

Anneau

Définition	Soit A un ensemble muni de deux lois de composition interne « $*$ » et « $+$ » Le triplet $(A, +, *)$ est un anneau ssi $(A, +)$ est un groupe commutatif - La loi « $*$ » est associative : $\forall (a, b, c) \in A^3 \quad a * (b * c) = (a * b) * c$ - La loi « $*$ » est distributive par rapport à la loi « $+$ » : $\forall (a, b, c) \in A^3 \quad a * (b + c) = a * b + a * c$ Lorsque la loi « $*$ » admet un élément neutre, l'anneau est appelé anneau unitaire.
Remarque	99% des anneaux que vous étudierez cette année seront des anneaux unitaires.
Exemple	$(\mathbb{Z}, +, *)$ est un anneau unitaire.
Remarque	Lorsque la loi « $*$ » est commutative, l'anneau $(A, +, *)$ est dit commutatif. L'anneau $(\mathbb{Z}, +, *)$ cité plus haut est donc commutatif.
Propriétés	Soit $(A, +, *)$ un anneau unitaire. Soient a, b, c et d quatre éléments quelconques de cet anneau. - En appelant 0 l'élément neutre de $(A, +)$ nous avons $a \cdot 0 = 0 \cdot a = 0$ (0 est dit élément absorbant) $a * (-b) = -(ab) = (-a) * b$ $(a + b) * (c + d) = a * c + a * d + b * c + b * d$ - En appelant 1 l'élément neutre de la loi « $*$ ». En définissant a^n par $\begin{cases} a^0 = 1 \\ a^{n+1} = a * a^n \end{cases}$ il vient pour p et n entiers naturels quelconques : $a^{n+p} = a^n * a^p$ et $(a^n)^p = a^{np}$ $a + a + \dots + a$ (n termes) $= n * a$
Preuve	
$a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \Rightarrow a \cdot 0 = a \cdot 0 + a \cdot 0 \Rightarrow a \cdot 0 - a \cdot 0 = a \cdot 0 + a \cdot 0 - a \cdot 0 \Rightarrow a \cdot 0 = 0$. De même à gauche. $a * (-b) + ab = a * (-b + b) = a \cdot 0 = 0$ Donc $a * (-b) = -ab$ De même $(-a) * b + ab = (-a + a) * b = 0 * b = 0$ Donc $(-a) * b = -ab$ $(a + b) * (c + d) = (a + b) * c + (a + b) * d$ (associativité) $= a * c + b * c + a * d + b * d$ (associativité) $a^{n+p} = a * a^{n-1+p} = a^2 * a^{n-2+p} = \dots a^n * a^{n-n+p} = a^n * a^p$ $(a^n)^p = a * a \dots a$ (np termes) $= a^{np}$ - Par récurrence sur n : - Si $n = 0$ c'est évident - Supposons que $a + a + \dots + a$ (n termes) $= n * a$ $a + a + \dots + a$ ($n + 1$ termes) $= a + [a + a + \dots + a]$ (n termes) $= 1 * a + n * a = (1 + n) * a$ On procède de même à droite avec $a + a + \dots + a$ ($n + 1$ termes) $= a * (n + 1)$. Donc l'égalité est vraie aussi à l'ordre $n + 1$	
Propriétés	Soit $(A, +, *)$ un anneau commutatif unitaire. $\forall (a, b) \in A^2, \forall n \in \mathbb{N}$ Binôme de Newton : $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$
Preuve	
Par recurrence sur n : - Pour $n = 0$ c'est évident. - Supposons que $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$ et essayons de le montrer à l'ordre $n + 1$ $(a + b)^{n+1} = (a + b)(a + b)^n = a \cdot (a + b)^n + b \cdot (a + b)^n = a \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} + b \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$ $(a + b)^{n+1} = \sum_{k=0}^n \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^n \binom{n}{k} a^k b^{n+1-k} \quad (\text{c'est là que } a * b = b * a \text{ intervient})$ $(a + b)^{n+1} = \sum_{k=0}^n \binom{n}{k} a^{k+1} b^{n+1-(k+1)} + \sum_{k=0}^n \binom{n}{k} a^k b^{n+1-k}$ Or $\sum_{k=0}^n \binom{n}{k} a^{k+1} b^{n+1-(k+1)} = \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k}$ (On réindice les k) Donc $(a + b)^{n+1} = \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=0}^n \binom{n}{k} a^k b^{n+1-k}$ $(a + b)^{n+1} = b^{n+1} + \sum_{k=1}^n \left[\binom{n}{k-1} + \binom{n}{k} \right] a^k b^{n+1-k} + a^{n+1} = b^{n+1} + \sum_{k=1}^n \binom{n+1}{k} a^k b^{n+1-k} + a^{n+1}$ $(a + b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}. \text{ L'égalité est vraie au rang } n + 1$	

