ALGÈBRE GÉNÉRALE

JEAN-PAUL CALVI

Le premier chapitre de ce cours est une introduction à la théorie élémentaires des groupes. Il part de la définition pour arriver jusqu'au (premier) théorème d'isomorphisme. L'étude du groupe symétrique, initialement prévue, n'a pas pu être incluse. Le second, portant sur la théorie des anneaux et des corps, se limite à présenter les définitions et les propriétés élémentaires. On y définit les anneaux $\mathbb{Z}/n\mathbb{Z}$, plus généralement les anneaux quotient, et les anneaux de polynômes à une indéterminée (à coefficients dans un anneau). L'étude s'arrête avant d'aborder la théorie de la divisibilité. Les connaissances préalables nécessaires sont limitées : le vocabulaire de la théorie des ensembles [(i)], une familiarité avec les calculs dans les ensembles de nombres usuels ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) et les notions fondamentales d'arithmétique (division euclidienne, nombres premiers entre eux, pgcd, théorème de Bezout). Pour tirer profit de l'ensemble des exemples quelques connaissances d'algèbre linéaire et de géométrie sont nécessaires.

Table des matières

Date: 5 août 2004.

(i). Malheureusement de nombreux étudiants éprouvent des difficultés à manier les notions d'ensemble, de cardinal, d'application, de bijection, de bijection réciproque...

Références

[1] Burn, R.P. *Groups, a path to geometry*, Cambridge university press, Cambridge, 1985.
[2] Kargapolov, M. et Merzliakov I. *Eléments de la théorie des groupes*, Mir, Moscou, 1985.
[3] Kostrikin, A. *Introduction à l'algèbre*, Mir, Moscou, 1981.
[4] Kurosh, A. *Cours d'algèbre supérieure*, Mir, Moscou, 1973.
[5] van der Waerden, A. *Cours d'algèbre supérieure*, Springer, New York, 1991. (Première édition, en allemand, 1930)
[6] Zariski, O and Samuel P., *Commutative algebra (vol 1)*, Springer, New York, 1958.

1. Introduction à la théorie des groupes

§ 1. La structure de groupe.

1.1. *Lois internes.* Soit E un ensemble non vide. Une application $*$ de $E \times E$ dans E s'appelle une **loi interne**(i). Si a et b sont dans E alors l'image du couple (a,b) par $*$ est notée $a * b$(ii). On parle de loi interne (à E) parce qu'avec deux éléments de E on fabrique un troisième élément de E. Les opérations de l'algèbre élémentaire $+,\times$ sont des lois internes sur $\mathbb{Z}$. L'élément $a * b$ s'appelle le **produit** de a par b ou, s'il faut être précis, le $*$-**produit** de a par b.

1.2. *Associativité, commutativité.* Soit $*$ une loi interne sur E. On dit que
(a) $*$ est **associative** si $\forall a,b,c \in E \quad (a * b) * c = a * (b * c)$.
(b) $*$ est **commutative** si $\forall a,b \in E \quad a * b = b * a$.

La propriété d'associativité est essentielle. Les lois non associatives ont très peu d'intérêt en mathématiques. Cependant il n'est pas difficile d'en construire. Voici un exemple de loi non associative :

$$* : \begin{array}{ccc} \mathbb{Q}^{\star+} \times \mathbb{Q}^{\star+} & \longrightarrow & \mathbb{Q}^{\star+} \\ (x,y) & \longmapsto & \frac{1}{x+y} \end{array}.$$

En effet, on a

$$(x * y) * z = \frac{1}{\frac{1}{x+y} + z} \quad \text{et} \quad x * (y * z) = \frac{1}{x + \frac{1}{y+z}}$$

(i). Une loi interne est parfois appelé une **opération**.
(ii). Si on utilisait la notation habituelle pour les applications, on devrait plutôt écrire $*(a,b)$.

et les deux quantités en général ne coïncident pas (par exemple pour $x = 1$, $y = 2$, $z = 2$ on trouve $(x*y)*r = 3/7$ et $x*(y*z) = 4/5$). On remarquera que cette loi est commutative et on verra par la suite de nombreux exemples de lois associatives qui ne sont pas commutatives. Cela montre que les propriétés d'associativité et de commutativité sont *indépendantes* — l'une peut être vérifiée sans que l'autre le soit.

1.3. *À quoi sert l'associativité ? la commutativité ?* Si on veut former des produits avec 4 éléments a,b,c et d en utilisant une loi interne quelconque $*$, il y a à priori cinq possibilités :

$$\begin{array}{c|c|c|c|c} (i) & (ii) & (iii) & (iv) & (v) \\ a*((b*c)*d) & a*(b*(c*d)) & (a*b)*(c*d) & (a*(b*c))*d & ((a*b)*c)*d. \end{array}$$

Or si la loi est associative, chacun de ces cinq calculs donne le même résultat. Montrons par exemple que (i)=(iv). On a, posant $\square = b*c$,

$$(i) = a*((b*c)*d) = a*(\square*d) \overset{\text{assoc.}}{=} (a*\square)*d = (a*(b*c))*d = (iv).$$

Puisque le résultat est le même quel que soit le placement des parenthèses il est inutile de les employer et on pourra simplement écrire, sans introduire de confusion, $a*b*c*d$[(i)]. En utilisant une démonstration par récurrence, on montre que la propriété indiquée ci-dessus est valable dans le cas où on forme le produit de n éléments, $n \geq 3$.

Théorème 1.1. *Lorsque la loi $*$ sur E est* associative*, on peut écrire les produits sans qu'il soit nécessaire de placer les parenthèses (autrement dit le résultat ne dépend pas de la manière dont celles-ci sont placées). En particulier, pour $a \in E$ et $n \in \mathbb{N}^\star$, on peut définir*

$$a^n \overset{def}{=} \underbrace{a*a*\cdots*a}_{n\ fois}$$

et on a les relations

$$\begin{cases} a^n * a^m &= a^{n+m} \qquad (n,m \in \mathbb{N}^\star) \\ (a^n)^m &= a^{nm} \qquad (n,m \in \mathbb{N}^\star) \end{cases}$$

Enfin, si, en plus d'être associative, la loi $*$ est aussi commutative *on peut permuter les éléments de $a_1*a_2*\cdots*a_n$ de manière arbitraire sans modifier le résultat.*

Démonstration. Les points non déjà vus se vérifient immédiatement. □

(i). Insistons sur le fait que ceci n'est qu'une simplification de notation. Si on souhaite effectuer le calcul de $a*b*c*d$, il faudra bien décider d'un *parenthésage*.

1.4. *Elément neutre pour une loi interne.* Soit $*$ une loi interne sur un ensemble (non vide) E. On dit qu'un élément $e \in E$ est **élément neutre** (pour $*$) si $\forall a \in E \quad a * e = e * a = a$.

Par exemple 0 est élément neutre de l'addition dans $\mathbb{N}$.

Théorème 1.2. *Une loi interne admet au plus un élément neutre.*

Démonstration. Supposons que e et e' soient éléments neutres de $*$. On a d'un côté $e * e' = e'$ car e est élément neutre et de l'autre $e * e' = e$ car e' est élément neutre. On en déduit $e = e'$. □

1.5. *Définition d'un groupe.* Un ensemble G muni d'une loi interne $*$ est appelé **groupe** si

(a) La loi $*$ est associative et admet un élément neutre, noté e — ou, s'il faut préciser, e_G.

(b) Pour tout $g \in G$, il existe un élément $y \in G$, appelé **élément symétrique** de g tel que $g * y = y * g = e$.

On parle alors du groupe $(G,*)$ ou — lorsqu'il n'y a pas d'ambiguïté sur la loi $*$ — simplement du groupe G. Lorsque la loi $*$ est commutative on dit que $(G,*)$ est un **groupe commutatif** ou encore un **groupe abélien**[(i)]. Lorsque G contient un nombre infini d'éléments, on dit que G est infini. Dans le cas contraire, on dit que G est fini. Le **cardinal** (c'est-à-dire le nombre d'éléments) d'un groupe G, appelé **ordre**, est noté $\mathrm{card}(G)$ ou $o(G)$ ou $|G|$. Dire qu'un groupe est fini est donc équivalent à dire qu'il est d'ordre fini.

