Loi de composition interne et introduction à la notion de groupe

La théorie des groupes trouve son application dans plusieurs domaines : la cristallographie en chimie, la physique des particules, la géométrie différentielle et la théorie de la relativité, la physique quantique, la cryptographie, le pavage du plan,…
Lors de son étude des équations algébriques, Evariste GALOIS utilise plusieurs propriétés liées à la théorie des groupes.

I. Loi de composition interne

• Produit cartésien d'un ensemble par lui même

Définition. Soit E un ensemble non vide.
Le produit cartésien de E par E est l'ensemble $E\times E$ des couples (x,y) tels que $x\in E$ et $y\in E$
C'est-à-dire $E\times E=\{(x,y)/\,x\in E, y\in E\}$
Donc $u\in E\times E$ signifie qu'il existe $x\in E$ et il existe $y\in E$ tel que $u=(x,y)$

Notation : Si E est un ensemble non vide. On note $E^2=E\times E$

Exemples
1) $\mathbf{R}^2=\mathbf{R}\times\mathbf{R}=\{(x,y)/\,x\in\mathbf{R}, y\in\mathbf{R}\}$

2) Si $E=\{a\}$ alors $E^2=E\times E=\{(a,a)\}$

3) Si $E=\{0,1\}$ alors $E^2=E\times E=\{(0,0);(0,1);(1,0);(1,1)\}$

• Loi de composition interne

Définition. Soit E un ensemble non vide.
Une loi de composition interne sur E est une **application** φ de $E\times E$ dans E.
C'est-à-dire pour chaque $(x,y)\in E^2$ on associe un unique élément z de E, noté $\varphi(x,y)$

Notation. Soit φ est une loi de composition interne sur E, c'est-à-dire
$\varphi: E\times E\to E$ est une application
$(x,y)\mapsto\varphi(x,y)$
Pour $(x,y)\in E^2$, $\varphi(x,y)$ représente le résultat de l'opération φ de x par y,
Il est noté à l'aide d'un symbole ($*$ ou $\perp$ ou $\Diamond$,…), exemple $\varphi(x,y)=x*y$

Exemples
1) L'addition « $+$ » et la multiplication « $\times$ » usuelles sont deux lois de composition interne sur $\mathbf{R}$:
$+:\mathbf{R}\times\mathbf{R}\to\mathbf{R}$; $\times:\mathbf{R}\times\mathbf{R}\to\mathbf{R}$
$(x,y)\mapsto x+y$; $(x,y)\mapsto x\times y$

2) La différence usuelle « $-$ » est une loi de composition interne sur $\mathbf{R}$ et $\mathbf{Z}$, mais elle n'est pas une loi de composition interne sur $\mathbf{N}$ car $(0,1)\in\mathbf{N}^2$, $0-1=-1$ et $-1\notin\mathbf{N}$

3) L'addition usuelle n'est pas une loi de composition interne sur l'ensemble $B=\{0,1\}$ car $(1,1)\in B^2$, $1+1=2$ et $2\notin B$

4) Soit $B=\{0,1\}$ on a $B^2=B\times B=\{(0,0);(0,1);(1,0);(1,1)\}$.
Sur B on définit l'opération $\oplus$ par :
$0\oplus 0=0$; $0\oplus 1=1$; $1\oplus 0=1$ et $1\oplus 1=0$
Alors l'opération $\oplus$ est une loi de composition interne sur B.
On peut alors identifier $(B,\oplus)$ à $(Z/2Z,+)$

5) Si $E=P(B)$ désigne l'ensemble des parties de $B=\{0,1\}$, alors $P(B)$ a pour éléments:
Ø ; $\{0\}$; $\{1\}$ et $\{0,1\}$.
L'intersection et l'union des ensembles sont deux lois de composition internes sur $P(B)$:

$$\cap: P(B)\times P(B)\to P(B) \quad ; \quad \cup: P(B)\times P(B)\to P(B)$$
$$(A,A')\mapsto A\cap A' \qquad\qquad (A,A')\mapsto A\cup A'$$

Exercice
La multiplication est-elle une loi de composition interne sur $[0,+\infty[$? sur $]-\infty,0]$?

II. Commutativité et Associativité

Préliminaires.
Soient $*$ une loi de composition interne sur E, $a\in E$, $b\in E$ et $c\in E$
Questions :

i) A-t-on $a*b=b*a$?
ii) A-t-on $(a*b)*c=a*(b*c)$?
iii) Comment calculer $a*b*c$?

