Université Aix–Marseille 2019–2020

Licence – Mathématiques
Algèbre 2

Cours à distance – Semaine 2 – Anneaux – Morphismes et idéaux

3 Morphismes d'anneaux

Nous allons maintenant nous intéresser aux applications qui respectent les structures d'anneaux.

Définition 3.1. Soit A_1, A_2 deux anneaux. On dit qu'une application $f : A_1 \to A_2$ est un *morphisme d'anneaux* si, pour tous $a_1, a_2 \in A_1$, on a $f(a_1 + a_2) = f(a_1) + f(a_2)$ et $f(a_1.a_2) = f(a_1).f(a_2)$. Comme dans le cas des groupes, on pourra préciser la nature de f en parlant

- de *monomorphisme (d'anneaux)* si f est injective ;
- d'*épimorphisme (d'anneaux)* si f est surjective ;
- d'*isomorphisme (d'anneaux)* si f est bijective ;
- d'*endomorphisme (d'anneau)* si $A_1 = A_2$;
- d'*automorphisme (d'anneau)* si $A_1 = A_2$ et que f est bijective.

De plus, si A_1 et A_2 sont unitaires, on dit que f est unitaire si $f(1_{A_1}) = 1_{A_2}$.

Remarque 3.2. Tout morphisme d'anneaux est également un morphisme de groupes pour l'addition. Cela permet déjà de déduire un certain nombre de propriétés, telles que $f(0_{A_1}) = f(0_{A_2})$ ou f injective si et seulement si $\mathrm{Ker}(f) := f^{-1}(0_{A_2}) = \{0_{A_1}\}$.

Définition 3.3. On dit que deux anneaux A_1 et A_2 sont *isomorphes* en tant qu'anneaux s'il existe un isomorphisme d'anneaux $f : A_1 \to A_2$. On note alors $A_1 \cong A_2$.

Remarque 3.4. Comme pour les groupes, on peut considérer que deux anneaux isomorphes sont deux représentations d'un même anneau abstrait, et on n'étudie en général les anneaux qu'à isomorphisme près. Il est toutefois important de préciser qu'on parle alors d'isomorphisme *d'anneaux*, car si tout isomorphisme d'anneaux induit un isomorphisme de groupes, la réciproque n'est pas vraie.

Exemples 3.5.

- Si A est un anneau (unitaire) et $B \subset A$ un sous-anneau (unitaire), alors l'injection $B \hookrightarrow A$ est un monomorphisme (unitaire) d'anneaux.
- Pour tout $n \in \mathbb{N}^*$, l'application
$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ k & \longmapsto & \overline{k} \end{array}$$
est un épimorphisme unitaire d'anneaux. Plus généralement, pour tout anneau unitaire A, il existe un unique morphisme d'anneaux unitaire allant de $\mathbb{Z}$ vers A, à savoir
$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & A \\ k & \longmapsto & k.1_A \end{array}.$$
- Soit X un ensemble et A un anneau. Alors pour tout $x \in X$, l'application
$$\mathrm{ev}_x : \begin{array}{ccc} \mathcal{F}(X, A) & \longrightarrow & A \\ f & \longmapsto & f(x) \end{array}$$
est un morphisme d'anneaux.

Comme pour les groupes, on a les propriétés suivantes :

Proposition 3.6.
- *La composée de deux morphismes d'anneaux (unitaires) est un morphisme d'anneaux (unitaire).*
- *Si f est un isomorphisme d'anneaux, alors f^{-1} est également un isomorphisme d'anneaux.*

Démonstration. La démonstration, rigoureusement similaire au cas des groupes, est laissée en exercice. □

Corollaire 3.7. *Pour tout anneau (unitaire) A, l'ensemble des automorphismes (unitaires) d'anneaux de A dans lui-même forme un groupe pour la composition.*

Et la notion de morphisme est toujours liée à la notion de sous-anneau par ce qui suit.