1.6. *L'élément symétrique.* On remarquera qu'on ne peut pas parler d'élément symétrique sans disposer au préalable d'un élément neutre. La propriété (b) de la définition d'un groupe requiert seulement l'existence d'un élément symétrique. En réalité un élément symétrique, s'il existe, ne peut être qu'unique. En effet supposons que y et y' soient éléments symétriques de $g \in G$ de sorte que l'on ait à la fois $g * y = y * g = e$ et $g * y' = y' * g = e$. On a

$$\begin{aligned}
(g * y) = e \Rightarrow \quad & y' * (g * y) = y' * e && \text{(on mult. par } y' \text{ à gauche)} \\
\Rightarrow \quad & (y' * g) * y = y' && (* \text{ assoc. et } e \text{ neutre}) \\
\Rightarrow \quad & e * y = y' && (\text{car } y' \text{ sym. de } g.) \\
\Rightarrow \quad & y = y' && (\text{car } e \text{ élt. neutre})
\end{aligned}$$

On a donc montré, en particulier, le théorème suivant.

Théorème 1.3. *Dans un groupe tout élément admet toujours un* unique *élément symétrique.*

(i). L'adjectif abélien est créé en hommage au mathématicien norvégien N. Abel (1802-1829) qui se servit du groupe $\mathbf{S}_n$ (voir 1.7) dans ses travaux sur la résolution des équations polynomiales par radicaux.

L'unique élément symétrique de g est noté g^{-1}. On a

(a) $e^{-1} = e$. L'élément neutre est son propre symétrique.

(b) $(g^{-1})^{-1} = g$.

(c) $(g * g')^{-1} = g'^{-1} * g^{-1}$. Le symétrique d'un produit est le produit *inverse* des symétriques.

(d) Plus généralement

$$(g_1 * g_2 * \cdots * g_n)^{-1} = g_n^{-1} * g_{n-1}^{-1} * \dots g_1^{-1}. \tag{1}$$

En particulier on a $(g^n)^{-1} = (g^{-1})^n$ $(n \in \mathbb{N}^\star)$. On note alors

$$g^{-n} \overset{def}{=} (g^n)^{-1}$$

ce qui permet de définir g^m pour $m \in \mathbb{Z}$ en convenant que $g^0 = e$. Dans ces conditions on a les relations.

$$(g^m)^{m'} = g^{mm'} \quad \text{et} \quad g^m * g^{m'} = g^{m+m'} \qquad (m,m' \in \mathbb{Z}).$$

Chacune des propriétés ci-dessus mérite une démonstration. Elles sont très simples. Le lecteur s'entraînera utilement à les rédiger.

1.7. *Sept exemples de groupes.*

a) $(\mathbf{U},.)$. C'est l'ensemble des nombres complexes de module 1 muni de la *multiplication des nombres complexes*. L'élément neutre est 1. C'est un groupe abélien infini. $(\mathbf{U} = \{z \in \mathbb{C} : |z| = 1\}.)$

b) $(\mathbb{Z},+)$. L'ensemble des entiers relatifs muni de *l'addition (habituelle)*. L'élément neutre est 0, le symétrique d'un élément est son *opposé*. C'est un groupe abélien infini.

c) $(\mathbf{U}_n,.)$ où $n \in \mathbb{N}^\star$. L'ensemble des racines n-ième de l'unité (dans $\mathbb{C}$). L'élément neutre est 1. C'est un groupe abélien fini. Il contient n éléments. On a

$$\mathbf{U}_n = \left\{ e^{\frac{2ik\pi}{n}} : k = 0,1,\dots,n-1 \right\}.$$

d) $(\mathbf{GL}_n(\mathbb{K}),.)$. L'ensemble des matrices inversibles à n lignes et n colonnes à coefficients dans $\mathbb{K} = \mathbb{C},\mathbb{R}$ ou $\mathbb{Q}$, muni de la *multiplication des matrices*. L'élément neutre est la matrice identité. L'élément symétrique est la matrice inverse. C'est un groupe non abélien (dès que $n > 1$) infini.

e) $(\mathbf{S}(\Omega),\circ)$. Ω est un ensemble quelconque non vide et $\mathbf{S}(\Omega)$ est l'ensemble des bijections de Ω sur Ω muni de *la composition des fonctions*. L'élément neutre est l'application identité, le symétrique est la bijection réciproque. C'est un groupe infini lorsque Ω est infini et il a pour cardinal $n!$ lorsque Ω est formé de n éléments. Il est non abélien dès que $\mathrm{card}(\Omega) > 2$. Lorsque $\Omega = \{1,2,\dots,n\}$ on note $\mathbf{S}(\Omega) = \mathbf{S}_n$.

f) (**Is**(P),$\circ$). L'ensemble des isométries affines du plan euclidien P muni de la *composition des fonctions*. C'est un groupe infini non abélien contenant en particulier les translations, les rotations, les réflexions (symétries orthogonales). L'élément neutre est l'application identité.

	f	f^{-1}
(translation de vecteur $\vec{u}$)	$t_{\vec{u}}$	$t_{-\vec{u}}$
(rotation de centre A et d'angle θ)	$r_{A,\theta}$	$r_{A,-\theta}$
(symétrie orthogonale d'axe Δ)	s_Δ	s_Δ

Le cas des symétries orthogonales montre qu'il est tout à fait possible qu'un élément différent du neutre soit égal à son symétrique.

g) **Produit de 2 groupes** Soient $(G_1,*_1)$ et $(G_2,*_2)$ deux groupes. On définit une loi $*$ sur $(G_1 \times G_2)$ par la relation suivante :

$$(g_1,g_2) * (g_1',g_2') = (g_1 *_1 g_1', g_2 *_2 g_2').$$

Alors $(G_1 \times G_2,*)$ est un groupe, appelé le **produit** (ou **produit direct**) de $(G_1,*_1)$ par $(G_2,*_2)$. On a

$$e_{G_1\times G_2} = (e_{G_1},e_{G_2}) \quad \text{et} \quad (g_1,g_2)^{-1} = (g_1^{-1},g_2^{-1}).$$

On peut généraliser la construction en faisant intervenir n groupes au lieu de deux. Lorsque tous les groupes coïncident, on note

$$\underbrace{G \times G \times \cdots \times G}_{n \text{ fois}} = G^n$$

et la loi de G^n est généralement notée comme celle de G

$$(g_1,g_2,\ldots,g_n) * (g_1',g_2',\ldots,g_n') = (g_1 * g_1', g_2 * g_2', \ldots, g_n * g'n).$$

1.8. *Notation additive, notation multiplicative.* Très souvent, pour une simple question de commodité d'écriture, on note toutes les lois de la même manière, généralement avec un point "$\cdot$" — de sorte que l'on écrit $g \cdot g'$ plutôt que $g * g'$, $g \circ g'$ etc, et, comme on le fait couramment avec le produit habituel dans $\mathbb{R}$ ou $\mathbb{C}$, lorsqu'il n'y a pas de confusion possible, on omet aussi le point. On écrit alors gg' plutôt que $g \cdot g'$. On parle dans ce cas (notation point ou notation vide) de **notation multiplicative**. Lorsque le groupe est abélien, on note souvent la loi avec un "$+$". On parle alors de **notation additive**. Dans ce cas, le symétrique d'un élément g n'est plus noté g^{-1} mais $-g$. Ces conventions nécessitent une attention soutenue lorsque plusieurs groupes entrent en jeu et que l'on utilise la *même* notation pour les *différentes* lois de ces groupes. S'agissant ici d'un cours d'introduction à l'algèbre qui s'adresse par définition à des lecteurs peu expérimentés, on essaiera, dans cette première partie, de garder des notations différentes pour des lois différentes.

§ 2. **Sous-Groupes.**

2.1. *Définition et notations.* Soient $(G,*)$ un groupe et H un sous-ensemble *non vide* de G. On dit que H est un **sous-groupe** de G si

(a) Pour tous $x,y \in H$ on a $x * y \in H$

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

Cela signifie que la restriction de $*$ à $H \times H$ donne une loi interne de H et que $(H,*)$ est alors lui-même un groupe. Les deux conditions ci-dessus peuvent être remplacées par

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

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

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 ensemble H est un sous-groupe, 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) $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < (\mathbb{C},+)$.

b) $m\mathbb{Z} < (\mathbb{Z},+)$ où $m\mathbb{Z} = \{mr : r \in \mathbb{Z}\}$ est l'ensemble des (entiers relatifs) multiples de m.

c) $\mathbf{U}_n < \mathbf{U} < (\mathbb{C}^\star,.)$ où $\mathbb{C}^\star = \mathbb{C}/\{0\}$ [(i)].

d) $\mathbf{GL}_n(\mathbb{Q}) < \mathbf{GL}_n(\mathbb{R}) < (\mathbf{GL}_n(\mathbb{C}),\cdot)$.

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

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

(i). D'une manière générale, lorsque $X = \mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $X^\star$ désigne $X/\{0\}$. Dans l'étude des anneaux on utilisera la notation A^* qui désigne en général un ensemble de nature différente.