Les propriétés i) et ii) sont fausses en général :
En effet sur $\mathbf{R}$, considérons la loi « $-$ » (différence usuelle) : $a-b$
pour $a=b=1$ et $c=2$ on a : $a*c\neq c*a$ et $(a*b)*c\neq a*(b*c)$
car $(1-2)\neq(2-1)$ et $[(1-1)-2]\neq[1-(1-2)]$

• Commutativité

Définition. (commutativité)
Soit $*$ une loi de composition interne sur E
On dit que la loi $*$ est commutative sur E si et seulement si pour tout $(a,b)\in E^2$ on a :
$a*b=b*a$

• Associativité

Définition. (associativité)
Soit $*$ une loi de composition interne sur E
On dit que la loi $*$ est associative sur E si et seulement si pour chaque $a\in E$, $b\in E$ et $c\in E$ on a : $(a*b)*c=a*(b*c)$

Notation. Lorsque la loi $*$ est associative sur E alors pour chaque $a\in E$, $b\in E$ et $c\in E$ l'expression $a*b*c$ est définie par : $a*b*c=(a*b)*c=a*(b*c)$

Exemples

1) Les lois « $+$ » et « $\times$ » sont commutatives et associatives sur les ensembles suivants : $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ et $\mathbf{Z}/nZ$

2) Considérons « $*$ », la loi de composition interne définie sur $\mathbf{R}$ par :
Pour tout $(x,y)\in\mathbf{R}^2$, $x*y=x+2y$.
Etudiez la commutativité et l'associativité de la loi « $*$ ».
On a $0*1=0+2\times1=2$ et $1*0=1+2\times0=1$ d'où $0*1\neq1*0$ donc la loi $*$ n'est pas commutative sur $\mathbf{R}$.
Soient $a\in\mathbf{R}$, $b\in\mathbf{R}$ et $c\in\mathbf{R}$ on a :
$(a*b)*c=(a+2b)*c=a+2b+2c$ et $a*(b*c)=a*(b+2c)=a+2(b+2c)=a+2b+4c$
D'où pour $a=b=c=1$, on a $(1*1)*1\neq1*(1*1)$ par conséquent la loi $*$ n'est pas associative sur $\mathbf{R}$.

3) D'après le préliminaire, la loi « $-$ » n'est ni commutative, ni associative.

3) Soient E un ensemble non vide et deux applications $f:E\to E$ et $g:E\to E$.
On note $f\circ g$ l'application composée définie par, $f\circ g:E\to E$ et pour tout $x\in E$, $(f\circ g)(x)=f[g(x)]$

Exemple : Considérons les applications suivantes :
$f:\mathbf{R}\to\mathbf{R}$, $x\mapsto x+1$ et $g:\mathbf{R}\to\mathbf{R}$, $x\mapsto 2x$ alors $f\circ g:\mathbf{R}\to\mathbf{R}$, $x\mapsto 2x+1$ et $g\circ f:\mathbf{R}\to\mathbf{R}$, $x\mapsto 2(x+1)$
Car Pour tout $x\in\mathbf{R}$, $(f\circ g)(x)=f[g(x)]=f(2x)=2x+1$
Et $(g\circ f)(x)=g[f(x)]=g(x+1)=2(x+1)$

De plus on remarque que $(f\circ g)(0)\neq(g\circ f)(0)$ donc $(f\circ g)\neq(g\circ f)$

Notons $G(E)$ l'ensemble des applications $f:E\to E$.
La loi « $\circ$ », composée d'applications, est une loi de composition interne sur $G(E)$ qui **est toujours associative.**
En effet, soient $f:E\to E$, $g:E\to E$ et $h:E\to E$ trois applications et $x\in E$ on a :
$[h\circ(g\circ f)](x)=h[(g\circ f)(x)]=h[g(f(x))]$ et $[(h\circ g)\circ f](x)=(h\circ g)[f(x)]=h[g(f(x))]$
D'où $h\circ(g\circ f)=(h\circ g)\circ f$
La loi « $\circ$ » est donc associative sur $G(E)$.

Attention. La loi « $\circ$ » **n'est pas commutative sur $G(E)$ en général (cf. exemple ci-dessus).**

Dans l'ensemble des matrices carrées, la multiplication usuelle est toujours associative mais pas commutative en général

III. Elément neutre, élément symétrique

- **Elément neutre** (s'il existe).

Définition. (élément neutre)
Soit $*$ une loi de composition interne sur E
On dit que E admet un élément neutre pour la loi $*$, s'il existe $e\in E$ tel que : pour tout $x\in E$, on a : $x*e=x$ et $e*x=x$

Théorème. Soit $*$ une loi de composition interne sur E
Si E admet un élément neutre pour la loi $*$ alors celui-ci est unique.

