Algèbre Cours 9

Anneaux

27 novembre 2009

Définition

Définition – Anneau. Un anneau unitaire est un triplet $(A, +, *)$ où A est un ensemble, $+ : A \times A \longrightarrow A$ et $* : A \times A \longrightarrow A$ deux lois internes sur A vérifiant les axiomes suivants :

1. $(A, +)$ est un groupe abélien (en particulier, il existe un (unique) élément $0 \in A$ tel que $0 + a = a + 0 = a$ pour tout $a \in A$) ;
2. $(A, *)$ est un monoïde (en particulier, il existe un (unique) élément $1 \in A$ tel que $1 * a = a * 1 = a$ pour tout $a \in A$) ;
3. la loi $*$ est distributive (à gauche et à droite) par rapport à $+$: pour tous $a, b, c \in A$, on a
$$(a + b) * c = a * c + b * c \qquad \text{et} \qquad a * (b + c) = a * b + a * c.$$

$(A, +, *)$ est dit commutatif si $*$ l'est c'est-à-dire si $a * b = b * a$ pour tous $a, b \in A$.

$\longrightarrow$ Abus de langue : soit A un anneau !

Exemples

Exemple – Anneau nul. Soit $A = \{x\}$ un ensemble réduit à un élément. Montrer qu'il existe sur A une unique structure d'anneau unitaire, que cette structure est commutative et que $1 = 0$. Inversement, que peut-on dire d'un anneau unitaire $(A, +, *)$ tel que $1 = 0$.

Exemple – Anneaux de nombres. Les ensembles suivants ont une structure naturelle d'anneau unitaire :$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Citons aussi $\mathbb{D} = \{a/10^n,\ a \in \mathbb{Z}, n \in \mathbb{Z}\}$. Peut-on remplacer 10 par un entier quelconque ?
Citons encore $\mathbb{Z}[i] = \{a + bi,\ a, b \in \mathbb{Z}\} \subset \mathbb{C}$ qui est appelé l'anneau des entiers de Gauss ou encore $\mathbb{Z}[j] = \{a + bj,\ a, b \in \mathbb{Z}\}$ (où $j = \exp(2i\pi/3)$).

Exemples : encore

Exemple – Anneau d'endomorphisme. Soit $(G, +)$ un groupe abélien. Alors $(\mathrm{End}_{\mathrm{gr.}}(G), +, \circ)$ est un anneau unitaire.
De même, si V est un k-espace vectoriel alors $\mathrm{End}_k(V) = \mathscr{L}(V)$ est un anneau unitaire (et même une k-algèbre...).
Si A est un anneau unitaire alors $\mathrm{M}_n(A)$ aussi. Que « vaut » $\mathrm{M}_n(\mathrm{M}_p(A))$?

Exemple – Anneaux produits. Soit $(A_i)_{i \in I}$ des anneaux.
L'addition et la multiplication terme à terme détermine sur $B = \prod_{i \in I} A_i$ une structure d'anneau unitaire. On dit que B est l'anneau produit des A_i.

Exemple – Anneaux de polynômes. $\mathbb{R}[X]$ et $\mathbb{C}[X]$ sont des anneaux unitaires.

Exemple – Anneaux quotient. $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{R}[X]/\langle X^2 + 1 \rangle$ sont des anneaux unitaires.

Calcul dans un anneau

Notation Comme d'habitude, pour une loi notée additivement, l'opposé de $a \in A$ pour la loi $+$ est noté $-a$.

Exercice On fixe $a \in A$. Montrer que $b \mapsto a * b$ et $b \mapsto b * a$ sont des endomorphismes du groupe $(A, +)$.
En déduire que 0 est absorbant pour $*$: $a * 0 = 0 * a = 0$ pour tout $a \in A$.
En déduire aussi que $a * (-b) = (-a) * b = -(a * b)$ et en particulier que $(-1) * x = x * (-1) = -x$.

Exercice Soit $a, b, c, d \in A$. Pourquoi a-t-on $(a + b) * (c + d) = a * c + b * c + a * d + b * d$? A-t-on $(a + b)^2 = a^2 + 2a * b + b^2$?

