Université Aix–Marseille 2019–2020

Licence – Mathématiques
Algèbre 2

Cours à distance – Semaine 1 – Anneaux – Théorie générale

Inspirée de plusieurs exemples comme la somme sur les entiers, la multiplication des matrices inversibles ou la composition de bijections, la notion de groupe a permis d'extraire de ces exemples une substantifique moelle commune, permettant d'axiomatiser ces opérations et d'en abstraire certains calculs. La notion d'anneau, quant à elle, vise à généraliser les situations où, comme sur les nombres ou les matrices, deux opérations cohabitent sur un même ensemble.

1 Anneaux et sous-anneaux

Définition 1.1. Un *anneau* est un ensemble A, muni de deux lois de composition internes, une addition $+ : A \times A \to A$ et une multiplication $\,.\, : A \times A \to A$, vérifiant les propriétés suivantes :

- $(A, +)$ est un groupe abélien dont on note 0_A l'élément neutre ;
- la multiplication est associative, c'est-à-dire $a_1.(a_2.a_3) = (a_1.a_2).a_3$ pour tous $a_1, a_2, a_3 \in A$;
- la multiplication est *distributive* sur l'addition, c'est-à-dire $a_1.(a_2 + a_3) = a_1.a_2 + a_1.a_3$ et $(a_1 + a_2).a_3 = a_1.a_3 + a_2.a_3$ pour tous $a_1, a_2, a_3 \in A$.

Si, de plus, $a_1.a_2 = a_2.a_1$ pour tous $a_1, a_2 \in A$, on dit que l'anneau est *commutatif*. Et s'il existe un élément $1 \in A \setminus \{0\}$ tel que $1.a = a.1 = a$ pour tout $a \in A$, on dit que l'anneau est *unitaire*.

Exemples 1.2.

- $(\mathbb{Z}, +, \,.\,)$, $(\mathbb{Q}, +, \,.\,)$, $(\mathbb{R}, +, \,.\,)$ et $(\mathbb{C}, +, \,.\,)$ sont des anneaux commutatifs et unitaires.
- Pour tout $n \in \mathbb{N}^*$, $(n\mathbb{Z}, +, \,.\,)$ est un anneau commutatif qui n'est unitaire que si $n = 1$.
- Pour tout $n \in \mathbb{N}^*$, $\left(\mathbb{Z}/n\mathbb{Z}, +, \,.\,\right)$ est un anneau commutatif qui n'est unitaire que si $n \geq 2$. En particulier $\{0\} = \mathbb{Z}/\mathbb{Z}$ et $\{0, 1\} = \mathbb{Z}/2\mathbb{Z}$ sont des anneaux commutatifs, le second étant unitaire, mais pas le premier.
- Pour tout $n \in \mathbb{N}^*$ et $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $\big(\mathcal{M}_n(\mathbb{K}), +, \,.\,\big)$ est un anneau unitaire, non commutatif si $n \geq 2$. Il en va donc de même pour $\big(\mathrm{End}(E), +, \circ\big)$ pour tout $\mathbb{K}$–espace vectoriel de dimension finie (et même de dimension infinie).
- L'ensemble $\mathbb{R}[X]$ des polynômes réels à une indéterminée, muni de l'addition et de la multiplication des polynômes, est un anneau.
- Pour tout anneau A et tout ensemble X, $\mathcal{F}(X, A) := \{f : X \to A\}$ est naturellement muni d'une structure d'anneau, la somme et la multiplication étant définies pour tous $f_1, f_2 : X \to A$ par

$$(f_1 + f_2)(x) = f_1(x) + f_2(x) \qquad\qquad (f_1.f_2)(x) = f_1(x).f_2(x)$$

  pour tout $x \in X$. Ce dernier est commutatif et/ou unitaire si et seulement si A l'est. Par exemple, l'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$, ou l'ensemble des suites à valeurs complexes forment des anneaux.

