Structures algébriques

I Lois de composition interne

Définition. Soit E un ensemble. Une loi de composition interne sur E est une application $* : E \times E \longrightarrow E$.

Remarques.
1. Pour $(x, y) \in E \times E$, l'élément $*(x, y)$ de E sera noté $x * y$.
2. Dans ce cours nous utiliserons l'abréviation "l.c.i." pour "loi de composition interne".

Définition. Soit E un ensemble et $*$ une loi de composition interne sur E.

(i) On dit que $*$ est associative lorsque : $\forall (x, y, z) \in E^3$, $(x * y) * z = x * (y * z)$.

(ii) On dit que $*$ est commutative lorsque : $\forall (x, y) \in E^2$, $x * y = y * x$.

(iii) On dit d'un élément $e \in E$ qu'il est un élément neutre (ou un neutre) pour $*$ lorsque : $\forall x \in E$, $x*e = e*x = x$.

Remarque. Si $*$ est une l.c.i. associative sur E et $(x, y, z) \in E^3$ on notera $x * y * z$ l'élément $(x * y) * z = x * (y * z)$.

Proposition (Unicité du neutre)**.** Si E admet un élément neutre pour $*$ alors il est unique.

Démonstration. Supposons que E admet des neutres e, e' pour $*$ et montrons que $e = e'$.
Comme e est neutre alors $e' * e = e'$. Comme e' est neutre alors $e' * e = e$. D'où $e' = e$. □

Définition. Soit E un ensemble et $*$ une l.c.i. sur E admettant un neutre e. On dit d'un élément $x \in E$ qu'il est inversible lorsqu'il existe $x' \in E$ tel que $x * x' = x' * x = e$. On dit alors que x' est un inverse (ou un symétrique) de x pour la loi $*$.

Proposition (Unicité de l'inverse)**.** Soit E un ensemble et $*$ une loi de composition interne sur E. On suppose :

— $*$ associative

— $*$ admet un élément neutre e

Alors tout élément de E admet au plus un inverse.

Démonstration. Soit $x \in E$ admettant un inverse x', il s'agit de montrer que celui-ci est unique. Soit alors x'' un inverse de x, montrons que $x'' = x'$. On a :

$$\begin{cases} (x' * x) * x'' = e * x'' = x'' \\ x' * (x * x'') = x' * e = x' \end{cases}$$

Mais par associativité de $*$ on a aussi $(x' * x) * x'' = x' * (x * x'')$ d'où $x'' = x'$. □

Remarques.
1. Si $x \in E$ est inversible, on notera généralement x^{-1} son inverse pour $*$. Seule exception : lorsque $*$ est une loi d'addition notée $+$, le symétrique d'un élément x est appelé son opposé et est noté $-x$.
2. L'élément neutre est toujours inversible et $e^{-1} = e$ puisque $e * e = e$.
3. Soit E un ensemble muni d'une l.c.i. $*$ associative ayant un neutre e. Alors pour tout élément inversible x de E on a :
$$(x^{-1})^{-1} = x$$
En effet, x est bien l'inverse de x^{-1} puisque $x^{-1} * x = x * x^{-1} = e$.

Définition. Soit E un ensemble et $*$, $\bullet$ deux lois de composition interne sur E. On dit que $*$ est distributive sur $\bullet$ lorsque :

$$\forall (x,y,z) \in E^3,\ \begin{cases} x*(y\bullet z) = (x*y)\bullet(x*z) \\ (y\bullet z)*x = (y*x)\bullet(z*x) \end{cases}$$

Exemples. 1. Les l.c.i. $+$ et $\times$ sont associatives et commutatives sur $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$ et $\mathbb{C}$. Elles admettent également des neutres (respectivement 0 et 1). La loi $\times$ est distributive sur la loi $+$ car on a toujours :

$$\begin{cases} x\times(y+z) = (x\times y)+(x\times z) \\ (y+z)\times x = (y\times x)+(z\times x) \end{cases}$$

2. Soit E un ensemble. On dispose des l.c.i. suivantes sur $\mathcal{P}(E)$:

$$\cap : \begin{array}{ccc} \mathcal{P}(E)\times\mathcal{P}(E) & \longrightarrow & \mathcal{P}(E) \\ (A,B) & \longmapsto & A\cap B \end{array},\quad \cup : \begin{array}{ccc} \mathcal{P}(E)\times\mathcal{P}(E) & \longrightarrow & \mathcal{P}(E) \\ (A,B) & \longmapsto & A\cup B \end{array},\quad \Delta : \begin{array}{ccc} \mathcal{P}(E)\times\mathcal{P}(E) & \longrightarrow & \mathcal{P}(E) \\ (A,B) & \longmapsto & A\Delta B \end{array}$$

Toutes ces l.c.i. sont commutatives, associatives et admettent un neutre (respectivement E, $\varnothing$, $\varnothing$). Les lois $\cap$ et $\cup$ admettent toutes deux leur neutre pour seul élément inversible. Tout élément $A\in\mathcal{P}(E)$ est inversible pour Δ d'inverse lui-même. Les lois $\cup$ et Δ se distribuent sur $\cap$.