Calcul dans un anneau : suite

Proposition – La formule du binôme de Newton. Soit $a, b \in A$ tel que $ab = ba$ alors, pour tout $n \in \mathbb{N}$, on a

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} .$$

En particulier, pour tout $a \in A$, on a

$$(1+a)^n = \sum_{k=0}^{n} \binom{n}{k} a^k .$$

Proposition – Identité remarquable. Soit $a, b \in A$ tel que $ab = ba$ alors, pour tout $n \in \mathbb{N}$, on a

$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k} .$$

En particulier, pour tout $a \in A$, on a

$$1 - a^n = (1-a) \sum_{k=0}^{n-1} a^k .$$

D'autres identités remarquables

Exercice – Formule du multinôme. Soient $a_1, \ldots, a_m \in A$ tel que $a_i * a_j = a_j * a_i$ pour tous i, j. Développer $(a_1 + \cdots + a_m)^n$.

Exercice Soit $a_1, \ldots, a_n \in A$. On pose $I = \{1, 2, \ldots, n\}$ et pour $H \subset I$, on définit $a_H = \sum_{i \in H} a_i$. On a

$$(-1)^n \sum_{\sigma \in \mathfrak{S}_n} a_{\sigma(1)} \cdots a_{\sigma(n)} = \sum_{H \subset I} (-1)^{|H|} (a_H)^n .$$

Qu'obtient-on lorsque les a_i commutent deux à deux ?

Morphisme d'anneaux

Définition – Morphisme. Soit $(A, +, *)$ et $(B, +, *)$ deux anneaux unitaires. Un morphisme d'anneaux unitaires $f : A \to B$ est une application vérifiant les deux propriétés suivantes

1. $f : (A, +) \to (B, +)$ est un morphisme de groupes : $f(a + b) = f(a) + f(b)$ pour tous $a, b \in A$;
2. $f : (A, *) \to (B, *)$ est un morphisme de monoïdes : $f(a * b) = f(a) * f(b)$ pour tous $a, b \in A$ et $f(1) = 1$.

On a automatiquement $f(0) = 0$.

Définition – Isomorphisme d'anneaux. Soit $(A, +, *)$ et $(B, +, *)$ deux anneaux unitaires. Un morphisme d'anneaux unitaires $f : A \to B$ est un isomorphisme s'il existe un morphisme d'anneaux $g : B \to A$ tel que $g \circ f = \mathrm{id}_A$ et $f \circ g = \mathrm{id}_B$. On dit alors que A et B sont isomorphes.

Comme d'habitude, on a « morphisme bijectif = isomorphisme ».

Exemples

Exemple L'application

$$\lambda : \begin{cases} A \longrightarrow \mathrm{End}_{\mathrm{gr.}}((A,+)) \\ a \longmapsto \lambda_a : x \mapsto ax \end{cases}$$

est un morphisme d'anneaux unitaires.

Exemple – Composition. Soit A, B, C trois anneaux unitaires et $f : A \to B$ et $g : B \to C$ deux morphismes d'anneaux unitaires. Alors $g \circ f : A \to C$ est un morphisme d'anneaux unitaires et id_A est un morphisme d'anneaux unitaires : les anneaux forment une sous-catégorie de la catégorie des ensembles.

Exemple – Anneau nul. Soit $A = \{0\}$ « l' »anneau nul et B un anneau unitaire. Existe-t-il un morphisme d'anneaux unitaires (et si oui combien) $f : A \to B$? Même question avec $f : B \to A$? On dit que A est un objet terminal dans la catégorie des anneaux unitaires.

Encore des exemples

Exemple – Quotient. Les surjections canoniques $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ et $\pi : \mathbb{R}[X] \to \mathbb{R}[X]/\langle X^2+1\rangle$ sont des morphismes d'anneaux unitaires.

Exemple – Polynômes. Pour $x \in \mathbb{R}$, l'application $\mathrm{ev}_x : P \in \mathbb{R}[X] \to P(x) \in \mathbb{R}$ est un morphisme d'anneaux unitaires.

Exemple – Produit. Soit $(A_i)_{i\in I}$ une famille d'anneaux unitaires alors la projection sur le i^{e} facteur :

$$p_i : \begin{cases} \prod_{i\in I} A_i & \longrightarrow A_i \\ (a_i)_{i\in I} & \longmapsto a_i \end{cases}$$

est un morphisme d'anneaux unitaires. Énoncer et démontrer une propriété universelle du produit pour les anneaux unitaires.

P.U. de l'anneau $\mathbb{Z}$

Théorème – Propriété universelle de l'anneau $\mathbb{Z}$. Soit A un anneau unitaire. Il existe un unique morphisme d'anneaux unitaires $f : \mathbb{Z} \to A$. Il est donné par $f(k) = k1_A$. On dit que $\mathbb{Z}$ est un objet initial de la catégorie des anneaux unitaires.

