est la multiplication qui nous intéresse et en particulier la décomposition (unique) en facteurs premiers.

? Problème 76 - Théorème de Bézout et le lemme de Gauss dans un anneau

Notons (a) et (b), l'ensemble des multiples de a et b respectivement.
Nous avons vu que le théorème de Bézout était d'une importance capitale. Il exprime que $\mathbb{Z} = (a) + (b)$ lorsque $a \wedge b = 1$.
Plus généralement, comment s'exprime-t-il pour des anneaux? Et le lemme de Gauss?

? Problème 77 - Quotienter un anneau

Considérons A, un anneau et munissons le d'une relation d'équivalence $\mathcal{R}$.
A quelle condition suffisante (nécessaire) sur $\mathcal{R}$, peut-on transformer l'ensemble des classes d'équivalence $\dfrac{A}{\mathcal{R}}$ (avec les lois induites) en anneau voire en corps?

2. Structures d'anneau

2.1. Définitions et propriétés premières

<u>Définition d'un anneau</u>

Définition - Anneaux
Soit A un ensemble muni de deux lois de composition internes notées $+$ et $\star$. On dit que $(A,+,\star)$ est un <u>anneau</u> si :
- $(A,+)$ est un groupe commutatif;
- la loi $\star$ est associative;
- la loi $\star$ est distributive par rapport à la loi $+$:

$$\forall (x,y,z) \in A^3,\ x \times (y+z) = x \times y + x \times z \qquad \text{(distibutive à gauche)}$$

$$\forall (x,y,z) \in A^3,\ (x+y) \times z = x \times z + y \times z \qquad \text{(distibutive à droite)}$$

- A possède un élément neutre pour $\star$, noté 1.

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

Exemple - Anneaux classiques

Soit $(A,+,\star)$ un anneau. On note 0 l'élément neutre de $+$ et 1 celui de $\star$.

Intégrité

Définition - Diviseur de 0 et anneau intègre
Soit $(A,+,\star)$ un anneau.
- $a \in A \setminus \{0\}$ est un diviseur de 0 si il existe $b \in A \setminus \{0\}$ tel que $a \star b = 0$ ou $b \star a = 0$.
- A est dit intègre s'il est commutatif et sans diviseurs de 0.

Pour aller plus loin - Commutativité
Il arrive que certains mathématiciens n'exigent pas la commutativité comme condition à l'intégrité (ex : cours d'Algèbre de Roger Godement), mais c'est une exception à la tradition largement adoptée.

Proposition - Simplification (division)
Si A est un anneau intègre, tout élément non nul a de A est régulier pour $\star$, c'est-à-dire que l'on peut simplifier par a :

$$a \star b = a \star c \Rightarrow b = c.$$

Démonstration

Exemple - $\mathbb{Z}$ et $\mathcal{M}_n(\mathbb{K})$

Savoir faire - Exploiter l'intégrité
On exploite l'intégrité dans son sens contraposée : $a \neq 0$ et $b \neq 0 \Longrightarrow ab \neq 0$.
En particulier, si on sait qu'un ensemble est un corps (comme $\frac{\mathbb{Z}}{p\mathbb{Z}}$, alors il est intègre.

Règles de calcul immédiates

Proposition - Lien $+$ et $\star$
On a les relations suivantes :
- $\forall x \in A$, $x \star 0 = 0 \star x = 0$ (on dit que 0 est absorbant).
- $\forall (x,y) \in A^2$, $(-x) \star y = x \star (-y) = -(x \star y)$
- $\forall (x,y) \in A^2$, $(-x) \star (-y) = x \star y$

Démonstration

Proposition - Quelques règles de calcul
Les règles de calculs fréquentes :

— $(a_i)_{1\leqslant i\leqslant n}$ et $(b_j)_{1\leqslant j\leqslant p}$ deux familles d'éléments de A. Alors on peut écrire :

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{p} b_j\right) = \sum_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]} a_i b_j$$

— formule du binôme : si a et b **commutent pour** $\star$ alors

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

— factorisation : si a et b **commutent pour** $\star$ alors

$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^{n-k-1} b^k$$

en notant $xy = x\star y$ et les puissances étant au sens de la loi $\star$.

Remarque - Démonstration ?
Il s'agit exactement des mêmes démonstrations que celles vues pour les nombres réels en début d'année.
En effet, les seules hypothèses qui ont été mobilisées étaient celles de commutativité des nombres (objets).