Un anneau est donc un groupe abélien pour l'addition, et à ce titre, tous les résultats du cours sur les groupes s'appliquent. La multiplication, quant à elle, n'induit pas une structure de groupe car il manque en général un élément neutre, et même si l'anneau est unitaire, il manquera toujours des inverses pour certains éléments. Toutefois, en regardant le détail des preuves, on peut observer que certains résultats demeurent.

Lemme 1.3. *Si A est un anneau unitaire, alors l'élément unité pour la multiplication est unique.*

Notation 1.4. Pour tout anneau, il est vraiment classique d'utiliser la notation additive pour l'addition et la notation multiplicative pour la multiplication.

À l'instar de la structure de groupe, la structure d'anneau induit naturellement un certain nombre de règles de calculs.

Proposition 1.5. *Soit A un anneau. On a*

- *pour tout $a \in A$, $0_A.a = a.0_A = 0_A$, on dit que 0_A est* absorbant *;*
- *pour tous $a_1, a_2 \in A$, $-(a_1.a_2) = (-a_1).a_2 = a_1.(-a_2)$, et notamment $(-a_1).(-a_2) = a_1.a_2$;*
- *pour tout $a \in A$ et $n_1, n_2 \in \mathbb{N}^*$, $a^{n_1}.a^{n_2} = a^{n_1+n_2}$ et $(a^{n_1})^{n_2} = a^{n_1.n_2}$;*
- *si A est unitaire, pour tout $a \in A$ et $n \in \mathbb{Z}$, $n.a = (n.1_A).a = a.(n.1_A)$;*
- *(formule du binôme de Newton) si A est unitaire et commutatif, pour tous $a_1, a_2 \in A$ et $n \in \mathbb{N}$,*

$$(a_1 + a_2)^n = \sum_{i=0}^{n} \binom{n}{i}.a_1^i.a_2^{n-i} \ ;$$

- *(identités remarquables) si A est unitaire et commutatif, pour tout $a_1, a_2 \in A$ et $n \in \mathbb{N}$,*

$$a_1^n - a_2^n = (a_1 - a_2).\sum_{i=0}^{n-1} a_1^i.a_2^{n-i-1}.$$

Démonstration. Pour le premier point, on observe que $0_A.a = (0_A + 0_A).a = 0_A.a + 0_A.a$ et $a.0_A = a.(0_A + 0_A) = a.0_A + a.0_A$ et on utilise dans le groupe $(A, +)$ le fait que, dans un groupe, le seul élément égal à son carré est l'élément neutre. La première partie du deuxième point provient des égalités $a_1.a_2 + (-a_1).a_2 = (a_1 - a_1).a_2 = 0_A.a_2 = 0_A$ et $a_1.a_2 + a_1.(-a_2) = a_1.(a_2 - a_2) = a_1.0_A = 0_A$; la seconde de $a_1.a_2 = -(-(a_1.a_2)) = -(a_1.(-a_2)) = (-a_1).(-a_2)$. Le troisième se montre par récurrence sur n comme dans un groupe.

De même, le quatrième point se montre d'abord par récurrence pour $n \in \mathbb{N}$. Le résultat est en effet vrai pour $n = 0$ d'après le premier point. Et si on suppose le résultat vrai pour $n - 1$, on a alors $n.a = (n-1).a + a = \big((n-1).1_A\big).a + 1_A.a = \big((n-1).1_A + 1_A\big).a = (n.1_A).a$ et de même à droite. Pour $n \in \mathbb{Z} \setminus \mathbb{N}$, on a $n.a = -(-n).a = -\big((-n).1_A\big).a = \big(-(-n).1_A\big).a = (n.1_A).a$ et de même à droite.