2.3. *Intersections de sous-groupes.*

Théorème 1.4. *Soient $(G,*)$ un groupe et $\mathcal{F}$ une famille non vide de sous-groupes de G ($\mathcal{F}$ peut contenir un nombre fini ou infini de sous-groupes). Si I est l'intersection de tous les éléments de $\mathcal{F}$, autrement dit $I = \bigcap_{H\in\mathcal{F}} H$ alors I est lui-même un sous-groupe de G.*

Démonstration. I est non vide. En effet, $\forall H \in \mathcal{F}$ on a $e \in H$ donc $e \in \bigcap_{H\in\mathcal{F}} H = I$ et I est non vide. Soient $x,y \in I$, on a $\forall H \in \mathcal{F}$ $x,y \in H$ donc, puisque H est un sous-groupe, $x * y^{-1} \in H$ et par suite $x * y^{-1} \in \bigcap_{H\in\mathcal{F}} H = I$. Cela montre que I est bien un sous groupe. □

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

$$\langle A\rangle = \bigcap_{H\in\mathcal{S}(A)} H$$

où $\mathcal{S}(A)$ 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 et, en vue du Théorème 1.4, la formule ci-dessus est bien définie et $\langle A\rangle$ est bien un sous-groupe de G.

Théorème 1.5. *Le sous-groupe $\langle A\rangle$ est le plus petit sous-groupe de G contenant A. Autrement dit les deux assertions suivantes sont équivalentes*

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

(b) *I vérifie les deux conditions suivantes*

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

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

Démonstration. D'après la définition, on a immédiatement que $\langle A\rangle$ vérifie (i) et (ii). Nous montrons que si I vérifie (i) et (ii) alors $I = \langle A\rangle$. A cause de (ii), on a $I \subset \bigcap_{H\in\mathcal{S}(A)} H = \langle A\rangle$. D'autre part, puisque, d'après (i), I est un sous-groupe contenant A, on a $I \in \mathcal{S}(A)$ et par conséquent $\langle A\rangle = \bigcap_{H\in\mathcal{S}(A)} H \subset I$. 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 1.6. *Soient $(G,*)$ un groupe, A un sous-ensemble non vide de G et $x \in \langle A\rangle$. 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*

$$x = x_1 * x_2 * \cdots * x_n. \tag{2}$$

Démonstration. Nous devons montrer que $I = \langle A \rangle$ où

$$I \stackrel{def}{=} \{x \in G : x \text{ s'écrit comme dans (2)}\}.$$

Pour cela, d'après le Théorème 1.5, il suffit de vérifier que (i) I est un sous-groupe de G contenant A et que (ii) tout sous-groupe de G contenant A contient aussi I. On a d'abord $A \subset I$, il suffit de prendre $n = 1$ dans (2). En particulier I est non vide. Montrons que I est un sous-groupe. Pour cela prenons x et y dans I et vérifions que $x * y^{-1} \in I$. On a

$$\begin{cases} x \in I \Rightarrow & x = x_1 * x_2 * \cdots * x_m \\ y \in I \Rightarrow & y = y_1 * y_2 * \cdots * y_p \end{cases} \quad \text{(Attention, en géné. } m \neq p\text{)}.$$

donc en utilisant la formule 1 (p. 5) 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 $m + p$ élements $\square$ du produit ci-dessus satisfait $\square \in A$ ou $\square^{-1} \in A$ 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 on a donc montré que I est un sous-groupe de G contenant A.

Soit maintenant H un sous-groupe de G contenant A et $x \in I$, $x = x_1 * x_2 * \cdots * x_n \in I$. Etudions l'élément x_i. Il y a deux possibilités:

- Soit $x_i \in A$ qui entraîne $x_i \in H$ puisque, par hypothèse $A \subset H$
- Soit $x_i^{-1} \in A$ ce qui entraîne $x_i^{-1} \in H$ 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, puisque H est un sous-groupe, $x \in H$. On a donc montré $I \subset H$ et cela achève la démonstration que $I = \langle A \rangle$. $\square$

Lorsque une partie (non vide) A vérifie $\langle A \rangle = G$, on dit que A **engendre** G ou bien 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 un ensemble générateur *le plus petit possible* car on peut alors décrire par la formule assez simple (2) 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 simplifier $G = \langle a \rangle$. D'après la formule (2), tout élément de G s'écrit alors

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

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 1.7. *Soit $(G,*)$ un groupe cyclique engendré par $a \in G$. 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*[(i)].

On remarquera que l'ordre d'un élément est égal au à l'ordre (au cardinal) du groupe qu'il engendre et cela justifie l'emploi du même mot *ordre* pour désigner deux concepts différents. Les groupes cycliques sont tous abéliens.

2.7. *Quatre exemples de sous-groupes engendrés.*

a) Dans $(\mathbb{Z},+)$, $\langle m\rangle = m\mathbb{Z}$. 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 $r \in \mathbb{Z}$.

b) Dans $(\mathbb{Z},+)$, $\langle m,n\rangle = pgcd(m,n)\mathbb{Z}$. 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 $\mathbf{pgcd}(m,n)\mathbb{Z}$.

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

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

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

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.

d) 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

$$\varphi(a * b) = \varphi(a) \circ \varphi(b) \qquad (a,b \in G) \tag{3}$$

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**[(i)].

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.

Montrons-le. 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

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

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 1.8. *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

(i). 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.

donc

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

□

Théorème 1.9. *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

$$\begin{array}{rl} & g * g^{-1} = e_G = g^{-1} * g \\ \Longrightarrow & \varphi(g * g^{-1}) = \varphi(e_G) = \varphi(g^{-1} * g) \\ \overset{\text{Th. 1.8}}{\Longrightarrow} & \varphi(g) \circ \varphi(g^{-1})) = e_{G'} = \varphi(g^{-1}) \circ \varphi(g). \end{array}$$

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 1.10. *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 $\varphi(H) \overset{\text{def}}{=} \{\varphi(h) : h \in H\}$ 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 1.8, $e_G \in H \Rightarrow \varphi(e_G) = e_{G'} \in \varphi(H)$. Quant au second point, si $x,y \in \varphi(H)$ alors $x = \varphi(a)$ et $y = \varphi(b)$ avec $a,b \in H$. Donc

$$\begin{array}{rcl} x \circ y^{-1} & = & \varphi(a) \circ [\varphi(b)]^{-1} \\ & \overset{\text{Th. 1.9}}{=} & \varphi(a) \circ \varphi(b^{-1}) = \varphi(a * b^{-1}) \\ & \in & \varphi(H) \quad \text{car } a,b \in H \text{ et } H \leq G, \end{array}$$

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

$$\ker\varphi \overset{def}{=} \{g \in G \ : \ \varphi(g) = e_{G'}\} \tag{4}$$

D'après le Théorème 1.8, on a toujours $\varphi(e_G) = e_{G'}$ donc $e_G \in \ker\varphi$ qui n'est ainsi jamais vide.

Théorème 1.11. *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

$$\begin{array}{rcll} \varphi(x * y^{-1}) & = & \varphi(x) \circ \varphi(y^{-1}) & \text{(déf. d'un morph.)} \\ & = & \varphi(x) \circ [\varphi(y)]^{-1} & \text{(Th. 1.9.)} \\ & = & e_{G'} \circ [e_{G'}]^{-1} & \text{(déf. du noyau.)} \\ & = & e_{G'}. & \end{array}$$

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,

$$\begin{array}{rcll} \varphi(g * x * g^{-1}) & = & \varphi(g) \circ \varphi(x) \circ \varphi(g^{-1}) & \\ & = & \varphi(g) \circ \varphi(x) \circ [\varphi(g)]^{-1} & \text{(par le Th. 1.9)} \\ & = & \varphi(g) \circ e_{G'} \circ [\varphi(g)]^{-1} & \\ & = & \varphi(g) \circ [\varphi(g)]^{-1} & \\ & = & e_{G'}. & \end{array}$$

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

Théorème 1.12. *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

$$\begin{array}{rrcll} & \varphi(x) \circ [\varphi(y)]^{-1} & = & e_{G'} & \\ \Rightarrow & \varphi(x) \circ \varphi(y^{-1}) & = & e_{G'} & \text{(par le Th. 1.9)} \\ \Rightarrow & \varphi(x * y^{-1}) & = & e_{G'} & \\ \Rightarrow & x * y^{-1} & \in & \ker \varphi & \\ \Rightarrow & x * y^{-1} & = & e_G & \text{(car } \ker \varphi = \{e_G\}\text{)} \\ \Rightarrow & x & = & y & \end{array}$$

