(ii) Pour tout $x \in H$, $x^{-1} \in H$

Cela signifie que la restriction de $*$ à $H \times H$ — que l'on note encore $*$ mais qu'il faudrait en toute rigueur désigner par $*_{|H}$ — donne une loi interne de H et que $(H,*)$ est alors lui-même un groupe.

Les deux conditions (i) et (ii) ci-dessus peuvent être remplacées par

(iii) Pour tous $x,y \in H$ on a $x * y^{-1} \in H$

Il est évident que les conditions (i) et (ii) entraînent (iii). Montrons que, réciproquement, la seule condition (iii) entraînent à la fois (i) et (ii). Puisque $H \neq \emptyset$, il existe $h \in H$. Appliquons (iii) avec $x = y = h$. On obtient $h * h^{-1} \in H$ donc $e_G \in H$. Appliquons maintenant (iii) avec $x = e_G$. Puisque $e_G * y^{-1} = y^{-1}$, on trouve (ii). Enfin, prenant $x,y \in H$, on a par (ii) qui vient d'être établi $y^{-1} \in H$ et appliquant (iii) avec y^{-1} à la place de y on obtient $x * (y^{-1})^{-1} \in H$ c'est-à-dire $x * y \in G$ qui donne (i).

La notation $H < G$ est employée pour dire *H est sous-groupe de G*. Lorsqu'on n'exclut pas la possibilité que H soit égal à G on écrit $H \leq G$.

Insistons sur le fait que pour montrer qu'un sous-ensemble H de G est un sous-groupe de G, il faut d'abord s'assurer qu'il est non vide. Un sous-groupe H contient toujours l'élément neutre e_G et le sous-groupe de G le plus simple est $\{e_G\}$. Un sous-groupe H de G qui est différent de G et de $\{e_G\}$ s'appelle un sous-groupe **propre**.

2.2 Six exemples de sous-groupes

a) Sous-groupes de $(\mathbb{C},+)$

On a $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < (\mathbb{C},+)$.

- ► Montrer que l'ensemble $\mathbb{D}$ des nombres décimaux est un sous-groupe de $(\mathbb{R},+)$.
- ► $(\mathbb{R},+)$ admet-il des sous-groupes finis propres ?

b) Sous-groupes de $(\mathbb{Z},+)$

Soit $m \in \mathbb{N}^\star$. On a $m\mathbb{Z} < (\mathbb{Z},+)$ où $m\mathbb{Z} = \{mr : r \in \mathbb{Z}\}$ est l'ensemble des (entiers relatifs) multiples de m. Réciproquement, on a le

THÉORÈME 4. — *Tout sous-groupe G de $(\mathbb{Z},+)$ est de la forme $G = m\mathbb{Z}$ pour un certain $m \in \mathbb{N}$ (dépendant de G).*

Démonstration. Soit G un sous-groupe de $(\mathbb{Z},+)$. Nous devons établir l'existence d'une entier positif m tel que $G = m\mathbb{Z}$. Traitons d'abord le cas où G est réduit à l'élément neutre, i.e. $G = \{0\}$. Dans ce cas on a bien évidemment $G = m\mathbb{Z}$ en prenant $m = 0$. Supposons maintenant que G ne soit pas réduit à l'élément neutre, il existe alors $g \in G$ avec $g \neq 0$. Puisque $G \leq \mathbb{Z}$, $g \in G \implies -g \in G$ et

nous sommes donc sûrs que G contiendra un élément strictement positif, autrement dit $G \cap \mathbb{N}^\star \neq \emptyset$. Prenons alors m comme le plus petit élément de $G \cap \mathbb{N}^\star$. Puisque $m \in G$ et que G est un sous-groupe, on a $km = m + m + \cdots + m \in G$. Toujours grâce au fait que G soit un sous-groupe on a aussi $-m \in G$ puis $-km = (-m) + (-m) + \cdots + (-m) \in G$ si bien que $m\mathbb{Z} \subset G$. Montrons maintenant que $G \subset m\mathbb{Z}$. Prenons g un élément quelconque de G. C'est un entier que l'on peut diviser par m pour obtenir une expression $g = qm + r$ où r est le reste ($0 \leq r < m$). Comme $qm \in G$ on a $r = g - qm \in G$. Comme en outre $0 \leq r < m$ et m est le plus petit entier positif dans G, la seule possibilité est que r soit égal à 0. Retournant à l'expression de g, il vient $g = qm \in m\mathbb{Z}$ d'où l'on déduit $G \subset m\mathbb{Z}$ et, par double inclusion, $G = m\mathbb{Z}$. □

