

Introduction : rappels sur les ensembles.

I) Groupes.

Définition. Un groupe est la donnée d'un ensemble G et d'une loi de composition interne notée $*$ définie de la manière suivante :

$$\begin{aligned} * : G \times G &\longrightarrow G \\ (x, y) &\longmapsto x * y \end{aligned}$$

et telle que $(G, *)$ vérifie les trois propriétés suivantes :

- (1) (Elément neutre) Il existe e dans G tel que $\forall x \in G, e * x = x * e = x$.
- (2) (Associativité) Pour tout $x, y, z \in G, (x * y) * z = x * (y * z) = x * y * z$.
- (3) (Elément inverse) Pour tout x dans G , il existe x' dans G tel que : $x * x' = x' * x = e$. On pourra noter : $x' = x^{-1}$ à ne pas confondre avec la notation $\frac{1}{x}$.

Si de plus $\forall x, y \in G, x * y = y * x$, on dit que la loi $*$ est commutative et que $(G, *)$ est un groupe commutatif ou abélien.

Exemples : $(\mathbb{Z}, +)$ est un groupe abélien. En effet, la loi $+$ est bien une loi de composition interne de $\mathbb{Z} \times \mathbb{Z}$ dans \mathbb{Z} (la somme de deux entiers relatifs est un entier relatif), $0 \in \mathbb{Z}$ est élément neutre pour la loi $+$, $+$ est associative et pour tout $x \in \mathbb{Z}$, il existe $y \in \mathbb{Z}$ tel que : $x + y = y + x = 0$: on prend $y = -x$. Enfin, la loi $+$ est commutative.

Par contre, $(\mathbb{N}, +)$ n'est pas un groupe. En effet, $2 \in \mathbb{N}$ mais 2 n'a pas d'inverse dans \mathbb{N} muni de $+$ car $-2 \notin \mathbb{N}$.

Propriétés. Soit $(G, *)$ un groupe.

- 1) L'élément neutre de G est unique.
- 2) L'inverse y d'un élément x de G est unique.
- 3) L'inverse de l'inverse de x est x .
- 4) Pour tous $x, y \in G, (x * y)^{-1} = y^{-1} * x^{-1}$.
- 5) Pour tous $x, y, z \in G$, si $x * y = x * z$ alors $y = z$.
- 6) Pour tout $x \in G$, pour tout $n \in \mathbb{Z}$, l'inverse de x^n est x^{-n} . On note : $(x^n)^{-1} = x^{-n}$.

Preuves.

1) Soient e et e' deux éléments neutres de G .

e' est élément neutre de G donc $e' * e = e * e' = e$ (c'est le point (1) de la définition pour $x = e$).

e est élément neutre de G donc $e * e' = e' * e = e'$. Ainsi, $e = e'$.

2) Soit $x \in G$ d'inverses : $y \in G$ et $z \in G$.

On a alors : $x * y = e$ ainsi $z * x * y = z * e = z$ de plus, $z * x = e$ donc $z * x * y = e * y = y$ ainsi $y = z$.

3) Soit $x \in G$.

On a : $(x^{-1})^{-1} * x^{-1} = e$ puisque $(x^{-1})^{-1}$ est l'inverse de x^{-1} .

De plus, $x * x^{-1} = e$ (car x est l'inverse de x^{-1}) donc par unicité de l'inverse (propriété 2), on a : $x = (x^{-1})^{-1}$.

4) Soient $x, y \in G$. On note : $x^{-1} \in G$ l'inverse de x et $y^{-1} \in G$ celui de y .

On a : $(x * y)^{-1} * (x * y) = e$ donc : $(x * y)^{-1} * (x * y) * y^{-1} = e * y^{-1} = y^{-1}$.

Par associativité de $*$, on a : $(x * y) * y^{-1} = x * (y * y^{-1}) = x * y * y^{-1} = x$. Dès lors, on obtient : $(x * y)^{-1} * (x * y) * y^{-1} = (x * y)^{-1} * x = y^{-1}$ ainsi, $(x * y)^{-1} * x * x^{-1} = y^{-1} * x^{-1}$ donc : $(x * y)^{-1} = y^{-1} * x^{-1}$.