Un groupe pour $\star$: le groupe des inversibles

Proposition - Groupe des inversibles
L'ensemble des éléments inversibles de $(A,\star)$ est un groupe pour la loi $\star$.
Classiquement, ce groupe est noté $A^\times$.

Démonstration

Exemple - $\mathbb{Z}^*$

Exemple - $(\mathcal{M}_n(\mathbb{K}))^*$

2.2. Construction d'anneaux

Sous-anneaux

Définition - Sous-anneau
Soit $(A,+,\star)$ un anneau. $B\subset A$ est un <u>sous-anneau</u> de A si B est stable pour les lois internes $+$ et $\star$ et si ces lois induites munissent B d'une structure d'anneau, donc, avec $1\in B$.

$(B,+)$ est nécessairement un groupe, stable également pour $\star$: la réciproque est suffisante :

Savoir faire - Caractérisation des sous-anneaux
Soit B une partie de A. B est un sous-anneau de A si et seulement si il vérifie :
- $1\in B$
- $\forall (x,y)\in B^2,\ x-y\in B$
- $\forall (x,y)\in B^2,\ x\star y\in B$

Morphisme (et image) d'anneaux

Définition - Morphisme d'anneaux
Soient $(A,+_A,\star_A)$ et $(A',+_{A'},\star_{A'})$ deux anneaux. Un morphisme d'anneaux de A dans A' est une application f de A dans A' vérifiant :
- $\forall (x,y)\in A^2,\ f(x+_A y)=f(x)+_{A'} f(y)$
- $\forall (x,y)\in A^2,\ f(x\star_A y)=f(x)\star_{A'} f(y)$
- $f(1_A)=1_{A'}$

Exemple - Projection canonique

Exemple - Sur $\mathbb{C}$

Exemple - Morphisme de Fröbenius

<u>Exercice</u>
Soit $f:A\to A'$ un morphisme d'anneaux.

1. Montrer que $f(0_A)=0_{A'}$, $\quad\forall\, x\in A, f(-x)=-f(x)\quad \forall\, x\in A^* f(x^{-1})=f(x)^{-1}$.
2. Montrer que $f^\times = A^\times\to A'^\times,\ x\mapsto f(x)$ est un morphisme de groupes.

<u>Exercice</u>
On dit que $I\subset A$ est un idéal de l'anneau A, si
- $(I,+)$ est un sous-groupe de $(A,+)$.
- $\forall\, x\in I, y\in A,\ x\star y\in I$ et $y\star x\in I$

Soit $f:A\to A'$ un morphisme d'anneaux. Montrer que $\operatorname{Ker} f$ est un idéal de A.

2.3. Idéaux

Dans la suite les anneaux sont considérés commutatifs.

Extension de la congruence

on étend à tous les anneaux, la notion de congruence vu dans $\mathbb{Z}$.

Pour aller plus loin - Cas A non commutatif
Si A n'est pas commutatif, il faut étudier les multiples à droite et les multiples à gauche...

Définition - Multiple dans un anneau
Soit a un élément d'un anneau A. On appelle multiple de a, les éléments de l'ensemble $(a) = \{a \times d, d \in A\}$, (parfois noté aA).
On dit que a divise b (noté $a|b$ si b est un multiple de a.

Définition - Congruence dans un anneau
Soit m un éléments d'un anneau A. Soient a, b deux éléments de A.
On dit que a est congru à b modulo m, noté $a \equiv b[m]$ ssi $b - a \in (m)$ (ou $m|b-a$).

Remarque - Notation multiple
On peut écrire au choix : $m|n$ ou $n \in (m)$ ou encore $(n) \subset (m)$.

Proposition - Relation d'équivalence
Dans un anneau, la relation de congruence modulo m est une relation d'équivalence

Exercice
Faire la démonstration

Compatibilité

Théorème - Compatibilité
Si A est un anneau (commutatif) et $m \in A$.
Alors l'addition et la multiplication sont compatibles pour la relation d'équivalence $\equiv [m]$.
Autrement écrit, l'addition et la multiplication sont indépendants du choix du représentant de la classe d'équivalence ; on peut donc définir une addition et une multiplication sur les classes d'équivalence :

$$\overline{x} \overline{+} \overline{x'} = \overline{x + x'} \qquad \overline{x} \overline{\times} \overline{x'} = \overline{x \times x'}$$

Démonstration

Idéaux

Analyse - Ce qui a marché

Définition - Idéal de A
Soit A un anneau.
On appelle idéal de A, toute partie I de A tel que :
- $0 \in I$
- $(I,+)$ est un sous-groupe de $(A,+)$ (noté $I < A$)
- $\forall\, a \in I, \forall\, b \in A, ab \in I$

Pour aller plus loin - Cas A non commutatif
Si A n'est pas commutatif, il faut étudier les idéaux à droite et les idéaux à gauche...