► Soient m et n deux entiers positifs. A quelle(s) condition(s) $m\mathbb{Z}$ est-il un sous-groupe de $(n\mathbb{Z},+)$? Déterminer l'ensemble des sous-groupes de $(n\mathbb{Z},+)$.

c) Sous-groupes de $(\mathbb{C}^\star,\cdot)$

Soit $n \in \mathbb{N}^\star$. On a par exemple $\mathbb{Q}^{\star+} < \mathbb{Q}^\star < \mathbb{R}^\star < (\mathbb{C}^\star,\cdot)$. On a aussi $\mathbf{U}_n < \mathbf{U} < (\mathbb{C}^\star,\cdot)$. Rappelons que, d'une manière générale, lorsque $X = \mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $X^\star$ désigne $X/\{0\}$ [*].

d) Sous-groupes de $\mathscr{GL}_n(\mathbb{C},\cdot)$

Soit $n \in \mathbb{N}$. On a $\mathscr{GL}_n(\mathbb{Q}) < \mathscr{GL}_n(\mathbb{R}) < (\mathscr{GL}_n(\mathbb{C}),\cdot)$.

e) Sous-groupes des bijections du plan dans lui-même

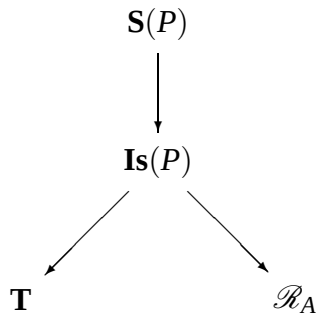
On a $\mathbf{T} < \mathbf{Is}(P) < (\mathbf{S}(P),\circ)$ où $\mathbf{T}$ l'ensemble des translations du plan euclidien. Pour montrer que $\mathbf{T} < \mathbf{Is}(P)$, on utilise $t_{\vec{u}} \circ t_{\vec{v}} = t_{\vec{u}+\vec{v}}$.

f) Sous groupes du groupe des isométries du plan euclidien

$\mathscr{R}_A < (\mathbf{Is}(P),\circ)$ où $\mathscr{R}_A$ l'ensemble des rotations de centre A du plan euclidien. On utilise $r_{A,\theta} \circ r_{A,\theta'} = r_{A,\theta+\theta'}$.

On représente souvent les chaînes de sous-groupes sous la forme d'un arbre comme celui ci-après qui correspond aux exemples e) et f)

[*] Dans l'étude des anneaux on utilisera la notation A^* qui représente en général un ensemble de nature différente.



(2.1)

► Construire l'arbre le plus fourni possible dont le sommet soit $(\mathbb{C},+)$.

2.3 Intersections de sous-groupes

THÉORÈME 5. — *Soient $(G,*)$ un groupe et $\mathscr{F}$ une famille non vide de sous-groupes de G. Si I est l'intersection de tous les éléments de $\mathscr{F}$, autrement dit $I = \bigcap_{H\in\mathscr{F}} H$ alors I est lui-même un sous-groupe de G.*

On notera que $\mathscr{F}$ peut contenir un nombre fini ou infini de sous-groupes.

Démonstration. D'abord I est non vide car e_G est élément de tout sous-groupe F de $\mathscr{F}$ et il appartient donc à I. Soient $x,y \in I$, nous voulons montrer que $x*y^{-1} \in H$. Par définition de I, pour tout $H \in \mathscr{F}$ on a $x,y \in H$ et puisque H est un sous-groupe $x*y^{-1} \in H$. Il suit que $x*y^{-1}$ appartient à tous les éléments de $\mathscr{F}$ et donc à I. Cela montre que I est bien un sous groupe. □

► Déterminer $8\mathbb{Z}\cap 12\mathbb{Z}$. Plus généralement si m et n sont deux entiers positifs, déterminer le sous-groupe de $\mathbb{Z}$ défini par $m\mathbb{Z}\cap n\mathbb{Z}$.

2.4 Sous-groupe engendré par une partie

Soit $(G,*)$ un groupe et A un sous-ensemble *non vide* de G. On appelle **sous-groupe engendré** par A le sous-groupe

$$\langle A\rangle := \bigcap_{H\in\mathscr{S}(A)} H \tag{2.2}$$

où $\mathscr{S}(A)$ est l'ensemble de tous les sous-groupes de G qui contiennent A. Cet ensemble n'est pas vide car il contient G lui-même. En vue du Théorème 5, la formule (2.2) définit bien le sous-groupe $\langle A\rangle$ de G.

