STRUCTURES ALGÉBRIQUES

Lois de composition internes

Dans ce paragraphe E est un ensemble non vide, et $(x,y,z)\in E^3$.

∘ Une loi de composition interne $\star$ aussi notée *lci* sur E est une application φ de $E\times E$ dans E notée $\varphi(x,y)=x\star y$.

∗ L'addition $+$ et le produit $\times$ sont des lci sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.
La multiplication est une lci sur $\mathbb{R}_+^*$ et sur $\{-1,1\}$.
La composition $\circ$ d'applications sur un ensemble est une lci.

∗ La soustraction n'est pas une lci sur $\mathbb{N}$ car il existe des entiers naturels dont la différence n'est pas un entier naturel :

$$\exists\,(x,y)\in\mathbb{N}^2 \quad x-y \text{ n'est pas défini dans } \mathbb{N}$$
par exemple $4-5$ n'est pas un entier naturel.

La division n'est pas une lci sur $\mathbb{Q}$ car un quotient par 0 n'est pas défini.
La multiplication n'est pas une lci sur $\mathbb{R}_-$ car le produit de deux nombres négatifs est positif, par exemple $(-1)\times(-2)=+2\notin\mathbb{R}_-$.

∘ Caractérisation d'une loi de composition interne $\star$:

Associativité : $\quad\forall\,(x,y,z)\in E^3 \quad (x\star y)\star z=x\star(y\star z)$

Commutatitivité : $\quad\forall\,(x,y)\in E^2 \quad x\star y=y\star x$

$e\in E$ est élément neutre : $\quad\forall\,x\in E \quad e\star x=x\star e=x$

Lorsque $e\in E$ est élément neutre, x a un symétrique $x'\in E$:

$$x\star x'=x'\star x=e$$

$u\in E$ est un élément régulier :

$$\forall\,(x,y)\in E^2 \qquad x\star u=y\star u\Longrightarrow x=y$$
$$\mathsf{ET}\; u\star x=u\star y\Longrightarrow x=y$$

a est élément absorbant : $\quad\forall\,x\in E \quad x\star a=a\star x=a$

La loi $\star$ est régulière si et seulement si tout élément de E est régulier.

∗ L'addition $+$ des nombres et la composition $\circ$ des applications sur un ensemble sont des lci associatives.
L'addition $+$ et la multiplication $\times$ sont commutatives.

∗ La soustraction $-$ et la puissance ne sont pas des lci associatives ; il existe des nombres pour lesquels l'égalité n'est pas vérifiée :

$$9-(7-1)=9-6=3 \qquad (9-7)-1=2-1=1\neq 3$$
$$\left(2^3\right)^2=8^2=64=2^6 \qquad 2^{3^2}=2^{(3^2)}=2^9=128\neq 64$$

∗ La puissance des nombres n'est pas commutative :

$$2^3=8 \qquad 3^2=9$$

∗ Le nombre 0 est élément neutre pour l'addition $+$.
Le nombre 1 est élément neutre pour la multiplication $\times$.
L'application Id est élément neutre pour la composition $\circ$.

∗ $-x$ est le symétrique du nombre x pour l'addition et est appelé opposé, et $1/x$ est le symétrique de x supposé non nul pour la multiplication, il est appelé inverse.
L'application réciproque d'une application bijective f sur un ensemble E est le symétrique de f pour la composition :

$$f\circ f^{-1}=f^{-1}\circ f=\mathrm{Id}_E$$

∗ L'addition $+$ est régulière sur les ensembles de nombre, le nombre 0 n'est pas régulier et est un élément absorbant pour la multiplication $\times$.

▶▶ La composition des applications sur tout ensemble E ayant au moins deux éléments n'est pas commutative.

▷▷ Notons a et $b\neq a$ deux éléments différents de E, et $f:E\to E$ et $g:E\to E$ les applications définies ainsi :

$$\begin{cases} f(a)=a \\ f(b)=a \\ f(x)=a \quad \text{si } x\neq a \text{ et } x\neq b \end{cases} \qquad \begin{cases} g(a)=b \\ g(b)=a \\ g(x)=a \quad \text{si } x\neq a \text{ et } x\neq b \end{cases}$$

$$(g\circ f)(b)=g(a)=b \qquad (f\circ g)(b)=f(a)=a\neq b \qquad f\circ g\neq g\circ f$$

Les applications $g\circ f$ et $f\circ g$ sont définies de E dans E.
Il existe donc un élément $u=a$ de E pour lequel les images sont différentes, les applications sont donc différentes :

$$g\circ f = f\circ g : E\to E \iff \big(\forall\, x\in E \quad (g\circ f)(x) = (f\circ g)(x)\big)$$
$$g\circ f \neq f\circ g \iff \mathsf{NON}\,(g\circ f = f\circ g)$$
$$\iff \mathsf{NON}\ \big(\forall\, x\in E \quad (g\circ f)(x) = (f\circ g)(x)\big)$$
$$\iff \exists\, u\in E \quad (g\circ f)(u) \neq (f\circ g)(u)$$

La lci $\circ$ n'est pas commutative sur l'ensemble E^E des applications de E dans E. Il existe en effet deux applications f et g telles que $g\circ f \neq f\circ g$.

►» La loi de composition $\circ$ des applications sur les ensembles à un élément est commutative.

»» Si l'ensemble E a un seul élément a alors l'ensemble des applications sur $E = \{a\}$ comporte uniquement l'application identité $\mathrm{Id}_{\{a\}}\, a \mapsto a$. Dans ce cas la loi de composition $\circ$ est commutative sur $\{a\}$.

$$E = \{a\} \qquad \{a\}^{\{a\}} = \big\{\mathrm{Id}_{\{a\}}\big\} \quad \mathrm{Id}_{\{a\}} : a\mapsto a \quad \mathrm{Id}_{\{a\}}\circ\mathrm{Id}_{\{a\}} = \mathrm{Id}_{\{a\}}$$

Distributivité

◦ La loi $\star$ est distributive par rapport à la loi $\perp$ si et seulement si elle vérifie ces deux propositions :

$$\forall\,(x,y,z)\in\mathbb{A}^3 \qquad x\star(y\perp z) = (x\star y)\perp(x\star z)$$
$$\mathsf{ET}\ (x\perp y)\star z = (x\star z)\perp(y\star z)$$

Ce deux égalités sont équivalentes lorsque la lci $\star$ est commutative.