3. Soit E un ensemble. La loi $\circ$ de composition des applications est une l.c.i. associative sur E^E. Elle admet un élément neutre Id_E et les éléments de E^E inversibles pour $\circ$ sont les applications bijectives de E vers E.
4. Soit E, F des ensembles. Si F est muni d'une l.c.i. $*$, alors pour toutes fonctions $f,g : E\longrightarrow F$ on note $f*g$ la fonction définie par :

$$\forall x\in E,\ (f*g)(x) = f(x)*g(x)$$

Cela définit naturellement une l.c.i. $(f,g)\longmapsto f*g$ sur F^E, que l'on note toujours $*$ mais qu'il conviendra de distinguer de $*$: $\begin{array}{ccc} F\times F & \longrightarrow & F \\ (x,y) & \longmapsto & x*y \end{array}$ qui est une l.c.i. sur F. Bien qu'elles soient notées de la même façon, c'est le contexte qui permet de savoir si l'on parle de $*$ en tant que l.c.i. sur F ou sur F^E. Les propriétés de $*$ en tant que l.c.i. sur F se transmettent à $*$ en tant que l.c.i. sur F^E (commutativité, associativité, existence d'un neutre). De même, si $*$ est distributive sur une autre l.c.i. $\bullet$ sur F, alors les l.c.i. induites sur F^E conservent cette propriété.

Définition. Soit E un ensemble, $*$ une l.c.i. sur E et $F\subset E$. On dit que F est stable par $*$ lorsque :

$$\forall (x,y)\in F^2,\ x*y\in F$$

Remarque. Si F est une partie de E stable par $*$ alors $*$ définit naturellement une l.c.i. $(x,y)\longmapsto x*y$ sur F, que l'on note encore $*$. Comme toujours, c'est le contexte qui permet de déterminer si l'on parle de $*$ en tant que l.c.i. sur E ou sur F.

Exemples. 1. E et $\varnothing$ sont toujours des parties de E stables par $*$.

2. $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$ sont des parties de $\mathbb{C}$ stables par $\times$ et par $+$.
3. $\mathbb{U}_n$ et $\mathbb{U}$ sont des parties de $\mathbb{C}$ stables par $\times$ mais pas par $+$.
4. Dans $\mathcal{P}(E)$, les parties de la forme $\{A\}$ avec $A\in\mathcal{P}(E)$ sont toutes stables par $\cap$ et $\cup$. La seule d'entre elles qui est stable par Δ est $\{\varnothing\}$. De façon générale, les plus petites parties non vides stables par Δ sont les parties de la forme $\{A,\varnothing\}$ où $A\in\mathcal{P}(E)$.

II Structure de groupe

1 Groupes

Définition. Soit G un ensemble et $*$ une loi de composition interne sur G. On dit que $*$ est une loi de groupe sur G (ou que $(G,*)$ est un groupe) lorsque :

(i) $*$ est associative

(ii) $*$ admet un élément neutre

(iii) tout élément de G est inversible pour $*$.

Si de plus $*$ est commutative on dira que G est un groupe commutatif.

Exemples. 1. $(\mathbb{N},+)$ n'est pas un groupe car 1 n'admet pas de symétrique dans $\mathbb{N}$ ($-1 \notin \mathbb{N}$).

2. $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ sont des groupes.
3. $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$, $(\mathbb{C}^*,\times)$ sont des groupes.
4. $(\mathbb{N}^*,\times)$ et $(\mathbb{Z}^*,\times)$ ne sont pas des groupes car 2 n'y admet pas d'inverse.
5. $(\mathbb{Q},\times),(\mathbb{R},\times),(\mathbb{C},\times)$ ne sont pas des groupes car 0 n'y admet pas d'inverse.
6. $(\mathbb{U},\times)$ est un groupe (où $\mathbb{U}=\{z\in\mathbb{C}\,|\,|z|=1\}$).
7. $(\mathfrak{S}(E),\circ)$ est un groupe (où E est un ensemble non vide et $\mathfrak{S}(E)=\{f\in E^E\,|\,f \text{ bijective}\}$). Il est appelé le groupe des permutations de E.
8. $(\mathcal{P}(E),\Delta)$ est un groupe.

Remarques. 1. Lorsque la loi de composition de G est une multiplication, i.e. notée $\times$ (ou $\cdot$), on dit que $(G,\times)$ (ou $(G,\cdot)$) est un groupe multiplicatif. Dans un groupe multiplicatif, le symétrique d'un élément x est appelé "inverse de x" et est noté x^{-1}. On notera également $x^n=\underbrace{x\times\cdots\times x}_{n \text{ fois}}$ pour tout $x\in G$ et $n\in\mathbb{N}$ ainsi que $x^n=(x^{-1})^{-n}$ si $n\in\mathbb{Z}$ est négatif. Enfin, si x,y sont des éléments de G on note souvent xy au lieu de $x\times y$.

2. Lorsque la loi de composition de G est une addition, i.e. notée $+$, on dit que $(G,+)$ est un groupe additif. Dans un groupe additif, le symétrique d'un élément x est appelé "opposé de x" et est noté $-x$. On notera également $nx=\underbrace{x+\cdots+x}_{n \text{ fois}}$ pour tout $x\in G$ et $n\in\mathbb{N}$ ainsi que $nx=(-n)(-x)$ si $n\in\mathbb{Z}$ est négatif.
3. En notation additive on notera également $x-y$ l'élément $x+(-y)$.
4. Les groupes commutatifs sont parfois appelés groupes abéliens, en pratique quand ce sont des groupes additifs.