THÉORÈME 6. — *Le sous-groupe $\langle A\rangle$ est le plus petit sous-groupe de G contenant A.*

Ici l'adjectif 'petit' réfère à la relation d'ordre définie par l'inclusion des ensembles : un ensemble X est plus petit qu'un ensemble Y si $X \subset Y$. De manière précise, le théorème 6 signifie que les deux assertions suivantes sont équivalentes

(E1) $I = \langle A \rangle$.

(E2) I vérifie les deux conditions suivantes

(a) I est un sous-groupe de G contenant A et

(b) Si H est un autre sous-groupe de G contenant A alors on a $I \subset H$.

Démonstration. D'après la définition, on a immédiatement que $\langle A \rangle$ vérifie les deux conditions de (E2). Nous montrons que si I vérifie (a) et (b) alors $I = \langle A \rangle$. A cause de (b), on a $I \subset \bigcap_{H \in \mathscr{S}(A)} H = \langle A \rangle$. D'autre part, puisque, d'après (a), I est un sous-groupe contenant A, on a $I \in \mathscr{S}(A)$ et par conséquent $\bigcap_{H \in \mathscr{S}(A)} H \subset I$ soit $\langle A \rangle \subset I$. Par double inclusion on en déduit $I = \langle A \rangle$. □

Ni la définition, ni cette caractérisation ne permettent de déterminer facilement les éléments de $\langle A \rangle$. Le paragraphe suivant donne une approche *constructive* des sous-groupes engendrés.

2.5 Description des éléments d'un sous-groupe engendré

THÉORÈME 7. — *Soient $(G,*)$ un groupe, A un sous-ensemble non vide de G et $x \in G$. Pour que $x \in \langle A \rangle$ alors il faut et il suffit qu'il existe $n \in \mathbb{N}^\star$ et des éléments $x_1, x_2, \ldots, x_n$ avec $x_i \in A$ ou $x_i^{-1} \in A$ pour $i = 1, 2, \ldots n$ tels que $x = x_1 * x_2 * \cdots * x_n$.*

Le théorème précédent affirme donc l'égalité

$$\langle A \rangle = \{x_1 * x_2 * \cdots * x_n \,:\, n \in \mathbb{N}^\star,\ x_i \text{ ou } x_i^{-1} \in A,\ i = 1, \ldots, n\}, \qquad (2.3)$$

ou encore

$$\langle A \rangle = \{g_1^{\pm 1} * g_2^{\pm 1} * \cdots * g_n^{\pm 1} \,:\, n \in \mathbb{N}^\star \text{ et } g_i \in A,\ i = 1, \ldots, n\}. \qquad (2.4)$$

Démonstration. Appelons I le membre de droite dans (2.3) (ou (2.4)), nous devons montrer que $I = \langle A \rangle$. Pour cela, d'après le Théorème 6, il suffit de vérifier l'assertion (E2) c'est-à-dire (a) I est un sous-groupe de G contenant A et (b) tout sous-groupe de G contenant A contient aussi I.

Étape 1. I est un sous-groupe de G contenant A.

En considérant les cas où $n = 1$ et $x_1 \in A$ dans (2.3) on voit que $A \subset I$. En particulier I est non vide. Montrons que c'est un sous-groupe de G. Pour cela prenons x et y dans I et vérifions que $x * y^{-1} \in I$. Ecrivons

$$\begin{cases} x = x_1 * x_2 * \cdots * x_m & x_i \in A \text{ ou } x_i^{-1} \in A \\ y = y_1 * y_2 * \cdots * y_p & y_i \in A \text{ ou } y_i^{-1} \in A \end{cases} \quad \text{(Attention, en général } m \neq p\text{).}$$

En utilisant la formule 1.1 (p. 7) sur l'inverse d'un produit on obtient

$$x * y^{-1} = x_1 * x_2 * \cdots * x_m * y_p^{-1} * \cdots * y_1^{-1}$$

Chacun des $m+p$ facteurs f du produit vérifie $f \in A$ ou $f^{-1} \in A$ de sorte que $x * y^{-1}$ a bien la forme requise (avec $n = m+p$) des éléments de I. Il suit que $x * y^{-1} \in I$ et I est donc bien un sous-groupe de G contenant A.

Étape 2. Si H est un sous-groupe de G contenant A alors $I \subset H$.

Prenons $x \in I$ que l'on écrit comme précédemment $x = x_1 * x_2 * \cdots * x_n$. Etudions le facteur x_i. Il y a deux possibilités:

- Soit $x_i \in A$ et alors $x_i \in H$ puisque $A \subset H$
- Soit $x_i^{-1} \in A$ et alors $x_i^{-1} \in H$ puis, puisque H est un sous-groupe, $x_i = (x_i^{-1})^{-1} \in H$.

