CH2) Anneaux

1. Généralités

1.1. **Définition.**

Définition 1.1. *Un anneau est la donnée d'un ensemble A, et de deux lois de composition interne $+$, $*$ telles que :*

- *$(A, +)$ est un groupe abélien (on notera 0 l'élément neutre),*
- *$(A, *)$ est associatif et admet un élément neutre 1,*
- *$*$ est distributive par rapport à $+$, i.e. :*

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

et :

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

*L'anneau est **commutatif** si la deuxième loi $*$ est commutative (la première l'est toujours).*

On ne considérera que des anneaux commutatifs. En pratique, on notera $\times$, ou . la deuxième loi "multiplicative", ou même, on l'omettra simplement, notant simplement xy le produit de deux éléments.

1.2. **Exemples d'anneaux :**

1.2.1. *Anneaux de nombres.* Les exemples rudimentaires sont les anneaux $(A, +, \times)$ pour les lois d'addition et multiplications usuelles, avec $A = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

1.2.2. *Matrices.* IL s'agit de l'anneau $(\mathrm{Mat}(n, \mathbb{R}), +, \times)$ où $\mathrm{Mat}(n, \mathbb{R})$ est l'ensemble des matrices $n \times n$ à coefficients réels, $+$ l'addition usuelle des matrices, et $\times$ la multiplication usuelle des matrices.

On peut aussi considérer l'anneau des matrices $n \times n$ à coefficients entiers, rationnels, ou complexes.

1.2.3. *Anneaux arithmétiques.* On a déjà vu que $(\mathbb{Z}/n\mathbb{Z}, \bar{+})$ est un groupe abélien. Mais la multiplication est aussi compatible avec la congruence modulo n : on peut définir le produit $k \bar{\times} l$ comme étant le reste modulo n du produit kl. Alors, $(\mathbb{Z}/n\mathbb{Z}, \bar{+}, \bar{\times})$ est un anneau.

1.3. **Premières propriétés.**

Théorème 1.2. *Soit $(A, +, .)$ un anneau (commutatif). Alors, pour tout x, y, z dans A :*

(1) $x.0 = 0.x = 0$,
(2) $x.(-y) = (-x).y = -(x.y)$
(3) $x.(y - z) = x.y - x.z$

□

Théorème 1.3 (Binôme de Newton)**.** *Soit $(A, +, \times)$ un anneau (commutatif). Alors, pour tout x, y dans A on a :*

$$(x + y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k}$$

où $C_n^k = \frac{n!}{k!(n-k)!}$ est le coefficient binômial. □

1.4. **Groupes des unités.**

Définition 1.4. *Une unité d'un anneau $(A, +, \times)$ est un élément de A inversible pour la loi $\times$, i.e. admettant un inverse.*

Théorème 1.5. *L'ensemble des unités A^* est stable par $\times$. Muni de cette loi, c'est un groupe.* □

1.5. **Diviseurs de** 0**.**

Définition 1.6. *Soit $(A, +, \times)$ un anneau (commutatif). Un **diviseur de** 0 est un élément x de A tel que :*
- *x est non nul : $x \neq 0$,*
- *il existe un élément non-nul y de A tel que $xy = yx = 0$.*

Définition 1.7. *Un anneau $(A, +, \times)$ est **intègre** s'il n'admet aucun diviseur de 0, ie. si :*

$$\forall x, y \in A,\ xy = 0 \Rightarrow x = 0 \text{ ou } y = 0$$

Exemple 1.8. *Les anneaux $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont tous intègres.*

Exercice 1.9. *Trouver tous les diviseurs de 0 dans :*
- $\mathbb{Z}/15\mathbb{Z}$,
- $\mathbb{Z}/13\mathbb{Z}$,
- $\mathrm{Mat}(2, \mathbb{R})$

1.6. **Sous-anneaux.**

Définition 1.10. *Soit $(A, +, \times)$ un anneau (commutatif). Un sous-ensemble B de A est un sous-anneau de A si :*
- *B est un sous-groupe de $(A, +)$,*
- *B est stable pour la loi $\times$,*
- *B contient l'unité 1.*

Remarque 1.11. *La troisième condition n'est pas un corollaire des deux premières, comme le montre l'exemple du sous-ensemble $2\mathbb{Z}$ de $\mathbb{Z}$.*

Exercice 1.12. *Montrer que le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$ lui-même.*

Théorème 1.13. *Un sous-ensemble $B \subset A$ est un sous-anneau si et seulement si :*
- $1 \in B$,
- $\forall x, y \in B,\ x - y \in B$,
- $\forall x, y \in B,\ xy \in B$.