Proposition. Soit $(G,*)$ un groupe. Alors :

$$\forall (x,y)\in G^2,\ (x*y)^{-1}=y^{-1}*x^{-1}$$

Démonstration. Soit $(x,y)\in G^2$, on vérifie que $y^{-1}*x^{-1}$ est l'inverse de $x*y$. On a :

$$(x*y)*(y^{-1}*x^{-1})=x*y*y^{-1}*x^{-1}=x*e*x^{-1}=x*x^{-1}=e$$
$$(y^{-1}*x^{-1})*(x*y)=y^{-1}*x^{-1}*x*y=y^{-1}*e*y=y^{-1}*y=e$$

Ce qui prouve que $y^{-1}*x^{-1}$ est bien l'inverse de $x*y$. Autrement dit : $(x*y)^{-1}=y^{-1}*x^{-1}$. □

2 Sous-groupes

Définition. Soit $(G,*)$ un groupe et $H\subset G$. On dit que H est un sous-groupe de G lorsque :

(i) $H\neq\varnothing$

(ii) H est stable par $*$

(iii) H est stable par passage à l'inverse : $\forall x\in H,\ x^{-1}\in H$.

Remarques. 1. La condition $H\neq\varnothing$ peut se remplacer par $e\in H$.
En effet, si $e\in H$ alors H est non vide et réciproquement si H est non vide alors il existe $x\in H$ puis en utilisant la stabilité de H par $*$ et par passage à l'inverse $x*x^{-1}\in H$, i.e. $e\in H$.

2. Si H est un sous-groupe de $(G,*)$ alors $*$ induit une application $\tilde{*}$: $\begin{array}{ccc} H\times H & \longrightarrow & H \\ (x,y) & \longmapsto & x*y \end{array}$ qui fait de $(H,\tilde{*})$ un groupe. En pratique on dira abusivement que $(H,*)$ est un groupe.

Exemples. 1. Si $(G,*)$ est un groupe de neutre e, alors G et $\{e\}$ sont des sous-groupes de $(G,*)$. On les appelle les sous-groupes triviaux des $(G,*)$.
2. $(\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{Q},+)$ qui est un sous-groupe de $(\mathbb{R},+)$ qui est lui-même un sous-groupe de $(\mathbb{C},+)$.
3. Pour tout $n\in\mathbb{N}$, l'ensemble $n\mathbb{Z}=\{nk\,|\,k\in\mathbb{Z}\}$ des multiples de n est un sous-groupe de $(Z,+)$.
4. $(\mathbb{Q}^*,\times)$ est un sous-groupe de $(\mathbb{R}^*,\times)$ qui est un sous-groupe de $(\mathbb{C}^*,\times)$.
5. $(\mathbb{U}_n,\times)$ est un sous-groupe de $(\mathbb{U},\times)$ qui est un sous-groupe de $(\mathbb{C}^*,\times)$.
6. L'ensemble des fonctions affines non constantes sur $\mathbb{R}$ est un sous-groupe de $(\mathfrak{S}(\mathbb{R}),\circ)$ (idem si l'on remplace $\mathbb{R}$ par $\mathbb{C}$ ou $\mathbb{Q}$).

Proposition. Soit $(G,*)$ un groupe et $H\subset G$ non vide. Alors H est un sous-groupe de G si et seulement si :

$$\forall (x,y)\in H^2,\ x*y^{-1}\in H$$

Démonstration. Supposons d'abord que H est une sous-groupe de G. Soit $(x,y)\in H^2$. Comme H est stable par passage à l'inverse alors $y^{-1}\in H$ puis par stabilité de H par $*$ on obtient $x*y^{-1}\in H$.
Réciproquement, supposons que $\forall (x,y)\in H^2$, $x*y^{-1}\in H$. Comme $H\neq\varnothing$ il existe $x_0\in H$. Alors $x_0*x_0^{-1}\in H$ i.e. $e\in H$. On en déduit alors $\forall x\in H$, $x^{-1}=e*x^{-1}\in H$ ce qui prouve que H est stable par passage à l'inverse. On en déduit ensuite que si $(x,y)\in H^2$, comme $y^{-1}\in H$ alors d'après ce qu'on a supposé $x*(y^{-1})^{-1}\in H$ i.e. $x*y\in H$. Ce qui prouve que H est stable par $*$ et ainsi que H est un sous-groupe de G. □

Proposition. Soit $(G,*)$ un groupe et $(H_i)_{i\in I}$ une famille de sous-groupes de G. Alors $\bigcap\limits_{i\in I} H_i$ est un sous-groupe de G.

Démonstration. On utilise la proposition précédente.
(i) $e\in\bigcap\limits_{i\in I} H_i$ car $\forall i\in I$, $e\in H_i$.
(ii) Soit $(x,y)\in\big(\bigcap\limits_{i\in I} H_i\big)^2$. Alors pour tout $i\in I$ on a $x*y^{-1}\in H_i$ (car H_i sous-groupe de G), i.e. $x*y^{-1}\in\bigcap\limits_{i\in I} H_i$.
□

3 Sous-groupes engendrés par une partie

Définition. Soit $(G,*)$ un groupe et $A\subset G$. On appelle sous-groupe de G engendré par A l'ensemble $\bigcap\limits_{\substack{H \text{ sg de } G\\ A\subset H}} H$.

Remarque. Le sous-groupe engendré par une partie A de E sera noté $\langle A\rangle$. On a toujours $\langle\varnothing\rangle=\{e\}$ et $\langle G\rangle=G$.