Dans les deux cas on a $x_i \in H$ de sorte que, toujours puisque H est un sous-groupe, $x \in H$ comme produit d'éléments de H. Cela achève la démonstration de la deuxième étape et du théorème. □

Lorsque une partie (non vide) A vérifie $\langle A \rangle = G$, on dit que A *engendre* G ou que G est *engendré* par A ou encore que A est une **partie génératrice** de G. Pour bien des questions, on considère qu'on a déjà acquis une bonne connaissance du groupe G si on a pu exhiber une partie génératrice *la plus petite possible* car on peut alors décrire par la formule assez simple (2.3) tous les éléments du groupe. Le cas le plus simple est celui où A est réduit à un seul élément. Nous l'étudions dans la partie suivante.

2.6 Groupes cycliques, ordre d'un élément

On dit qu'un groupe $(G,*)$ est **cyclique** s'il est engendré par un ensemble réduit à un seul élément i.e. $G = \langle \{a\} \rangle$. On note aussi pour alléger l'écriture $G = \langle a \rangle$. D'après la formule (2.3), tout élément de G s'écrit alors

$$x = a^{\pm 1} * a^{\pm 1} * \cdots * a^{\pm 1} = a^m \quad \text{avec } m \in \mathbb{Z}$$

de sorte que

$$G = \{a^m : m \in \mathbb{Z}\}.$$

Il se peut que les éléments dans l'ensemble de droite ne soient pas tous deux à deux distincts. Si on $a^{m_1} = a^{m_2}$ avec, disons, $m_1 > m_2$ alors $a^{m_1 - m_2} = e$ et dans ce cas la description de G peut encore être simplifiée. Appelons d le plus petit entier strictement positif tel que $a^d = e$. Notre supposition implique l'existence de cet entier d avec $d \leq m_1 - m_2$. On dit que a est d'**ordre** (fini) d et on écrit $o(a) = d$. On a

$$G = \{a^i : i = 0,1,\ldots,d-1\}.$$

En effet, si m est un entier quelconque, on peut en effectuant une division euclidienne l'écrire $m = dq + r$ avec $r \in \{0,1,\ldots,d-1\}$ d'où

$$a^m = a^{dq+r} = (a^d)^q * a^r = e^q * a^r = a^r$$

de sorte que $\{a^m : m \in \mathbb{Z}\} = \{a^i : i = 0,1,\ldots,d-1\}$. Notons que l'ensemble $\{a^i : i = 0,1,\ldots,d-1\}$ ne peut pas être davantage réduit. En effet si $a^i = a^{i'}$ avec $i > i'$ alors $a^{i-i'} = e$ or $0 < i - i' \leq i < d$ et cela contredit le fait que d est le plus petit entier positif vérifiant $a^d = e$. On a démontré le théorème suivant.

THÉORÈME 8. — *Soit $(G,*)$ un groupe cyclique engendré par a. Il y a deux possibilités.*

- Ou bien *a est d'ordre fini $d \in \mathbb{N}^\star$ et on a $G = \{a^i : i = 0,1,\ldots d-1\}$*
- ou bien *a n'est pas d'ordre fini (on dit alors qu'il est d'ordre infini) et $G = \{a^m : m \in \mathbb{Z}\}$.*

Dans chaque cas les éléments des ensembles indiqués sont deux à deux distincts[*].

On remarquera que l'ordre d'un élément est égal au à l'ordre (au cardinal) du groupe qu'il engendre, i.e. $o(a) = |\langle a \rangle|$, et cela justifie l'emploi du même mot *ordre* pour désigner deux concepts différents. Notons que les groupes cycliques sont toujours abéliens.

2.7 Trois exemples de sous-groupes engendrés

a) Dans $(\mathbb{Z},+)$

Exemple 2.7.1 Pour tout $m \in \mathbb{Z}$, $\langle m \rangle = m\mathbb{Z}$.

En effet, les éléments de $\langle m \rangle$ sont les entiers x qui s'écrivent $x = \pm m + \pm m + \cdots + \pm m = rm$ avec $r \in \mathbb{Z}$.

Exemple 2.7.2 Quels que soient les entiers m et n, $\langle m,n \rangle = pgcd(m,n)\mathbb{Z}$.