∗ La multiplication $\times$ est distributive par rapport à l'addition $+$:

$$x(y+z) = xy + xz \qquad (x+y)z = xz + yz$$

∗ La puissance est distributive à droite par rapport à la multiplication et n'est pas distributive à gauche :

$$\forall\,(x,y)\in{\mathbb{R}_+^*}^2 \quad \forall\, z\in\mathbb{R} \quad (x\times y)^z = x^z\times y^z \ [\text{et } x^{y+z} = x^y\times x^z]$$
$$\exists\, x\in\mathbb{R}_+^* \quad \exists\,(y,z)\in\mathbb{R}^2 \quad x^{(yz)} \neq x^y\times x^z$$
$$\text{par exemple } 2^{3\times 2} = 2^6 = 128 \neq 2^3\times 2^2 = 2^5 = 32$$

□ Si la loi $\perp$ est régulière, d'élément neutre n, et distributive par rapport à la loi $\star$ alors l'élément n est absorbant pour la loi $\star$:

$$(n\star a)\perp\underline{n} = n\star a = (n\perp n)\star a = (n\star a)\perp(\underline{n\star a})$$
$$(a\star n)\perp\underline{n} = a\star n = a\star(n\perp n) = (a\star n)\perp(\underline{a\star n})$$
$$n = n\star a = n = a\star n$$

Les groupes

Dans ce paragraphe G est un ensemble et $\star$ est une lci sur G.

Définition des groupes

- $(G,\star)$ est un groupe si et seulement si la lci $\star$ vérifie ces propriétés :

$\star$ est associative $\qquad \forall\,(x,y,z)\in E^3 \quad (x\star y)\star z = x\star(y\star z)$

$\mathsf{ET}\ \star$ possède un élément neutre $e\in E \quad \forall\, x\in E \quad x\star e = e\star x = x$

ET tout élément x de E possède un symétrique

$$\forall\, x\in E \quad \exists\, x'\in E \quad x\star x' = x'\star x = e$$

◦ Le groupe est dit commutatif si et seulement si la loi $\star$ est commutative.

∗ L'associativité de la loi $\star$ permet d'omettre les parenthèses dans l'écriture des produits.
Un groupe quelconque n'est généralement pas commutatif et les produits $x\star y$ et $y\star x$ sont *a priori* différents.

Premières propriétés des groupes

■ L'élément neutre d'un groupe est unique, il est généralement noté e.
Le symétrique d'un élément x est unique et généralement noté x^{-1}.

◊ La définition des éléments neutres justifie que des éléments neutres e et e' de $(G,\star)$ sont nécessairement égaux :

$$\forall\, u\in G \quad u\star e = \underline{e\star u = u} \qquad \forall\, v\in G \quad e'\star v = v\star e' = v$$
$$\underline{e' = e\star e'} = e$$

La première égalité correspond à $u = e'$ et la seconde à $v = e$.

◊ La méthode de démonstration de l'unicité du symétrique repose sur l'associativité. L'élément neutre de G est noté e. Soit $x\in G$, et $\widetilde{x}$ et $\widetilde{x}$ et $\widehat{x}$ deux symétriques de x :

$$\widetilde{x}\star x = x\star\widetilde{x} = e \qquad \widehat{x}\star x = x\star\widehat{x} = e$$
$$\begin{aligned}\widetilde{x}\star x\star\widehat{x} &= (\widetilde{x}\star x)\star\widehat{x} = e\star\widehat{x} = \widehat{x}\\ &= \widetilde{x}\star(x\star\widehat{x}) = \widetilde{x}\star e = \widetilde{x}\end{aligned}$$

∗ L'élément neutre des lois d'addition + et de multiplication × est généralement noté 0 ou 1, et le symétrique appelé opposé et noté $-x$, ou inverse et noté $1/x = x^{-1}$.

■ L'élément neutre e et les symétriques vérifient ces propriétés :

$$e^{-1} = e \qquad (x^{-1})^{-1} = x \qquad (x\star y)^{-1} = y^{-1}\star x^{-1}$$

Autrement dit le symétrique d'un produit, est écrit dans l'autre sens, le produit des symétriques.

◊ La définition de l'élément neutre justifie en particulier $e\star e = e$. Cette égalité $e\star e = e$ traduit la définition $x\star x^{-1} = x^{-1}\star x = e$ du symétrique x^{-1} de x avec $x = x^{-1} = e$. Ainsi $e^{-1} = e$.
L'associativité justifie la dernière égalité :
$(x\star y)\star(y^{-1}\star x^{-1}) = x\star(y\star y^{-1})\star x^{-1} = x\star e\star x^{-1} = x\star x^{-1} = e$
$(y^{-1}\star x^{-1})\star(x\star y) = y^{-1}\star(x^{-1}\star x)\star y = y^{-1}\star e\star y = y^{-1}\star y = e$

∗ L'associativité de la loi $\star$ généralise la formule reliant l'inverse d'un produit et, écrit dans l'autre sens, le produit des inverses, par exemple $(x\star y\star z)^{-1} = z^{-1}\star y^{-1}\star x^{-1}$:

$$\begin{aligned}z^{-1}\star y^{-1}\star x^{-1}\star x\star y\star z &= z^{-1}\star y^{-1}\star(x^{-1}\star x)\star y\star z\\ &= z^{-1}\star(y^{-1}\star y)\star z = z^{-1}\star z = e\\ x\star y\star z\star z^{-1}\star y^{-1}\star x^{-1} &= x\star y\star(z\star z^{-1})\star y^{-1}\star x^{-1}\\ &= x\star(y\star y^{-1})\star x^{-1} = x\star x^{-1} = e\end{aligned}$$

★ Tout groupe est non vide car il contient un élément neutre.

□ Tout élément u d'un groupe $(G,\star)$ est régulier.