5) Soient $x, y, z \in G$ tels que : $x * y = x * z$. On a alors : $x^{-1} * x * y = x^{-1} * x * z$ donc $y = z$.

6) Soit $n \in \mathbb{N}$. Montrons le résultat par récurrence sur n .

On note pour tout entier naturel n , $P(n)$ la propriété telle que : $(x^n)^{-1} = x^{-n}$.

Pour $n = 0$, on a : $(x^0)^{-1} = e^{-1} = e$ et $x^{-0} = x^0 = e$ donc on a : $(x^0)^{-1} = x^{-0}$ d'où $P(0)$ est vraie.

Supposons qu'il existe un entier naturel n tel que $P(n)$ soit vraie. On a alors : $(x^n)^{-1} = x^{-n}$. De plus, $x^{n+1} = x^n * x$ donc $(x^{n+1})^{-1} = (x^n * x)^{-1} = x^{-1} * (x^n)^{-1} = x^{-1} * x^{-n} = x^{-1-n} = x^{-(n+1)}$. Ainsi, $P(n+1)$ est vraie !

Conclusion : $P(n)$ est vraie pour tout entier naturel n .

Soit maintenant $n \in \mathbb{Z}^-$. En appliquant la propriété 6 à $(x^{-n})^{-1}$ (on peut car $-n \in \mathbb{N}$), on a : $(x^{-n})^{-1} =$

$x^{-(-n)} = x^n$. Donc $(x^n)^{-1} = ((x^{-n})^{-1})^{-1} = x^{-n}$ d'après la propriété 3. Donc pour tout entier $n \in \mathbb{Z}^-$, on a : $(x^n)^{-1} = x^{-n}$.

Définition. Un groupe dit fini est un groupe qui a un nombre fini d'éléments. Son nombre d'éléments est appelé ordre ou cardinal et est noté : $\text{Card } G$ ou $\#(G)$.

Définition. Soit $(G, *)$ un groupe. Soit $x \in G$.

Si pour tout $n \geq 1$, $x^n \neq e$, on dit que x est d'ordre infini. Sinon, on appelle ordre de x le plus petit entier naturel k tel que $x^k = e$ où e est l'élément neutre de G .

Exercice 1. Soit $(G, *)$ un groupe. Soit $x \in G$ d'ordre $n \geq 2$.

Montrer que $\forall 1 \leq m < n, x^m \neq e$.

Solution de l'exercice 1.

Raisonnons par l'absurde : supposons alors qu'il existe un entier m tel que $1 \leq m < n$ et tel que $x^m = e$. Alors, on a un entier strictement inférieur à n tel que $x^m = e$: ce qui contredit le fait que n est le plus petit entier tel que $x^n = e$ (puisque n est l'ordre de x). Donc $\forall 1 \leq m < n, x^m \neq e$.

Exercice 2. Soit $(G, *)$ un groupe. On suppose que tous les éléments de G sauf l'élément neutre sont d'ordre 2. Montrer que G est commutatif.

Solution de l'exercice 2.

Remarquons d'abord que pour tout $x \in G$, $x^{-1} = x$. C'est le cas si $x = e$. Si $x \neq e$, on a : $x^2 = e$ (car tous les éléments de G sauf l'élément neutre sont d'ordre 2) donc $x * x = e$ donc $x^{-1} = x$.

Soient $x, y \in G$. On veut montrer que $x * y = y * x$.

On a $(x * y)^{-1} = x * y$ et $(x * y)^{-1} = y^{-1} * x^{-1} = y * x$ donc par unicité de l'inverse de $x * y$, on a : $x * y = y * x$.

II) Sous-groupes.

Définition. Soient $(G, *)$ un groupe et H un sous-ensemble non-vide de G . On dit que H est un sous-groupe de G lorsque les deux conditions suivantes sont vérifiées :

- (1) H est stable pour la loi $*$ ($\forall x, y \in H, x * y \in H$).
- (2) H est stable par passage à l'inverse ($\forall x \in H, x^{-1} \in H$).

Exemples.

\mathbb{Z} est un sous-groupe de \mathbb{R} muni de l'addition mais pas \mathbb{N} .

Remarques.