Preuve.
Soient $e \in E$ et $e' \in E$ tels que :
pour tout $x \in E$, on a , (1) : $x * e = x$, (2) : $e * x = x$, (3) : $x * e' = x$ et (4) : $e' * x = x$
montrons que $e = e'$
d'après (1) on a $e' * e = e'$ car $e' \in E$ et d'après (4) on a $e' * e = e$ car $e \in E$
d'où on a $e' * e = e'$ et $e' * e = e$ par suite $e = e'$

Exemples
1) 0 est l'élément neutre de $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ et $\mathbf{C}$ pour la loi $+$
2) 1 est l'élément neutre de $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ et $\mathbf{C}$ pour la loi $\times$
3) $\mathbf{Z}$ muni de la loi « $-$ » n'admet pas d'élément neutre.
En effet supposons que $\mathbf{Z}$ admet un élément neutre e
pour la loi « $-$ »,
on a alors pour tout $x \in \mathbf{Z}$, (1) : $x - e = x$ et (2) : $e - x = x$.
D'où d'après (1) on a : $0 - e = 0$ car $0 \in \mathbf{Z}$ d'où $e = 0$
Et donc d'après (2) on a : $0 - 1 = 1$ car $1 \in \mathbf{Z}$ par suite $-1 = 1$ et ceci est impossible.

- **Elément symétrique** (s'il existe)

Définition. (élément symétrique)
Soit $*$ une loi de composition interne sur E. On suppose que E **admet un élément neutre** e **pour la loi** $*$**.**
Soit $x \in E$. On dit que x admet un symétrique dans E muni de la loi $*$, s'il existe $y \in E$ tel que $x * y = e$ et $y * x = e$

Théorème. Soit $*$ une loi de composition interne sur E. On suppose que E **admet un élément neutre** e **pour la loi** $*$ **et que la loi** $*$ **est associative,** alors on a :
Si un élément $x \in E$ admet un élément symétrique dans E muni la loi $*$, alors celui-ci est unique.

Preuve.
Soient $x \in E$, $y \in E$ et $y' \in E$ tels que,
(1) : $x * y = e$, (2) : $y * x = e$, (3) : $x * y' = e$ et (4) : $y' * x = e$ montrons que $y = y'$
D'après (1) on a $y' * (x * y) = y' * e = y'$ d'où $(y' * x) * y = y'$ car la loi $*$ est associative
et d'après (4) on a $(y' * x) * y = e * y = y$
par suite $(y' * x) * y = y' = y$ donc $y = y'$

Exemples
1) Dans $\mathbf{R}$ muni par la loi usuelle « $+$ », chaque $x \in \mathbf{R}$ admet pour symétrique le réel $-x$ car $x + (-x) = (-x) + x = 0$
2) Dans $\mathbf{N}$ muni par la loi usuelle « $+$ », 1 n'admet pas de symétrique car si $y \in \mathbf{N}$ est le symétrique de 1 alors $1 + y = 0$ d'où $y = -1$ mais $-1 \notin \mathbf{N}$
3) Dans $\mathbf{R}^*$ muni par la loi $\times$, chaque $x \in \mathbf{R}^*$ admet pour symétrique le réel $\frac{1}{x}$ car
$x \times (\frac{1}{x}) = (\frac{1}{x}) \times x = 1$

V. Groupe

Définition. Soit $*$ une **loi de composition interne** sur G
On dit que $(G,*)$ est un groupe si on a les propriétés suivantes :
1) La loi $*$ est associative

2) G admet un élément neutre pour la loi $*$, c'est-à-dire il existe $e \in G$ vérifiant pour tout $x \in G$, $x*e = x$ et $e*x = x$

3) Tout élément de G admet un symétrique pour la loi $*$ c'est-à-dire : pour chaque $x \in G$, il existe un $y \in G$ tel que $x*y = e$ et $y*x = e$,

Définition. Soit $(G,*)$ un groupe

Si la loi $*$ est commutative, on dit que $(G,*)$ est un groupe abélien ou groupe commutatif.

Exemples

1) $(\mathbf{Z},+)$, $(\mathbf{Q},+)$, $(\mathbf{R},+)$ et $(\mathbf{C},+)$ sont des groupes abéliens ayant 0 pour élément neutre.

2) $(\mathbf{Q}^*,\times)$, $(\mathbf{R}^*,\times)$ et $(\mathbf{C}^*,\times)$ sont des groupes abéliens ayant 1 pour élément neutre.

3) Si $(G,*)$ est un groupe d'élément neutre e alors $(\{e\},*)$ est un groupe.

D'où $(\{0\},+)$ et $(\{1\},\times)$ sont des groupes car $(\mathbf{R},+)$ et $(\mathbf{C}^*,\times)$ sont des groupes

4) Soit $U = \{z \in \mathbf{C}^* / \ |z| = 1\}$ où $|z|$ désigne le module du nombre complexe z .

