HAX501X – Groupes et anneaux 1

CM12 10/11/2023

Clément Dupont

Rappel de l'épisode précédent

Anneau

Définition

Un **anneau** *est un triplet* $(A, +, \times)$ *où* A *est un ensemble et* $+$, $\times$ *sont deux lois de composition internes sur* A *qui vérifient les axiomes suivants :*

(1) $(A, +)$ *est un groupe abélien.*

(2) *Associativité de* $\times$ *:* $\forall x, y, z \in A\,,\ (x \times y) \times z = x \times (y \times z)$ *(qu'on peut donc noter* $x \times y \times z$*).*

(3) *Élément neutre pour* $\times$ *: il existe un élément* $1_A \in A$ *tel que* $\forall x \in A\,,\ x \times 1_A = x = 1_A \times x$*. On l'appelle le* **un** *de l'anneau.*

(4) *Distributivité de* $\times$ *par rapport à* $+$ *:* $\forall x, y, z \in A$*,* $x \times (y + z) = x \times y + x \times z$ *et* $(x + y) \times z = x \times z + y \times z$*.*

Définition

Un anneau $(A, +, \times)$ *est* **commutatif** *si la multiplication est commutative, c'est-à-dire si :* $\forall x, y \in A\,,\ x \times y = y \times x$*.*

Corps, anneau intègre

Définition

Un **corps** *est un anneau $K \neq \{0_K\}$ qui est commutatif et tel que tout élément $x \in K \setminus \{0_K\}$ est inversible.*

Définition

Un anneau commutatif A est dit **intègre** *si $A \neq \{0\}$ et pour tous $x, y \in A$ on a*

$$xy = 0 \implies (x = 0 \text{ ou } y = 0).$$

Proposition

Si A est un corps alors A est intègre.

- $\mathbb{Z}$ est un anneau intègre (qui n'est pas un corps).
- $\mathbb{R}[X]$ est un anneau intègre (qui n'est pas un corps).

Produit d'anneaux

Soient A et B deux anneaux. On munit le produit cartésien $A \times B$ de lois $+$ et $\times$ par les formules :

$$(x, y) + (x', y') = (x + x', y + y') \quad \text{et} \quad (x, y)(x', y') = (xx', yy')$$

Proposition

Muni de ces lois, $A \times B$ est un anneau.

- Le zéro de $A \times B$ est $(0_A, 0_B)$ et le un est $(1_A, 1_B)$.

Définition

*On appelle $A \times B$ l'***anneau produit** *de A et B.*

- Si A et B ne sont pas l'anneau nul, alors $A \times B$ n'est pas intègre car

$$(1_A, 0_B)(0_A, 1_B) = (0_A, 0_B).$$

Définition

Définition

Soit $(A, +, \times)$ un anneau. Un **sous-anneau** *de A est un sous-ensemble $B \subset A$ qui vérifie les conditions suivantes :*

(1) *$(B, +)$ est un sous-groupe de $(A, +)$.*

(2) *$1_A \in B$.*

(3) *B est stable par $\times$: $\forall x, y \in B$, $x \times y \in B$;*

Proposition

Soit A un anneau et B un sous-anneau de A. Alors B, muni des restrictions des lois $+$ et $\times$, est un anneau, dont le zéro est $0_B = 0_A$ et le un est $1_B = 1_A$.

Remarque

C'est une manière pratique de montrer que quelque chose est un anneau en montrant que c'est un sous-anneau d'un anneau déjà connu.

Remarque

Si A est commutatif alors B l'est aussi. Si A est intègre alors B l'est aussi.

Exemples

Des exemples de sous-anneaux :

- A est toujours un sous-anneau de A.
- $\mathbb{Z}$ et $\mathbb{Q}$ sont des sous-anneaux de $\mathbb{R}$.
- L'ensemble des polynômes pairs $\mathbb{R}[X^2]$ est un sous-anneau de $\mathbb{R}[X]$.
- L'ensemble de suites convergentes est un sous-anneau de l'anneau $\mathbb{R}^{\mathbb{N}}$.
- L'ensemble des fonctions continues $\mathcal{C}^0(\mathbb{R}, \mathbb{R})$ est un sous-anneau de l'anneau $\mathbb{R}^{\mathbb{R}}$.

Des non-exemples de sous-anneaux :

- Pour un anneau $A \neq \{0_A\}$, le sous-groupe $\{0_A\}$ de A n'est pas un sous-anneau de A car il ne contient pas 1_A.
- Le sous-groupe $2\mathbb{Z} \subset \mathbb{Z}$ n'est pas un sous-anneau de $\mathbb{Z}$ car il ne contient pas 1.

Exercice 66
Montrer que le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$.