- 1) Les conditions de la définition peuvent être réunies en une seule : H est un sous-groupe de G si et seulement si H est non-vide et $\forall x, y \in H, x * y^{-1} \in H$.
- 2) Pour montrer que H est non-vide, il est en général très facile de vérifier qu'il contient l'élément neutre de G . Si H ne contient pas l'élément neutre de G , H ne peut pas être un sous-groupe de G .
- 3) Tout sous-groupe d'un groupe abélien est abélien.
- 4) Tout groupe G admet au moins deux sous-groupes dits triviaux : G et $\{e\}$ (e étant l'élément neutre de G).

Théorème de Lagrange. Soit H un sous-groupe d'un groupe fini G . Alors H est fini et l'ordre (le cardinal) de H divise celui de G .

Définition et propriété. Soient G un groupe et x un élément de G . On appelle sous-groupe monogène engendré par x dans G le sous-groupe engendré par le singleton $\{x\}$. On le note $\langle x \rangle$. C'est le plus petit sous-groupe de G contenant x et l'on a : $\langle x \rangle = \{x^m, m \in \mathbb{Z}\}$.

Preuve. Le sous-groupe $\langle x \rangle$ contient x donc (par stabilité pour la loi de G), il contient aussi $x.x = x^2$, $x^2.x = x^3$ et par récurrence x^m pour tout entier $m \geq 1$. Il contient aussi nécessairement le symétrique x^{-1} de x donc aussi $x^{-1}.x^{-1} = x^{-2}$ et par récurrence x^{-m} pour tout entier $m \geq 1$. Enfin, il contient le neutre $e = x.x^{-1}$ que l'on note par convention : x^0 . Ceci montre que $\langle x \rangle \supseteq \{x^m, m \in \mathbb{Z}\}$. Il est clair réciproquement que $\{x^m, m \in \mathbb{Z}\}$ est un sous-groupe de G contenant x .

Propriété. Soit G un groupe. Soit x un élément de G . Si x est d'ordre fini $n \geq 1$ dans G , alors le sous-groupe $\langle x \rangle$ est fini d'ordre n et l'on a : $\langle x \rangle = \{e, x, x^2, x^3, \dots, x^{n-1}\}$.

Preuve. Soit x^m avec $m \in \mathbb{Z}$, un élément quelconque de $\langle x \rangle$. Par division euclidienne de m par n , il existe des entiers uniques q et r tels que : $m = nq + r$ avec $0 \leq r \leq n - 1$. On a : $x^m = x^{nq+r} = (x^n)^q.x^r = e^q.x^r = x^r$ ce qui prouve que $\langle x \rangle$ est inclus dans l'ensemble $E = \{x^r, 0 \leq r \leq n - 1\}$. La réciproque étant claire, on a : $\langle x \rangle = E$. Il reste à vérifier que E est formé des n éléments distincts : $e, x, x^2, x^3, \dots, x^{n-1}$. Pour cela, supposons que $x^i = x^j$ avec $0 \leq i, j \leq n - 1$, alors $x^{i-j} = e$ avec $-n < i - j < n$, ce qui, par minimalité de l'ordre n de x , implique $i - j = 0$ donc $i = j$. On a donc bien $E = \{e, x, x^2, \dots, x^{n-1}\}$.

Propriété. Soit G un groupe fini de cardinal n . Soit x un élément de G d'ordre m . Alors m divise n .

Preuve. On a vu que, comme x est d'ordre m , le sous-groupe $\langle x \rangle$ de G s'écrit : $\langle x \rangle = \{e, x, x^2, \dots, x^{m-1}\}$. Ce sous-groupe de G a m éléments donc par le théorème de Lagrange, on en déduit que m divise n .

Exercice 3. Soit G un groupe.

Que dire des sous-groupes de G si G est de cardinal 1 ? De cardinal 2 ? De cardinal 3 ? De cardinal premier p ?

Solution de l'exercice 3.

Si G est de cardinal 1 alors $G = \{e\}$. Soit H un sous-groupe de G . Par le théorème de Lagrange, le cardinal de H divise 1 donc est égal à 1 (c'est un nombre positif !). Donc H contient un seul élément qui est nécessairement l'élément neutre de G donc $H = G = \{e\}$.

