Algèbre 2

Hugo SALOU

ENS DE LYON

26 janvier 2025

Table des matières

1 Anneaux.

1.1 Généralités.

Définition 1.1. Un *anneau* est un ensemble A contenant $0, 1$ et munis de deux lois internes notées $+$ et $\cdot$ telles que

- $(A, +)$ est un groupe abélien de neutre 0 ;
- $\forall a, b, c \in A, \quad a(bc) = (ab)c$;
- $\forall a \in A, \quad a \cdot 1 = 1 \cdot a = a$;
- $\forall a, b, c \in A, \quad a(b + c) = ab + ac$ et $(b + c)a = ba + ca$.

Remarque 1.1. De cette définition, on peut en déduire certaines règles de calculs :

- $\forall a \in A, \quad 0 \cdot a = 0$;
- $\forall a, b \in A, \quad (-a)b = -ab$;
- $\forall a, b \in A, \quad (-a)(-b) = ab$;
- $\forall a, b \in A, \quad (a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ quand A est *commutatif*.

Définition 1.2. On dit que A est *commutatif* si pour tous $a, b \in A$, on a $ab = ba$.

Exemple 1.1. Les ensembles $\mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{Q}$ sont des anneaux commutatifs. L'ensemble

$$\mathbb{Z}[\sqrt{3}] := \left\{ n + m\sqrt{3} \;\middle|\; n, m \in \mathbb{Z} \right\} \subseteq \mathbb{R}$$

est un anneau : en effet,

$$(n+m\sqrt{3})(n'+m'\sqrt{3}) = nn' + (nm'+n'm)\sqrt{3} + 3mm' \in \mathbb{Z}[\sqrt{3}].$$

Mais, $\mathbb{Z}[\sqrt[3]{3}]$ ***n'est pas*** un anneau.

De même, l'ensemble $\mathbb{Q}[\sqrt{3}] \subseteq \mathbb{R}$ est un anneau, c'est même un corps car il est stable par passage à l'inverse.

Définition 1.3. Soit A un anneau. Une partie $B \subseteq A$ est appelée un *sous-anneau* si B contient 1 et si la restriction des lois de A à B lui confère une structure d'anneau.

Autrement dit, si B contient 1 et est stable par somme et produit, c'est un sous-anneau de A.

Exemple 1.2. L'ensemble $\mathbb{Z}[i] \subseteq \mathbb{C}$ est un sous-anneau de $\mathbb{C}$. De même que pour $\mathbb{Z}[\sqrt{3}]$, on vérifie facilement qu'il est stable par produit.

Définition 1.4. Soient $A \subseteq B$ des anneaux et E une partie de B. On note $A[E]$ l'anneau *engendré par E sur A* le plus petit sous-anneau de B contenant A et E. C'est l'intersection des sous-anneaux de B contenant A et E.

Remarque 1.2. Si B est commutatif, alors $A[E]$ est l'ensemble des sommes finis de monômes de la forme $ae_1^{n_1} \cdots e_s^{n_s}$ avec $a \in A$, $e_i \in E$ et $n_i \in \mathbb{N}$.

Exemple 1.3. Soit G un groupe.

On note $\mathbb{C}[G] := \mathbb{C}^{|G|} = \bigoplus_{g\in G} \mathbb{C} \cdot \langle g \rangle$. Ses éléments sont de la forme $\sum_{g\in G} a_g \langle g \rangle$ avec $a_g \in \mathbb{C}$. On définit $\langle g \rangle \cdot \langle h \rangle = \langle gh \rangle$ et puis $\langle g \rangle a = a\langle g \rangle$, pour tout $a \in \mathbb{C}$. On définit alors le produit

sur $\mathbb{C}[G]$ par :

$$\begin{aligned}\left(\sum_{g\in G} a_g\langle g\rangle\right)\cdot\left(\sum_{h\in G} b_h\langle g\rangle\right) &= \sum_{g\in G}\sum_{h\in H} a_g b_h\langle gh\rangle \\ &= \sum_{\ell\in G}\left(\sum_{gh=\ell} a_g b_h\right)\langle \ell\rangle \\ &= \sum_{\ell\in G}\left(\sum_{g\in G} a_g b_{g^{-1}\ell}\right)\langle \ell\rangle\end{aligned}$$

.

Définition 1.5. Soit A un anneau. On appelle *A-module* un ensemble M muni d'une loi interne $+$ et d'une loi externe $A\times M\to M, (a,m)\mapsto am$ telle que $(M,+)$ est un groupe abélien et que, pour tous $a,b\in A$ et $m,n\in M$, on a :

- $a(bm)=(ab)m$;
- $1_A m = m$;
- $0_A m = m$;
- $(a+b)m = am+bm$;
- $(-b)m = -(bm)$;
- $a(m+n)=am+an$.