◊ Un produit par u^{-1} justifie la propriété :

$$\begin{array}{ll} x\star u = y\star u & x\star u = y\star u\\ \Longrightarrow x\star u\star u^{-1} = y\star u\star u^{-1} & \Longrightarrow x\star u\star u^{-1} = y\star u\star u^{-1}\\ \Longrightarrow x = y & \Longrightarrow x = y\end{array}$$

□ Si deux éléments x et y d'un groupe d'élément neutre e vérifie $x\star y = e$ alors $x = y^{-1}$ et $y = x^{-1}$.

◊ Des produits par à gauche par x^{-1} ou à droite par y^{-1} justifient les deux égalités :

$$\begin{aligned}x^{-1}\star x\star y &= (x^{-1}\star x)\star y = e\star y = y\\ &= x^{-1}\star(x\star y) = x^{-1}\star e = x^{-1}\\ x\star y\star y^{-1} &= x\star(y\star y^{-1}) = x\star e = x\\ &= (x\star y)\star y^{-1} = e\star y^{-1} = y^{-1}\end{aligned}$$

Exemples de groupes

∗ Les structures suivantes sont des groupes commutatifs :

$$(\mathbb{Z},+) \quad (\mathbb{Q},+) \quad (\mathbb{R},+) \quad (\mathbb{C},+) \quad (\{1,-1\},\times)$$
$$(\mathbb{Q}^*,\times) \quad (\mathbb{R}^*,\times) \quad (\mathbb{Q}_+^*,\times) \quad (\mathbb{R}_+^*,\times) \quad (\mathbb{C}^*,\times)$$

∗ Ces structures ne sont pas des groupes :
— $(\mathbb{N},+)$ n'est pas un groupe car 1 n'a pas d'opposé dans $\mathbb{N}$.
— $(\mathbb{Z}\setminus\{0\},\times)$ car 2 n'a pas d'inverse entier.
— $(\mathbb{Q},\times)$ car 0 n'a pas d'inverse dans $\mathbb{Q}$.

∗ La structure $(\mathcal{S}_E,\circ)$ est un groupe, où $\mathcal{S}_E$ l'ensemble des bijections d'un ensemble E dans E.
L'élément neutre est l'application Id_E et la définition même de l'application réciproque est celle du symétrique :

$$(\mathrm{Id}_E, f)\in\mathcal{S}_E^2 \qquad f\circ\mathrm{Id}_E = \mathrm{Id}_E\circ f = f \qquad f\circ f^{-1} = f^{-1}\circ f = \mathrm{Id}_E$$

∗ Le groupe $(\mathcal{S}_E,\circ)$ n'est pas commutatif dès que l'ensemble E a au moins trois éléments.

∗ L'ensemble E^E des applications sur un ensemble E ayant au moins deux éléments n'est pas un groupe car une application constante n'est pas bijective, et ne possède donc pas de symétrique, c'est-à-dire d'application réciproque.

∗ La propriété $x\star y = e$ entraine $x = y^{-1}$ et $y = x^{-1}$ n'est valable que dans les groupes.
Dans l'ensemble des applications sur $\mathbb{N}$, les applications f et g ci-dessous vérifient $g\circ f = \mathrm{Id}_{\mathbb{N}}$ sans que g et f soient bijectives, ni réciproques l'une de n'autre :

$$f : n\mapsto n+1 \qquad g : n\mapsto \max(n-1,0) \qquad g\circ f = \mathrm{Id}_{\mathbb{N}}$$
$$(f\circ g)(0) = 1 \qquad f\circ g \neq \mathrm{Id}_{\mathbb{N}}$$

L'application f n'est pas surjective car 0 n'a pas d'antécédents ; l'application g n'est pas injective car $g(0) = g(1)$.
L'ensemble $\mathbb{N}^{\mathbb{N}}$ des applications sur $\mathbb{N}$ n'est pas un groupe.

Présentation des sous-groupes

Dans cette partie $(G,\star)$ est un groupe d'élément neutre e.

• Le sous-ensemble $H \subset G$ est dit stable pour la loi $\star$ lorsqu'il vérifie les conditions équivalentes ci-dessous :

$$\begin{aligned}
&\forall\,(x,y)\in H^2 \quad x\star y\in H\\
\iff & H\star H\subset H \qquad \text{où } H\star H=\left\{x\star y \;\middle/\; (x,y)\in H^2\right\}\\
\iff & {}^{\star}\!/_{H^2} : H\times H \longrightarrow H,\ (x,y)\longmapsto x\star y \text{ est une application bien définie}\\
\iff & {}^{\star}\!/_{H^2} \text{ est une lci sur } H.
\end{aligned}$$

∘ De même un sous-ensemble H est stable par symétrique si et seulement s'il vérifie cette proprosition :

$$\forall\, x\in H \quad x^{-1}\in H$$

• Un sous-groupe H de $(G,\star)$ est un sous-ensemble de G qui a une structure de groupe pour la restriction de la loi $\star$ à H^2.

□ Tout sous-groupe H de $(G,\star)$ est stable par produit et par inverse, et contient l'élément neutre de G :

$$e\in H \qquad \big(\forall\,(x,y)\in H^2 \quad x\star y\in H\big) \qquad \big(\forall\, x\in H \quad x^{-1}\in H\big)$$

◊ La restriction de la loi $\star$ à $H\times H$ est une lci sur H, ainsi tout couple $(a,b)\in H^2$ vérifie $a\star b\in H$.