Si G est de cardinal 2, on peut écrire $G = \{e, x\}$ où x est d'ordre 2 : x est son propre inverse. Soit H un sous-groupe de G . Par le théorème de Lagrange, le cardinal de H divise celui de G donc H contient 1 ou 2 éléments donc $H = \{e\}$ ou $H = G$.

Si G est de cardinal 3, on peut écrire $G = \{e, x, y\}$ où $y = x^{-1}$. Soit H un sous-groupe de G . Par le théorème de Lagrange, le cardinal de H divise celui de G donc H contient 1 ou 3 éléments. Donc $H = \{e\}$ ou $H = G$.

Plus généralement, si G contient p éléments et que p est premier alors, par le théorème de Lagrange, chaque sous-groupe de G contient 1 ou p éléments. (Les seuls diviseurs de p étant 1 et lui-même car p est premier) donc $H = \{e\}$ ou $H = G$.

Exercice 4. Soit G un groupe (muni d'une loi de composition interne $*$) de cardinal 4. On note e l'élément neutre de G .

1) Montrer que G peut s'écrire sous la forme : $\{e, x, y, z\}$ (où x, y et z sont 3 éléments de G deux à deux distincts et tous distincts de e).

2) Montrer que x, y et z sont chacun d'ordres 2 ou 4.

3) Dans cette question uniquement, on suppose que x, y et z sont chacun d'ordre 2.

Déterminer tous les sous-groupes de G dans ce cas.

On suppose maintenant que y est l'inverse de x .

4) Montrer que x et y sont d'ordres 4 et que z est d'ordre 2.

5) Montrer que $x^2 = x * x = z$ et que $x^3 = x * x * x = y$.

6) Déterminer tous les sous-groupes de G dans ce cas.

Solution de l'exercice 4.

1) G est un groupe de cardinal 4 donc il contient un élément neutre noté e et 3 éléments notés x, y et z , deux à

deux distincts et tous distincts de e . Donc on peut écrire G sous la forme : $\{e, x, y, z\}$.

2) Le cardinal de G est égal à 4. On a vu que l'ordre de tous les éléments de G divise le cardinal de G . Donc x, y et z sont d'ordres 1, 2 ou 4. Comme x, y et z sont tous différents de e , ils sont d'ordres 2 ou 4.

3) Soit H un sous-groupe de G . Par le théorème de Lagrange, le cardinal de H divise celui de G donc H a 1, 2 ou 4 éléments.

Si H a 1 élément, alors $H = \{e\}$.

Si H a 2 éléments, alors $H = \{e, x\}$ ou $H = \{e, y\}$ ou $H = \{e, z\}$ car x, y et z sont chacun d'ordre 2.

Si H a 4 éléments, alors $H = G$.

En conclusion, si x, y et z sont chacun d'ordre 2, alors les sous-groupes de G sont : $\{e\}, \{e, x\}, \{e, y\}, \{e, z\}$ et G .

4) Si x est d'ordre 2 alors $x^{-1} = x$ donc par unicité de l'inverse $x = y$ ce qui est impossible. Donc x n'est pas d'ordre 2. Donc x est d'ordre 4 (par la question 2). De plus, comme on a : $y = x^{-1}$, on a aussi : $y^{-1} = (x^{-1})^{-1} = x$ donc x est l'inverse de y .

Si y est d'ordre 2 alors y est son propre inverse mais alors par unicité de l'inverse, on a : $x = y$ ce qui est impossible donc y est d'ordre 4.

Montrons maintenant que z est d'ordre 2. Pour cela, on va montrer que z est son propre inverse. Si l'inverse de z est e alors $z = e$ ce qui est impossible. Si l'inverse de z est x alors on a : $x * z = z * x = e$ donc $z * x * y = e * y = y$. Or, $x * y = e$ car y est l'inverse de x , donc $z = y$ ce qui est impossible. Enfin, si l'inverse de z est y alors on a : $y * z = z * y = e$ donc $z * y * x = x$ donc $z = x$ ce qui est impossible. Donc l'inverse de z est z . Donc z est son propre inverse, ce qui prouve que z est d'ordre 2.