En effet, les élément de $\langle m,n \rangle$ sont les entiers s qui s'écrivent

$$s = \pm \begin{pmatrix} m \\ \text{ou} \\ n \end{pmatrix} + \pm \begin{pmatrix} m \\ \text{ou} \\ n \end{pmatrix} + \cdots + \pm \begin{pmatrix} m \\ \text{ou} \\ n \end{pmatrix} = pm + rn \quad \text{avec } p,r \in \mathbb{Z}.$$

Or le théorème de Bezout de l'arithmétique élémentaire dit que lorsque p et r parcourent $\mathbb{Z}$ alors l'entier $pm + rn$ parcourt **pgcd**$(m,n)\mathbb{Z}$.

[*] Beaucoup d'auteurs appellent **groupe monogène** ce que nous avons appelé groupe cyclique infini et garde la dénomination de cyclique au seuls groupes finis.

b) Eléments générateurs du groupe des racines de l'unité

$\mathbf{U}_n = \langle \exp(2i\pi/n) \rangle$. En effet,

$$\mathbf{U}_n = \{\exp \frac{2ik\pi}{n} : k = 0,1,\ldots,n-1\} = \{\phi^k : k = 0,1,\ldots,n-1\}$$

où $\phi = \exp \frac{2i\pi}{n}$. En particulier on a $o(\phi) = n$. Le groupe $\mathbf{U}_n$ est donc cyclique d'ordre n.

c) Parties génératrices de $\mathbf{Is}(P)$

On démontre en géométrie que toute isométrie du plan s'écrit comme la composée d'au plus *trois* réflexions (symétries orthogonales) on a donc

$$\mathbf{Is}(p) = \langle s_D : D \text{ droite du plan} \rangle.$$

§ 3 MORPHISMES

3.1 Definition

Soit $(G,*)$ et $(G',\circ)$ deux groupes et φ une application de G dans $G' : \varphi : G \to G'$. On dit que φ est un **morphisme de groupe** (ou simplement un **morphisme**) lorsqu'elle vérifie

$$\varphi(a*b) = \varphi(a) \circ \varphi(b) \qquad (a,b \in G) \tag{3.1}$$

Autrement dit, *φ est un morphisme si l'image d'un $*$-produit est le $\circ$-produit des images*.

Il y a une terminologie assez sophistiquée pour décrire divers types de morphismes. D'abord, les morphismes sont aussi appelés **homomorphismes**. Lorsque le groupe de départ et le groupe d'arrivée sont les mêmes on parle d'**endomorphisme**. Un morphisme bijectif est un **isomorphisme**. Enfin, un isomorphisme de G dans lui-même s'appelle un **automorphisme**[*].

THÉORÈME 9. — *Si $\varphi : G \to G'$ est un isomorphisme alors l'application réciproque $\varphi^{-1} : G' \to G$ (qui existe puisque φ est bijective) est elle-même un isomorphisme.*

Démonstration. Si $x,y \in G'$ alors, puisque φ est bijective, il existe a et b dans G tels que $\varphi(a) = x$ et $\varphi(b) = y$. De plus on a

$$x \circ y = \varphi(a) \circ \varphi(b) = \varphi(a*b)$$

[*] On trouve encore dans la littérature le terme de **monomorphisme** pour désigner un morphisme injectif et celui d'**épimorphisme** pour un morphisme surjectif. Ce vocabulaire ne sera pas employé dans ce cours.

car φ est un morphisme. Il suit que

$$\varphi^{-1}(x \circ y) = \varphi^{-1}(\varphi(a * b)) = a * b = \varphi^{-1}(x) * \varphi^{-1}(y).$$

□

Lorsqu'il existe un isomorphisme entre G et G', on dit que G et G' sont *isomorphes* et on note $G \simeq G'$.

THÉORÈME 10. — *L'image de l'élément neutre du groupe de départ par un morphisme est l'élément neutre du groupe d'arrivée.* [$\varphi(e_G) = e_{G'}$].

Démonstration. Soit φ un morphisme de $(G,*)$ dans $(G',\circ)$. On a $\varphi(e_G * e_G) = \varphi(e_G) \circ \varphi(e_G)$ et puisque e_G est élément neutre $e_G * e_G = e_G$. On a donc

$$\begin{array}{ll} & \varphi(e_G) = \varphi(e_G) \circ \varphi(e_G) \\ \Rightarrow & [\varphi(e_G)]^{-1} \circ \varphi(e_G) = [\varphi(e_G)]^{-1} \circ \varphi(e_G) \circ \varphi(e_G) \\ \Rightarrow & e_{G'} = e_{G'} \circ \varphi(e_G) \\ \Rightarrow & e_{G'} = \varphi(e_G). \end{array}$$

□

THÉORÈME 11. — *Par un morphisme l'image du symétrique d'un élément est le symétrique de l'image de cet élément.* [$\varphi(g^{-1}) = [\varphi(g)]^{-1}$.]