La formule du binôme de Newton se montre par récurrence sur $n \in \mathbb{N}$. Le résultat est en effet vrai pour $n = 0$. On suppose ensuite le résultat vrai au rang $n - 1$, on a alors

$$\begin{aligned}
(a_1 + a_2)^n &= (a_1 + a_2).(a_1 + a_2)^{n-1} = (a_1 + a_2).\sum_{i=0}^{n-1} \binom{n-1}{i}.a_1^i.a_2^{n-1-i} \\
&= \sum_{i=0}^{n-1} \binom{n-1}{i}.(a_1 + a_2).a_1^i.a_2^{n-1-i} = \sum_{i=0}^{n-1} \binom{n-1}{i}.\big(a_1.a_1^i.a_2^{n-1-i} + a_2.a_1^i.a_2^{n-1-i}\big) \\
&= \sum_{i=0}^{n-1} \binom{n-1}{i}.\big(a_1^{i+1}.a_2^{n-1-i} + a_1^i.a_2^{n-i}\big)
\end{aligned}$$

car A est commutatif. En regroupant les termes selon la puissance de a_1, on obtient alors

$$(a_1 + a_2)^n = \sum_{i=0}^{n} \left(\binom{n-1}{i-1} + \binom{n-1}{i}\right).a_1^i.a_2^{n-i} = \sum_{i=0}^{n} \binom{n}{i}.a_1^i.a_2^{n-i},$$

avec la convention que $\binom{n-1}{-1} = \binom{n-1}{n} = 0$; on a en effet, pour tout $0 < i < n$,

$$\begin{aligned}
\binom{n-1}{i-1} + \binom{n-1}{i} &= \frac{(n-1)!}{(i-1)!(n-i)!} + \frac{(n-1)!}{i!(n-1-i)!} = \frac{(n-1)!}{(i-1)!(n-1-i)!}.\Big(\frac{1}{n-i} + \frac{1}{i}\Big) \\
&= \frac{(n-1)!}{(i-1)!(n-1-i)!}.\frac{i+n-i}{i(n-i)} = \frac{n!}{i!(n-i)!} = \binom{n}{i},
\end{aligned}$$

ainsi que $\binom{n-1}{-1} + \binom{n-1}{0} = 1 = \binom{n}{0}$ et $\binom{n-1}{n-1} + \binom{n-1}{n} = 1 = \binom{n}{n}$.

Enfin, les identités remarquables découlent du calcul direct :

$$(a_1 - a_2).\sum_{i=0}^{n-1} a_1^i.a_2^{n-i-1} = \sum_{i=0}^{n-1}(a_1 - a_2).a_1^i.a_2^{n-i-1} = \sum_{i=0}^{n-1}(a_1^{i+1}.a_2^{n-i-1} - a_1^i.a_2^{n-i})$$

car A est commutatif, et donc

$$\begin{aligned}(a_1 - a_2).\sum_{i=0}^{n-1} a_1^i.a_2^{n-i-1} &= \sum_{i=0}^{n-1} a_1^{i+1}.a_2^{n-i-1} - \sum_{i=0}^{n-1} a_1^i.a_2^{n-i} \\ &= \sum_{i=1}^{n} a_1^i.a_2^{n-i} - \sum_{i=0}^{n-1} a_1^i.a_2^{n-i} \\ &= a_1^n + \sum_{i=1}^{n-1} a_1^i.a_2^{n-i} - \sum_{i=1}^{n-1} a_1^i.a_2^{n-i} - a_2^n \\ &= a_1^n - a_2^n.\end{aligned}$$

□

Remarque 1.6. Si l'anneau A n'est pas unitaire, la convention $a^0 = 1_A$ est caduque. On peut cependant adapter les deux derniers points de la proposition dans ce cas. Si A est un anneau commutatif (mais pas supposé unitaire), pour tous $a_1, a_2 \in A$ et $n \in \mathbb{N}^*$, la formule du binôme de Newton s'écrit

$$(a_1 + a_2)^n = a_1^n + \sum_{i=1}^{n-1} \binom{n}{i}.a_1^i.a_2^{n-i} + a_2^n \ ,$$

et les identités remarquables s'écrivent

$$a_1^n - a_2^n = (a_1 - a_2).\left(a_1^{n-1} + \sum_{i=1}^{n-2} a_1^i.a_2^{n-i-1} + a_2^{n-1}\right).$$

Comme pour les groupes, on peut s'intéresser aux sous-ensembles d'un anneau qui sont eux-mêmes des anneaux.