Proposition 3.8. *Soit A_1, A_2 deux anneaux (unitaires), et $f : A_1 \to A_2$ un morphisme (unitaire) d'anneaux.*
- *Pour tout sous-anneau (unitaire) $B \subset A_2$, $f^{-1}(B)$ est un sous-anneau (unitaire).*
- *Pour tout sous-anneau (unitaire) $B \subset A_1$, $f(B)$ est un sous-anneau (unitaire).*

Démonstration. Là encore, la preuve, similaire au cas des groupes, est laissée en exercice. □

4 Idéaux et anneaux quotients

Si A est un anneau et $B \subset A$ un sous-anneau, alors $(B, +)$ est un sous-groupe de $(A, +)$, et ce sous-groupe est distingué puisque $(A, +)$ est abélien. On peut donc considérer le groupe quotient A/B et se demander si la mutliplication de A induit une structure d'anneau sur A/B. La réponse n'est pas toujours oui. Pour $\mathbb{Z} \subset \mathbb{Q}$, par exemple, on a $1 \sim_{\mathbb{Z}} 2$ et pourtant $1.\frac{1}{2} = \frac{1}{2} \nsim_{\mathbb{Z}} 1 = 2.\frac{1}{2}$. Plus généralement, pour que A/B puisse être un anneau, il faut que $0_{A/B}$ soit absorbant, et donc que $a.b \sim_B b.a \sim_B 0_A$ pour tout $b \in B$ et $a \in A$, puisqu'alors $b \sim_B 0$.

Définition 4.1. Soit A un anneau. On dit que $I \subset A$ est un *idéal* si $(I, +)$ est un sous-groupe de $(A, +)$ et que $A.I := \{a.x \mid a \in A, x \in I\} \subset I$ et $I.A := \{x.a \mid a \in A, x \in I\} \subset I$.

Remarques 4.2.
- On peut raffiner la définition en parlant d'idéal *à droite* ou *à gauche* selon que l'impose seulement $A.I \subset I$ ou $I.A \subset I$. La définition ci-dessus correspond alors à la notion d'idéal *bilatère*. Bien entendu, si A est commutatif, les notions d'idéal à droite, à gauche ou bilatère sont équivalentes.
- Un idéal (à droite, à gauche ou bilatère) est toujours un sous-anneau. La réciproque n'est par contre pas vrai : $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$ mais n'en est pas un idéal.
- De même que la notion de sous-groupe distingué $H \lhd G$ dépend de G, la notion d'idéal $I \subset A$ dépend de A. L'ensemble $\mathbb{Z}$ est en effet un idéal de lui-même, mais pas de $\mathbb{Q}$.

Exemples 4.3.
- Pour tout anneau A, $\{0\}$ et A sont des idéaux.
- Pour tout $n \in \mathbb{N}^*$, $n\mathbb{Z} \subset \mathbb{Z}$ est un idéal.
- Aucun des sous-groupes $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ n'est un idéal. Plus généralement, aucun sous-anneau unitaire strict n'est un idéal. Ainsi, les sous-groupes $C^\infty(\mathbb{R}, \mathbb{R}) \subset \cdots \subset C^k(\mathbb{R}, \mathbb{R}) \subset \cdots \subset C^0(\mathbb{R}, \mathbb{R}) \subset \mathcal{F}(\mathbb{R}, \mathbb{R})$ ne sont pas non plus des idéaux.

Lemme 4.4. *Si A est un anneau unitaire et que $I \subset A$ contient un élément inversible, alors $I = A$. En particulier, les seuls idéaux d'un corps $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$.*

Démonstration. Si $x \in I$ est un élément inversible de A, alors $1 = x^{-1}.x \in I$. Du coup, pour tout $a \in A$, $a = a.1 \in I$. Donc $I = A$. La deuxième assertion en découle car, par définition d'un corps, tous les éléments non nuls d'un corps sont inversibles. □

La théorie se déroule alors comme dans le cas des sous-groupes distingués.

Proposition 4.5. *Soit A un anneau (commutatif et/ou unitaire) et $I \subset A$ un idéal. Alors la multiplication de A induit une structure d'anneau (commutatif et/ou unitaire) sur A/I.*

Démonstration. On a déjà vu que A/I est un groupe abélien pour l'addition. Vérifions maintenant que la multiplication de A induit, par $\overline{a}.\overline{b} := \overline{a.b}$, une opération bien définie sur A/I. Pour cela, on considère $a_1, a_2, b_1, b_2 \in A$ tels que $a_1 \sim_I a_2$ et $b_1 \sim_I b_2$, c'est-à-dire tels que $a_2 - a_1, b_2 - b_1 \in I$. On a alors

$$a_2.b_2 - a_1.b_1 = a_2.b_2 - a_2.b_1 + a_2.b_1 - a_1.b_1 = a_2.(b_2 - b_1) + (a_2 - a_1).b_1 \in I$$

car, I étant un idéal, $a_2.(b_2 - b_1) \in I$ et $(a_2 - a_1).b_1 \in I$. On a donc bien $a_2.b_2 \sim_I a_1.b_1$.