◊ Par définition le sous-groupe H possède un élément neutre noté $e'\in H$, la restriction du produit à H vérifie $e'\star e'=e'$. Par ailleurs tout élément de H est élément de G et la loi $\star$ sur G vérifie $e'\star e=e'$ par définition de l'élément neutre de G :

$$\begin{aligned}
e' &= e'\star e'\in H\subset G\\
&= e'\star e\in G \qquad \text{par régularité } e'=e.
\end{aligned}$$

◊ Soit $x\in H$, notons $x'\in H$ est le symétrique de x pour la structure de groupe H et $x^{-1}\in G$ le symétrique de x dans le groupe G. La démonstration précédente a prouvé que l'élément neutre est le même

dans G et dans H :

$$\begin{aligned}
e &= x\star x' \ \in H\subset G\\
&= x\star x^{-1}\in G \qquad \text{par régularité } x'=x^{-1}\in H
\end{aligned}$$

Propriétés caractéristiques des sous-groupes

■ Les trois propositions suivantes sont équivalentes :

$$\begin{aligned}
&H \text{ est un sous-groupe de } (G,\star)\\
\iff\quad & H\subset G \ \mathsf{ET}\ e\in H\\
& \mathsf{ET}\ H \text{ est stable par produit } \mathsf{ET}\ H \text{ est stable par inverse}\\
\iff & H\subset G \ \mathsf{ET}\ H\neq\emptyset \ \mathsf{ET}\ \big(\forall\,(x,y)\in H^2 \quad x\star y^{-1}\in H\big)
\end{aligned}$$

∗ Autrement dit un sous-groupe de $(G,\star)$ est un sous-ensemble non vide de G stable par produit et par calcul du symétrique.

◊ La démonstration opère par implications circulaires.

◊ Si H est un sous-groupe de $(G,\star)$ alors la définition des sous-groupes énonce que $H\subset G$ et que H est stable par produit, et la propriété du paragraphe précédente affirme que $e\in H$ et que H est stable par inverse.

◊ La deuxième proposition entraîne la troisième car $e\in H$ implique $H\neq\emptyset$, et la combinaison de la stabilité par produit et inverse énonce la stabilité par la dernière opération :

$$\begin{aligned}
\forall\,(x,y)\in H^2 \qquad & y^{-1}\in H \quad \text{stabilité par inverse}\\
\text{puis} \quad & x\star y^{-1}\in H \quad \text{stabilité par produit.}
\end{aligned}$$

◊ Il reste à démontrer que la troisième proposition suffit pour que H soit un sous-groupe.
Si $H\neq\emptyset$ alors H contient un élément u et donc $x=y=u\in H$ vérifie $x\star y^{-1}=u\star u^{-1}=e\in H$ L'élément neutre de G est dans H :

$$e\in H \qquad \forall\, v\in H \quad v\star e=e\star v=v\in H$$

Soit $u\in H$, donc $u^{-1}=x\star y^{-1}=e\star u^{-1}\in H$ pour $x=e$ et $y=u$; ainsi le sous-ensemble H est stable par inverse :

$$\forall\, v\in H \quad v^{-1}\in H \ \mathsf{ET}\ v\star v^{-1}=v^{-1}\star v=e\in H$$

Enfin si $(u,v)\in H^2$ alors $v^{-1}\in H$ car H est stable par inverse et $u\star v=x\star y=u\star(v^{-1})^{-1}$ pour $x=u$ et $y=v^{-1}$, donc H est stable par produit :

$$\forall\,(u,v)\in H^2 \quad u\star v\in H$$

Ainsi $\star_{/H^2}$ est une lci sur H, $e\in H$ et H est stable par inverse. Pour montrer que H est un groupe il reste à montrer que la restriction $\star_{/H^2}$ est une associative :

$$\forall\,(u,v,w)\in H^3 \quad (u\star v)\star w = u\star(v\star w)$$

Cette égalité est valable pour tout triplet (u,v,w) de G^3, et est donc vérifiée pour tout triplet de H^3 car $H\subset G$.
Le sous-ensemble H de G vérifie bien la définition des groupes pour la restriction de la loi $\star$.

$*$ Dans ces propositions les conditions $H\neq\emptyset$ et $e\in H$ sont équivalentes.
Si H est un sous-groupe alors il contient nécessairement e.
Réciproquement si $e\in H$ alors $H\neq\emptyset$.

$*$ La proposition la plus élémentaire à rédiger est souvent la deuxième, et la proposition dont la rédaction est la plus concise est la dernière.

Exemples et intersection de sous-groupes

▶ L'ensemble $n\mathbb{Z}$ des multiples de $n\in\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$.

▷ L'inclusion $n\mathbb{Z}\subset\mathbb{Z}$ est vérifiée pour tout $n\in\mathbb{Z}$.
L'ensemble $n\mathbb{Z}$ n'est pas vide car $0=n\times 0\in n\mathbb{Z}$.
Soient $(u,v)\in(n\mathbb{Z})^2$ alors il existe $(a,b)\in\mathbb{Z}^2$ tel que $u=na$ et $v=nv$. L'opération $\star$ du groupe est ici l'addition, et le symétrique correspond à l'opposé :

$$u-v=na-nb=n(a-b)\in n\mathbb{Z}$$

Donc $n\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$.

▶ L'ensemble $\mathbb{U}_n$ des $n\in\mathbb{N}^*$ racines complexes de l'unité a une structure de groupe multiplicatif : $\mathbb{U}_n$ est un sous-groupe de $(\mathbb{C}^*,\times)$.

▷ Les racines complexes de l'unité sont de module un, donc non nulles et $\mathbb{U}_n\subset\mathbb{C}^*$.
Le nombre 1 est racine n-ème de 1, ainsi $1\in\mathbb{U}_n$ et $\mathbb{U}_n\neq\emptyset$.
Soit $(\omega,\zeta)\in\mathbb{U}_n^2$, donc $\omega^n=\zeta^n=1$ et $\omega/\zeta\in\mathbb{U}_n$ pour la raison suivante :

$$(\omega\zeta^{-1})^n=(\omega\overline{\zeta})^n=\omega^n\overline{\zeta^n}=1$$

En conclusion $\mathbb{U}_n$ est un sous-groupe multiplicatif de $\mathbb{C}^*$.

★ Le sous-ensemble $\{e_G\}$ de G est un sous-groupe de $(G,\star)$ car il vérifie la propriété caractéristique :

$$x\star y^{-1}=e_G\star e_G^{-1}=e_G\in\{e_G\}$$

$*$ Le sous-ensemble $G\subset G$ est un sous-groupe du groupe $(G,\star)$.

$*$ L'ensemble vide n'est pas un sous-groupe de G, car il ne contient par l'élément neutre.