□

1.7. **Morphismes d'anneaux.**

Définition 1.14. *Soient $(A, +, \times)$ et $(A', +, \times)$ deux anneaux. Une application $f : A \to A'$ est un (homo)morphisme d'anneaux si et seulement si :*
- *$\forall x, y \in A,\ f(x + y) = f(x) + f(y)$,*
- *$\forall x, y \in A,\ f(xy) = f(x)f(y)$,*
- *$f(1) = 1$.*

Remarque 1.15. *Si $f : A \to A'$ est un morphisme d'anneaux, alors $f : (A, +) \to (A', +)$ est un morphisme de groupes. En particulier, $f(0) = 0$ et $f(-x) = -f(x)$.*

Exercice 1.16. *Le noyau $f^{-1}(0)$ est-il un sous-anneau de A ?*

1.8. **Anneau produit.**

Théorème - Définition 1.17. *Soit $(A_i)_{i\in I}$ une famille d'anneaux. Alors, le produit $\prod_{i\in I} A_i$ muni des lois produits est un anneau.* □

Cas particulier : si les A_i sont tous égaux, alors $\prod_{i\in I} A_i$ est l'ensemble A^I des applications de I vers A. En tant qu'anneau, il est isomorphe à A^I muni des lois suivantes :

$$\forall f, g \in A^I, \quad \forall i \in I, \quad (f+g)(i) := f(i) + g(i)$$
$$\forall f, g \in A^I, \quad \forall i \in I, \quad f.g(i) := f(i).g(i)$$

2. Idéaux

2.1. **Définition.**

Définition 2.1. *Soit $(A, +, \times)$ un anneau commutatif. Un sous-ensemble I de A est un **idéal** si :*
- *$(I, +)$ est un sous-groupe de $(A, +)$,*
- *$\forall a \in A,\ \forall x \in I,\ ax \in I$.*

Lemme 2.2. *Une partie $I \subset A$ est un idéal de A si et seulement si :*
- *$\forall x, y \in I,\ x + y \in I$,*
- *$\forall a \in A,\ \forall x \in I,\ ax \in I$.*

□

Exercice 2.3. *Soit I un idéal de $(A, +, \times)$. Montrer l'équivalence :*

$$I = A \Leftrightarrow 1 \in I$$

Exercice 2.4. *Montrer que le noyau d'un morphisme d'anneaux est un idéal.*

2.2. **Idéal engendré.**

Théorème 2.5. *Soit $(A, +, \times)$ un anneau (commutatif), et $(I_i)_{i\in I}$ une famille d'idéaux de A. Alors, l'intersection :*

$$\bigcap_{i\in I} I_i$$

est un idéal de A. □

Théorème - Définition 2.6. *Soit $(A, +, \times)$ un anneau (commutatif), et X un sous-ensemble de A non vide. Alors, l'intersection de tous les idéaux de A qui contiennent X est un idéal, appelé **idéal engendré par X**. On le note XA. Il est caractérisé par les propriétés suivantes :*
- *il contient X,*
- *il est contenu dans tout idéal contenant X.* □

Proposition 2.7. *Soient x, y deux éléments de A. Alors, l'idéal engendré par x et y est le sous-ensemble $I(x, y)$ de A suivant :*

$$I(x, y) := \{ux + vy \ / \ u, v \in A\}$$

On le note :

$$xA + yA$$

Démonstration. $I(x, y)$ est un idéal et contient x et y, il contient donc l'idéal engendré par x et y. Inversement, soit I contenant x et y. Alors, il contient tous les $ux + vy$, et donc $I(x, y)$. □

2.3. **Idéal produit, idéal somme.**

Théorème - Définition 2.8. *Soit $(A, +, \times)$ un anneau (commutatif), et I, J deux idéaux de A. Alors, le sous-ensemble de A formé des éléments de la forme $x + y$ est un idéal de A, noté $I + J$ et appelé **idéal somme de I et J**.* □

Exercice 2.9. *Montrer que $I + J$ est l'idéal engendré par $I \cup J$.*

Théorème - Définition 2.10. *Soit $(A, +, \times)$ un anneau (commutatif), et I, J deux idéaux de A. Soit $I.J$ le sous-ensemble de A formé des éléments de la forme $\sum_{i=1}^{n} x_i y_j$ où n est un entier quelconque et où pour tout i entre 1 et n on a $x_i \in I$ et $y_i \in J$. Alors, $I.J$ est un idéal de A, appelé **idéal produit de I et J**.* □