Proposition. Soit $(G,*)$ un groupe et $A\subset G$ non vide.
(i) $\langle A\rangle$ est le plus petit sous-groupe de G (au sens de l'inclusion) contenant A.
(ii) $\langle A\rangle$ est l'ensemble des mots formés d'éléments de $A\cup\{x^{-1}\,|\,x\in A\}$.

Remarque. Ce qu'on appelle ici un mot formé d'éléments d'une partie E de G est un $x_1*\cdots*x_n$ où $x_1,\dots,x_n$ sont des éléments de E. Cette expression prend particulièrement son sens en notation multiplicative, où $x_1*\cdots*x_n$ est noté $x_1\cdots x_n$.

Démonstration. (i) Tout d'abord $\langle A\rangle$ est un sous-groupe de G en tant qu'intersection de sous-groupes de G (d'après la proposition précédente). De plus $\langle A\rangle$ contient A en tant qu'intersection d'ensembles contenant A. Ainsi $\langle A\rangle$ est un sous-groupe de G contenant A, reste à vérifier que c'est le plus petit.
Soit H un sous-groupe de G contenant A. Alors par définition de $\langle A\rangle$ on a $H\subset\langle A\rangle$ (c'est une intersection entre H et d'éventuels autres sous-groupes de G).
Ceci prouve que $\langle A\rangle$ est bien le plus petit sous-groupe de G contenant A.

(ii) Notons $A^{-1} = \{a^{-1} \,|\, a \in A\}$ et $\tilde{A} = \{x_1 * \cdots * x_n \,|\, n \in \mathbb{N}^* \text{ et } (x_1, \ldots, x_n) \in (A \cup A^{-1})^n\}$ l'ensemble des mots formés d'éléments de $A \cup A^{-1}$.
On doit montrer que $\tilde{A} = \langle A \rangle$. D'après (i) cela revient à montrer que $\tilde{A}$ est le plus petit sous-groupe de G contenant A.
Tout d'abord on a bien $A \subset \tilde{A}$ car si $x \in A$ alors $x \in \tilde{A}$ (x est clairement un mot d'une lettre de $A \cup A^{-1}$).
Vérifions maintenant que $\tilde{A}$ est un sous-groupe de G.
Soit $(x, y) \in \tilde{A}$, il existe donc $n, m \in \mathbb{N}^*$ et $x_1, \ldots, x_n, y_1, \ldots, y_m \in A \cup A^{-1}$ tels que $x = x_1 * \cdots * x_n$ et $y = y_1 * \cdots * y_m$. Alors :

$$x * y = x_1 * \cdots * x_n * y_1 * \cdots * y_m \in \tilde{A}$$

car c'est aussi un mot formé d'éléments de $A \cup A^{-1}$. Comme $\tilde{A} \neq \varnothing$ (car contient $A \neq \varnothing$) alors $\tilde{A}$ est un sous-groupe de G.
On a montré que $\tilde{A}$ est un sous-groupe de G contenant A, reste à vérifier que c'est le plus petit.
Soit H un sous-groupe de G contenant A. Comme H est stable par passage à l'inverse alors $A^{-1} \subset H$ d'où $A \cup A^{-1} \subset H$. Comme H est stable par $*$ alors les mots formés d'éléments de $A \cup A^{-1}$ sont aussi dans H i.e. $\tilde{A} \subset H$.
Ceci prouve que $\tilde{A}$ est le plus petit sous-groupe de G contenant A, i.e. d'après (i) que $\tilde{A} = \langle A \rangle$.

□

Remarque. Dans le cas où $A = \{a\}$ est un singleton, on dira que $\langle A \rangle$ est le sous-groupe de G engendré par a et on notera $\langle A \rangle = \langle a \rangle$. Lorsque $\langle a \rangle$ est fini, son cardinal est appelé l'ordre de a. Les groupes G de la forme $G = \langle a \rangle$ pour un $a \in G$ sont appelés groupes monogènes. Si un groupe monogène est fini, on dit que c'est un groupe cyclique.

Exemples.
1. $\mathbb{Z}$ est le sous-groupe de $(\mathbb{C}, +)$ engendré par 1 (ou -1).
2. $n\mathbb{Z}$ est le sous-groupe de $(\mathbb{Z}, +)$ engendré par n (ou $-n$).
3. $\mathbb{Q}^*$ est le sous-groupe de $(\mathbb{C}^*, \times)$ engendré par $\mathbb{Z}^*$.
4. $\mathbb{U}_n$ est le sous-groupe de $(\mathbb{U}, \times)$ engendré par $e^{i\frac{2\pi}{n}}$.
5. Le sous-groupe de $(\mathcal{P}(E), \Delta)$ engendré par les singletons est $\mathcal{P}(E)$ lui-même.

4 Groupes produit

Définition. Soit $(G_1, *_{G_1})$ et $(G_2, *_{G_2})$ deux groupes de neutres respectifs e_1 et e_2. On définit une loi de composition interne $*$ sur $G_1 \times G_2$ par :

$$\forall ((x_1, x_2), (y_1, y_2)) \in (G_1 \times G_2)^2,\ (x_1, x_2) * (y_1, y_2) = (x_1 *_{G_1} y_1\ ,\ x_2 *_{G_2} y_2)$$

Remarque. Lorsqu'on sait que x_1 et y_1 sont des éléments de G_1 on notera abusivement $x_1 * y_1$ au lieu de $x_1 *_{G_1} y_1$.