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

Corollaire. *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 1.13. *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

$$\begin{array}{rrcll} & \varphi(x * y^{-1}) & = & \varphi(x) \circ \varphi(y^{-1}) & \text{(déf. d'un morph.)} \\ & & = & \varphi(x) \circ [\varphi(y)]^{-1} & \text{(Th. 1.9.)} \\ \Rightarrow & \varphi(x * y^{-1}) & \in & W \circ W \subset W & \text{(car } W \leq G\text{.)} \end{array}$$

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

3.5. *Cinq exemples de morphismes.*

a)
$$\exp : \begin{array}{ccc}(\mathbb{R},+) & \longrightarrow & (\mathbb{R}^{\star +},.) \\ x & \longmapsto & \exp x.\end{array}$$
C'est un isomorphisme, on a $\exp^{-1} = \ln$.

b)
$$E_{\mathbb{C}} : \begin{array}{ccc}(\mathbb{R},+) & \longrightarrow & (\mathbf{U},.) \\ x & \longmapsto & \exp ix.\end{array}$$
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)
$$\det : \begin{array}{ccc}\mathbf{GL}_n(\mathbb{K}) & \longrightarrow & (\mathbb{K}^{\star},.) \\ A & \longmapsto & \det A\end{array}$$
On a
$$\begin{array}{rcl}\ker \det & = & \{A \in \mathbf{GL}_n(\mathbb{K}) : \det A = 1\} \\ & \overset{\text{def}}{=} & \mathbf{SL}_n(\mathbb{K}).\end{array}$$

d) 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. Les automorphismes construits de cette manière s'appellent des **automorphismes intérieurs**. 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 (cf. exercices).

e) Soit $(G,*)$ un groupe quelconque et $g \in G$. L'application suivante est un morphisme de groupe.
$$p_g : \begin{array}{ccc}(\mathbb{Z},+) & \longrightarrow & (G,*) \\ m & \longmapsto & g^m.\end{array}$$

(a) Si g est d'ordre infini p_g est injective.
(b) 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 $\ker p_g = d\mathbb{Z}$.

§ 4. **Relation d'équivalence définie par un sous-groupe.**

4.1. *Définition.* Soient $(G,*)$ un groupe et H un sous-groupe de G. On définit la relation R_H sur G par

$$x \,\mathsf{R}_H\, y \overset{def}{\iff} x^{-1} * y \in H.$$

Exemples.

a) Dans $(\mathbb{Z},+)$, prenant $H = m\mathbb{Z}$, on a

$$\begin{array}{rcl} x \,\mathsf{R}_H\, y & \iff & (-x) + y \in m\mathbb{Z} \\ & \iff & y - x \text{ est un multiple de } m \\ & \iff & m \text{ divise } y - x \\ & \iff & x \text{ et } y \text{ ont le même reste dans la division par } m \\ & \overset{\text{def}}{\iff} & x \equiv y \quad [m] \quad (x \text{ est égal à } y \text{ modulo } m). \end{array}$$

b) Dans $(\mathbb{R},+)$, prenant $H = \mathbb{Z}$, on a

$$\begin{array}{rcl} x \,\mathsf{R}_H\, y & \iff & (-x) + y \in \mathbb{Z} \\ & \iff & y - x \text{ est un entier} \\ & \iff & x \text{ et } y \text{ ont la même "partie décimale"} \end{array}$$

Théorème 1.14. *La relation R_H est une relation d'équivalence sur G.*

Rappelons que R_H relation d'équivalence signifie

(a) R_H est **réflexive** $(\forall x \in G,\, x \,\mathsf{R}_H\, x)$,
(b) R_H est **symétrique** $(\forall x,y \in G,\, x \,\mathsf{R}_H\, y \Rightarrow y \,\mathsf{R}_H\, x)$
(c) R_H est **transitive** $(\forall x,y,z \in G,\, (x \,\mathsf{R}_H\, y \text{ et } y \,\mathsf{R}_H\,) \Rightarrow x \,\mathsf{R}_H\, z)$.

Démonstration. Soit $x \in G$. $x \,\mathsf{R}_H\, x$ signifie $x^{-1} * x \in H$ or $x^{-1} * x = e_G$ et $e_G \in H$ car $H \leq G$. Cela montre que R_H est réflexive. Ensuite

$$\begin{array}{rcl} x \,\mathsf{R}_H\, y & \iff & x^{-1} * y \in H \\ & \Longrightarrow & (x^{-1} * y)^{-1} \in H \quad (\text{car } H \text{ sous-groupe}) \\ & \Longrightarrow & y^{-1} * (x^{-1})^{-1} \in H \quad (\text{on utilise (1) p. 5}) \\ & \Longrightarrow & y^{-1} * x \in H \\ & \Longrightarrow & y \,\mathsf{R}_H\, x \end{array}$$

ce qui montre que R_H est symétrique.

Enfin

$$\begin{array}{rcl} \left.\begin{array}{l} x \,\mathsf{R}_H\, y \\ y \,\mathsf{R}_H\, z \end{array}\right\} & \Longrightarrow & \left.\begin{array}{l} x^{-1} * y \in H \\ y^{-1} * z \in H \end{array}\right\} \\ & \Longrightarrow & (x^{-1} * y) * (y^{-1} * z) \in H \\ & \Longrightarrow & x^{-1} * (y * y^{-1}) * z \in H \\ & \Longrightarrow & x^{-1} * e_G * z \in H \\ & \Longrightarrow & x^{-1} * z \in H \\ & \Longrightarrow & x \,\mathsf{R}_H\, z \end{array}$$

donc R_H est transitive et cela achève la preuve qu'elle est une relation d'équivalence. □

La **classe d'équivalence** de $x \in G$, notée $\mathbf{cl}(x)$ ou $\overline{x}$ ou $\dot{x}$ est l'ensemble des éléments de G qui sont en relation avec x

$$\mathbf{cl}(x) = \{g \in G : x \ \mathsf{R}_H \ g\}.$$

Il faut toujours bien garder à l'esprit que les classes d'équivalences sont des ensembles.

Si x et x' sont deux éléments de G, il y a seulement deux possibilités

(a) ou bien $x \,\mathsf{R}_H\, x'$ auquel cas on a $\mathbf{cl}(x) = \mathbf{cl}(x')$,

(b) ou bien $x \neg\, \mathsf{R}_H\, x'$ [(i)] auquel cas on a $\mathbf{cl}(x) \cap \mathbf{cl}(x') = \emptyset$.

Autrement dit, deux classes d'équivalence sont des ensemble égaux ou disjoints. En effet, si $x \,\mathsf{R}_H\, x'$ et $y \in \mathbf{cl}(x)$ alors

$$\begin{cases} x \,\mathsf{R}_H\, x' \\ y \,\mathsf{R}_H\, x \end{cases} \overset{\text{trans.}}{\Longrightarrow} y \,\mathsf{R}_H\, x' \Rightarrow y \in \mathbf{cl}(x),$$

de sorte que $\mathbf{cl}(x) \subset \mathbf{cl}(x')$. On montre de la même manière que $\mathbf{cl}(x') \subset \mathbf{cl}(x)$ d'où $\mathbf{cl}(x) = \mathbf{cl}(x')$.

Réciproquement, si on suppose que $x \neg\, \mathsf{R}_H\, x'$ et $\mathbf{cl}(x) \cap \mathbf{cl}(x') \neq \emptyset$ on obtient une contradiction puisque

$$y \in \mathbf{cl}(x) \cap \mathbf{cl}(x') \Rightarrow \begin{cases} y \,\mathsf{R}_H\, x \\ y \,\mathsf{R}_H\, x' \end{cases} \overset{\text{trans.}}{\Longrightarrow} x \,\mathsf{R}_H\, x' \quad \text{contradiction !}$$

L'ensemble de toutes les classes d'équivalence est noté G/H et est appelé le **quotient** de G par H. Lorsque $y \in \mathbf{cl}(x)$, on dit que y est un **représentant** de $\mathbf{cl}(x)$. On a toujours que x est un représentant de $\mathbf{cl}(x)$ mais, en général, $\mathbf{cl}(x)$ admet beaucoup d'autre représentants.

Nous utiliserons le fait que G est réunion des classes d'équivalence (distinctes)

$$G = \bigcup_{i \in I} \mathbf{cl}(x_i) \quad \text{avec} \quad \mathbf{cl}(x_i) \cap \mathbf{cl}(x_j) = \emptyset \quad \text{pour} \quad i \neq j. \tag{5}$$

Les classes d'équivalence forment une **partition** de G. La formule (5) peut être réécrite comme

$$G = \bigcup_{A \in G/H} A.$$

(i). Le symbole $\neg$ est employé pour indiquer la négation : $x \neg\, \mathsf{R}_H\, x'$ signifie que x n'est pas en relation avec x'.