Définition – Caractéristique d'un anneau unitaire. Le noyau de l'unique morphisme $f : \mathbb{Z} \to A$ est de la forme $n\mathbb{Z}$ pour un unique $n \in \mathbb{N}$. Cet entier n est appelé la caractéristique de l'anneau A. C'est le plus petit entier non nul(s'il existe) tel que $n1_A = 0$. Il vérifie aussi $na = 0$ pour tout $a \in A$ (pourquoi ?).

Exercice Montrer qu'il n'existe aucun morphisme d'anneaux unitaires de $\mathbb{Q}$ (resp. $\mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}$ avec $n \geqslant 1$) dans $\mathbb{Z}$.
Montrer que l'unique morphisme d'anneaux unitaires $f : \mathbb{Z} \to \mathbb{Q}$ vérifie que pour tous morphismes d'anneaux unitaires $g, h : \mathbb{Q} \to A$ tel que $g \circ f = h \circ f$, on a $h = g$.

Sous-anneaux

Définition – Sous-anneaux. Soit A un anneau unitaire. Un sous-anneau unitaire B de A est une partie de A telle que $(B, +)$ soit un sous-groupe de A et $(B, *)$ soit un sous-monoïde de A (en particulier, on doit avoir $1 \in B$). Les lois induites donnent à B une structure d'anneau unitaire telle que l'application d'inclusion $i : B \to A$ soit un morphisme d'anneaux unitaires.

Remarque – Sous-anneau : un critère. Pour que B soit un sous-anneau unitaire de A, il suffit que B soit stable par $+$ et $*$, $1 \in B$ et $-1 \in B$.

Proposition – Sous-anneau engendré. Une intersection de sous-anneau unitaire de A est un sous-anneau unitaire de A. Si $S \subset A$, on peut considérer $\langle\langle S \rangle\rangle$ le sous-anneau unitaire engendré par S qui est par définition l'intersection des sous-anneaux unitaires contenant S. C'est le plus petit sous-anneau de A contenant S. Décrire les éléments de $\langle\langle S \rangle\rangle$.

Sous-anneaux : exercices

Exercice Quel est le sous-anneau de $\mathbb{R}$ engendré par $1/2$? et celui engendré par $\sqrt{2}$? Quel est le sous-anneau de $\mathbb{R}$ engendré par les inverses des nombres premiers ? Quel est le sous-anneau de $\mathbb{C}$ engendré par i ?
Soit A un anneau unitaire. Montrer qu'il existe un plus petit sous-anneau unitaire contenu dans A (dit anneau premier de A) et que ce sous-anneau unitaire est commutatif et l'image de l'unique morphisme $f : \mathbb{Z} \to A$.

Exercice Montrer que l'image (resp. l'image réciproque) d'un sous-anneau unitaire par un morphisme d'anneaux unitaires est un sous-anneau unitaire. Énoncer et démontrer un théorème de correspondance pour les sous-anneaux unitaires de A et B pour un morphisme surjectif d'anneaux unitaires $f : A \to B$.

Convention

À partir de maintenant, « anneau » signifiera « anneau unitaire » et « morphisme d'anneaux » signifiera « morphisme d'anneaux unitaires ».

Idéal

Définition – Idéal. Soit A un anneau. Un idéal à gauche I (resp. à droite) de A est un sous-groupe additif de $(A, +)$ tel que pour tout $a \in A$ et tout $x \in I$, on ait $ax \in I$ (resp. $xa \in I$).
Un idéal bilatère de A est une partie de A qui est à la fois un idéal à gauche et à droite c'est-à-dire un sous-groupe additif de $(A, +)$ tel que pour tous $a, b \in A$ et tout $x \in I$, on ait $axb \in I$.

Exemple $\{0\}$ et A sont des idéaux bilatères. Un anneau est dit simple si ce sont les seuls idéaux bilatères et qu'ils sont distincts.

Exercice Déterminer les idéaux bilatères de $\mathrm{M}_n(A)$ en fonction de ceux de A. En déduire que si k est un corps alors $\mathrm{M}_n(k)$ est un anneau simple.
Montrer qu'un anneau simple et commutatif est un corps.
Déterminer les idéaux à gauche et à droite de $\mathrm{M}_n(k)$ (où k est un corps).