Sous-corps

Définition

Soit L un corps. Un **sous-corps** *de L est un sous-anneau $K \subset L$ qui vérifie en plus :*

$$\forall x \in K \setminus \{0\}, \ \frac{1}{x} \in K \ .$$

De manière équivalente, c'est un corps K qui est inclus dans L et dont les lois $+$ et $\times$ sont les restrictions de celles de L. On dit aussi que L est une **extension** *de K.*

Proposition

Soit L un corps, soit K un sous-corps de L. Alors L acquiert une structure de K-espace vectoriel, où la somme est la somme dans L, et la multiplication externe $a.x$, avec $a \in K$ et $x \in L$, est simplement la multiplication ax dans le corps L.

Exemple

$\mathbb{R}$ est un sous-corps de $\mathbb{C}$, ce qui fait de $\mathbb{C}$ un $\mathbb{R}$-espace vectoriel (de dimension 2). $\mathbb{Q}$ est un sous-corps de $\mathbb{C}$, ce qui fait de $\mathbb{C}$ un $\mathbb{Q}$-espace vectoriel (de dimension infinie).

Définition

Définition

Soient A et B deux anneaux. Un **morphisme d'anneaux** *de A vers B est une application $f : A \to B$ qui vérifie les axiomes suivants :*

(1) *Compatibilité à la somme $+$: $\forall x, y \in A$, $f(x+y) = f(x) + f(y)$ (dit autrement, f est un morphisme de groupes) ;*

(2) *Compatibilité au produit $\times$: $\forall x, y \in A$, $f(x \times y) = f(x) \times f(y)$;*

(3) *Compatibilité aux unités : $f(1_A) = 1_B$.*

- La condition (1) implique que $f(0_A) = 0_B$, mais la condition (2) n'implique pas la condition (3). Par exemple le morphisme nul donné pour tout $x \in A$ par $f(x) = 0_B$ vérifie (1) et (2) mais pas (3).

Définition

Un **endomorphisme** *d'un anneau A est un morphisme d'anneaux de A dans A.*

Exercice 67

Montrer que la composée de deux morphismes d'anneaux est un morphisme d'anneaux.

Morphismes de $\mathbb{Z}$ dans A

Proposition

Pour un anneau A donné, il existe un unique morphisme d'anneaux $f : \mathbb{Z} \to A$. Il est donné par la formule $f(n) = n1_A$ pour $n \in \mathbb{Z}$.

Démonstration.

- Il est clair que la formule $f(n) = n1_A$ définit bien un morphisme d'anneaux, par les propriétés $(m+n)1_A = m1_A + n1_A$, $(mn)1_A = (m1_A)(n1_A)$, et $1\,1_A = 1_A$.
- Maintenant, si $g : \mathbb{Z} \to A$ est un morphisme d'anneaux quelconque, alors on doit avoir $g(1) = 1_A$ par la condition (3). La condition (1) implique, par une récurrence évidente sur $n \in \mathbb{N}$, qu'on a $g(n) = n1_A$ pour tout $n \in \mathbb{N}$. Comme on doit aussi avoir, toujours par la condition (1), $g(-n) = -g(n)$, on a $g(n) = n1_A$ pour tout $n \in \mathbb{Z}$. On a donc $g = f$, ce qui montre l'unicité.

□

Exemples

- Soit $n \in \mathbb{N}^*$. L'application $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définie par $f(k) = \overline{k}$ est un morphisme d'anneaux. (C'est le seul, par la proposition précédente.)

- La conjugaison $c : \mathbb{C} \to \mathbb{C}$ définie par $c(z) = \overline{z}$ est un morphisme d'anneaux.

Morphismes d'anneaux et inversibles

Proposition

Soit $f : A \to B$ un morphisme d'anneaux et soit $x \in A^\times$, alors $f(x) \in B^\times$ et $f(x)^{-1} = f(x^{-1})$. De plus, l'application induite $f : A^\times \to B^\times$ est un morphisme de groupes.

Démonstration. On calcule : $f(x)f(x^{-1}) = f(xx^{-1}) = f(1_A) = 1_B$, et de même $f(x^{-1})f(x) = 1_B$. Le fait que $f : A^\times \to B^\times$ est un morphisme de groupes est évident puisqu'on a $f(xy) = f(x)f(y)$ pour tous $x, y \in A$ et donc notamment pour tous $x, y \in A^\times$. □

Image réciproque / directe d'un sous-anneau par un morphisme d'anneaux

Proposition

Soit $f : A \to B$ un morphisme d'anneaux.