5) $x^2 \neq e$ car x est d'ordre 4. Si $x^2 = x$ alors $x = e$ ce qui est impossible. Si $x^2 = y$ alors $x^2 * x = y * x = e$ donc $x^3 = e$: ce qui est impossible car x est d'ordre 4. Donc $x^2 = z$.

Si $x^3 = e$ alors cela contredit le fait que x est d'ordre 4 donc $x^3 \neq e$. Si $x^3 = x$ alors $x^3 * y = x * y = e$ donc $x^2 = e$ ce qui contredit le fait que x est d'ordre 4. Donc $x^3 \neq x$. Si $x^3 = z$ alors $x^3 = x^2$ donc $x = e$ ce qui est impossible. Donc $x^3 = y$.

6) Soit H un sous-groupe de G . Alors, par le théorème de Lagrange, le cardinal de H est égal à 1, 2 ou 4.

Si le cardinal de H est égal à 1, alors $H = \{e\}$.

Si le cardinal de H est égal à 2, alors H contient e et un élément de G qui est son propre inverse. Seul z est son propre inverse donc H ne peut contenir que e et z . Donc si H contient deux éléments, H est égal à $\{e, z\}$.

Si le cardinal de H est égal à 4, alors $H = G$.

Donc dans le cas où $y = x^{-1}$, les sous-groupes de G sont : $\{e\}, \{e, z\}$ et G .

III) Morphismes de groupes.

Définition. Soient G un groupe muni d'une loi de composition interne $.$ et G' un groupe muni d'une loi de composition interne $*$. On appelle morphisme de groupes ou homomorphisme de groupes de G dans G' toute application $f : G \rightarrow G'$ telle que : $\forall x, y \in G, f(x.y) = f(x) * f(y)$.

Exemple. L'application $f : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$ définie pour tout entier n par : $f(n) = 2n$ est un morphisme de groupes. En effet, pour tous entiers m et n , $f(m + n) = 2(m + n) = 2m + 2n = f(m) + f(n)$.

Propriétés. Soient G un groupe muni d'une loi de composition interne $.$ et G' un groupe muni d'une loi de composition interne $*$ et $f : G \rightarrow G'$ un morphisme de groupes. On a :

(1) $f(e) = e'$, où e désigne l'élément neutre de G et e' celui de G' .

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

(3) $\forall x \in G, \forall n \in \mathbb{Z}, f(x^n) = f(x)^n$.

(4) Pour tout sous-groupe H de G , l'image directe $f(H) = \{f(x), x \in H\}$ est un sous-groupe de G' .

(5) Pour tout sous-groupe H' de G' , l'image réciproque $f^{-1}(H') = \{x \in G, f(x) \in H'\}$ est un sous-groupe de G .

(6) La composée de deux morphismes de groupes est un morphisme de groupes.

Exercice 5. Démontrer les 6 propriétés précédentes.

Solution de l'exercice 5.

(1) On écrit : $f(e.e) = f(e) * f(e)$ donc $f(e) = f(e) * f(e)$ ainsi, $f(e)^{-1} * f(e) = f(e)^{-1} * f(e) * f(e)$ d'où : $e' = e' * f(e)$ donc $e' = f(e)$.

(2) On a : $f(x.x^{-1}) = f(x) * f(x^{-1}) = f(e) = e'$ donc $f(x^{-1}) = f(x)^{-1}$.

(3) Soient $x \in G$ et $n \in \mathbb{N}$. Commençons par démontrer la propriété dans le cas : $n \in \mathbb{N}$.

On procède par récurrence sur n . Pour $n = 0$ on a bien : $f(x^0) = f(e) = e' = f(x)^0$.

Supposons que $f(x^n) = f(x)^n$ pour un certain rang $n \in \mathbb{N}$, on a : $f(x^{n+1}) = f(x^n.x) = f(x^n) * f(x) = f(x)^n * f(x)$ car $f(x^n) = f(x)^n$ par hypothèse de récurrence. Donc $f(x^{n+1}) = f(x)^{n+1}$.

Ainsi, $\forall x \in G, \forall n \in \mathbb{N}, f(x^n) = f(x)^n$.