Idéaux engendrés

Proposition Une intersection d'idéaux à gauche (resp. à droite, bilatère) est un idéal à gauche (resp. à droite bilatère).
Soit S est une partie de A. L'intersection des idéaux à gauche (resp...) contenant S est un idéal à gauche (resp...) appelé idéal à gauche (resp...) engendré par S. C'est le plus petit idéal à gauche (resp...) contenant S. Il est noté $\langle S \rangle$ ou (S) (attention aux confusions !) Donner la forme de ses éléments.

Exercice – Idéaux de $\mathbb{Z}$. Déterminer les idéaux de $\mathbb{Z}$ (resp. $k[X]$ où k est un corps). Montrer qu'ils sont engendrés par un élément (on dit que ce sont des idéaux principaux).

Anneau quotient

Proposition – Bonne relation d'équivalence. Soit A un anneau commutatif unitaire et $\mathscr{R}$ une relation d'équivalence sur A. On a équivalence entre

1. Il existe une structure d'anneau sur $A/\mathscr{R}$ tel que la surjection canonique $\pi : A \to A/\mathscr{R}$ soit un morphisme d'anneaux ;
2. $\mathscr{R}$ est compatible avec $*$ et $+$;
3. Il existe un idéal bilatère I de A tel que $x\mathscr{R}y$ si et seulement si $x - y \in I$.

L'idéal I est bien déterminé : c'est la classe de 0 et donc le noyau de π.

Corollaire – Une autre caractérisation des idéaux bilatères. Le noyau d'un morphisme d'anneaux est un idéal bilatère. Les idéaux bilatères de A sont exactement les noyaux des morphismes (surjectifs) d'anneaux.

Propriété universelle du quotient

Proposition Soit I un idéal bilatère de A et $\pi : A \to A/I$ la surjection canonique. On considère un morphisme d'anneaux $f : A \to B$. On a alors équivalence entre

- Il existe une application $\overline{f} : A/I \to B$ telle que $\overline{f} \circ \pi = f$;
- $f(I) = 0$;
- $I \subset \operatorname{Ker} f$.

L'application $\overline{f}$ est uniquement déterminée, c'est un morphisme d'anneaux. L'image de $\overline{f}$ est la même que celle de f. Le noyau de $\overline{f}$ est $\operatorname{Ker} f/I$.

Corollaire – Théorème d'isomorphisme. Soit A, B deux anneaux et $f : A \to B$ un morphisme d'anneaux. Alors, f induit un isomorphisme d'anneaux $\varphi : A/\operatorname{Ker} f \to \operatorname{Im} f$ donné par

$$\varphi(a + \operatorname{Ker} f) = f(a)\,.$$

Si f est surjectif, on a $B \overset{\text{ann.}}{\simeq} A/\operatorname{Ker} f$.

Théorème de correspondance

Soit A, B deux anneaux, $f : A \to B$ un morphisme d'anneaux. Si J est un idéal de B (à gauche, à droite, bilatère), $f^{-1}(J)$ est un idéal (à gauche, à droite, bilatère) de A. Mais attention I est un idéal de A alors $f(I)$ n'est pas un idéal de B.

Proposition – Théorème de correspondance. On suppose que f est surjectif alors on a des bijections qui conservent inclusion et intersection, entre les idéaux bilatères (resp. à gauche, à droite) de A contenant $\operatorname{Ker} f$ et les idéaux bilatères (resp. à gauche, à droite) de B.
De plus, si $I \subset A$ et $J \subset B$ sont deux idéaux bilatères qui se correspondent alors $A/I \overset{\text{ann.}}{\simeq} B/J$.

Éléments remarquables d'un anneau

Définition Soit A un anneau.
Un élément $a \in A$ est dit régulier à gauche (resp. à droite) si l'application $\lambda_a : x \mapsto ax$ (resp. $\rho_a : x \mapsto xa$) est injective.
Un élément $a \in A$ est dit inversible à gauche (resp. à droite) si l'application ρ_a (resp. λ_a) est surjective ; un élément $a \in A$ est dit inversible s'il est inversible à droite et à gauche.
Un élément $a \in A$ est dit nilpotent s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$.

Définition – Anneau à division. Soit A un anneau. On dit que A est un anneau à division ou un corps non nécessairement commutatif si $A \neq \{0\}$ et tout élément non nul de A est inversible.
Un anneau à division commutatif est un corps.
Exprimer la propriété d'anneaux à division en terme d'idéaux.

Définition – Anneau intègre. Soit A un anneau. On dit que A est intègre si A est commutatif, $A \neq 0$ et tout élément non nul est régulier. Dans un anneau commutatif, les éléments non réguliers sont appelés les diviseurs de 0.

Suite dans 10 minutes !