Exercice
Quels sont les idéaux de $\mathbb{Z}$?

Pour aller plus loin - Sous-anneau ?
Un idéal est donc stable par addition et hemi-multiplication. Mais ce n'est pas un sous-anneau (sauf à être égal à A entier).

Sous-anneaux quotients

Heuristique - Quotientage d'un anneau par un idéal
Parmi les sous-groupes, les sous-groupes distingués permettaient de prolonger la loi interne (par compatibilité) à la structure quotiente qui devenait ainsi un groupe (quotient).
Formellement : si $(H,+) \lhd (G,+)$, alors $\left(\frac{G}{H}, \overline{+}\right)$ est un groupe.
Il en est de même pour le quotient d'un anneau par un idéal

Proposition - Anneau quotient
Soit $(A,+,\star)$ un anneau (commutatif) et I un idéal.
Alors $\left(\frac{A}{I}, \overline{+}, \overline{\star}\right)$ est un anneau (quotient).

Rappelons que $\frac{A}{I}$ désigne l'ensemble des classes d'équivalence de A pour la relation $a \equiv b \Longleftrightarrow a - b \in I$.

Démonstration

Exercice
Montrer que si f est un morphisme d'anneaux A sur B.
Alors $\mathrm{Ker}\, f = \{x \in A \mid f(x) = 0_B\}$ est un idéal de A.
Puis en déduire que $\frac{A}{\mathrm{Ker}\, f}$ est un anneau

Nous avons enfin une définition propre d'un ensemble dont on a beaucoup parlé.
Puis $a\mathbb{Z}$ est un idéal :

Corollaire - Anneau quotient de $\mathbb{Z}$
Soit $a \in \mathbb{Z}$, l'ensemble $\left(\frac{\mathbb{Z}}{a\mathbb{Z}}, \overline{+}, \overline{\times}\right)$ des classes d'équivalence de $\mathbb{Z}$ est un anneau

2.4. Anneau euclidien. Anneau principal

Pour aller plus loin - Anneau non principal
L'anneau des polynômes à coefficients entiers $\mathbb{Z}[X]$ n'est pas prinicipal.
En effet, l'idéal engendré dans $\mathbb{Z}[X]$ par $< 2, X >$ n'est pas principal.

Proposition - Anneau principal
Soit A un anneau.
On dit qu'un idéal I de A est principal si il existe $a \in I$ tel que $I = (a)$.
On dit qu'un anneau est principal si tous ses idéaux sont principaux.

Exemple - $\mathbb{Z}$ est principal

Savoir faire - Montrer qu'un anneau est principal
Une méthode qui ne marche pas toujours est de montrer qu'un tel anneau est d'abord euclidien

Définition - Anneau euclidien
Soit A un anneau. On dit que A est euclidien s'il existe une application $\varphi : A \setminus \{0\} \to \mathbb{N}$ (appelé **stathme**) telle que :

$$\forall\ (a,b) \in A \times A \setminus \{0\}, \exists\ (q,r) \in A^2 \text{ tel que } a = bq + r \text{ avec } r = 0 \text{ ou } \varphi(r) < \varphi(b)$$

Notons que l'unicité n'est pas demandé.

Proposition - Anneau euclidien $\Rightarrow$ Anneau principal
Si A est euclidien, alors A est principal

Démonstration

Exemple - Nombreux

Exercice
On note $\mathbb{Z}[i] = \{a + ib; a, b \in \mathbb{Z}\}$, l'ensemble des entiers de Gauss.

1. Trouver une division euclidienne sur $\mathbb{Z}[i]$
   On prendra, le carré de la fonction module comme stathme
2. En déduire que $\mathbb{Z}[i]$ est principal

3. Structures de corps

3.1. Corps

Définition - Corps
Un corps est un anneau commutatif $(K,+,\times)$ dans lequel tous les éléments autres que 0 sont inversibles pour $\times$ c'est-à-dire que :
$(K,+,\times)$ est un corps si :
- $(K,+)$ est un groupe commutatif;
- $(K^*,\times)$ est un groupe commutatif, où 0 désigne l'élément neutre de K pour $+$ et $K^* = K \setminus \{0\}$.
- la loi $\times$ est distributive par rapport à la loi $+$;

Exemple - Nombreux

Proposition - Tout élément est régulier
Un corps n'a pas de diviseurs de 0. Tout élément autre que 0 est donc régulier (on peut simplifier).