4.2. *Description des classes d'équivalence (à gauche).* Dans la relation R_H définie ci-dessus on a

$$\begin{aligned}\mathbf{cl}(x) &= \{g \in G : x\,\mathsf{R}_H\, g\}\\ &= \{g \in G : x^{-1} * g \in H\}\\ &= \{g \in G : g \in x * H\}\\ &= x * H\end{aligned}$$

où, par définition, $x * H = \{x * h : h \in H\}$. Ces ensembles $x * H$ s'appellent les classes (d'équivalence à gauche) définies par le sous-groupe H. La formule (5) devient

$$G = \bigcup_{i\in I} x_i * H \quad \text{avec} \quad {x_i}^{-1} * x_j \notin H \quad \text{pour} \quad i \neq j. \tag{6}$$

Exemples

a) Lorsque $(G,*) = (\mathbb{Z},+)$ et $H = 6\mathbb{Z}$,

$$\mathbf{cl}(x) = \overline{x} = x + 6\mathbb{Z} = \{x + 6k : k \in \mathbb{Z}\}.$$

On a par exemple

$$\begin{aligned}\mathbf{cl}(2) = \mathbf{cl}(8) \quad \text{car} \quad 2\,\mathsf{R}_H\,8 \quad (-2)+8 \in 6\mathbb{Z}\\ \mathbf{cl}(0) = \mathbf{cl}(-6) \quad \text{car} \quad 0\,\mathsf{R}_H\,6 \quad (-0)+(-6) \in 6\mathbb{Z}\\ \mathbf{cl}(11) = \mathbf{cl}(29) \quad \text{car} \quad 11\,\mathsf{R}_H\,29 \quad (-11)+29 \in 6\mathbb{Z}.\end{aligned}$$

Ainsi 8 est un représentant de $\mathbf{cl}(2)$, 11 et 29 sont des représentant de $\mathbf{cl}(5)$. On vérifie facilement qu'il y a seulement 6 classes d'équivalences $\mathbf{cl}(0)$, $\mathbf{cl}(1)$, $\mathbf{cl}(2)$, $\mathbf{cl}(3)$, $\mathbf{cl}(4)$, $\mathbf{cl}(5)$ et on a

$$\mathbb{Z} = \mathbf{cl}(0) \cup \mathbf{cl}(1) \cup \mathbf{cl}(2) \cup \mathbf{cl}(3) \cup \mathbf{cl}(4) \cup \mathbf{cl}(5)$$

où, pour $i = 0,1,\ldots,5$,

$\mathbf{cl}(i)$ est l'ensemble des entiers dont le reste dans la division par 6 est égal à i.

D'une manière générale, si $(G,*) = (\mathbb{Z},+)$ et $H = m\mathbb{Z}$ ($m \in \mathbb{Z}^*$), il y a m classes d'équivalence

$$\mathbb{Z} = \mathbf{cl}(0) \cup \mathbf{cl}(1) \cup \mathbf{cl}(2) \cdots \cup \mathbf{cl}(m-1).$$

b) Lorsque $(G,*) = (\mathbb{R},+)$ et $H = \mathbb{Z}$,

$$\mathbf{cl}(x) = \{x + k : k \in \mathbb{Z}\} = x + \mathbb{Z}.$$

On a par exemple

$$\mathbf{cl}(\frac{12}{7}) = \mathbf{cl}(\frac{5}{7}) \quad \text{car} \quad \frac{12}{7}\,\mathsf{R}_H\,\frac{5}{7} \quad \text{car} - \frac{12}{7} + \frac{5}{7} \in \mathbb{Z}.$$

On vérifie que chaque classe admet un et un seul représentant dans [0,1[. DE manière plus précise, l'unique représentant de $x \in \mathbb{R}$ dans [0,1[est donné par $x - \mathsf{E}(x)$ où E désigne la fonction **partie entière**. Par exemple,

$\mathbf{cl}(\pi)$ admet $\pi - 3$ comme représentant. On a donc une bijection entre $\mathbb{R}/\mathbb{Z}$ et $[0,1[$.

La première application des ensembles quotients est données dans le paragraphe suivant. Nous verrons ensuite (§ 5) que, sous réserve que H possède la propriété requise, il possible de définir une loi $\overline{*}$ qui fera de $(G/H,\overline{*})$ un groupe.

4.3. *Le théorème de Lagrange.*

Théorème 1.15 (Lagrange[(i)]). *Soit $(G,*)$ un groupe fini et H un sous-groupe de G. Le cardinal de H divise le cardinal de G, autrement dit $o(H)|o(G)$.*

Démonstration. On considère la relation d'équivalence R_H qui donne une partition de G de la forme

$$G = \bigcup_{i\in I} \mathbf{cl}(x_i).$$

Ici, puisque G est fini, I et, pour chaque $i \in I$, $\mathbf{cl}(x_i)$ sont aussi des ensembles finis. On a alors

$$\operatorname{card}(G) = \sum_{i\in I} \operatorname{card}(\mathbf{cl}(x_i)) \tag{7}$$

car les classes sont des ensembles deux à deux disjoints ($\mathbf{cl}(x_i) \cap \mathbf{cl}(x_j) = \emptyset$ dès que $i \neq j$). Maintenant, nous savons depuis le paragraphe précédent, que $\mathbf{cl}(x_i) = x_i * H$. Nous allons voir que cela implique que $\operatorname{card}(\mathbf{cl}(x_i)) = \operatorname{card}(H)$. Pour démontrer cette égalité, considèrons l'application

$$\phi : \begin{array}{ccc} H & \to & x_i * H \\ h & \mapsto & x_i * h \end{array}$$

et montrons qu'elle est bijective. La bijectivité impliquera que les ensembles de départ et d'arrivée sont de même cardinal. D'abord, ϕ est surjective par définition de l'ensemble $x_i * H$. Elle est aussi injective. En effet $\phi(h_1) = \phi(h_2) \Rightarrow x_1 * h_1 = x_2 * h_2 \Rightarrow (x_i)^{-1} * (x_i * h_1) = (x_i)^{-1} * (x_i * h_2) \Rightarrow h_1 = h_2$. Reportant $\operatorname{card}(\mathbf{cl}(x_i)) = \operatorname{card}(H)$ dans (7) on obtient

$$\operatorname{card}(G) = \sum_{i\in I} \operatorname{card}(H) = \operatorname{card}(H) \times \sum_{i\in I} = \operatorname{card}(H) \times \operatorname{card}(I) \tag{8}$$

d'où il résulte $\operatorname{card}(H) \,|\, \operatorname{card}(G)$ i.e. $o(H) \,|\, o(H)$. □

(i). Joseph-Louis Lagrange (1736-1813) a apporté des contributions fondamentales à de nombreuses branches des mathématiques et de la mécanique. Ses travaux sur le groupe $\mathbf{S}_n$ auquel l'on conduit ses réflexions sur la résolution par radicaux des équations polynomiales en font un précurseur de la théorie des groupes.

Nous avons démontré davantage que ce qu'annonce le théorème. En effet dans (8), $\mathrm{card}(I)$ est le nombre de classes d'équivalence c'est-à-dire le cardinal du quotient G/H. On en déduit le

Corollaire (de la démonstration)**.** *Sous les mêmes hypothèses, on a plus précisément*

$$\mathrm{card}(G) = \mathrm{card}(G/H) \times \mathrm{card}(H)$$

Corollaire. *Dans un groupe fini, l'ordre de tout élément divise l'ordre du groupe.* $[\forall x \in G, o(x)|o(G)]$

Démonstration. Nous savons d'après le Théorème 1.7 (et la remarque qui le suit) que $o(x)$ est égal au cardinal du groupe engendré par x i.e. $o(x) = \mathrm{card}(\langle x\rangle)$. En appliquant le theorème de Lagrange avec $H = \langle x\rangle$ on obtient que $o(x) \,|\, o(G)$. □

4.4. *Application à la caractérisation des groupes d'ordre premier.* Soit $(G,*)$ un groupe fini contenant p éléments avec p premier (> 1). D'après le second corollaire, si $x \in G$ alors $o(x) \,|\, o(G)$ c'est-à-dire ici $o(x) \,|\, p$. Puisque p est premier, on a nécessairement $o(x) = 1$ ou $o(x) = p$. dans le premier cas $x = e$, et dans le second, $\langle x\rangle$ est un sous-groupe de G qui contient le même nombre d'élément que G en sorte que $\langle x\rangle = G$. On a ainsi démontré le

Théorème 1.16. *Tout groupe d'ordre premier $p > 1$ est cyclique et il est engendré par n'importe lequel de ses éléments différents du neutre.* $[\forall x \in G/\{e\}, G = \langle x\rangle]$

En particulier, un groupe fini d'ordre premier n'admet aucun sous-groupe propre.