Proposition. $(G_1 \times G_2, *)$ forme un groupe dont le neutre est (e_1, e_2).

Démonstration. (i) $*$ est associative car si $((x_1, x_2), (y_1, y_2), (z_1, z_2)) \in (G_1 \times G_2)^3$ alors :

$$\begin{aligned}
\big((x_1, x_2) * (y_1, y_2)\big) * (z_1 * z_2) &= (x_1 * y_1, x_2 * y_2) * (z_1, z_2) \\
&= \big((x_1 * y_1) * z_1\big), (x_2 * y_2) * z_2) \\
&= \big(x_1 * (y_1 * z_1), x_2 * (y_2 * z_2)\big) \quad \text{par associativité de } *_{G_1} \text{ et } *_{G_2} \\
&= (x_1, x_2) * (y_1 * z_1, y_2 * z_2) \\
&= (x_1, x_2) * \big((y_1, y_2) * (z_1, z_2)\big)
\end{aligned}$$

(ii) $*$ admet bien pour neutre (e_1, e_2) pour tout $(x_1, x_2) \in G_1 \times G_2$ on a :

$$\begin{aligned}
(x_1, x_2) * (e_1, e_2) &= (x_1 * e_1, x_2 * e_2) = (x_1, x_2) \\
(e_1, e_2) * (x_1, x_2) &= (e_1 * x_1, e_2 * x_2) = (x_1, x_2)
\end{aligned}$$

(iii) Tout élément (x_1, x_2) de $G_1 \times G_2$ admet un inverse pour $*$, c'est (x_1^{-1}, x_2^{-1}) :

$$(x_1, x_2) * (x_1^{-1}, x_2^{-1}) = (x_1 * x_1^{-1}, x_2 * x_2^{-1}) = (e_1, e_2)$$
$$(x_1^{-1}, x_2^{-1}) * (x_1, x_2) = (x_1^{-1} * x_1, x_2^{-1} * x_2) = (e_1, e_2)$$

□

Remarques. 1. Si G_1 et G_2 sont des groupes commutatifs alors $G_1 \times G_2$ aussi.

2. On peut étendre cette définition et cette propriété à un produit cartésien de n groupes avec $n \in \mathbb{N}^*$.
3. Lorsqu'il n'y a pas d'ambiguïté, on se contentera de noter abusivement $*$ au lieu de $*_{G_1}$ ou $*_{G_2}$.

5 Morphismes de groupes

Définition. Soit $(G, *_G)$ et $(H, *_H)$ deux groupes. On dit d'une application $f : G \longrightarrow H$ que c'est un morphisme de groupes de $(G, *_G)$ vers $(H, *_H)$ lorsque :

$$\forall (x, x') \in G^2,\ f(x * x') = f(x) * f(x')$$

Remarque. Comme indiqué dans la remarque précédente, $f(x * x') = f(x) * f(x')$ est une notation abusive mais non ambiguë pour $f(x *_G x') = f(x) *_H f(x')$.

Proposition. Soit $f : G \longrightarrow H$ un morphisme de groupes. Alors :

(i) $f(e_G) = e_H$
(ii) $\forall x \in G,\ f(x^{-1}) = f(x)^{-1}$.

Démonstration. (i) $f(e_G) * f(e_G) = f(e_G * e_G) = f(e_G)$ donc en composant par $f(e_G)^{-1}$ on obtient $f(e_G) = e_H$.

(ii) Soit $x \in G$, on vérifie que $f(x^{-1})$ est l'inverse de $f(x)$:

$$f(x) * f(x^{-1}) = f(x * x^{-1}) = f(e_G) = e_H$$
$$f(x^{-1}) * f(x) = f(x^{-1} * x) = f(e_G) = e_H$$

D'où $f(x^{-1}) = f(x)^{-1}$.

□

Remarque. Dans le même esprit que la remarque précédente :

— lorsqu'il n'y a pas d'ambiguïté on se contentera de noter $f(e) = e$ au lieu de $f(e_G) = e_H$;
— ici x^{-1} représente l'inverse de x pour la loi $*_G$ et $f(x)^{-1}$ représente l'inverse de $f(x)$ pour la loi $*_H$.

Exemples. 1. L'application $\begin{array}{c} \mathbb{C}^* \longrightarrow \mathbb{R}^* \\ z \longmapsto |z| \end{array}$ est un morphisme de groupes de $(\mathbb{C}^*, \times)$ vers $(\mathbb{R}^*, \times)$.

2. L'application $\begin{array}{c} \mathbb{R} \longrightarrow \mathbb{U} \\ \theta \longmapsto e^{i\theta} \end{array}$ est un morphisme de groupes de $(\mathbb{R}, +)$ vers $(\mathbb{U}, \times)$.

Définition. Si f est un morphisme de groupes bijectif, on dit que f est un isomorphisme de groupes.
S'il existe un isomorphisme de $(G, *_G)$ vers $(H, *_H)$ on dira qu'ils sont isomorphes.
Si f est un isomorphisme d'un groupe G vers lui-même, on dit que f est un automorphisme de groupes.

Exemples. 1. L'application $\begin{array}{c} \mathbb{R} \longrightarrow \mathbb{R}_+^* \\ x \longmapsto e^x \end{array}$ est un isomorphisme de groupes de $(\mathbb{R}, +)$ vers $(\mathbb{R}_+^*, \times)$.