Il faut bien prendre garde ici de ne pas confondre $[\varphi(g)]^{-1}$ avec $\varphi^{-1}(g)$. La première formule désigne le symétrique de l'élément $\varphi(g) \in G'$ qui existe toujours puisque G' est un groupe. En particulier on $[\varphi(g)]^{-1} \in G'$. La seconde n'a de sens que lorsque φ est une bijection et $g \in G'$ et dans ce cas elle désigne un élément de G.

Démonstration. Soient φ un morphisme de $(G,*)$ dans $(G',\circ)$ et $g \in G$. On

$$\begin{array}{ll} & g * g^{-1} = e_G = g^{-1} * g \\ \Longrightarrow & \varphi(g * g^{-1}) = \varphi(e_G) = \varphi(g^{-1} * g) \\ \overset{\text{Th. 10}}{\Longrightarrow} & \varphi(g) \circ \varphi(g^{-1})) = e_{G'} = \varphi(g^{-1}) \circ \varphi(g). \end{array}$$

Cela signifie que $\varphi(g^{-1})$ vérifie les deux conditions définissant le symétrique de $\varphi(g)$ donc $\varphi(g^{-1}) = [\varphi(g)]^{-1}$. □

3.2 Morphismes et image des sous-groupes

THÉORÈME 12. — *Soient φ un morphisme de G dans G' et H un sous-groupe de G alors $\varphi(H)$ est un sous-groupe de G'. En particulier $\varphi(G)$ est un sous-groupe de G'.* [$H \leq G \Rightarrow \varphi(H) \leq G'$.]

Rappelons que $\varphi(H) \stackrel{\text{def}}{=} \{\varphi(h) : h \in H\}$ et s'appelle l'**image** de H par φ.

Démonstration. Pour montrer que $\varphi(H)$ est un sous-groupe de G' nous devons vérifier (1) qu'il est non vide et (2) pour tous $x,y \in \varphi(G)$ on a $x \circ y^{-1} \in \varphi(G)$. Que $\varphi(H)$ soit non vide est clair car, d'après le Théorème 10, $e_G \in H \Rightarrow \varphi(e_G) = e_{G'} \in \varphi(H)$. Quant au second point, si $x,y \in \varphi(H)$ alors $x = \varphi(a)$ et $y = \varphi(b)$ avec $a,b \in H$. Donc

$$\begin{array}{rcl} x \circ y^{-1} & = & \varphi(a) \circ [\varphi(b)]^{-1} \\ & \stackrel{\text{Th. 11}}{=} & \varphi(a) \circ \varphi(b^{-1}) = \varphi(a * b^{-1}) \\ & \in & \varphi(H) \quad \text{car } a,b \in H \text{ et } H \leq G, \end{array}$$

donc $\varphi(H)$ est bien un sous-groupe de G'. □

3.3 Le noyau

Soit φ un morphisme de $(G,*)$ dans $(G',\circ)$. On appelle **noyau** de φ et on note $\ker\varphi$ — "ker" est l'abbréviation du mot allemand *kernel* qui signifie noyau — l'ensemble

$$\ker\varphi \stackrel{def}{=} \{g \in G \ : \ \varphi(g) = e_{G'}\} \tag{3.2}$$

D'après le Théorème 10, on a toujours $\varphi(e_G) = e_{G'}$ donc $e_G \in \ker\varphi$ qui n'est ainsi jamais vide.

THÉORÈME 13. — *Le noyau d'un morphisme est un sous-groupe du groupe de départ.* [$\ker\varphi \leq G$].

Démonstration. Puisque $\ker\varphi \neq \emptyset$ il suffit de vérifier que $x,y \in \ker\varphi \Rightarrow x * y^{-1} \in \ker\varphi$. Or

$$\begin{array}{rcll} \varphi(x * y^{-1}) & = & \varphi(x) \circ \varphi(y^{-1}) & \text{(déf. d'un morph.)} \\ & = & \varphi(x) \circ [\varphi(y)]^{-1} & \text{(Th. 11.)} \\ & = & e_{G'} \circ [e_{G'}]^{-1} & \text{(déf. du noyau.)} \\ & = & e_{G'}. & \end{array}$$