L'associativité et la distributivité, ainsi que les éventuelles commutativité et unitarité de cette multiplication sur A/I découlent alors directement des propriétés dans A. □

Exemple 4.6. Pour tout $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ est un anneau quotient.

La notion d'anneau quotient jouera un rôle important dans le cas des anneaux de polynômes, notamment pour l'étude des extensions de corps, mais ceci sort du cadre de ce cours.

Proposition 4.7. *Pour tout morphisme $f : A_1 \to A_2$ d'anneaux,* $\mathrm{Ker}(f)$ *est un idéal de A_1.*

Démonstration. On sait déjà que $\mathrm{Ker}(f)$ est un sous-groupe de A_1 pour l'addition, il suffit de vérifier qu'il est stable par multiplication à droite ou à gauche par un élément de A_1. Or clairement, si $x \in \mathrm{Ker}(f)$ et $a \in A_1$, on a $f(a.x) = f(a).f(x) = f(a).0 = 0$ et $f(x.a) = f(x).f(a) = 0.f(a) = 0$. □

Proposition 4.8. *Si $(I_i)_{i\in I}$ est une famille d'idéaux d'un anneau A, alors $\cap_{i\in I} I_i$ est un idéal de A.*

Démonstration. On sait déjà que $\cap_{i\in I} I_i$ est un sous-groupe pour l'addition, et si $x \in \cap_{i\in I} I_i$ et $a \in A$, alors $x \in I_i$ pour tout $i \in I$, donc $a.x, x.a \in I_i$ pour tout $i \in I$, et donc $a.x, x.a \in \cap_{i\in I} I_i$. □

Définition 4.9. Soit A un anneau et $X \subset A$ un sous-ensemble. On appelle *idéal engendré par X* l'intersection de tous les idéaux de A contenant X. On le note (X) ou $(x_1, \ldots, x_k)$ si $X = \{x_1, \ldots, x_k\}$ est un ensemble fini.

Proposition 4.10. *Si A est un anneau et $X \subset A$ un sous-ensemble, alors (X) est un idéal de A, minimal pour l'inclusion parmi tous les idéaux contenant X.*

Démonstration. La preuve de ce résultat est rigoureusement similaire au cas des groupes. □

Exemples 4.11.

- Si A est un anneau commutatif et $a \in A$ un élément, alors (a) est égal à l'ensemble $\{a.b \mid b \in A\}$ des multiples de a.
- Dans $\mathbb{Z}$, l'idéal engendré par $\{n\}$ est $(n) = n\mathbb{Z}$.

Plus généralement, on a :

Proposition 4.12. *Soit A un anneau et $X \subset A$ un sous-ensemble. Alors*

$$(X) = \Big\{ \sum_{i=1}^{k} a_i.x_i.b_i \mid k \in \mathbb{N}, \forall i \in [\![1, k]\!], x_i \in X, a_i, b_i \in A \Big\}.$$

Si A est commutatif, on a même $(X) = \big\{ \sum_{i=1}^{k} a_i.x_i \mid k \in \mathbb{N}, \forall i \in [\![1, k]\!], x_i \in X, a_i \in A \big\}$.

Démonstration. Notons $B := \left\{ \sum_{i=1}^{k} a_i.x_i.b_i \mid k \in \mathbb{N}, \forall i \in [\![1,k]\!], x_i \in X, a_i, b_i \in A \right\}$. Par stabilité de (X) par somme et produits, on a clairement $B \subset (X)$. Mais réciproquement, on vérifie facilement que B est un idéal de A contenant X ; par minimalité de (X), on a donc $(X) \subset B$.

Si A est commutatif, on a alors $a_i.x_i.b_i = a_i.b_i.x_i = a'_i.x_i$ avec $a'_i := a_i.b_i$. □

On vient de voir que l'intersection permet de définir une opération sur les idéaux. La proposition suivante en donne une seconde.

Proposition 4.13. *Soit A un anneau et $I_1, I_2 \subset A$ deux idéaux. Alors $I_1 + I_2 := \left\{ a_1 + a_2 \mid a_1 \in I_1, a_2 \in I_2 \right\}$ est un idéal.*

Démonstration. L'ensemble $I_1 + I_2$ est non vide car I_1 et I_2 le sont. Si $a, b \in I_1 + I_2$, il existe $a_1, b_1 \in I_1$ et $a_2, b_2 \in I_2$ tels que $a = a_1 + a_2$ et $b = b_1 + b_2$. On a alors $a - b = (a_1 - b_1) + (a_1 - b_2) \in I_1 + I_2$. Donc $I_1 + I_2$ est un sous-groupe additif de A.