Soit maintenant $n \in \mathbb{Z}^-$, alors $-n \in \mathbb{N}$ et on a : $\forall x \in G, f(x^{-n}) = f(x)^{-n}$. Or, $x^n = (x^{-n})^{-1}$ donc par la propriété (2), on a : $f(x^n) = f((x^{-n})^{-1}) = f(x^{-n})^{-1} = (f(x)^{-n})^{-1} = f(x)^n$.

(4) H est un sous-groupe de G donc e (l'élément neutre de G) est dans H et $f(e) = e'$ (e' étant le neutre de G') donc $e' \in f(H)$ et $f(H)$ est non vide.

Soient $y, z \in f(H)$. Montrons que $y * z^{-1} \in f(H)$.

$y, z \in f(H)$ donc il existe x et $x' \in H$ tels que $y = f(x)$ et $z = f(x')$. On a : $y * z^{-1} = f(x) * f(x')^{-1} = f(x) * f(x'^{-1}) = f(x.x'^{-1})$ et $x.x'^{-1} \in H$ (car $x, x' \in H$ et H est un sous-groupe de G) donc $y * z^{-1} \in f(H)$.

Ainsi, $f(H)$ est un sous-groupe de G' .

(5) H' est un sous-groupe de G' donc $e' \in H'$ et on a : $f(e) = e'$ et $e' \in H'$ donc $e \in f^{-1}(H')$ donc $f^{-1}(H')$ est non vide.

Soient $x, y \in f^{-1}(H')$. Montrons que $x.y^{-1} \in f^{-1}(H')$. On a : $f(x.y^{-1}) = f(x) * f(y^{-1}) = f(x) * f(y)^{-1}$. Comme $x, y \in f^{-1}(H')$, $f(x)$ et $f(y) \in H'$ et comme H' est un sous-groupe de G' , $f(x) * f(y)^{-1} \in H'$ donc $f(x.y^{-1}) \in H'$ ainsi, $x.y^{-1} \in f^{-1}(H')$.

D'où $f^{-1}(H')$ est un sous-groupe de G .

(6) Soient G, G' et G'' trois groupes munis respectivement des lois : $\cdot, *$ et \times et $f : G \rightarrow G'$ et $g : G' \rightarrow G''$ deux morphismes deux groupes.

Montrons que $g \circ f : G \rightarrow G''$ est un morphisme de groupes.

Soient $x, y \in G$. On a : $(g \circ f)(x.y) = g(f(x.y)) = g(f(x) * f(y)) = g(f(x)) \times g(f(y)) = (g \circ f)(x) \times (g \circ f)(y)$.
Donc $g \circ f : G \rightarrow G''$ est un morphisme de groupes.

Définitions-propriétés. Soient G et G' deux groupes et $f : G \rightarrow G'$ un morphisme de groupes.

(1) L'ensemble $f(G) = \{f(x), x \in G\}$ est un sous-groupe de G' appelé image de f et noté $\text{Im } f$.

(2) L'ensemble $f^{-1}(\{e'\}) = \{x \in G, f(x) = e'\}$ est un sous-groupe de G , appelé noyau de f et noté $\text{Ker } f$.

Preuves. Pour (1), $f(G)$ est un sous-groupe de G' donc par la propriété précédente, $f(G) = \text{Im } f$ est un sous-groupe de G' . Pour (2), $\{e'\}$ est un sous-groupe de G' donc par la propriété précédente, $f^{-1}(\{e'\}) = \text{Ker } f$ est un sous-groupe de G .

Propriété. Soient G (muni de \cdot) et G' (muni de $*$) deux groupes et $f : G \rightarrow G'$ un morphisme de groupes.

(1) f est surjective si et seulement si $\text{Im } f = G'$.

(2) f est injective si et seulement si $\text{Ker } f = \{e\}$.

Preuve. Le point (1) est immédiat par la définition même de la surjectivité.

Pour (2), supposons d'abord f injective. Soit $x \in \text{Ker } f$ alors $f(x) = e' = f(e)$ donc par injectivité de f , $x = e$. Ainsi, $\text{Ker } f = \{e\}$.

Réciproquement, supposons que $\text{Ker } f = \{e\}$. Soient $x, y \in G$ tels que $f(x) = f(y)$, on a donc $f(x) * f(y)^{-1} = e'$ ainsi, $f(x.y^{-1}) = e'$ donc $x.y^{-1} \in \text{Ker } f$ donc $x.y^{-1} = e$ donc $x = (y^{-1})^{-1} = y$. Ainsi, f est injective.