Démonstration

3.2. Idéaux maximaux. Idéaux premiers

Analyse - A quel condition un anneau quotient est-il un corps ?

Définition - Idéal maximal
Soit I un idéal de A.
On dit que I est maximal s'il $I \neq A$ et A est le seul idéal distinct de I, contenant I

Proposition - Corps
Soit I un idéal maximal de A. Alors $\left(\frac{A}{I}, \overline{+}, \overline{\times}\right)$ est un corps.

Pour aller plus loin - Idéal engendré
Si I_1 et I_2 sont deux idéaux, alors $I_1 + I_2 = \{a_1 + a_2 ; a_1 \in I_1, a_2 \in I_2\}$ est un idéal; c'est le plus petit des idéaux qui contient à la fois I_1 et I_2.

Remarque - Réciproque
Comme le montre l'analyse la réciproque est vrai.

Exemple - $6\mathbb{Z}$ n'est pas maximal

Démonstration

Pour aller plus loin - Idéal premier
On dit que I est premier ssi $x \notin I$ et $y \notin I \Rightarrow xy \notin I$.
On a, par exemple, $n\mathbb{Z}$ est premier ssi n est premier.
Et plus généralement, $\frac{A}{I}$ est un anneau intègre ssi I idéal premier.
Dans le cadre de $A = \mathbb{Z}$, $\frac{A}{n\mathbb{Z}}$ est intègre ssi $\frac{A}{n\mathbb{Z}}$ est un corps...

Exemple - $\frac{\mathbb{Z}}{p\mathbb{Z}}$ avec p premier

3.3. Sous-corps. Morphisme (de corps)

Définition - Sous-corps, morphisme
On peut généraliser les définitions précédentes.
- Un sous-corps est un sous-anneau muni d'une structure de corps.
- Un morphisme de corps est un morphisme d'anneaux.
- L'image d'un corps par un morphisme de corps est un corps.

Le dernier point est un exercice à démontrer.

4. Bilan

Synthèse

- Les anneaux sont les structures naturelles pour deux lois internes (addition, et multiplication, ou composition). Nous avons de nombreux exemples : $\mathbb{Z}$, $\mathbb{K}[X]$, $\mathcal{M}_n(\mathbb{K})$...
  Avec l'inversibilité de tous les éléments non nuls, la structure est encore plus riche, elle s'appelle un corps. Les exemples classiques sont $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, voire $\frac{\mathbb{Z}}{p\mathbb{Z}}$ (p premier)
- Mais pour ce dernier exemple, il faut commencer par s'assurer de la bonne définition des lois $\overline{+}$ et $\overline{\times}$, lorsqu'on passe de $\mathbb{Z}$ à $\frac{\mathbb{Z}}{n\mathbb{Z}}$.
  Nous avons vu qu'il fallait que l'ensemble $n\mathbb{Z}$, soit un d'abord un idéal pour que le calcul ait un sens.
  Mieux pour que $\frac{\mathbb{Z}}{n\mathbb{Z}}$ soit un corps, (il faut et)il suffit que $n\mathbb{Z}$ soit un idéal maximal (équivalent à idéal premier, dans ce contexte)
- Les structures d'anneaux ou de corps, se transfère par morphisme (d'anneaux) ou par restriction.

Savoir-faire et Truc & Astuce du chapitre

- Savoir-faire - Caractérisation des sous-anneaux
- Savoir-faire - Montrer qu'un anneau est principal

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$(A,+,\star)$ parfois A	Anneau	$(A,+)$ groupe ; $\star$ l.c.i. associative et unifère ; distributivité	Exemples courants : $\mathbb{Z}$, $\mathbb{K}[X]$, $\mathcal{M}_n(\mathbb{K})$, $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$
I	Idéal de A	$(I,+) < (A,+)$ & $\forall\ a \in A, x \in I,\ ax \in I$	
$(\mathbb{K},+,\star)$ parfois $\mathbb{K}$	Corps	$(\mathbb{K},+,\star)$ anneau, tout élément non nul inversible	Exemples courants : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $F_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$

Retour sur les problèmes

75. Cours
76. Bézout : $(a)+(b)=A$ et lemme de Gauss : $bc \in (a)$ et $(b)+(a)=A$ (a et b étrangers) alors $c \in (a)$.
77. Cours