§ 5. **Groupes quotients.**

5.1. *Sous-groupes distingués.* Soit $(G,*)$ un groupe et H un sous-groupe de G. On dit que H est **distingué** dans G [(i)] (ou **normal** dans G, ou encore **invariant**) s'il vérifie la propriété suivante

$$\forall x \in G \quad x^{-1} * H * x \subset H, \tag{9}$$

c'est-à-dire $\forall x \in G, \forall h \in H, x^{-1}*h*x \in H$. L'élément $x^{-1}*h*x$ s'appelle le **conjugué** de h par x. Un sous-groupe H de G est distingué si les conjugués de ses éléments appartiennent encore à H. On dit parfois que H est *fermé* pour la conjugaison. En réalité la condition (9) est équivalente à

$$\forall x \in G \quad x^{-1} * H * x = H, \tag{10}$$

(i). Lorsqu'il n'y a pas de confusion possible sur le groupe G, on dit seulement que H est distingué. Lorsque, dans le contexte, H est à la fois sous-groupe de G_1 et de G_2, il faut préciser car H peut être distingué dans G_1 et ne pas l'être dans G_2.

qui est en apparence plus forte. Montrons-le. Prenons un élément x_0 quelconque de G et appliquons (9) avec $x = x_0$ puis avec $x = x_0^{-1}$, il vient

$$x_0^{-1} * H * x_0 \subset H \tag{11}$$

$$x_0 * H * x_0^{-1} \subset H. \tag{12}$$

En multipliant à droite par x_0^{-1} et à gauche par x_0, la formule (12) donne

$$x_0^{-1} * (x_0 * H * x_0^{-1}) * x_0 \subset x_0^{-1} * H * x_0 \Rightarrow H \subset x_0^{-1} * H * x_0.$$

Comme, par (11), nous savons déjà $x_0^{-1} * H * x_0 \subset H$, nous avons $x_0^{-1} * H * x_0 = H$. Le même raisonnement est valide avec n'importe quel $x_0 \in G$ et on obtient ainsi (10).

La notation $H \triangleleft G$ signifie que H est un sous-groupe distingué de G. Lorsqu'on n'exclut pas que H soit égal à G on écrit $H \trianglelefteq G$

5.2. *Trois exemples de sous-groupes distingués.*

a) Si $(G,*)$ est abélien alors n'importe lequel de ses sous-groupes est distingué dans G.

b) Si φ est un morphisme de $(G,*)$ dans $(T,\circ)$ alors $\ker\varphi$ est un sous-groupe distingué de G. [$\ker\varphi \trianglelefteq G$.]

c) Soit $H = \{\lambda Id : \lambda \in \mathbb{R}^\star\}$ où Id est la matrice identité dans $\mathbf{GL}_n(\mathbb{R})$. On a $H \trianglelefteq \mathbf{GL}_n(\mathbb{R})$.

5.3. *Compatibilité de R_H avec la loi de G lorsque $H \trianglelefteq G$.* Soit $(G,*)$ un groupe et $H \trianglelefteq G$. La relation d'équivalence R_H définie par le sous-groupe distingué H a la propriété remarquable d'être **compatible** avec la loi. Cela signifie que, pour $g_1,g_2,r_1,r_2 \in G$,

$$\left.\begin{array}{l} g_1 \,\mathsf{R}_H\, g_2 \\ r_1 \,\mathsf{R}_H\, r_2 \end{array}\right\} \Rightarrow (g_1 * r_1) \;\mathsf{R}_H\; (g_2 * r_2).$$

En effet, $g_1 \,\mathsf{R}_H\, g_2 \Rightarrow g_1^{-1} * g_2 \in H \Rightarrow g_1^{-1} = h * g_2^{-1}$ pour un certain $h \in H$. De même $r_1 \,\mathsf{R}_H\, r_2 \Rightarrow r_1^{-1} = h' * r_2^{-1}$ pour un certain $h' \in H$. Ensuite on a

$$\begin{array}{rcl} (g_1 * r_1)^{-1} * (g_2 * r_2) & = & r_1^{-1} * g_1^{-1} * g_2 * r_2 \\ & = & (h' * r_2^{-1}) * (h * g_2^{-1}) * g_2 * r_2 \\ & = & h' * r_2^{-1} * h * r_2 \\ & = & h' * (\text{un élément de } H) \;\; (\text{car } H \text{ est distingué}) \end{array}$$

Etant le produit de deux éléments du sous-groupe H, $(g_1 * r_1)^{-1} * (g_2 * r_2)$ appartient aussi à H et cela montre que $g_1 * r_1 \,\mathsf{R}_H\, g_2 * r_2$.

On peut montrer que, réciproquement, toutes les relations d'équivalence sur G qui sont compatibles avec la loi de G sont de la forme $\mathsf{R} = \mathsf{R}_H$ avec $H \trianglelefteq G$.

5.4. *Loi interne sur l'ensemble des classes. Groupe quotient. Projection canonique.* Soit $(G,*)$ un groupe et H un sous-groupe distingué de G. On rappelle que G/H désigne l'ensemble des classes d'équivalence de R_H. On peut définir une loi $\overline{*}$ sur G/H comme suit

$$(13)\quad \overline{*}\ : \begin{array}{ccc} G/H \times G/H & \longrightarrow & G/H \\ (\mathtt{C}_1\,,\mathtt{C}_2) & \longmapsto & \mathbf{cl}\left(\begin{array}{c}\text{n'importe quel}\\ \text{représentant de } \mathtt{C}_1\end{array} * \begin{array}{c}\text{n'importe quel}\\ \text{représentant de } \mathtt{C}_2\end{array}\right)\end{array}$$

Cette définition présente une difficulté évidente. L'élément $\mathtt{C}_1 * \mathtt{C}_2$ doit avoir une valeur et une seule alors que, à priori, la définition ci-dessus lui en attribue $\mathrm{card}(\mathtt{C}_1) \times \mathrm{card}(\mathtt{C}_2)$ [(i)] Pour que notre définition soit acceptable — on dit consistante — nous devons montrer qu'en réalité le choix des représentants n'influe en rien sur la valeur trouvée. Autrement dit, nous devons vérifier que

$$\left.\begin{array}{rcl} x_1, x_1' & \in & \mathtt{C}_1 \\ x_2, x_2' & \in & \mathtt{C}_2 \end{array}\right\} \Rightarrow \mathbf{cl}(x_1 * x_2) = \mathbf{cl}(x_1' * x_2').$$

Il en est bien ainsi. En effet, en utilisant la compatibilité pour la deuxième implication, on a

$$\left.\begin{array}{l} x_1, x_1' \in \mathtt{C}_1 \\ x_2, x_2' \in \mathtt{C}_2 \end{array}\right\} \Rightarrow \left\{\begin{array}{ll} x_1\,\mathsf{R}_H\,x_1' & \Rightarrow\ (x_1 * x_2)\,\mathsf{R}_H(x_1' * x_2') \\ x_2\,\mathsf{R}_H\,x_2' & \Rightarrow\ \mathbf{cl}(x_1 * x_2) = \mathbf{cl}(x_1' * x_2'). \end{array}\right.$$

La loi $\overline{*}$ est par conséquent bien définie et c'est une loi interne sur G/H.