Donc $x * y^{-1} \in \ker\varphi$ qui est bien un sous-groupe. □

Le noyau vérifie une autre propriété. Si $g \in G$ et $x \in \ker\varphi$ alors $g * x * g^{-1} \in \ker\varphi$. En effet,

$$\begin{array}{rcll} \varphi(g * x * g^{-1}) & = & \varphi(g) \circ \varphi(x) \circ \varphi(g^{-1}) & \\ & = & \varphi(g) \circ \varphi(x) \circ [\varphi(g)]^{-1} & \text{(par le Th. 11)} \\ & = & \varphi(g) \circ e_{G'} \circ [\varphi(g)]^{-1} & \\ & = & \varphi(g) \circ [\varphi(g)]^{-1} & \\ & = & e_{G'}. & \end{array}$$

Les groupes vérifiant cette propriété sont dits distingués. Cette notion très utile sera étudiée par la suite.

THÉORÈME 14. — *Pour qu'un morphisme soit injectif il faut et il suffit que son noyau se réduisent à l'élément neutre.* [$\varphi : G \overset{\text{morph.}}{\longrightarrow} G'$ injective $\Leftrightarrow \ker\varphi = \{e_G\}$.]

Rappelons qu'une application φ est dite **injective** lorsque deux éléments distincts ont nécessairement deux images distinctes. Autrement dit l'hypothèse $\varphi(x) = \varphi(y)$ doit toujours impliquer $x = y$.

Démonstration. ($\Longrightarrow$) *On suppose que φ est injective et on montre que* $\ker\varphi = \{e_G\}$.

On sait que $e_G \in \ker\varphi$. Si x est un autre élément de $\ker\varphi$ avec $x \neq e_G$ alors $\varphi(e_G) = e_{G'} = \varphi(x)$ donc x et e_G ont la même image sans être égaux, ce qui contredit l'injectivité de φ.

($\Longleftarrow$) *On suppose que* $\ker\varphi = \{e_G\}$ *et on montre que φ est injective.*

Supposons que x et y soient deux éléments de G tels que $\varphi(x) = \varphi(y)$. On a

$$\begin{array}{rrcl}
 & \varphi(x) \circ [\varphi(y)]^{-1} & = & e_{G'} \\
\Rightarrow & \varphi(x) \circ \varphi(y^{-1}) & = & e_{G'} \quad \text{(par le Th. 11)} \\
\Rightarrow & \varphi(x * y^{-1}) & = & e_{G'} \\
\Rightarrow & x * y^{-1} & \in & \ker\varphi \\
\Rightarrow & x * y^{-1} & = & e_G \quad (\text{car } \ker\varphi = \{e_G\}) \\
\Rightarrow & x & = & y
\end{array}$$

L'hypothèse $\varphi(x) = \varphi(y)$ implique donc $x = y$ et φ est bien injective. □

THÉORÈME 15. — *Soient G et G' deux groupes finis de* même cardinal *et φ un morphisme de G dans G'. Pour que φ soit un isomorphisme il faut et il suffit que* $\ker\varphi$ *soit réduit à l'élément neutre.*

Démonstration. Lorsque G et G' sont des ensembles finis, de même cardinal, dire que $\varphi : G \to G'$ est bijective est équivalent à dire qu'elle est injective. □

3.4 Morphismes et image-réciproque des sous-groupes

Soit φ un morphisme de $(G,*)$ dans $(G',\circ)$. S'il n'est permis de parler de l'élément $\varphi^{-1}(g)$ que lorsque φ est bijective (et $g \in G'$), on peut toujours considérer l'ensemble $\varphi^{-1}(\{g\})$, qui est formé, par définition, de tous les éléments $x \in G$ tels que $\varphi(x) = g$. Cet ensemble $\varphi^{-1}(\{g\})$ peut-être vide et il est égal à $\{\varphi^{-1}(g)\}$ lorsque (mais pas seulement) φ est bijective. D'un manière générale,

si $Y \subset G'$ on appelle **image-réciproque** ou **pré-image** de Y par φ et on note $\varphi^{-1}(Y)$ l'ensemble défini par

$$\varphi^{-1}(Y) = \{x \in G : \varphi(x) \in Y\}.$$

On remarquera que $\ker\varphi = \varphi^{-1}(\{e_{G'}\})$.

THÉORÈME 16. — *Soient φ un morphisme de G dans G' et W un sous-groupe de G' alors $\varphi^{-1}(W)$ est un sous-groupe de G qui contient* $\ker\varphi$. [$W \leq G' \Rightarrow \varphi^{-1}(W) \leq G$.]