Prenons maintenant $a \in A$ et $b \in I_1 + I_2$, et notons à nouveau $b = b_1 + b_2$ avec $b_1 \in I_1$ et $b_2 \in I_2$. Alors $a.b = a.(b_1 + b_2) = a.b_1 + a.b_2 \in I_1 + I_2$ et $b.a = (b_1 + b_2).a = b_1.a + b_2.a \in I_1 + I_2$. Donc $I_1 + I_2$ est un idéal de A. □

Nous verrons plus tard que ces deux opérations sur les idéaux, intersection et somme, généralisent en un certain sens les notions de ppcm et de pgcd des entiers.

Terminons maintenant par l'équivalent pour les anneaux du premier théorème d'isomorphisme.

Théorème 4.14. *Tout morphisme d'anneaux $f : A_1 \to A_2$ induit un isomorphisme d'anneaux $\overline{f} : {}^{A}\!/_{\mathrm{Ker}(f)} \to \mathrm{Im}(f)$.*

Démonstration. La preuve de ce résultat est rigoureusement identique au cas des groupes. □

On peut maintenant revisiter le théorème des restes chinois.

Théorème 4.15. *Soit $n_1, \ldots, n_k \in \mathbb{N}^*$ deux à deux premiers entre eux. Alors ${}^{\mathbb{Z}}\!/_{n_1\mathbb{Z}} \times \cdots \times {}^{\mathbb{Z}}\!/_{n_k\mathbb{Z}}$ est isomorphe à ${}^{\mathbb{Z}}\!/_{n_1 \ldots n_k\mathbb{Z}}$ en tant qu'anneau.*

Démonstration. Commençons par le cas $k = 2$. Pour cela, on considère l'application

$$\varphi : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & {}^{\mathbb{Z}}\!/_{n_1\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{n_2\mathbb{Z}} \\ k & \longmapsto & \left(k[n_1], k[n_2]\right) \end{array}.$$

Il s'agit clairement d'un morphisme d'anneaux. Ce morphisme est de plus surjectif. En effet, pour l'addition, $(\overline{1}, \overline{0})$ est d'ordre n_1 et $(\overline{0}, \overline{1})$ d'ordre n_2 ; puisque ${}^{\mathbb{Z}}\!/_{n_1\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{n_2\mathbb{Z}}$ est abélien et que $\mathrm{pgcd}(n_1, n_2) = 1$, on a vu en exercice que $(\overline{1}, \overline{0}) + (\overline{0}, \overline{1}) = (\overline{1}, \overline{1})$ est d'ordre $n_1 n_2 = \left|{}^{\mathbb{Z}}\!/_{n_1\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{n_2\mathbb{Z}}\right|$, c'est-à-dire que $(\overline{1}, \overline{1})$ est générateur de ${}^{\mathbb{Z}}\!/_{n_1\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{n_2\mathbb{Z}}$. Or $(\overline{1}, \overline{1}) = \varphi(1) \in \mathrm{Im}(\varphi)$, et donc ${}^{\mathbb{Z}}\!/_{n_1\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{n_2\mathbb{Z}} \subset \mathrm{Im}(\varphi)$, l'inclusion réciproque étant évidente. Enfin, si $k \in \mathrm{Ker}(\varphi)$, n_1 et n_2 divisent k, et donc $k \in n_1 n_2\mathbb{Z}$ puisque $\mathrm{pgcd}(n_1, n_2) = 1$. On en conclut que $\mathrm{Ker}(\varphi) \subset n_1 n_2\mathbb{Z}$; l'inclusion réciproque étant immédiate, on déduit du théorème 4.14 que ${}^{\mathbb{Z}}\!/_{n_1\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{n_2\mathbb{Z}} \cong {}^{\mathbb{Z}}\!/_{n_1 n_2\mathbb{Z}}$.

On travaille ensuite par récurrence sur k en observant que n_k est premier avec $n_1 \ldots n_{k-1}$. On a donc, par hypothèse de récurrence et d'après le cas $k = 2$,

$${}^{\mathbb{Z}}\!/_{n_1\mathbb{Z}} \times \cdots \times {}^{\mathbb{Z}}\!/_{n_k\mathbb{Z}} \cong {}^{\mathbb{Z}}\!/_{n_1 \ldots n_{k-1}\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{n_k\mathbb{Z}} \cong {}^{\mathbb{Z}}\!/_{n_1 \ldots n_k\mathbb{Z}}.$$

□