Remarquons qu'on a toujours

$$(14)\qquad \mathbf{cl}(x_1)\,\overline{*}\,\mathbf{cl}(x_2) = \mathbf{cl}(x_1 * x_2) \qquad (x_2,x_2 \in G).$$

C'est une conséquence de la définition dans laquelle on prend $\mathtt{C}_1 = \mathbf{cl}(x_1)$, $\mathtt{C}_2 = \mathbf{cl}(x_2)$ et dans laquelle on choisit x_1 comme représentant de $\mathtt{C}_1$ et x_2 comme représentant de $\mathtt{C}_2$. En particulier, *si x_1 est représentant de $\mathtt{C}_1$ et x_2 est représentant de $\mathtt{C}_2$ alors $x_2 * x_2$ est représentant de $\mathtt{C}_1\,\overline{*}\,\mathtt{C}_2$.*

Théorème 1.17. *Soit $(G,*)$ un groupe et $H \trianglelefteq G$, $(G/H,\overline{*})$ est un groupe.*

Démonstration. Nous avons déjà vu que $\overline{*}$ est une loi interne. L'associativité provient immédiatement de celle de $*$ [(ii)] Montrons que $\mathbf{cl}(e)$ est élément neutre pour $\overline{*}$. Soient $\mathtt{C} \in G/H$ et x un représentant de $\mathtt{C}$. On a

$$\mathtt{C}\,\overline{*}\,\mathbf{cl}(e) = \mathbf{cl}(x)\,\overline{*}\,\mathbf{cl}(e) = \mathbf{cl}(x * e) = \mathbf{cl}(x) = \mathtt{C}.$$

De même on montre que $\mathbf{cl}(e)\,\overline{*}\,\mathtt{C} = \mathtt{C}$ et cela prouve que $\mathbf{cl}(e)$ est élément neutre de $\overline{*}$. Il reste à établir que tout élément de G/H admet un élément

(i). Le nombre $\mathrm{card}(\mathtt{C}_1)$ correspond au nombre de choix possibles pour le représentant de $\mathtt{C}_1$ et $\mathrm{card}(\mathtt{C}_2)$ au nombre de choix possibles pour le représentant de $\mathtt{C}_2$.

(ii). En effet, si $\mathtt{C}_1$,$\mathtt{C}_2$ et $\mathtt{C}_3$ sont trois éléments de G/H de représentants respectifs x_2,x_2 et x_3, on a $(\mathtt{C}_1\,\overline{*}\,\mathtt{C}_2)\,\overline{*}\,\mathtt{C}_3 = \mathbf{cl}(x_1 * x_2)\,\overline{*}\,\mathbf{cl}(x_3) = \mathbf{cl}((x_1 * x_2) * x_3) = \mathbf{cl}(x_1 * (x_2 * x_3)) = \mathbf{cl}(x_1)\,\overline{*}\,\mathbf{cl}(x_2 * x_3) = \mathtt{C}_1\,\overline{*}(\mathtt{C}_2\,\overline{*}\,\mathtt{C}_3)$.

symétrique pour $\overline{*}$. Prenons $\mathtt{C}_1 \in G/H$ et x un représentant de $\mathtt{C}_1$ et posons $\mathtt{C}_2 = \mathbf{cl}(x^{-1})$. On a

$$\mathtt{C}_1 \,\overline{*}\, \mathtt{C}_2 = \mathbf{cl}(x) \,\overline{*}\, \mathbf{cl}(x^{-1}) = \mathbf{cl}(x * x^{-1}) = \mathbf{cl}(e) = \text{neutre de } \overline{*}.$$

On montre de même que $\mathtt{C}_2 \,\overline{*}\, \mathtt{C}_1 = \mathbf{cl}(e)$ ce qui prouve que $\mathtt{C}_2$ est élément symétrique de $\mathtt{C}_1$ et cela conclut la démonstration que G/H est un groupe. □

On retiendra que

$$e_{G/H} = \mathbf{cl}(e_G)$$

et

$$[\mathbf{cl}(x)]^{-1} = \mathbf{cl}(x^{-1}) \qquad (x \in G).$$

De manière générale on a

$$\mathbf{cl}(x^m) = [\mathbf{cl}(x)]^m \qquad x \in G, m \in \mathbb{Z}.$$

Théorème 1.18. *Soit $(G,*)$ un groupe et $H \trianglelefteq G$. L'application s définie par*

$$s : \begin{array}{ccc} (G,*) & \longrightarrow & (G/H,\overline{*}) \\ x & \longmapsto & \mathbf{cl}(x). \end{array}$$

est un morphisme de groupe. Il est surjectif. Son noyau est égal à H.

Démonstration. Notons d'abord que s est surjective par définition des classes: toute classe $\mathtt{C} \in G/H$ admet au moins un représentant i.e. $\mathtt{C} = \mathbf{cl}(x) = s(x)$. Montrons que s est un morphisme. Pour $x,y \in G$ on a $s(x*y) = \mathbf{cl}(x*y) = \mathbf{cl}(x) * \mathbf{cl}(y) = s(x) * s(y)$. Enfin, $x \in \ker s \iff s(x) = e_{G/H} = \mathbf{cl}(e) \iff \mathbf{cl}(x) = \mathbf{cl}(e_G) \iff e \,\mathsf{R}_H\, x \iff x \in H$ et cela prouve $\ker s = H$. □

Le morphisme s s'appelle la **surjection** (ou **projection**) **canonique** de G sur[(i)] G/H. On note parfois $s = s_H$.

5.5. *Le groupe $\mathbb{Z}/n\mathbb{Z}$.* Le groupe Z/nZ. Soit $n \in \mathbb{N}^\star$. Puisque $(\mathbb{Z},+)$ est un groupe commutatif tous ses sous-groupes sont distingués et $n\mathbb{Z} < \mathbb{Z}$. Le groupe $(\mathbb{Z}/n\mathbb{Z},\overline{+})$ est un groupe commutatif d'ordre n

$$\mathbb{Z}/n\mathbb{Z} = \{\mathbf{cl}(0),\mathbf{cl}(l).,...,\mathbf{cl}(n-l)\}.$$

On notera $\mathbf{cl}(i) = \overline{i}$. Formons par exemple la table de $\mathbb{Z}/5\mathbb{Z}$.

(i). La préposition *sur* est souvent (pas toujours) employée devant l'ensemble d'arrivée lorsque on considère une surjection. Si $f : A \longrightarrow B$ est surjective on dit que f est une surjection de A *sur* B. La même convention vaut pour les bijections qui sont des surjections particulières.

$\overline{+}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$

(Calculs bruts)

$\overline{+}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

(Calculs simplifiés)

Les termes nuls permettent d'identifier les symétriques de chaque élément. Par exemple, le symétrique de $\overline{1}$ est $\overline{4}$ i.e. $= \overline{4} = \overline{-1}$. (i)

Le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique, engendré par l'élément 1. En effet

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0},\overline{1},\overline{1}+\overline{1},\ldots,\underbrace{\overline{1+\cdots+1}}_{n-1 \text{ fois}}) = \langle 1\rangle\,.$$

En général, un élément quelconque (non nul) n'engendre pas $\mathbb{Z}/n\mathbb{Z}$. Par exemple, dans $\mathbb{Z}/6\mathbb{Z}$ on a $\langle\overline{3}\rangle = \{\overline{0},\overline{3}\}$ et $\langle\overline{2}\rangle = \{\overline{0},\overline{2},\overline{4}\}$. Le théorème suivant donne une condition nécessaire et suffisante pour qu'un élément donné engendre $\mathbb{Z}/n\mathbb{Z}$.

Théorème 1.19. *Soit $n > 1$ et $a \in \mathbb{N}$. Pour que $\overline{a} = \mathbf{cl}(a)$ engendre $\mathbb{Z}/n\mathbb{Z}$ (i.e. $\mathbb{Z}/n\mathbb{Z} = \langle\overline{a}\rangle$) il faut et il suffit que a et n soient premiers entre eux.*

Démonstration. i) Supposons que $\mathbb{Z}/n\mathbb{Z}$ soit engendré par $\overline{a}$. Puisque $n = \mathrm{card}(\mathbb{Z}/n\mathbb{Z}) = \mathrm{card}(\langle\overline{a}\rangle)$ on a $o(\overline{a}) = n$ et

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0},\overline{a},\overline{a}+\overline{a},\ldots,\underbrace{\overline{a}+\overline{a}+\cdots+\overline{a}}_{n-1 \text{ fois}}\} = \{\overline{0},\overline{a},\overline{2a},\ldots,\overline{(n-l)a}\}.$$

Il existe donc $i \in \{0,\ldots,n-l\}$ (ii) tel que $\overline{ia} = \overline{1}$ soit encore $ia = 1 + kn$ avec $k \in \mathbb{Z}$ ce qui implique que $ia - kn = 1$ et, par le théorème de Bezout, que a et n sont premiers entre eux.

ii) Réciproquement, si a et n sont premiers entre eux alors, toujours par le théorème de Bezout, il existe des entiers u et v tels que $au+nv = 1 \implies \overline{ua} = \overline{1}$

$$\implies \underbrace{\overline{a}+\overline{a}+\cdots+\overline{a}}_{u \text{ fois}} = \overline{1} \implies \overline{1} \subset \langle\overline{a}\rangle \implies \langle\overline{1}\rangle \subset \langle\overline{a}\rangle$$

et donc puisque $\langle\overline{1}\rangle = \mathbb{Z}/n\mathbb{Z}$, on a $\mathbb{Z}/n\mathbb{Z} \subset \langle\overline{a}\rangle$. Comme l'inclusion inverse est évidente on en déduit $\mathbb{Z}/n\mathbb{Z} = \langle\overline{a}\rangle$. □

(i). La relation $-\overline{1} = \overline{-1}$ est un cas particulier de la relation $[\mathbf{cl}(x)]^{-1} = \mathbf{cl}(x^{-1})$. D'une manière générale dans, $\mathbb{Z}/n\mathbb{Z}$, on a toujours $-\overline{k} = \overline{-k}$, on peut intervertir les symboles $-$ et $\overline{\cdot}$.