Définition 1.7. Soit A un anneau. On dit que $B \subset A$ est un *sous-anneau* si B est un sous-groupe de $(A, +)$ stable par multiplication, c'est-à-dire si

- $B \neq \emptyset$;
- $\forall a_1, a_2 \in B, a_1 - a_2 \in B$;
- $\forall a_1, a_2 \in B, a_1.a_2 \in B$.

De plus, si A est unitaire et que $1_A \in B$, on dit que B est un sous-anneau *unitaire*.

Proposition 1.8. *Soit $(A, +, \ .\ )$ un anneau. Alors pour tout $B \subset A$, B est un sous-anneau si et seulement si $(B, +, \ .\ )$ est un anneau.*

Démonstration. On sait déjà que $(B, +)$ est un groupe si et seulement si B est un sous-groupe de A pour l'addition. De plus, la multiplication étant déjà associative et distributive dans A, elle ne peut que le rester dans B ; la seule question qui reste est donc de savoir si B est stable par multiplication. □

Exemples 1.9.

- Pour tout anneau A, $\{0_A\}$ et A sont des sous-anneaux de A.

- On a la suite d'inclusion d'anneaux unitaires

$$\{0\} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

- Pour tout $n \in \mathbb{N}^*$, $n\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}$ qui n'est unitaire que si $n = 1$.
- On a la suite d'inclusion d'anneaux unitaires

$$C^\infty(\mathbb{R},\mathbb{R}) \subset \cdots \subset C^k(\mathbb{R},\mathbb{R}) \subset \cdots \subset C^1(\mathbb{R},\mathbb{R}) \subset C^0(\mathbb{R},\mathbb{R}) \subset \mathcal{F}(\mathbb{R},\mathbb{R}),$$

où $\mathcal{F}(\mathbb{R},\mathbb{R})$ est l'ensemble des applications de $\mathbb{R}$ de $\mathbb{R}$, $C^0(\mathbb{R},\mathbb{R})$ le sous-ensemble des fonctions continues, $C^k(\mathbb{R},\mathbb{R})$ celui des fonctions k fois dérivables, et $C^\infty(\mathbb{R},\mathbb{R})$ celui des fonctions indéfiniment dérivables.

Remarque 1.10. Comme pour les groupes, on peut montrer qu'une intersection de sous-anneaux est un sous-anneau et définir une notion de sous-anneau engendré par un sous-ensemble. Dans ce cours, nous ne développerons toutefois ces notions que pour les idéaux, un cas particulier de sous-anneau, introduit plus tard.

2 Inversibilité et intégrité

Dans un anneau, on n'oblige pas tous les éléments à avoir un inverse pour la multiplication, mais cela n'interdit pas certains d'en avoir. Bien entendu, cela n'a de sens que si A est unitaire.

Définition 2.1. Soit A un anneau unitaire. On dit que $a \in A$ est *inversible* s'il existe $b \in A$ tel que $a.b = b.a = 1_A$. On note $A^\times := \{a \in A \mid a \text{ inversible}\}$.

Avertissement 2.2. Ne pas confondre $A^\times$ et $A^* := A \setminus \{0_A\}$. On a $A^\times \subset A^*$, car l'égalité $0_A.b = 0_A$ pour tout $b \in A$ interdit l'existence d'un inverse pour 0_A, mais l'inclusion inverse est en général fausse.

Exemples 2.3.

- Pour tout anneau unitaire A, $1_A \in A^\times$.
- On a $\mathbb{Z}^\times = \{\pm 1\}$, mais $\mathbb{Q}^\times = \mathbb{Q}^*$, $\mathbb{R}^\times = \mathbb{R}^*$ et $\mathbb{C}^\times = \mathbb{C}^*$.
- Pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ et tout $n \in \mathbb{N}^*$, $\big(\mathcal{M}_n(\mathbb{K})\big)^\times = \mathrm{GL}_n(\mathbb{K})$.