■ L'intersection de sous-groupes d'un même groupe est un sous-groupe.

◊ Suposons que H et K soient des sous-groupes d'un groupe $(G,\star)$ d'élément neutre $e\in G$.
Démontrons que $H\cap G$ est un sous-groupe en vérifiant la propriété caractéristique des sous-groupes.
Les sous-ensembles H et K sont des sous-groupes, d'où ces inclusions :

$$H\cap K\subset H\subset G$$

Ces sous-groupes contiennent l'élément neutre e :

$$e\in H \qquad e\in K \qquad e\in H\cap K \qquad H\cap K\neq\emptyset$$

Ces implications terminent la démonstration que $H\cap K$ est un sous-groupe. Soit $(a,b)\in(H\cap K)^2$:

$$\left.\begin{array}{ll}(a,b)\in H^2 & a\star b^{-1}\in H\\ (a,b)\in K^2 & a\star b^{-1}\in K\end{array}\right\}\Longrightarrow a\star b^{-1}\in H\cap K$$

Les anneaux

Dans ce paragraphe $\mathbb{A}$ est un ensemble muni des lois de composition internes $\star$ et $\perp$, et $(x,y,z)\in\mathbb{A}^3$.

Definition et premières propriété des anneaux

• La structure $(\mathbb{A},\perp,\star)$ est un anneau si et seulement si les lois de composition internes $\perp$ et $\star$ vérifient ces propriétés :

$(\mathbb{A}, \perp)$ est un groupe commutatif d'élément neutre noté $0_\mathbb{A}$.

ET $\star$ est associative

ET $\star$ est distributive par rapport à $\perp$

ET $\star$ possède un élément neutre $1_\mathbb{A} \neq 0_\mathbb{A}$ autre que $0_\mathbb{A}$

L'anneau $\mathbb{A}$ est dit commutatif lorsque la loi $\star$ est commutative.

$*$ Ces structures sont des anneaux commutatifs :

$$(\mathbb{Z}, +, \times) \qquad (\mathbb{Q}, +, \times) \qquad (\mathbb{R}, +, \times) \qquad (\mathbb{C}, +, \times)$$

La structure d'anneau traduit les propriétés de l'addition et de la multiplication des nombres, dans la suite les lois $\perp$ et $\star$ sont notées $+$ et $\times$; les notations employées appliquent les règles algébriques usuelles de priorité de la multiplication sur l'addition et de l'omition éventuelle du signe produit $\times$.

$\circ$ L'élément neutre pour la loi $+$ est appelé élément nul et noté $0_\mathbb{A}$. Le symétrique de x pour la loi $+$ est noté $-x$ et appelé opposé de x. L'élément neutre pour la loi $\times$ d'un anneau est appelé élément unité et est noté $1_\mathbb{A} \neq 0_\mathbb{A}$.
L'éventuel symétrique de x pour la loi $\times$ est noté x^{-1} et appelé inverse.

$*$ Un anneau $(\mathbb{A}, +, \times)$ est en particulier un groupe additif et possède les propriétés des groupes commutatifs :

$$-0_\mathbb{A} = 0_\mathbb{A}$$
$$-(x+y) = (-y) + (-x) = (-x) + (-y) \text{ aussi noté } -x-y$$

$\square$ Dans tout anneau $\mathbb{A}$, l'élément neutre $0_\mathbb{A}$ est absorbant pour la loi $\times$ et la règle des signes énonce ces égalités :

$$x \times 0_\mathbb{A} = 0_\mathbb{A} \times x = 0_\mathbb{A}$$
$$-(x \times y) = (-x) \times y = x \times (-y) \qquad -x = (-1_\mathbb{A}) \times x$$

$\diamond$ La démonstration de la règle des signes dans l'anneau $\mathbb{A}$ est identique à celle effectuée dans les ensembles de nombres :

$$(xy) + (\underline{-(xy)}) = 0_\mathbb{A} = 0_\mathbb{A} \times y = (x + (-x))y = (xy) + (\underline{(-x)y})$$
$$(xy) + (\underline{-(xy)}) = 0_\mathbb{A} = x \times 0_\mathbb{A} = x(y + (-y)) = (xy) + (\underline{x(-y)})$$
$$-(x \times y) = (-x) \times y = x \times (-y)$$

La dernière égalité est un cas particulier de facteur $-1_\mathbb{A}$:

$$-x = -(1_\mathbb{A}) \times x$$

Produit par un entier et puissance

$\circ$ Le produit $m \cdot x$ est défini ainsi pour $m \in \mathbb{Z}$:

$$m \cdot x = \begin{cases} x + x + \cdots + x & m \text{ fois lorsque } m > 0 \\ -(x + x + \cdots + x) = (-m) \cdot (-x) & -m \text{ fois si } m < 0 \\ 0 \cdot x = 0_\mathbb{A} & \text{si } m = 0 \end{cases}$$

$\diamond$ Cette définition doit justifier l'égalité $(-m) \cdot (-x) = -(-m) \cdot x$ lorsque $m < 0$ pour être cohérente.
Cette preuve se fait par récurrence sur $p = -m \in \mathbb{N}$. Ces égalités traduisent la condition initiale de la récurrence :

$$0 \cdot (-x) = 0_\mathbb{A} = -(0 \cdot x)$$
$$1 \cdot (-x) = -x = -(1 \cdot x)$$

la deuxième égalité démontre l'implication de récurrence à partir de l'hypothèse de récurrence à l'ordre $p \in \mathbb{N}$:

$$\begin{aligned} & p \cdot (-x) = -(p \cdot x) \\ & (p+1) \cdot (-x) \\ =& p \cdot (-x) + (-x) && \text{par définition de l'opération } \cdot \\ =& -(p \cdot x) + (-x) && \text{à partir de l'hypothèse de récurrence} \\ =& -(p \cdot x + x) && \text{à partir de } -(u+v) = -u - v \\ =& -((p+1) \cdot x) && \text{par définition de l'opération } \cdot \end{aligned}$$