(ii). En réalité, $i \in \{1,\ldots,n-l\}$ car le cas $i = 0$ ne peut jamais se produire.

5.6. *Théorème d'isomorphisme.*

Théorème 1.20. *Soient G_1 et G_2 deux groupes*(i) *et ϕ un homomorphisme de G_1 dans G_2. Il existe un* isomorphisme γ *de $G_1/\ker\phi$ sur $\phi(G_1)$ tel que $\phi = \gamma \circ s$ où s est la surjection canonique de G_1 sur $G_1/\ker\phi$. On a donc*

$$G_1/\ker\phi \simeq \phi(G_1).$$

Le théorème dit essentiellement que les projection canoniques permettent de *factoriser* les morphismes de groupes avec la projection canonique et un isomorphisme. La figure 1 schématise cette propriété.

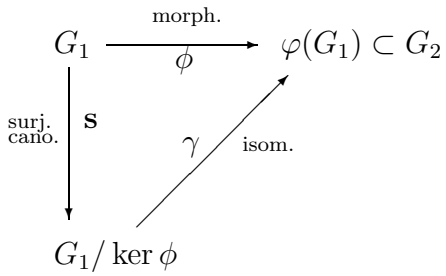

FIG. 1. *Schéma du théorème d'isomorphisme $\phi = \gamma \circ \mathbf{s}$*

Démonstration. Nous définirons γ comme suit

$$\gamma : \begin{array}{ccc} G_1/\ker\phi & \longrightarrow & \phi(G_1) \subset G_2 \\ \mathtt{C} & \longmapsto & \phi\left(\begin{array}{c}\text{n'importe quel}\\ \text{représentant de } \mathtt{C}\end{array}\right). \end{array}$$

Vérifions d'abord que cette définition est consistante c'est-à-dire que l'on peut effectivement utiliser n'importe quel représentant de $\mathtt{C}$ sans modifier le résultat. Prenons deux représentants x_l et x_2 de $\mathtt{C}$. On a $x_1 \,\mathsf{R}_{\ker\phi}\, x_2$ i.e. $x_1^{-1} * x_2 \in \ker\phi \implies x_2 = x_1 * h$ avec $h \in \ker\phi$ d'où $\phi(x_2) = \phi(x_1 * h) = \phi(x_1) * \phi(h) = \phi(x_1)$ car $h \in \ker\phi$. Deux représentants quelconques de $\mathtt{C}$ donnent le même résultat et notre définition de s est consistante. L'application γ vérifie $\gamma(\mathbf{cl}(x)) = \phi(x)$ car x est représentant de $\mathbf{cl}(x)$. Ceci montre que tous les éléments de $\phi(G_1)$ (et seulement ceux-là) sont dans l'ensemble image de γ qui est par conséquent une surjection de $G_1/\ker\phi$ sur $\phi(G_1)$.

(i). Les lois (différentes) des groupes G_1 et G_2 seront ici représentées par le même symbole $*$.

Montrons que γ est un morphisme. Prenons $\mathtt{C}_1$ et $\mathtt{C}_2$ deux éléments de $G_1/\ker\phi$ et x_1 un représentant de $\mathtt{C}_1$, x_2 un représentant de $\mathtt{C}_2$. On a

$$\begin{aligned}
\gamma(\mathtt{C}_1 \mathbin{\overline{*}} \mathtt{C}_2) &= \phi\left(\begin{array}{l}\text{n'importe quel}\\ \text{représentant de } \mathtt{C}_1 \mathbin{\overline{*}} \mathtt{C}_2\end{array}\right)\\
&= \phi(x_1 * x_2) \quad (\text{car } x_1 * x_2 \text{ est un représentant de } \mathtt{C}_1 \mathbin{\overline{*}} \mathtt{C}_2)\\
&= \phi(x_1) * \phi(x_2)\\
&= \gamma(\mathbf{cl}(x_1)) * \gamma(\mathbf{cl}(x_2))\\
&= \gamma(\mathtt{C}_1) \mathbin{\overline{*}} \gamma(\mathtt{C}_2)
\end{aligned}$$

Montrons maintenant que γ est injective.

$$\begin{aligned}
\mathtt{C} \in \ker\gamma &\Longrightarrow \gamma(\mathtt{C}) = e_{G_2}\\
&\Longrightarrow \phi(x) = e_{G_2} \qquad (\text{ où } x \text{ est un représentant quelconque de } \mathtt{C})\\
&\Longrightarrow x \in \ker\phi\\
&\Longrightarrow e_{G_1}\, \mathsf{R}_{\ker\phi}\, x\\
&\Longrightarrow \mathbf{cl}(x) = \mathbf{cl}(e_{G_1})\\
&\Longrightarrow \mathtt{C} = \text{neutre de } G/\ker\phi.
\end{aligned}$$

Ceci montre que $\ker\gamma = \{e_{G/\ker\phi}\}$ donc que γ est injective. On a ainsi établi que γ est un isomorphisme de $G/\ker\phi$ sur $\phi(G_1)$. Il reste à vérifier que $\phi = \gamma \circ s$. C'est immédiat car, pour $x \in G_1$, $\gamma(s(x)) = \gamma(\mathbf{cl}(x)) = \phi(x)$. □

5.7. *Trois exemples d'application du théorème d'isomorphisme.*

a) Considérons le morphisme

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

Nous avons vu (3.5) que $\ker\exp = 2\pi\mathbb{Z} = \{2k\pi \,:\, k \in \mathbb{Z}\}$. De plus exp est surjective car tout nombre complexe z de $\mathbf{U}$ s'écrit $z = \exp i\theta$ avec $\theta \in \mathbb{R}$ [(i)]. On a donc $\exp(\mathbb{R}) = \mathbf{U}$. Le théorème d'isomorphisme donne $\mathbb{R}/2\pi\mathbb{Z} \simeq \exp(\mathbb{R})$, soit

$$\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbf{U}.$$

b) Considérons le morphisme

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

Nous avons vu (3.5) que $\ker\det = \mathbf{SL}_n(\mathbb{K})$ et det est surjectif — $\forall\lambda \in \mathbb{K}^\star$, $\exists A \in \mathbf{GL}_n(\mathbb{K})$ tel que $\det(A) = \lambda$ (prendre A avec $A_{11} = \lambda$ puis tous les autres éléments de la diagonale égaux à 1, puis tous les éléments restant nuls) — donc $\det(\mathbf{GL}_n(\mathbb{K})) = \mathbb{K}^\star$. Le théorème d'isomorphisme donne $\mathbf{GL}_n(\mathbb{K})/\ker\det \simeq \det(\mathbf{GL}_n(\mathbb{K}))$ c'est-à-dire

$$\mathbf{GL}_n(\mathbb{K})/\mathbf{SL}_n(\mathbb{K}) \simeq \mathbb{K}^\star.$$

(i). Cette propriété est très loin d'être évidente. On la démontre en analyse par une étude très fine de la série définissant la fonction exponentielle.

c) Soit $(G,*)$ un groupe cyclique d'ordre n i.e. $G = \langle a \rangle$ avec $o(a) = n$ de sorte que $G = \{e,a,a^2,...,a^{n-1}\}$. Considérons le morphisme

$$p_a : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ m & \longmapsto & a^m. \end{array}$$

Nous savons que p_a est surjectif (parce que a est générateur de G) et avons déjà vu dans (3.5) que $\ker p_a = n\mathbb{Z}$ de sorte que le théorème d'isomorphisme donne $\mathbb{Z}/\ker p_a \simeq p_a(G)$ soit

$$\mathbb{Z}/n\mathbb{Z} \simeq G.$$

On a démontré que *tout groupe cyclique fini d'ordre n est isomorphe à* $\mathbb{Z}/n\mathbb{Z}$. En particulier $\mathbf{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$.

(**fin de la première partie**)

LABORATOIRE DE MATHÉMATIQUES E. PICARD, UNIVERSITÉ PAUL SABATIER 31062 TOULOUSE CEDEX 4 FRANCE.

E-mail address: calvi@picard.ups-tlse.fr