2. L'application $\begin{array}{c} \mathbb{R}_+^* \longrightarrow \mathbb{R} \\ x \longmapsto \ln(x) \end{array}$ est un isomorphisme de groupes de $(\mathbb{R}_+^*, \times)$ vers $(\mathbb{R}, +)$.

3. En notant $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des entiers modulo n (où $n \in \mathbb{N}^*$ fixé) l'application $\begin{array}{c} \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{U}_n \\ k \longmapsto e^{\frac{2ik\pi}{n}} \end{array}$ est un isomorphisme de groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ vers $(\mathbb{U}_n, \times)$.

Proposition. Si f est un isomorphisme de groupes alors f^{-1} aussi.

Démonstration. Soit $f : G \longrightarrow H$ un isomorphisme de groupes.
Soit $(y, y') \in G^2$. Comme f est un morphisme de groupes alors :

$$f(f^{-1}(y) * f^{-1}(y')) = f(f^{-1}(y)) * f(f^{-1}(y')) = y * y'$$

En appliquant f^{-1} on obtient :

$$f^{-1}(y) * f^{-1}(y') = f^{-1}(y * y')$$

Ceci prouve que f^{-1} est également un morphisme de groupes. Comme par ailleurs f^{-1} est bijectif alors c'est bien un isomoprhisme de groupes. □

Exemples.
1. Si G est un groupe l'application identité $\mathrm{Id}_G : \begin{array}{c} G \longrightarrow G \\ x \longmapsto x \end{array}$ est un automorphisme de G.
2. Si G est un groupe commutatif l'application inverse $\begin{array}{c} G \longrightarrow G \\ x \longmapsto x^{-1} \end{array}$ est un automorphisme de G.
3. Si $(G, *)$ est un groupe et $g \in G$ l'application $\iota_g : \begin{array}{c} G \longrightarrow G \\ x \longmapsto g * x * g^{-1} \end{array}$ est un automorphisme. Les ι_g sont appelés les automorphismes intérieurs de G.

Remarque. Si G est un groupe, alors en notant $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G et $\mathrm{Int}(G)$ l'ensemble des automorphismes intérieurs de G on a l'inclusion de sous-groupes :

$$\mathrm{Int}(G) \subset \mathrm{Aut}(G) \subset \mathfrak{S}(G)$$

Proposition. Les images directe et réciproque d'un sous-groupe par un morphisme sont des sous-groupes.

Démonstration. Soient $(G, *_G), (H, *_H)$ des groupes et $f : G \longrightarrow H$ un morphisme de groupes.

— Soit G' un sous-groupe de G, par définition $f(G') \subset H$. Vérifions que $f(G')$ est un sous-groupe de H.
  (i) $e_H = f(e_G) \in f(G)$ car $e_G \in G'$ car G' sous-groupe de G.
  (ii) Soit $(y_1, y_2) \in f(G)^2$. Il existe $(x_1, x_2) \in G^2$ tel que $y_1 = f(x_1)$ et $y_2 = f(x_2)$. Alors :

$$y_1 * y_2^{-1} = f(x_1) * f(x_2)^{-1} = f(x_1) * f(x_2^{-1}) = f(x_1 * x_2^{-1}) \in f(G')$$

  car $x_1 * x_2^{-1} \in G'$ puisque x_1 et x_2 appartiennent à G' sous-groupe de G.
  Ce qui prouve que $f(G')$ est un sous-groupe de H.

— Soit H' un sous-groupe de H, par définition $f^{-1}(H') \subset G$. Vérifions que $f^{-1}(H')$ est un sous-groupe de G.
  (i) $e_G \in f^{-1}(H')$ car $f(e_G) = e_H \in H'$ car H' sous-groupe de H.
  (ii) Soit $(x_1, x_2) \in f^{-1}(H')^2$. Alors $f(x_1) \in H'$ et $f(x_2) \in H'$. Comme f est un morphisme on a :

$$f(x_1 * x_2) = f(x_1) * f(x_2)$$

  qui appartient donc à H' car H' sous-groupe de H. Ainsi $f(x_1 * x_2) \in H'$ i.e. $x_1 * x_2 \in f^{-1}(H')$.
  Ce qui prouve que $f^{-1}(H')$ est un sous-groupe de G.

□

Définition. Soit $f : G \longrightarrow H$ un morphisme de groupes. On pose :
— $\mathrm{Im}\, f = \{y \in H \mid \exists x \in G : y = f(x)\}$ que l'on appelle image de f
— $\mathrm{Ker}\, f = \{x \in G \mid f(x) = e_H\}$ que l'on appelle noyau de f.

Remarque.
— $\mathrm{Im}\, f = f(G)$ est l'image directe de G par l'application f.
— $\mathrm{Ker}\, f = f^{-1}(\{e_H\})$ est l'image réciproque de $\{e_H\}$ par f.

Proposition. $\mathrm{Im}\, f$ est un sous-groupe de H et $\mathrm{Ker}\, f$ est un sous-groupe de G.

Démonstration. C'est une conséquence directe de la proposition précédente. □

Proposition. Soit $f : G \longrightarrow H$ un morphisme de groupes.

(i) f surjectif $\iff \operatorname{Im} f = H$.

(ii) f injectif $\iff \operatorname{Ker} f = \{e_G\}$.

Démonstration. (i) Puisque $\operatorname{Im} f = f(G)$ c'est simplement la définition de la surjectivité de l'application f.