Proposition 2.4. *Pour tout anneau unitaire A, $(A^\times, \ .\ )$ est un groupe. En particulier, l'élément unité et les inverses sont uniques.*

Démonstration. Le seul point à vérifier est que $A^\times$ est bien stable par multiplication. L'associativité et l'existence d'un élément neutre découlent en effet du fait que A est un anneau unitaire, et l'existence d'inverses de la définition même de $A^\times$. Or si $a_1, a_2 \in A^\times$, alors ils ont des inverses $b_1, b_2 \in A$ et on a $(b_2.b_1).(a_1.a_2) = b_2.(b_1.a_1).a_2 = b_2.1_A.a_2 = b_2.a_2 = 1_A$ et pareil pour $(a_1.a_2).(b_2.b_1)$. On a donc bien $a_1.a_2 \in A^\times$. □

Notation 2.5. Si A est un anneau unitaire, alors pour tout $a \in A^\times$, on note a^{-1} l'inverse de a et, pour tout $n \in \mathbb{N}$, $a^{-n} := (a^{-1})^n$. Dès lors, toutes les règles usuelles de calcul dans le groupe $A^\times$ s'appliquent.

Remarque 2.6. On appelle *corps* tout anneau unitaire A tel que $A^\times = A^*$, c'est-à-dire tel que tout élément non nul soit inversible. Les anneaux $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, lorsque p est un nombre premier, sont des corps. L'étude des corps est en soi un domaine important des mathématiques, mais que nous n'aborderons cependant pas dans ce cours.

Nous avons vu que, dans un anneau A, 0_A n'est jamais inversible. C'est en réalité un élément dans une famille d'éléments non inversibles potentiellement plus grande.

Définition 2.7. Soit A un anneau. On dit que a est un *diviseur de zéro* s'il existe $b \in A^*$ tel que $a.b = 0_A$ ou $b.a = 0_A$.

Exemples 2.8.

- Dans $\mathbb{Z}$, il n'y a aucun diviseur de zéro non trivial.
- Si $n \in \mathbb{N}^*$ n'est pas premier, alors il existe $a, b \in [\![2, n-1]\!]$ tels que $n = a.b$ et alors $\overline{a}$ et $\overline{b}$ sont des diviseurs de zéro dans $\mathbb{Z}/n\mathbb{Z}$.

Proposition 2.9. *Dans un anneau, aucun élément ne peut être simultanément inversible et diviseur de zéro.*

Démonstration. Supposons par l'absurde qu'il existe a inversible et $b \neq 0$ tels que $b.a = 0$. On a alors $0 = b.a.a^{-1} = b.1 = b$, ce qui contredit l'hypothèse de non trivialité de b. □

Plus que la non inversibilité, c'est d'être un diviseur de zéro qui interdit de "simplifier" par un élément.

Lemme 2.10. *Soit A un anneau et $a \in A$ un élément qui n'est pas un diviseur de zéro. Si $a.b = a.c$ ou $b.a = c.a$ avec $b, c \in A$, alors $b = c$.*

Démonstration. Si $a.b = a.c$, alors $a.(b-c) = a.b - a.c = 0_A$. Mais puisque a n'est pas un diviseur de zéro, on a nécessairement $b - c = 0_A$, et donc $b = c$. On raisonne de même si $b.a = c.a$. □

On comprendra donc l'intérêt de travailler dans un anneau qui ne possède pas d'autre diviseur de zéro que 0 lui-même : dans un tel anneau, à l'instar de $\mathbb{Z}$, on peut simplifier par tout élément non nul.

Définition 2.11. On dit qu'un anneau A est *intègre* si 0_A y est le seul diviseur de zéro.

Remarque 2.12. Autrement dit, A est intègre si l'égalité $a.b = 0_A$ dans A implique $a = 0_A$ ou $b = 0_A$.

Exemples 2.13.

- $\mathbb{Z}$ est intègre, mais $\mathbb{Z}/n\mathbb{Z}$ ne l'est que si $n \in \mathbb{N}^*$ est premier.
- Tout corps est intègre. En particulier, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ le sont.