Définitions. Soit G un groupe.

Un morphisme de groupes bijectif est un isomorphisme de groupes.

Un morphisme de groupes de G dans lui-même est appelé : endomorphisme de groupes.

Un morphisme de groupes bijectif de G dans lui-même est appelé : automorphisme de groupes.

Propriété. Si f est un isomorphisme de groupes de G (muni de \cdot) dans G' (muni de $*$), alors la bijection réciproque f^{-1} est un isomorphisme de groupes de G' dans G .

Preuve. Soient $x', y' \in G'$. Posons : $x = f^{-1}(x')$ et $y = f^{-1}(y')$. De plus, on a : $f(x.y) = f(x) * f(y)$ donc $f(x.y) = x' * y'$ ainsi, $x.y = f^{-1}(x' * y')$ d'où $f^{-1}(x' * y') = f^{-1}(x').f^{-1}(y')$. Donc f^{-1} est un morphisme de groupes de G' dans G .

Définition. Soient G et G' deux groupes. On dit que G et G' sont isomorphes s'il existe un isomorphisme de groupes de G dans G' . On note : $G \simeq G'$.

Exercice 6. Soient G et G' deux groupes et $f : G \rightarrow G'$ un morphisme de groupes. Soit $x \in G$ d'ordre $n \geq 1$. Montrer que $f(x)$ est d'ordre au plus n .

Solution de l'exercice 6.

x est d'ordre n donc on a : $x^n = e$. Ainsi, $f(x^n) = f(x)^n = f(e) = e'$ donc $f(x)^n = e'$ donc $f(x)$ est d'ordre au plus n .

Exercice 7. Soit (G, \cdot) un groupe. On note e son élément neutre.

Pour $a \in G$, on note τ_a l'application de G dans G définie par : $\tau_a(x) = axa^{-1}$.

- 1) Que vaut τ_e ?
- 2) Montrer que τ_a est un morphisme de groupes de G dans lui-même.
- 3) Vérifier que $\forall a, b \in G, \tau_a \circ \tau_b = \tau_{ab}$.
- 4) Montrer que l'application τ_a est bijective et déterminer sa bijection réciproque.
- 5) En déduire que $\mathcal{T} = \{\tau_a, a \in G\}$ muni de la composition : \circ est un groupe.

Solution de l'exercice 7.

- 1) On a pour tout $x \in G, \tau_e(x) = exe^{-1} = exe = x$. Donc $\tau_e = id$.
- 2) Soient $x, y \in G$. On a : $\tau_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \tau_a(x)\tau_a(y)$. Donc τ_a est un endomorphisme de G .
- 3) Soient $a, b \in G$. Soit $x \in G$. On a : $\tau_a \circ \tau_b(x) = \tau_a(bxb^{-1}) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \tau_{ab}(x)$. Donc $\tau_{ab} = \tau_a \circ \tau_b$.
- 4) On a pour tout $x \in G, \tau_a \circ \tau_{a^{-1}}(x) = \tau_a(a^{-1}xa) = aa^{-1}xaa^{-1} = x$ et pour tout $x \in G, \tau_{a^{-1}} \circ \tau_a(x) = \tau_{a^{-1}}(axa^{-1}) = a^{-1}axa^{-1}a = x$. Donc l'application τ_a est bijective et sa bijection réciproque est $\tau_{a^{-1}}$.
- 5) Pour tous $a, b \in G, \tau_a \circ \tau_b = \tau_{ab} \in \mathcal{T}$ donc la loi \circ est une loi de composition interne de $\mathcal{T} \times \mathcal{T}$ dans \mathcal{T} . De plus, l'ensemble $\mathcal{T} = \{\tau_a, a \in G\}$ contient $\tau_e = id$ qui est l'élément neutre pour la loi \circ . Pour tout a, τ_a a un inverse : $\tau_{a^{-1}}$ car τ_a est une bijection de G dans lui-même et sa bijection réciproque est $\tau_{a^{-1}}$. Enfin, \circ est associative. Ainsi, l'ensemble \mathcal{T} muni de la composition est un groupe.