Propriété	Soit $(A, +, *)$ un anneau commutatif unitaire. $\forall (a, b) \in A^2, \forall n \in \mathbb{N}$ $a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$
Preuve	
	$\begin{aligned} (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k} &= a \sum_{k=0}^{n-1} a^k b^{n-1-k} - b \sum_{k=0}^{n-1} a^k b^{n-1-k} = \sum_{k=0}^{n-1} a^{k+1} b^{n-1-k} - \sum_{k=0}^{n-1} a^k b^{n-k} = \sum_{k=0}^{n-1} a^{k+1} b^{n-1-k} - \sum_{k=0}^{n-1} a^k b^{n-k} \\ &= \sum_{k=1}^n a^k b^{n-k} - \sum_{k=0}^{n-1} a^k b^{n-k} = a^n - b^n \end{aligned}$
Remarque	Nous nous sommes placés dans un anneau commutatif. C'est une hypothèse forte. Les deux propriétés précédentes restent vraies lorsque seuls les éléments a et b commutent.
Définition	Soit A un anneau unitaire. A est dit intègre lorsque $\forall (a, b) \in A^2, a * b = 0 \Rightarrow \begin{cases} a = 0 \\ \text{ou} \\ b = 0 \end{cases}$
Exemples	- L'anneau $(\mathbb{Z}, +, *)$ est bien sur intègre. - Pour l'instant il est difficile de rencontrer dans votre vécu de mathématicien un anneau non intègre. Ces ensembles existent pourtant et vous les côtoierez abondamment très bientôt. Nous allons donc en avance de phase vous en présenter un : $\mathbb{Z}/4\mathbb{Z}$ que vous reverrez très bientôt. Le reste de la division d'un entier relatif par 4 est 0, 1, 2 ou 3. Donc n'importe quel entier relatif est congru à 0, 1, 2 ou 3 modulo 4. La relation « être congru à » est une relation d'équivalence sur $\mathbb{Z}$. $\mathbb{Z}$ peut donc être compartimenté en 4 classes d'équivalence que nous noterons $\dot{0}, \dot{1}, \dot{2}$ ou $\dot{3}$. $8 \in \dot{0}$ car $8 = 4 * 2 + 0$ $-5 \in \dot{3}$ car $-5 = 4 * (-2) + 3$ Ces quatre classes d'équivalence $\{\dot{0}, \dot{1}, \dot{2}, \dot{3}\}$ constituent l'ensemble $\mathbb{Z}/4\mathbb{Z}$: Nous allons maintenant munir cet ensemble de deux lois $+$ et $*$ définies par $\forall (\dot{x}, \dot{y}) \in (\mathbb{Z}/4\mathbb{Z})^2 \quad \dot{x} + \dot{y} = (x + y)$ et $\dot{x} * \dot{y} = (x * y)$ Par exemple $\dot{2} + \dot{3} = \dot{1}$ et $\dot{2} * \dot{3} = \dot{2}$ Il vous reste à vérifier que $(\mathbb{Z}/4\mathbb{Z}, +, *)$ est un anneau unitaire d'élément neutre $\dot{0}$ pour l'addition et $\dot{1}$ pour la multiplication. Et bien cet anneau n'est pas intègre ! En effet $\dot{2} * \dot{2} = \dot{0}$.
Propriété	Soit $(A, +, *)$ un anneau unitaire. L'ensemble des éléments inversibles pour la loi $*$ noté $Inv(A)$ est un groupe pour la multiplication.
Preuve	
	- Remarquons que la loi $*$ est une loi de composition interne pour $Inv(A)$ $\forall (x, y) \in (Inv(A))^2, x * y$ est inversible. En effet si x et y sont inversibles, il suffit de construire $y^{-1} * x^{-1}$ Nous avons $(y^{-1} * x^{-1}) * (x * y) = y^{-1} * (x^{-1} * x) * y = 1 = (x * y) * (y^{-1} * x^{-1})$. Donc $x * y$ est bien inversible. 1 est inversible. Donc $1 \in Inv(A)$ - La loi $*$ est associative par rapport à l'addition dans $(A, +, *)$ donc aussi dans $Inv(A)$ - Si $x \in Inv(A)$ alors $x^{-1} \in Inv(A)$. (Son inverse est x)
Exemple	- Si $A = (\mathbb{R}, *, +)$ alors $Inv(A) = (\mathbb{R}^*, *)$ - Si $A = (\mathbb{Z}, *, +)$ alors $Inv(A) = \{1; -1\}$
Définition	Soit $(A, +, *)$ un anneau unitaire. Soit B une partie stable de A pour les lois $+$ et $*$. On dit que B est un sous anneau de A ssi $1_A \in B$ et si $(B, +, *)$ est un sous anneau pour les lois $+$ et $*$.
Exemples	$(A, +, *)$ est un sous anneau de $(A, +, *)$ $(\mathbb{Z}, +, *)$ est un sous anneau de $(\mathbb{Q}, +, *)$ qui est un sous anneau de $(\mathbb{R}, +, *)$ qui est un sous anneau de $(\mathbb{C}, +, *)$