Remarque 1.3. Les groupes abéliens correspondent exactement aux $\mathbb{Z}$-modules. On peut ainsi définir généralement les A-modules comme une donné d'un morphisme

$$f : A\to \mathrm{End}(M).$$

Définition 1.6. Un *morphisme d'anneau* $f : A\to B$ est une application telle que, pour tous $a,b\in A$, on a :

- $f(a+b)=f(a)+f(b)$;
- $f(ab)=f(a)\,f(b)$;
- $f(1_A)=1_B$.

Exemple 1.4. On considère

$$\begin{aligned} \varphi : G &\longrightarrow \mathbb{C}[G] \\ g &\longmapsto \langle g \rangle. \end{aligned}$$

Alors, $\varphi(G)$ est un sous-groupe de $(\mathbb{C}[G], \cdot)$ isomorphe à G. Les représentations de G correspondent exactement aux $\mathbb{C}[G]$-modules. En effet, la donnée d'un morphisme de groupes $G \to \mathrm{Aut}_{\mathbb{C}}(V)$ est équivalente à la donnée d'un morphisme d'anneau $\mathbb{C}[G] \to \mathrm{End}_{\mathbb{C}}(V)$.

À partir de maintenant, tous les anneaux considérés sont commutatifs.

Définition 1.7. Soit A un anneau et $a \in A$.

1. On dit que a est *nilpotent* s'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$.
2. On dit que a est une *racine de l'unité* s'il existe $n \in \mathbb{N}^*$ tel que $a^n = 1$.
3. On dit que a est *idempotent* si $a^2 = a$.
4. On dit que $a \neq 0$ est un *diviseur de zéro* s'il existe $b \neq 0$ tel que $ab = 0$.
5. On dit que a est *inversible* s'il existe $b \in A$ tel que $ab = 1$. On notera $A^\times$ l'ensemble des éléments inversibles. L'ensemble $(A^\times, \cdot)$ forme un groupe.
6. On dit que A est un *corps* si $A^\times = A \setminus \{0\}$.
7. On dit que A est *intègre* si A ne contient pas de diviseurs de zéro.

Remarque 1.4.
- ▷ On verra que A est intègre si et seulement si A est un sous-anneau d'un corps.
- ▷ Un sous-anneau d'un anneau intègre est intègre.

Lemme 1.1. Soit A un anneau intègre. Soient $a, b, c \in A$ avec $a \neq 0$. Alors, si $ab = ac$ on a $b = c$, *i.e.* on peut simplifier par a.

Preuve. On a $ab - ac = 0$ donc $a(b - c) = 0$. Alors $b - c = 0$ car A est intègre et $a \neq 0$. D'où, $b = c$. □

1.2 Divisibilité.

Définition 1.8. Soit A un anneau. On dit que a *divise* b et on note $a \mid b$ s'il existe $c \in A$ tel que $b = ac$.

Remarque 1.5. Cette relation dépend de A. En effet, on peut avoir $A \subseteq B$ et $a, b \in A$ tels que $a \mid b$ dans B mais $a \nmid b$ dans A. Par contre, si $a \mid b$ dans A alors $a \mid b$ dans B.

Proposition 1.1. Soient A un anneau et $a, b, c \in A$.

1. On a $a \mid a$.
2. Si $a \mid b$ et $b \mid c$ alors $a \mid c$.
3. Si $a \mid b$ et $a \mid c$ alors $a \mid \alpha b + \beta c$ pour $\alpha, \beta \in A$.
4. Si $ca \mid cb$ avec $c \neq 0$ et A intègre alors $a \mid b$. Autrement dit, on peut simplifier par c.
5. Si $c \in A^\times$ alors $c \mid a$ (car $a = ac^{-1}c$).
6. On a $a \mid 0$ (car $0 = a \cdot 0$).
7. Si $a \mid b$ et $b \mid a$ et a n'est pas un diviseur de zéro, alors $a = xb$ avec $x \in A^\times$.
8. Pour tout $x \in A^\times$ on a équivalence :

$$a \mid b \iff a \mid xb \iff xa \mid b.$$

Remarque 1.6. La divisibilité se comporte mieux dans les *modules inversibles*.

Remarque 1.7. On a la chaîne d'inclusions :

Anneaux
$\cup|$
Anneaux commutatifs
$\cup|$
Anneaux commutatifs intègres
$\cup|$
Anneaux intègres noethériens
$\cup|$
Anneaux factoriels
$\cup|$
Anneaux principaux
$\cup|$
Anneaux euclidiens
$\cup|$
Corps