(ii) $\boxed{\Rightarrow}$: Supposons que f est un morphisme injectif. Comme $\operatorname{Ker} f$ est un sous-groupe de G on sait déjà que $\{e_G\} \subset \operatorname{Ker} f$. Reste à vérifier que $\operatorname{Ker} f \subset \{e_G\}$.
Soit $x \in \operatorname{Ker} f$. On a alors $f(x) = e_H = f(e_G)$. Par injectivité de f on en déduit que $x = e_G$ i.e. $x \in \{e_G\}$. D'où $\operatorname{Ker} f \subset \{e_G\}$, ce qui donne $\operatorname{Ker} f = e_G$.
$\boxed{\Leftarrow}$: Supposons que $f$est un morphisme tel que $\operatorname{Ker} f = \{e_G\}$.
Soit $(x, x') \in G^2$ tel que $f(x) = f(x')$. Alors $f(x^{-1} * x') = f(x)^{-1} f(x') = f(x)^{-1} f(x) = e$ i.e. $x^{-1} * x' \in \operatorname{Ker} f$. Comme $\operatorname{Ker} f = \{e_G\}$ alors $x^{-1} * x' = e_G$ i.e. $x' = x$.
D'où l'injectivité de f.

□

Proposition. Si deux groupes sont isomorphes, leurs sous-groupes sont en correspondance bijective.

Démonstration. Soient $(G, *_G), (H, *_H)$ des groupes et $f : G \longrightarrow H$ un isomorphisme de groupes. Notons $\mathcal{S}(G)$ l'ensemble des sous-groupes de G et $\mathcal{S}(H)$ l'ensemble des sous-groupes de H. Comme f est bijective on sait déjà que :

$$\varphi : \begin{array}{c} \mathcal{P}(G) \longrightarrow \mathcal{P}(H) \\ G' \longmapsto f(G') \end{array} \text{ est une bijection de réciproque } \varphi^{-1} : \begin{array}{c} \mathcal{P}(H) \longrightarrow \mathcal{P}(G) \\ H' \longmapsto f^{-1}(H') \end{array}$$

Reste à vérifier que φ réalise une bijection de $\mathcal{S}(G)$ vers $\mathcal{S}(H)$.
D'après une proposition précédente on sait déjà que $\forall G' \in \mathcal{S}(G)$, $\varphi(G) \in \mathcal{S}(H)$ et $\forall H' \in \mathcal{S}(H)$, $\varphi^{-1}(H') \in \mathcal{S}(G)$. Autrement dit φ induit bien une fonction de $\mathcal{S}(G)$ vers $\mathcal{S}(H)$ et φ^{-1} induit aussi une fonction de $\mathcal{S}(H)$ vers $\mathcal{S}(G)$. De plus φ^{-1} étant la bijection réciproque de φ on a :

$$\forall G' \in \mathcal{S}(G),\ (\varphi \circ \varphi^{-1})(G') = G'$$
$$\forall H' \in \mathcal{S}(H),\ (\varphi^{-1} \circ \varphi)(H') = H'$$

Ce qui prouve que :

$$\begin{array}{c} \mathcal{S}(G) \longrightarrow \mathcal{S}(H) \\ G' \longmapsto \varphi(G') \end{array} \text{ est bijective de réciproque } \begin{array}{c} \mathcal{S}(H) \longrightarrow \mathcal{S}(H) \\ H' \longmapsto \varphi^{-1}(H') \end{array}$$

□

Remarque. Il n'existe malheureusement pas de réciproque à ce résultat.

III Structures d'anneau et de corps

1 Anneaux

Définition. Un <u>anneau</u> (ou anneau unitaire) est un ensemble A muni de deux l.c.i. $+$ et $\times$ telles que :

(i) $(A, +)$ est un groupe abélien (son neutre est noté 0)

(ii) $\times$ est associative et admet un neutre noté 1

(iii) $\times$ est distributive sur $+$

Si de plus $\times$ est commutative on dira que $(A, +, \times)$ est un <u>anneau commutatif</u>.

Remarque. Par commodité on notera ab l'élément $a \times b$ de A si $a, b \in A$.

Exemples. 1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux commutatifs.
2. $(\mathcal{M}_n(\mathbb{K}), +, \times)$ est un anneau non commutatif.
3. $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif.

Proposition. Si A est un anneau alors :

$$\forall x \in A,\ 0_A x = x 0_A = 0_A$$

Démonstration. Par distributivité de $\times$ sur $+$ on a :

$$\forall x \in A, \left\{ \begin{array}{l} x0_A = x(1_A - 1_A) = x1_a - x1_a = x - x = 0_A \\ 0_A x = (1_A - 1_A)x = 1_A x - 1_A x = x - x = 0_A \end{array} \right.$$

□

Proposition. Soit A un anneau. Alors pour tout $(a, b) \in A^2$ et tout $n \in \mathbb{N}^*$:

(i) $a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k}$ (ii) si a et b commutent $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

Démonstration. (i) On développe le terme de gauche et un télescopage apparaît :

$$\begin{aligned}(a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k} &= a\sum_{k=0}^{n-1} a^k b^{n-1-k} - b\sum_{k=0}^{n-1} a^k b^{n-1-k} = \sum_{k=0}^{n-1} \left(a^{k+1} b^{n-(k+1)} - a^k b^{n-k}\right) \\ &= a^n b^{n-n} - a^0 b^{n-0} = a^n - b^n\end{aligned}$$

(ii) Démonstration habituelle du binôme de Newton (par récurrence ou dénombrement).