Démonstration. Puisque W est sous-groupe de G' on a $e_{G'} \in W$ de sorte que $\ker\varphi = \varphi^{-1}(\{e_{G'}\}) \subset \varphi^{-1}(W)$ qui n'est donc pas vide. Il suffit de vérifier que $x,y \in \varphi^{-1}(W) \Rightarrow x*y^{-1} \in \varphi^{-1}(W)$. Or

$$\begin{array}{rrcll} & \varphi(x*y^{-1}) & = & \varphi(x)\circ\varphi(y^{-1}) & \text{(déf. d'un morph.)} \\ & & = & \varphi(x)\circ[\varphi(y)]^{-1} & \text{(Th. 11.)} \\ \Rightarrow & \varphi(x*y^{-1}) & \in & W\circ W \subset W & \text{(car } W \leq G.\text{)} \end{array}$$

Donc $x*y^{-1} \in \varphi^{-1}(W)$ qui est bien un sous-groupe. □

3.5 Cinq exemples de morphismes

a) Exponentielle et logarithme

L'application

$$\exp : \begin{array}{ccc} (\mathbb{R},+) & \longrightarrow & (\mathbb{R}^{\star+},.) \\ x & \longmapsto & \exp x. \end{array}$$

est un isomorphisme, on a $\exp^{-1} = \ln$.

b) Exponentielle complexe

Est un morphisme l'application

$$E_{\mathbb{C}} : \begin{array}{ccc} (\mathbb{R},+) & \longrightarrow & (\mathbf{U},.) \\ x & \longmapsto & \exp ix. \end{array}$$

On a

$$\begin{array}{rcl} \ker E_{\mathbb{C}} & = & \{x \in \mathbb{R} : \exp(ix) = 1\} \\ & = & \{x \in \mathbb{R} : x = 2k\pi,\, k \in \mathbb{Z}\} \\ & = & 2\pi\mathbb{Z}. \end{array}$$

c) Le déterminant

$$\det : \begin{array}{ccc} \mathscr{GL}_n(\mathbb{K}) & \longrightarrow & (\mathbb{K}^\star,.) \\ A & \longmapsto & \det A \end{array}$$

On a

$$\begin{array}{rcl} \ker\det & = & \{A \in \mathscr{GL}_n(\mathbb{K}) : \det A = 1\} \\ & \stackrel{\text{def}}{=} & \mathbf{SL}_n(\mathbb{K}). \end{array}$$

d) Les automorphismes intérieurs

Soit $(G,.)$ un groupe et $x \in G$. L'application

$$\phi_x : \begin{array}{ccc} (G,.) & \longrightarrow & (G,.) \\ g & \longmapsto & x^{-1}gx. \end{array}$$

est un automorphisme. Tout automorphisme construit de cette manière s'appelle un **automorphisme intérieur**. L'ensemble des automorphismes intérieurs, noté $\mathbf{Int}(G)$, forme lui-même un groupe lorsqu'on le munit de la loi de composition des applications.

e) L'application puissance

Soit $(G,*)$ un groupe quelconque et $g \in G$. L'application suivante est un morphisme de groupe.

$$p_g : \begin{array}{ccc} (\mathbb{Z},+) & \longrightarrow & (G,*) \\ m & \longmapsto & g^m. \end{array}$$

(i) Si g est d'ordre infini p_g est injective.

(ii) Si g est d'ordre d $\ker p_g = d\mathbb{Z}$.

Montrons le second point. Si $m \in \ker p_g$ alors $g^m = e$ mais, effectuant une division euclidienne, on peut écrire $m = qd + r$ avec $r \in \{0,1,\ldots,d-1\}$. Par conséquent $g^m = e \Rightarrow g^{qd+r} = e \Rightarrow (g^d)^q * g^r = e \Rightarrow e^q g^r = e \Rightarrow g^r = e$. La seule possibilité est que $r = 0$ car $r < d$ et d est l'ordre de g c'est-à-dire le plus petit entier positif pour lequel $g^d = e$. Maintenant $r = 0$ donne $m = qd$ i.e. $m \in d\mathbb{Z}$. Cela prouve $\ker p_g \subset d\mathbb{Z}$. On montre facilement qu'on a aussi $d\mathbb{Z} \subset \ker p_g$ d'où $\ker p_g = d\mathbb{Z}$.

Du premier point on déduit le théorème suivant.

THÉORÈME 17. — *Si $(G,*)$ est un groupe cyclique infini alors $(G,*) \simeq (\mathbb{Z},+)$.*

Démonstration. Si $G = \langle g \rangle$ alors, par définition p_g est surjectif et puisque nous avons que c'est un morphisme injectif, c'est un isomorphisme. □