2.4. **Idéaux de $(\mathbb{Z}, +, \times)$.** On sait déjà que les sous-groupes de $(\mathbb{Z}, +)$ sont les sous-ensembles $n\mathbb{Z}$. Mais on vérifie aisément que $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$, puisque le produit d'un multiple de n par n'importe quel entier est toujours un multiple de n. Donc :

Théorème 2.11. *Tout idéal de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ avec $n \in \mathbb{Z}$.* □

Exercice 2.12. *Montrer que $n\mathbb{Z}$ est l'idéal engendré par $\{n\}$.*

2.5. **Quotient par un idéal.**

Théorème - Définition 2.13. *Soit $(A, +, \times)$ un anneau, et $I \subset A$ un idéal. La relation $\sim_I$ sur A définie par :*

$$\forall x, y \in A,\ x \sim_I y \Leftrightarrow x - y \in I$$

est une relation d'équivalence.

On note A/I l'espace quotient, et $p_I : A \to A/I$ la surjection canonique. Il existe une unique structure d'anneau $(A/I, \bar{+}, \bar{\times})$ telle que la surjection canonique $p_I : A \to A/I$ soit un morphisme d'anneaux.

Le noyau de p_i est l'idéal I □.

Exercice 2.14. *On rappelle que pour tout entier n, $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$. Montrer que l'anneau quotient de $\mathbb{Z}$ par $n\mathbb{Z}$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, \bar{+}, \bar{\times})$.*

3. Caractéristique d'un anneau

Théorème - Définition 3.1. *Soit $(A, +, \times)$ un anneau. Il existe un unique morphisme d'anneaux $\varphi_A : \mathbb{Z} \to A$. D'après le Théorème 2.11 le noyau de φ_A est de la forme $n\mathbb{Z}$. L'entier positif (ou nul) n est la **caractéristique** de $(A, +, \times)$.*

Démonstration. Pour tout entier positif n, l'unité 1_A de A ajoutée n fois à elle-même (pour la loi $+$) est notée $n.1_A$. Par exemple :

$$3.1_A = 1_A + 1_A + 1_A$$

Lorsque n est négatif, on convient :

$$n.1_A := -(|n|.1_A)$$

Un morphisme d'anneaux $\varphi : \mathbb{Z} \to A$ envoie nécessairement l'entier 1 sur l'unité 1_A de A. On doit donc avoir aussi :

$$\begin{aligned} \varphi(2) &= \varphi(1+1) = 2\varphi(1) = 2.1_A \\ \varphi(3) &= \varphi(1+2) = \varphi(1) + 2\varphi(1) = 3.1_A \end{aligned}$$

De plus, on doit avoir $\varphi(-1) = -\varphi(1) = -1_A$. Par récurrence, on obtient donc que si $\varphi : \mathbb{Z} \to A$ est un morphisme d'anneaux, alors il doit vérifier :

$$\forall n \in \mathbb{Z},\ \varphi(n) = n.1_A$$

Inversement, on vérifie (grâce à la distributivité) que ceci définit bien un morphisme d'anneaux. □

Exercice 3.2. *Montrer que la caractéristique de $\mathbb{Z}/n\mathbb{Z}$ est n.*

Exercice 3.3. *Montrer que la caractéristique d'un anneau intègre est soit nulle, soit un nombre premier.*

4. Corps

Définition 4.1. *Un **corps** est un anneau $(K, +, \times)$ dont tous les éléments non-nuls sont des unités, i.e. inversibles pour la loi $\times$.*

Exercice 4.2. *Parmi les anneaux suivants, quels sont les corps ?*

$$(\mathbb{Z}, +, \times),\ \ (\mathbb{Q}, +, \times),\ \ (\mathbb{R}, +, \times),\ \ (\mathbb{C}, +, \times),\ \ (\mathrm{Mat}(n, \mathbb{R}), +, \times)$$

Exercice 4.3. *Montrer que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.*

Exercice 4.4. *Montrer que dans un corps, le seul idéal non nul est le corps tout entier.*

Proposition 4.5. *La caractéristique d'un corps $(K, +, \times)$ est soit nulle, soit un nombre premier.* □