1) *Soit B' un sous-anneau de B. Alors $f^{-1}(B')$ est un sous-anneau de A.*
2) *Soit A' un sous-anneau de A. Alors $f(A')$ est un sous-anneau de B. Notamment, $\mathrm{Im}(f) = f(A)$ est un sous-anneau de B.*

Remarque

Attention : $\ker(f)$ n'est pas un sous-anneau de A puisqu'il ne contient pas l'unité 1_A (sauf si B est l'anneau nul, c'est-à-dire si $0_B = 1_B$). La bonne notion est ici celle d'**idéal**, qui sera introduite et étudiée plus loin.

Isomorphismes d'anneaux

Définition

Un **isomorphisme** *d'anneaux de A vers B est un morphisme d'anneaux $f : A \to B$ qui est bijectif. On dit alors que A et B sont* **isomorphes** *et on note parfois simplement $A \simeq B$.*

La proposition suivante montre que si $A \simeq B$ alors $B \simeq A$.

Proposition

Soit $f : A \to B$ un isomorphisme d'anneaux. Alors sa réciproque $f^{-1} : B \to A$ est aussi un isomorphisme d'anneaux.

Exercice 68

Montrer que si $A \simeq B$ et $B \simeq C$ alors $A \simeq C$.

Définition

Soit A un anneau. Un **automorphisme** *de A est un isomorphisme de A dans A. (Ou dit autrement, c'est un endomorphisme de A qui est bijectif.)*

Un exemple

Exemple

Soit V un $\mathbb{R}$-espace vectoriel de dimension finie n, et choisissons une base $\mathcal{B}$ de V. On a l'application

$$\mathrm{Mat}_{\mathcal{B}} : \mathrm{End}(V) \to \mathrm{M}_n(\mathbb{R}) \ , \ f \mapsto \mathrm{Mat}_{\mathcal{B}}(f)$$

qui est bijective d'après le cours d'algèbre linéaire. (On rappelle que $\mathrm{Mat}_{\mathcal{B}}(f)$ désigne la matrice de f dans la base $\mathcal{B}$.) C'est un isomorphisme d'anneaux car on a, pour deux endomorphismes linéaires $f, g : V \to V$:

$$\mathrm{Mat}_{\mathcal{B}}(f+g) = \mathrm{Mat}_{\mathcal{B}}(f) + \mathrm{Mat}_{\mathcal{B}}(g),$$

$$\mathrm{Mat}_{\mathcal{B}}(f \circ g) = \mathrm{Mat}_{\mathcal{B}}(f) \times \mathrm{Mat}_{\mathcal{B}}(g),$$

$$\mathrm{Mat}_{\mathcal{B}}(\mathrm{id}_V) = I_n.$$

On a donc un isomorphisme d'anneaux :

$$\mathrm{End}(V) \simeq \mathrm{M}_n(\mathbb{R}).$$

Un autre exemple

Exemple

Soient $m, n \in \mathbb{N}$ avec $m \wedge n = 1$. Alors le théorème chinois des restes affirme qu'on a une bijection

$$f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\ ,\ \overline{k} \mapsto (\widetilde{k}\ ,\ \widehat{k}\ ).$$

C'est un isomorphisme d'anneaux. En effet, on a pour tous $\overline{k}, \overline{l} \in \mathbb{Z}/mn\mathbb{Z}$:

$$f(\overline{k}+\overline{l}) = f(\overline{k+l}) = (\widetilde{k+l}, \widehat{k+l}) = (\widetilde{k}+\widetilde{l}, \widehat{k}+\widehat{l}) = (\widetilde{k}, \widehat{k})+(\widetilde{l}, \widehat{l}) = f(\overline{k})+f(\overline{l}),$$

$$f(\overline{k}\times\overline{l}) = f(\overline{k\times l}) = (\widetilde{k\times l}, \widehat{k\times l}) = (\widetilde{k}\times\widetilde{l}, \widehat{k}\times\widehat{l}) = (\widetilde{k}, \widehat{k})\times(\widetilde{l}, \widehat{l}) = f(\overline{k})\times f(\overline{l}),$$

et

$$f(\overline{1}) = (\widetilde{1}, \widehat{1}).$$

Une remarque importante

Remarque

Deux anneaux A et B qui sont isomorphes ont **les mêmes propriétés** (qui s'énoncent dans le langage de la théorie des anneaux). Ainsi, pour montrer que deux anneaux ne sont pas isomorphes, il suffit de trouver une propriété (qui s'énonce dans le langage de la théorie des anneaux) qui est vraie dans A et pas dans B, ou vice versa. À titre d'exemple, on conseille l'exercice suivant.

Exercice 69

Soient A et B deux anneaux qui sont isomorphes.