Montrons que $(U,\times)$ est un groupe abélien

- Pour $(z,z') \in U^2$, on a : $|z \times z'| = |z| \times |z'| = 1 \times 1 = 1$ car $|z| = 1$ et $|z'| = 1$ de plus $(z,z') \in (\mathbf{C}^*)^2$ et $(z \times z') \in \mathbf{C}^*$ d'où $(z \times z') \in U$ par suite « $\times$ » est une loi de composition interne sur U .
- La loi « $\times$ » est associative sur U car elle est associative sur $\mathbf{C}^*$
- La loi « $\times$ » est commutative sur U car elle est commutative sur $\mathbf{C}^*$
- $1 \in U$ et pour tout $z \in U$ on a : $1 \times z = z \times 1 = z$ d'où 1 est l'élément neutre de U pour la loi « $\times$ »
- Pour $z \in U$, on a $z \in \mathbf{C}^*$ et $|z| = 1$ d'où $\left(\frac{1}{z}\right) \in \mathbf{C}^*$ et $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$ donc $\left(\frac{1}{z}\right) \in U$

De plus $z \times \left(\frac{1}{z}\right) = \left(\frac{1}{z}\right) \times z = 1$ donc $\left(\frac{1}{z}\right)$ est le symétrique de z pour la loi « $\times$ »

Conclusion. $(U,\times)$ est un groupe abélien

5) Pour $n \in \mathbf{N}^*$, on note S_n l'ensemble des bijections de $\{1,2,\ldots,n\}$ sur $\{1,2,\ldots,n\}$.

Un élément $\sigma \in S_n$ est donc une application de $\{1,2,\ldots,n\}$ sur $\{1,2,\ldots,n\}$ qui vérifie: pour chaque $y \in \{1,2,\ldots,n\}$, il existe un unique $x \in \{1,2,\ldots,n\}$ tel que $y = \sigma(x)$.

Un élément $\sigma \in S_n$ est souvent représenté par : $\sigma = \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(k) & \cdots & \sigma(n) \end{pmatrix}$

Par exemple l'application $\sigma \in S_3$ définie par $\sigma(1) = 1$; $\sigma(2) = 3$ et $\sigma(3) = 2$ est notée $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ et $id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ où $id \in S_3$ est définie par : pour tout $k \in \{1,2,3\}$, $\sigma(k) = k$

On montre que $(S_n,\circ)$ est un groupe d'élément neutre $id = \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n \\ 1 & 2 & \cdots & k & \cdots & n \end{pmatrix}$

où « $\circ$ » désigne la loi de compositions des fonctions

Exemples

1) Si $\sigma \in S_n$ et $\tau \in S_n$ alors $\sigma \circ \tau = \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n \\ (\sigma \circ \tau)(1) & (\sigma \circ \tau)(2) & \cdots & (\sigma \circ \tau)(k) & \cdots & (\sigma \circ \tau)(n) \end{pmatrix}$

Pour chaque $k \in \{1,2,\ldots,n\}$ on a : $(\sigma \circ \tau)(k) = \sigma(\tau(k))$

Donc pour définir $\sigma \circ \tau$ il faut d'abord appliquer τ puis σ : c'est-à-dire pour calculer $(\sigma \circ \tau)(k)$ il faut d'abord calculer $\tau(k)$ puis appliquer σ à $\tau(k)$

2) Soient $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ deux éléments de S_3 on a :

$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ et $\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ donc $\sigma \circ \tau \neq \tau \circ \sigma$

Proposition. (unicité de l'élément neutre et du symétrique d'un élément dans un groupe)
Si $(G,*)$ est un groupe alors

1) $(G,*)$ admet **un unique élément neutre**

2) Chaque élément de G admet **un unique symétrique** dans $(G,*)$

Preuve. D'après les propriétés démontrées ci-dessus

Notations (importantes)

1) Dans un groupe $(G,*)$, le symétrique d'un élément $x \in G$ est noté x^{-1}

2) Dans un groupe $(G,+)$, le symétrique d'un élément $x \in G$ est noté $-x$

Proposition. Soient $(G,*)$ un groupe

Si $(a,b) \in G^2$, alors $(a*b)^{-1} = b^{-1} * a^{-1}$

Preuve. Notons e l'élément neutre de $(G,*)$, on a :

$(a*b)*(b^{-1}*a^{-1}) = a*b*b^{-1}*a^{-1} = a*e*a^{-1} = a*a^{-1} = e$ (d'après l'associativité et la définition du symétrique d'un élément)

Idem $(b^{-1}*a^{-1})*(a*b) = b^{-1}*a^{-1}*a*b = b^{-1}*e*b = b^{-1}*b = e$

D'où $(a*b)^{-1} = (b^{-1}*a^{-1})$ d'après l'unicité de l'inverse d'un élément.