□

2 Groupe des inversibles

Définition. L'ensemble des éléments inversibles pour la loi $\times$ d'un anneau A est noté $A^\times$.

Proposition. $(A^\times, \times)$ est un groupe.

Démonstration. On remarque d'abord que $\times$ induit bien une l.c.i. sur $A^\times$ i.e. que $A^\times$ est stable par $\times$. Ce qui provient du fait que le produit de deux inversibles est un inversible. Ainsi, $\times$ induit une l.c.i. associative de neutre $1 \in A^\times$ et par définition de $A^\times$ tous ses éléments sont inversibles pour la loi $\times$. Autrement dit, $(A^\times, \times)$ est un groupe. □

Exemples. 1. Le groupe des inversibles de $\mathbb{Z}$ est $\{-1, 1\}$, isomorphe à $(\mathbb{Z}/2\mathbb{Z}, +)$.
2. Pour tout $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ on a $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$.

3 Anneaux intègres, corps

Définition. Soit $(A, +, \times)$ un anneau.
— Un élément $a \in A$ non nul est un diviseur de 0 lorsqu'il existe $b \in A$ non nul tel que $ab = 0$ ou $ba = 0$.
— Un anneau intègre est un anneau commutatif n'ayant pas de diviseur de 0.
— Un corps est un anneau intègre vérifiant $A^\times = A \setminus \{0\}$.

Exemples. 1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ (p premier) sont des corps.
2. $\mathbb{Z}, \mathcal{M}_n(\mathbb{K}), \mathcal{P}(E), \mathbb{Z}/n\mathbb{Z}$ (n non premier) ne sont pas des corps.

4 Sous-anneaux

Définition. Soit $(A, +, \times)$ un anneau. Un sous-anneau de A est une partie B de A vérifiant :

(i) B est un sous-groupe de $(A, +)$

(ii) $1_A \in B$

(iii) B est stable par $\times$.

Exemples.

1. L'unique sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$ lui-même.
2. On a l'inclusion de sous-anneaux : $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
3. L'unique sous-anneau de $\mathbb{Z}/n\mathbb{Z}$ est $\mathbb{Z}/n\mathbb{Z}$ lui-même ($n \in \mathbb{N}^*$ quelconque).
4. Si l'on note $\mathcal{D}_n(\mathbb{K})$ l'ensemble des matrices diagonales à coefficients dans $\mathbb{K}$ et $\mathcal{T}_n(\mathbb{K})$ l'ensemble des matrices triangulaires supérieures à coefficients dans $\mathbb{K}$, on a l'inclusion de sous-anneaux $\mathcal{D}_n(\mathbb{K}) \subset \mathcal{T}_n(\mathbb{K}) \subset \mathcal{M}_n(\mathbb{K})$.

5 Morphismes d'anneaux

Définition. Soit A et A' deux anneaux. On dit d'une application $f : A \longrightarrow A'$ que c'est un morphisme d'anneaux lorsque :

(i) $\forall (a, b) \in A^2,\ f(a + b) = f(a) + f(b)$

(ii) $\forall (a, b) \in A^2,\ f(ab) = f(a)f(b)$

(iii) $f(1_A) = 1_{A'}$.

Remarque. Un morphisme d'anneaux est en particulier un morphisme de groupes.

Exemples.

1. L'unique morphisme d'anneaux de $\mathbb{Z}$ vers $\mathbb{Z}$ est $\mathrm{Id}_{\mathbb{Z}}$.
2. L'unique morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$ est $\mathrm{Id}_{\mathbb{Z}/n\mathbb{Z}}$.
3. L'unique morphisme d'anneaux de $\mathbb{Q}$ vers $\mathbb{Q}$ est $\mathrm{Id}_{\mathbb{Q}}$.

Définition. Un morphisme d'anneaux bijectif est appelé un isomorphisme d'anneaux. Un isomorphisme d'un anneau vers lui-même est appelé un automorphisme d'anneaux.

Proposition. Si f est un isomorphisme d'anneaux alors f^{-1} aussi.

Démonstration. On a déjà montré que f^{-1} est un morphisme de groupes, reste à montrer que f^{-1} vérifie les points (ii) et (iii) de la définition précédente. Soit $a', b' \in A'$. Comme f est un morphisme d'anneaux alors :

$$\begin{cases} f\big(f^{-1}(a')f^{-1}(b')\big) = f\big(f^{-1}(a')\big)f\big(f^{-1}(b')\big) = a'b' \\ 1_{A'} = f(1_A) \end{cases}$$

En appliquant f^{-1} on obtient alors :

$$\begin{cases} f^{-1}(a')f^{-1}(b') = f^{-1}(a'b') \\ f^{-1}(1_{A'}) = 1_A \end{cases}$$

Ce qui prouve bien que f^{-1} vérifie les points (ii) et (iii) de la définition précédente. □

Exemples.

1. Si A est un anneau, l'application Id_A est un automorphisme.
2. L'application $z \longmapsto \overline{z}$ est une automorphisme d'anneaux.
3. L'anneau $(\mathcal{P}(E), \Delta, \cap)$ est isomorphe à l'anneau $(\{0,1\}^E, *, \times)$ où $*$ est une l.c.i. définie sur $\{0,1\}^E$ par :

$$\forall f, g \in \{0,1\}^E,\ f * g = f + g - 2fg$$