$\square$ Le produit par un entier vérifie ces propriétés du fait de l'associativité et de la commutativité de la loi $+$ lorsque $(m, n) \in \mathbb{Z}^2$:

$$m \cdot x + n \cdot x = (m+n) \cdot x \quad m \cdot (n \cdot x) = (mn) \cdot x \quad m \cdot 0_\mathbb{A} = 0_\mathbb{A}$$
$$m \cdot x + m \cdot y = m \cdot (x+y) \quad m \cdot (x \times y) = (m \cdot x) \times y = x \times (m \cdot y)$$
$$-(m \cdot x) = (-m) \cdot x = m \cdot (-x) \quad 1 \cdot x = x \quad -x = -1 \cdot x$$

$\diamond$ Ces manipulations de sommes illustrent ces propriétés à partir de l'associativité, de la commutativité ou de la distributivité, par exemple :

par associativité : $m\cdot x+n\cdot x=\sum_{k=1}^{m}x+\sum_{k=1}^{n}x$
$=\sum_{k=1}^{m+n}x=(m+n)\cdot x$

par commutativité : $m\cdot x+m\cdot y=\sum_{k=1}^{m}x+\sum_{k=1}^{m}y$
$=\sum_{k=1}^{m}(x+y)=m\cdot(x+y)$

par distributivité : $x\times(m\cdot y)=x\times\Big(\sum_{k=1}^{m}y\Big)$
$=\sum_{k=1}^{m}(x\times y)=m\cdot(x\times y)$

Ces égalités se limitent au cas des coefficients $(m,n)\in\mathbb{N}^2$ positifs et admettent implicitement les manipulations précédentes des sommes finies.

◊ Une démonstration complète doit distinguer les cas $m\geq 0$ et $m\leq 0$, et opérer par récurrence sur m ou n pour appliquer la définition *stricto sensu* de l'associativité, la commutativité ou la distributivité.
À titre d'exemple les égalités ci-dessous correspondent à l'initialisation de la récurrence démontrant $x\times(m\cdot y)=m\cdot(x\times y)$:

$$x\times(0\cdot y)=x\times 0_{\mathbb{A}}=0_{\mathbb{A}}=0\cdot(x\times y)$$
$$x\times(1\cdot y)=x\times y=1\cdot(x\times y)$$

L'égalité suivante démontre la relation à l'ordre $m+1$ à partir de l'hypothèse de récurrence à l'ordre $m\in\mathbb{N}$:

$x\times(m\cdot y)=m\cdot(x\times y)$
$x\times((m+1)\cdot y)$
$=x\times(m\cdot y+y)$ par définition de l'opération $\cdot$
$=x\times(m\cdot y)+(x\times y)$ par distributivité
$=m\cdot(x\times y)+(x\times y)$ par hypothèse de récurrence
$=(m+1)\cdot(x\times y)$ par définition de l'opération $\cdot$

La fin de la démonstration pour $m<0$ repose de même sur la définition de l'opération $\cdot$ et la règle des signes, en posant $p=-m\in\mathbb{N}$:

$x\times(m\cdot y)=x\times(-(p\cdot y))$ par définition de l'opération $\cdot$
$=-(x\times(p\cdot y))$ par la règle des signes
$=-(p\cdot(x\times y))$ à partir du cas $p\geq 0$ précédent
$=m\cdot(x\times y)$ par définition de l'opération $\cdot$

∗ Les produits « $\times$ » et « $\cdot$ » ne sont pas interchangeables ; le produit de $\mathbb{A}$ est une lci alors que le produit par un entier n'en est pas une :

$$\times:\mathbb{A}\times\mathbb{A}\to\mathbb{A}\qquad\cdot:\mathbb{Z}\times\mathbb{A}\to\mathbb{A}$$

∗ De même $0\in\mathbb{Z}$ et $0_{\mathbb{A}}\in\mathbb{A}$, et $1\in\mathbb{Z}$ et $1_{\mathbb{A}}\in\mathbb{Z}$ ne sont pas égaux, sauf dans l'anneau $\mathbb{Z}$. Ces éléments sont reliés par les égalités suivantes :

$$m\cdot 0_{\mathbb{A}}=0_{\mathbb{Z}}\cdot x=0_{\mathbb{A}}\times x=x\times 0_{\mathbb{A}}=0_{\mathbb{A}}$$
$$1_{\mathbb{Z}}\cdot x=1_{\mathbb{A}}\times x=1_{\mathbb{A}}\times x=x$$

∗ Le formulaire précédent justifie les notations classiques de ces produits, par exemple :

$$mxy=m\cdot(x\times y)=(m\cdot x)\times y=x\times(m\cdot y)$$

∘ La puissance x^m où $m\in\mathbb{N}$ est définie ainsi :

$$x^m=\begin{cases}x\times x\times\cdots\times x & n\text{ fois lorsque }n>0\\ x^0=1_{\mathbb{A}}\end{cases}$$

□ Les propriétés de la puissances sont bien connues :
$x^m\times x^n=x^{m+n}\quad 1_{\mathbb{A}}^m=1_{\mathbb{A}}\quad(x^m)^n=x^{mn}\quad$ quand $(m,n)\in\mathbb{N}^2$

◊ Les méthodes de démonstrations sont similaires à celles appliquées pour les produits par des entiers.

∗ Ces égalités illustrent les deux définitions précédentes :

$$(-x)^n=(-1_{\mathbb{A}}\times x)^n=(-1_{\mathbb{A}})^n\times x^n$$
$$=(-1_{\mathbb{Z}}\cdot x)^n=(-1_{\mathbb{Z}})^n\cdot x^n$$

Anneau intègre

▶ Un anneau commutatif $(\mathbb{A},+,\times)$ est dit intègre si et seulement s'il vérifie ces deux propositions équivalentes :

$$\Big(\forall\,(a,b)\in\mathbb{A}^2\quad a\times b=0\Longrightarrow a=0\ \mathsf{OU}\ b=0\Big)$$
$$\Longleftrightarrow\Big(\forall\,(u,v)\in\mathbb{A}^2\quad\forall\,w\in\mathbb{A}\setminus\{0_{\mathbb{A}}\}\quad u\times w=v\times w\Longrightarrow u=v\Big)$$

⋗ Si un anneau $\mathbb{A}$ vérifie la première proposition alors, par distributivité, l'égalité $uw = vw$ entraîne $uw - vw = 0 = (u - v)w$. La condition $w \neq 0$ et l'hypothèse initiale justifient $u - v = 0$ puis $u = v$.

⋗ Réciproquement supposons qu'un anneau $\mathbb{A}$ vérifie la seconde proposition et montrons la première implication.
Si $ab = 0$ alors deux cas sont possibles $a = 0$ ou $a \neq 0$. Dans le premier cas la démonstration est terminée, et dans le cas $a \neq 0$ l'hypothèse précédente appliquée à $a \times b = 0 = a \times 0$ et à $a \neq 0$ justifie que $b = 0$.

∗ Les anneaux comme $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont intègres.

Produits remarquables

Remarques sur les produits

∗ Dans un anneau quelconque $(x \times y)^2$ et $x^2 \times y^2$ ne sont généralement pas égaux car la multiplication n'est pas nécessairement commutative :

$$\begin{aligned}(x \times y)^2 &= x \times y \times x \times y\\ x^2 \times y^2 &= x \times x \times y \times y\\ (x+y)^2 &= x^2 + x \times y + y \times x + y^2\\ (x+y)(x-y) &= x^2 - x \times y + y \times x - y^2\end{aligned}$$

⊠ L'hypothèse $x \times y = y \times x$ aboutit à ces égalités :

$$x^m \times y = y \times x^m \qquad x^m \times y^n = y^n \times x^m$$
$$(x^m y^n) \times (x^p y^q) = x^{m+p} y^{n+q}$$

◊ La première égalité peut se démontrer par récurrence en appliquant m fois la commutativité du produit $xy = yx$:

$$\begin{aligned}x^m \times y &= x \times x \times \cdots \times x \times x \times y\\ &= x \times x \times \cdots \times x \times y \times x\\ &= x \times x \times \cdots \times y \times x \times x\\ &\quad \cdots \qquad \cdots \qquad \cdots\\ &= x \times y \times \cdots \times x \times x \times x\\ &= y \times x \times \cdots \times x \times x \times x = y \times x^m\end{aligned}$$

En conclusion x^m et y commutent dès que $xy = yx$.

◊ La deuxième égalité provient de la précédente où n remplace m :

$$\begin{aligned}x \times y = y \times x &\Longrightarrow x^m \times y = y \times x^m\\ &\Longrightarrow X \times y = y \times X \qquad \text{où } X = x^m\\ &\Longrightarrow X \times y^n = y^n \times X\\ &\Longrightarrow x^m \times y^n = y^n \times x^m\end{aligned}$$

◊ La dernière égalité provient de la deuxième et de l'associativité du produit :

$$\begin{aligned}(x^m \times y^n) \times (x^p \times y^q) &= x^m \times (y^n \times x^p) \times y^q = x^m \times (x^p \times y^n) \times y^q\\ &= (x^m \times x^p) \times (y^n \times y^q) = x^{m+p} \times y^{n+q}\end{aligned}$$

∗ Ces produits remarquables sont des conséquences des produits précédents, où les signes de mutiplication $\times$ et $\cdot$ peuvent être omis comme dans les formules numériques :

$$(x+y)^2 = x^2 + 2xy + y^2 \quad (x+y)(x-y) = x^2 - y^2 \quad \text{si } xy = yx$$

Dans la suite $(\mathbb{A}, +, \times)$ est un anneau d'élément unité noté $1_{\mathbb{A}}$, par convention $x^0 = 1_{\mathbb{A}}$.
La suite de ce paragraphe suppose en plus que $x \times y = y \times x$, pour cela il suffit par exemple que l'anneau soit commutatif.

Binôme de Newton

■ Lorsque $xy = yx$ la formule du binôme énonce cette égalité dans n'importe quel anneau unitaire :

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \qquad \binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

◊ La vérification de la récurrence est immédiate pour $n = 0$, $n = 1$ et $n = 2$.

$$(x+y)^0 = 1 = \sum_{k=0}^{0} \binom{0}{k} x^k y^{-k} = 1 \times x^0 \times y^0$$

$$(x+y)^1 = x + y = \binom{1}{0} x^0 y^1 + \binom{1}{1} x^1 y^0$$

$$(x+y)^2 = x^2 + 2xy + y^2 = \sum_{k=0}^{2} \binom{2}{k} x^k y^{2-k}$$

La démonstration de la formule à l'ordre $n+1$ à partir de celle à l'ordre n termine la récurrence :

$$
\begin{aligned}
&(x+y)^{n+1} = (x+y)(x+y)^n = (x+y)\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}\\
&= \sum_{k=0}^{n}\binom{n}{k}x^{k+1}y^{n-k} + \sum_{k=0}^{n}\binom{n}{k}x^k y^{n+1-k} \qquad \text{par distributivité}\\
&= \sum_{j=1}^{n+1}\binom{n}{j-1}x^j y^{n+1-j} + \sum_{k=0}^{n}\binom{n}{k}x^k y^{n+1-k} \qquad \text{avec } j=k+1\\
&= \sum_{j=1}^{n}\binom{n}{j-1}x^j y^{n+1-j} + x^{n+1} + \sum_{j=1}^{n}\binom{n}{j}x^j y^{n+1-j} + y^{n+1}\\
&= y^{n+1} + \sum_{j=1}^{n}\left(\binom{n}{j-1} + \binom{n}{j}\right)x^j y^{n+1-j} + x^{n+1}\\
&= \binom{n+1}{0}x^0 y^{n+1} + \sum_{j=1}^{n}\binom{n+1}{j}x^j y^{n+1-j} + \binom{n+1}{n+1}x^{n+1}y^0\\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}x^k y^{n+1-k}
\end{aligned}
$$

∗ La formule du binôme précédente s'applique au calcul de $(x-y)^n$ et de $(1_{\mathbb{A}} \pm x)^n$ pour ces raisons :

$$x \times (-y) = -(xy) = -(yx) = (-y) \times x \qquad 1_{\mathbb{A}} \times x = x \times 1_{\mathbb{A}}$$

Séries géométriques

■ Lorsque $xy = yx$ un autre produit remarquable énonce cette égalité des séries géométriques dans n'importe quel anneau unitaire :

$$x^{n+1} - y^{n+1} = \Big(\sum_{k=0}^{n} x^k y^{n-k}\Big)(x-y) = (x-y)\Big(\sum_{k=0}^{n} x^k y^{n-k}\Big)$$

◊ Ces égalités prouvent directement ce produit remarquable :

$$
\begin{aligned}
&(x-y)\Big(\sum_{k=0}^{n} x^k y^{n-k}\Big)\\
&= x\sum_{k=0}^{n} x^k y^{n-k} + y\sum_{k=0}^{n} x^k y^{n-k}\\
&\qquad \text{par distributivité du produit par } x-y\\
&= \sum_{k=0}^{n} x x^k y^{n-k} + \sum_{k=0}^{n} y x^k y^{n-k}\\
&\qquad \text{par distributivité sur les sommes}\\
&= \sum_{k=0}^{n} x^{k+1} y^{n-k} + \sum_{k=0}^{n} x^k y^{n+1-k}\\
&\qquad \text{à partir des puissances lorsque } xy = yx\\
&= \sum_{j=1}^{n+1} x^j y^{n+1-j} + \sum_{k=0}^{n} x^k y^{n+1-k}\\
&\qquad \text{par changement d'indice } j = k+1\\
&= x^{n+1} - y^{n+1} \quad \text{par simplification des deux sommes.}
\end{aligned}
$$

La démonstration de l'autre égalité est comparable.

∗ Les factorisations suivantes découlent de la formule précédente :

$$1_{\mathbb{A}} - x^{n+1} = 1_{\mathbb{A}}^{n+1} - x^{n+1} \qquad x^{2n+1} + y^{2n+1} = x^{2n+1} - (-y)^{2n+1}$$

Le groupe des éléments inversibles

Dans la suite $(\mathbb{A}, +, \times)$ *est un anneau unitaire d'élément unité noté* $1_{\mathbb{A}}$*, par convention* $x^0 = 1_{\mathbb{A}}$.

∘ Un élément x de $\mathbb{A}$ est inversible si et seulement si il existe $y \in \mathbb{A}$ tel que $xy = yx = 1_{\mathbb{A}}$. L'associativité de la multiplication montre que y est unique et est notée $y = x^{-1}$.

□ L'ensemble des éléments inversibles de $\mathbb{A}$ qui est noté $\mathbb{U}(\mathbb{A})$ vérifie ces propriétés lorsque $(x, y) \in (\mathbb{U}(\mathbb{A}))^2$:

$$
\begin{array}{lll}
1_{\mathbb{A}} \in \mathbb{U}(\mathbb{A}) & \text{et} & 1_{\mathbb{A}}^{-1} = 1_{\mathbb{A}}\\
x^{-1} \in \mathbb{U}(\mathbb{A}) & & (x^{-1})^{-1} = x\\
(xy)^{-1} \in \mathbb{U}(\mathbb{A}) & & (xy)^{-1} = y^{-1}x^{-1}
\end{array}
$$

◊ Ces produits justifient les égalités précédentes :

$$1_{\mathbb{A}} \times 1_{\mathbb{A}} = 1_{\mathbb{A}} \qquad x^{-1} \times x = x \times x^{-1} = 1_{\mathbb{A}}$$
$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xx^{-1} = 1_{\mathbb{A}}$$
$$(y^{-1}x^{-1})(xy) = y(xx^{-1})y^{-1} = yy^{-1} = 1_{\mathbb{A}}$$

▫ Lorsque x est un élément inversible de $\mathbb{A}$ la notation x^n et ses propriétés s'étendent aux entiers n négatifs :
$$x^n = x^{-1} \times x^{-1} \times \cdots \times x^{-1} = (x^{-n})^{-1}$$

◊ L'inverse d'un produit xy de deux éléments inversibles justifie l'égalité $(x^2)^{-1} = (x^{-1})^2$ lorsque $x = y$. Une récurrence généralise l'égalité.
L'extension du formulaire des puissances s'effectue directement.

▫ $(\mathbb{U}(\mathbb{A}), \times)$ est un groupe appelé groupe des éléments inversibles. de $\mathbb{A}$.

◊ La propriété précédente justifie que $\mathbb{U}(\mathbb{A})$ est stable par produit.
La loi $\times$ est associative sur $\mathbb{A}$, elle est donc associative sur le sous-ensemble $\mathbb{U}(\mathbb{A}) \subset \mathbb{A}$.
L'élément unité $1_{\mathbb{A}} \in \mathbb{U}(\mathbb{A})$ est l'élément neutre pour le produit.
La propriété précédente justifie également que tout élément $x \in \mathbb{U}(\mathbb{A})$ possède un inverse qui appartient à $\mathbb{U}(\mathbb{A})$.
En conclusion $(\mathbb{U}(\mathbb{A}), \times)$ est un groupe multiplicatif.

∗ Par exemple $\mathbb{U}(\mathbb{Z}) = \{-1, 1\}$ dans l'anneau $\mathbb{Z}$, et $\mathbb{U}(\mathbb{Q}) = \mathbb{Q}^*$.

Les corps

• La structure $(\mathbb{K}, +, \times)$ est un corps si et seulement si $(\mathbb{K}, +, \times)$ est un anneau commutatif dont tous les éléments non nuls sont inversibles ; l'ensemble des éléments inversibles d'un corps est généralement noté $\mathbb{K}^*$ à la place de $\mathbb{U}(\mathbb{K})$:
$$\mathbb{K}^* = \mathbb{U}(\mathbb{K}) = \mathbb{K} \setminus \{0_{\mathbb{K}}\}$$

★ Les ensembles suivants sont des corps :
$$(\mathbb{Q}, +, \times) \qquad (\mathbb{R}, +, \times) \qquad (\mathbb{C}, +, \times)$$