1) Montrer que si A est commutatif alors B est commutatif.
2) Montrer que si A est intègre alors B est intègre.
3) Montrer que si l'équation $x^2 = -1_A$ n'a pas de solution dans A alors l'équation $y^2 = -1_B$ n'a pas de solution dans B.

Exercice 70

Montrer que $\mathbb{C}$ et $\mathbb{R}^2$ sont isomorphes en tant que groupes mais pas en tant qu'anneaux.

Morphismes d'un corps vers un anneau non nul

Proposition

Soient K un corps et $A \neq \{0\}$ un anneau non nul. Tout morphisme d'anneaux $f : K \to A$ est injectif.

Démonstration. Soit $x \in K$ tel que $f(x) = 0_A$, et supposons que $x \neq 0_K$. Alors $0_A = f(\frac{1}{x})f(x) = f(\frac{1}{x} \times x) = f(1_K) = 1_A$, donc A est l'anneau nul, contradiction. □

- Notamment, un morphisme d'anneaux d'un corps K vers un corps L est injectif.

La caractéristique d'un anneau

Définition

Soit A un anneau. La **caractéristique** *de A est le plus petit entier $n \in \mathbb{N}^*$ tel que $n1_A = 0_A$, si ce nombre existe, et 0 sinon.*

- Dit autrement, la caractéristique de A est l'ordre de 1_A dans le groupe $(A, +)$ si celui-ci est fini, et 0 si celui-ci est infini.

Exemple

$\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n, et $\mathbb{Z}$ est de caractéristique 0.

- De manière équivalente : on considère le morphisme d'anneaux canonique $\varphi : \mathbb{Z} \to A$, qui est donné par $\varphi(k) = k1_A$. Alors φ est notamment un morphisme de groupes abéliens et donc $\ker(\varphi)$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$ pour un certain entier $n \in \mathbb{N}$. Cet entier n est la caractéristique de A.

Deux cas assez différents...

- Cas $n = 0$. Alors $\ker(\varphi) = \{0\}$ et donc φ est injectif, et donc induit un isomorphisme entre $\mathbb{Z}$ et le sous-anneau $\mathrm{Im}(\varphi) \subset A$. Conclusion :

$$A \text{ contient un sous-anneau isomorphe à } \mathbb{Z}.$$

- Cas $n > 0$. Alors φ passe au quotient par la relation de congruence modulo n (vérifiez-le). On a donc une application

$$\psi : \mathbb{Z}/n\mathbb{Z} \to A \ , \ \overline{k} \mapsto k1_A.$$

On vérifie facilement que ψ est un morphisme d'anneaux. On montre maintenant qu'il est injectif. Pour $k \in \{1, \ldots, n-1\}$ on a $\psi(\overline{k}) = k1_A \neq 0_A$ puisque n est minimal. Donc $\ker(\psi) = \{\overline{0}\}$ et ψ est injectif. Il induit donc un isomorphisme entre $\mathbb{Z}/n\mathbb{Z}$ et le sous-anneau $\mathrm{Im}(\psi) \subset A$. Conclusion :

$$A \text{ contient un sous-anneau isomorphe à } \mathbb{Z}/n\mathbb{Z}.$$

Caractéristique d'un anneau intègre

Proposition

Un anneau intègre est soit de caractéristique 0 soit de caractéristique p premier.

Démonstration. Soit A un anneau intègre. Comme $A \neq \{0\}$ on a $0_A \neq 1_A$ et A n'est pas de caractéristique 1. Supposons que A est de caractéristique $n \geqslant 2$ un nombre composé, c'est-à-dire tel qu'on peut écrire $n = ab$ avec $1 < a, b < n$. On peut réécrire $n1_A = 0_A$ comme $(a1_A)(b1_A) = 0_A$, et comme A est intègre cela implique qu'on a $a1_A = 0_A$ ou $b1_A = 0_A$. Comme $a, b < n$, c'est en contradiction avec le fait que n est minimal. □

Caractéristique d'un corps

La notion de caractéristique est particulièrement importante dans le cas des corps.

- Soit K un corps de caractéristique zéro. Alors on a un morphisme d'anneaux
$$\widetilde{\varphi} : \mathbb{Q} \to K \ , \ \frac{a}{b} \mapsto \frac{a1_K}{b1_K}$$
qui est nécessairement injectif car $\mathbb{Q}$ est un corps. Donc
$$K \text{ contient un sous-corps isomorphe à } \mathbb{Q}.$$
En particulier, c'est un $\mathbb{Q}$-espace vectoriel.

- Soit K un corps de caractéristique p premier. Alors
$$K \text{ contient un sous-corps isomorphe à } \mathbb{Z}/p\mathbb{Z}.$$
En particulier, c'est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel.