Licence de mathématique
Université Paris-Saclay

Groupes et géométrie

N. Perrin

Université de Versailles Saint-Quentin-en-Yvelines
Année 2019-2020

Table des matières

Première partie .

Groupes

1. Morphismes de groupes, sous-groupes

Dans ce premier chapitre, nous faisons des rappels sur les groupes, leurs sous-groupes et les morphismes de groupes.

1.1. La notion de groupe

Définition 1.1.1 (i) Un **groupe** est la donnée d'une paire $(G, \star)$ où G est un ensemble et $\star : G \times G \to G$ est une **loi de composition** telle que les trois propriétés suivantes sont satisfaites :

(Unité) il existe un élément $e \in G$ tel que $e \star g = g \star e = g$ pour tout $g \in G$;

(Inverse) pour tout $g \in G$, il existe $h \in G$ tel que $g \star h = h \star g = e$;

(Associativité) pour tout $(g, h, k) \in G^3$, on a $(g \star h) \star k = g \star (h \star k)$.

(ii) Si de plus on a $g \star h = h \star g$ pour tout $(g, h) \in G^2$, on dire que le groupe G es **commutatif** ou encore **abelien**.

(iii) Le cardinal $|G|$ (fini ou infini) d'un groupe G est appelé **ordre du groupe**.

Remarque 1.1.2 Un groupe n'est jamais vide

Lemme 1.1.3 Soit G un groupe.

(i) L'élément unité e du groupe tel que $e \star g = g \star e = g$ pour tout $g \in G$ est unique.

(ii) Pour tout $g \in G$, l'élémnt $h \in G$ tel que $g \star h = h \star g = e$ est unique. □

Preuve. 1. Soient e et e' des éléments unités. Alors on a $e' = e \star e' = e$.

2. Soient h et h' deux éléments tel que $g \star h = h \star g = e$ et $g \star h' = h' \star g = e$. Alors on a $h' = h' \star e = h' \star (g \star h) = (h' \star g) \star h = e \star h = h$. ■

Définition 1.1.4 Soit G un groupe et $g \in G$. L'unique élémnt $h \in G$ tel que $g \star h = h \star g = e$ est appelé **inverse** de g dans G.

Notation 1.1.5 On utilisera essentiellement deux notations pour la loi de composition d'un groupe :

(i) la **notation multiplicative** dans laquelle le produit $g \star h$ est noté gh et l'unité e est notée 1. L'inverse de g est alors noté g^{-1}. C'est la notation que nous utiliserons par défaut. En particulier dans cette notation, on ne suppose pas le groupe commutatif, donc a priori, on a $gh \neq hg$.

(ii) la **notation additive** ne sera utilisée **que si le groupe G est commutatif**. Le produit $g \star h$ est noté $g + h$ et l'unité e est notée 0. L'inverse de g est alors noté $-g$. Dans cette notation, on a toujours $g + h = h + g$ donc le groupe est commutatif.

Lemme 1.1.6 Soit G un groupe.

(i) Pour $g \in G$, on a $(g^{-1})^{-1} = g$.

(ii) Pour $g, h \in G$, on a $(gh)^{-1} = h^{-1}g^{-1}$.

(iii) Si $(g_i)_{i\in[1,n]}$ sont des éléments de G, on a $(g_1 \cdots g_n)^{-1} = g_n^{-1} \cdots g_1^{-1}$. □

Preuve. 1. En effet, on a $gg^{-1} = g^{-1}g = 1$ donc $(g^{-1})^{-1} = g$.

2. On calcule $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1}) = gg^{-1}) = 1$ et $(h^{-1}g^{-1})(gh) = h^{-1})hg^{-1}g)h = h^{-1})h = 1$.

3. Par récurrence en utilisant 1. ■

Corollaire 1.1.7 L'application $f : G \to G$, $g \mapsto g^{-1}$ est bijective.

Preuve. Il suffit de montrer que f est son propre inverse. Mais pour tout $g \in G$, on a $(f \circ f)(g) = f(f(g)) = f(g^{-1}) = (g^{-1})^{-1} = g$. ■

Exemple 1.1.8 (i) Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la loi $+$ sont des groupes commutatifs.

(ii) Les ensembles $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$ munis de la loi $\times$ sont des groupes commutatifs.

(iii) L'ensemble $\mathrm{GL}_n(\mathbb{R})$ des matrices réelles inversibles de taille n est un groupe pour la multiplication des matrices. Il est non commutatif si et seulement si $n \geq 2$.

(iv) L'ensemble $\mathrm{GL}(V)$ des endomorphismes bijectifs d'un $\mathbb{R}-$espace vectoriel V est un groupe pour la composition. Il est non commutatif si et seulement si $\dim V \geq 2$.

(v) L'ensemble $\mathfrak{S}_n$ des permutations de l'ensemble $[1, n]$ est un groupe pour la composition. Son ordre est $n!$. Il est non commutatif si et seulement si $n \geq 3$.

(vi) L'ensemble des rotations planes de centre O forme un groupe pour la composition. Il est commutatif.

(vii) Soit E un ensemble. L'ensemble $\mathfrak{S}(E)$ des bijections de E dans E est un groupe pour la composition.

Notation 1.1.9 Soit G un groupe et $g \in G$.

(i) En notation multiplicative, on définit g^m pour $m \in \mathbb{Z}$ de la manière suivante :

$$g^m = \begin{cases} g \cdot g \cdots g & \text{produit de } m \text{ fois } g & \text{si } m \geq 1 \\ 1 & \text{produit vide} & \text{si } m = 0 \\ g^{-1} \cdot g^{-1} \cdots g^{-1} & \text{produit de } |m| = -m \text{ fois } g^{-1} & \text{si } m \leq -1. \end{cases}$$

(ii) En notation additive, on définit mg pour $m \in \mathbb{Z}$ de la manière suivante :

$$mg = \begin{cases} g + g + \cdots + g & \text{somme de } m \text{ fois } g & \text{si } m \geq 1 \\ 0 & \text{somme vide} & \text{si } m = 0 \\ (-g) + (-g) + \cdots (-g) & \text{somme de } |m| = -m \text{ fois } -g & \text{si } m \leq -1. \end{cases}$$

1.2. Morphisme de groupes

Définition 1.2.1 Soient G et G' deux groupes.

(i) Un **morphisme de groupes** de G dans G' est une application $\varphi : G \to G'$ telle que $\varphi(gh) = \varphi(g)\varphi(h)$ pour tout $(g, h) \in G^2$. L'ensemble des morphisme de groupes de G dans G' est note $\mathrm{Hom}(G, G')$.

(ii) Un morphisme de groupe $\varphi : G \to G'$ est appelé **isomorphisme de groupes** si φ est bijective. L'ensemble des morphisme de groupes de G dans G' est note $\mathrm{Isom}(G, G')$.

(iii) Lorsque G' est égal à G, un morphisme de groupe est appelé **endomorphisme de groupes**. L'ensemble des endomorphismes de groupes de G dans lui-même est note $\mathrm{End}(G)$.

(iv) Lorsque G' est égal à G, un isomorphisme de groupe est appelé **automorphisme de groupes**. L'ensemble des automorphismes de groupes de G dans lui-même est note $\mathrm{Aut}(G)$.

Remarque 1.2.2 On utilise parfois **homomorphisme de groupes** à la place de morphisme de groupes.

Lemme 1.2.3 Soit $\varphi : G \to G'$ un isomorphisme de groupes et soit $\varphi^{-1} : G' \to G$ l'inverse de φ. Alors φ^{-1} est un morphisme de groupes. □

Preuve. Soient $x, y \in G'$, on veut montrer que $\varphi^{-1}(xy) = \varphi^{-1}(x)\varphi^{-1}(y)$.

Posons $g = \varphi^{-1}(x)$ et $h = \varphi^{-1}(y)$. Comme φ est un morphisme de groupes, on a $\varphi(gh) = \varphi(g)\varphi(h) = xy$. En particulier $\varphi^{-1}(xy) = gh = \varphi^{-1}(x)\varphi^{-1}(y)$. ■

Proposition 1.2.4 Soit $\varphi : G \to G'$ un morphisme de groupes. Alors on a les égalités suivantes :

(i) $\varphi(1) = 1$;

(ii) $\varphi(g^{-1}) = \varphi(g)^{-1}$, pour tout $g \in G$;

(iii) $\varphi(g^m) = \varphi(g)^m$, pour tout $g \in G$ et tout $m \in \mathbb{Z}$.

Preuve. 1. On a $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$ et en multipliant (à gauche ou à droite) par $\varphi(1)^{-1}$, on a $\varphi(1) = 1$.

2. On a $\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(1) = 1 = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$. On a donc $\varphi(g^{-1}) = \varphi(g)^{-1}$.

3. Pour $m = 0$ c'est le 1. Pour $m \geq 1$, on procède par récurrence sur m. Pour $m \leq -1$, on procède par récurrence sur $|m| = -m$ en utilisant le 2. ∎

Exemple 1.2.5 (i) L'application $\log : (\mathbb{R}_+^*, \times) \to (\mathbb{R}, +)$ est un isomorphisme de groupes.

(ii) L'application $\exp : (\mathbb{R}, +) \to (\mathbb{R}_+^*, \times)$ est l'isomorphisme de groupe réciproque de log.

(iii) L'application $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}$ est un morhisme de groupes surjectif (et non injectif si et seulement si $n \geq 2$.

(iv) L'application $\varphi : (\mathbb{R}, +) \to (\mathbb{C}^*, \times)$ définie par $\varphi(x) = e^{2i\pi x}$ est un morphisme de groupes non injectif et non surjectif.

(v) L'application $\varphi : (\mathbb{C}^*, \times) \to (\mathbb{C}^*, \times)$ déinie par $\varphi(z) = z^n$ est un morphisme surjectif mais non injectif de groupes.

Proposition 1.2.6 Soit $\varphi : G \to G'$ et $\psi : G' \to G''$ deux morphismes de groupes. Alors $\psi \circ \varphi : G \to G''$ est un morphisme de groupes.

Preuve. On a $(\psi \circ \varphi)(gh) = \psi(\varphi(gh)) = \psi(\varphi(g)\varphi(h)) = \psi(\varphi(g))\psi(\varphi(h)) = (\psi \circ \varphi)(g)(\psi \circ \varphi)(h)$ ∎

Corollaire 1.2.7 Soit G un groupe, alors $(\mathrm{Aut}(G), \circ)$ est un groupe (c'est un sous-groupe de $\mathfrak{S}(G), \circ)$).

Preuve. L'identité est un automorphisme de groupes. On vient de voir que la composée de deux automorphismes de groupes est encore un automorphisme de groupes. Enfin, on a vu que l'inverse d'un automorphisme de groupes est un automorphisme de groupes. ∎

1.3. Sous-groupes

Définition 1.3.1 Soit G un groupe. Un sous-ensemble $H \subset G$ est appelé **sous-groupe** de G s'il vérifie les trois conditions suivantes :

(i) $1 \in H$;

(ii) si $g \in H$, alors $g^{-1} \in H$;

(iii) si $g, h \in H$, alors $gh \in H$.

Remarque 1.3.2 (i) On vérifie aisément que si $H \subset G$ est un sous-groupe, alors H muni du produit de G est un groupe.

(ii) Si on oublie la condition (ii) ci-dessus, alors H n'est pas nécessairement un sous-groupe (par exemple $H = \mathbb{N} \subset G = \mathbb{Z}$).

Notation 1.3.3 Soit G un groupe.

(i) Les sous-ensembles $\{1\}$ et G forment toujours des sous-groupes de G. On les appele **sous-groupes triviaux** de G.

(ii) Un sous-groupe $H \subset G$ tel que $H \neq G$ est appelé **sous-groupe propre** de G.

Proposition 1.3.4 Soit G un groupe de $H \subset G$ un sous-ensemble de G. Alors H est un sous-groupe de H si et seulement si les deux conditions suivantes sont satisfaites :

(i) H est non vide ;

(ii) si $g, h \in H$, alors $gh^{-1} \in H$.

Preuve. Commençons par supposer que H est un sous-groupe. Alors $1 \in H$ et H est non vide. De plus, si $g, h \in H$, alors $h^{-1} \in H$ et donc $gh^{-1} \in H$.

Réciproquement, si H satisfait les deux conditions ci-dessus, montrons que c'est un sous-groupe. Montrons que $1 \in H$. Soit $g_0 \in H$ un élément quelconque (c'est possible car H est non vide). Alors on a $1 = g_0 g_0^{-1} \in H$ par (ii) appliqué à $(g, h) = (g_0, g_0)$. Soit $h \in H$, montrons que $h^{-1} \in H$. Comme $1 \in H$, on peut appliquer (ii) à $(g, h) = (1, h)$ et on a $h^{-1} = 1h^{-1} \in H$. Finalement, si $g, h \in H$, montrons que $gh \in H$. Par ce qui précède, on sait que $h^{-1} \in H$ donc en appliquant (ii) à $(g, h) = (g, h^{-1})$, on a $gh = g(h^{-1})^{-1} \in H$. ∎

Exemple 1.3.5 (i) Les sous-ensembles $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ sont des sous-groupes de $(\mathbb{C}, +)$.

(ii) Les sous-ensembles $\mathbb{Q}^*$ et $\mathbb{R}^*$ sont des sous-groupes de $(\mathbb{C}^*, \times)$.

(iii) Le sous-ensemble $\{1, -1\}$ de $(\mathbb{Q}^*, \times)$ est un sous-groupe.

(iv) Le sous-ensemble $\mathrm{O}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^{-1} = A^t\}$ où A^t designe la transposé de A est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

(v) Le sous-ensemble $\mathrm{Aff}_+(\mathbb{R}^2)$ défini par

$$\mathrm{Aff}_+(\mathbb{R}^2) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \;\middle|\; a^2 + b^2 \neq 0 \right\}$$

est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$.

(vi) Le sous-ensemble $\mathrm{Isom}_+(\mathbb{R}^2)$ défini par

$$\mathrm{Isom}_+(\mathbb{R}^2) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \;\middle|\; a^2 + b^2 = 1 \right\}$$

est un sous-groupe de $\mathrm{Aff}_+(\mathbb{R}^2)$ et de $\mathrm{GL}_2(\mathbb{R})$.

Lemme 1.3.6 Soit G un groupe.

(i) Si H et K sont des sous-groupes de G, alors $H \cap K$ est un sous-groupe de G.

(ii) Plus généralement, si $(H_\lambda)_{\lambda\in\Lambda}$ est une famille de sous-groupes de G, alors l'intersection $\cap_{\lambda\in\Lambda}H_\lambda$ est un sous-groupe de G. □

Preuve. La première assertion est une conséquence de la seconde. Nous montrons la seconde. Notons $K = \cap_{\lambda\in\Lambda}H_\lambda$. Il suffit de montrer que K est non-vide et que pour tout $g, h \in K$, on a $gh^{-1} \in K$. Comme H_λ est un sous-groupe, on a $1 \in H_\lambda$ pour tout λ et donc $1 \in K$ et K est non-vide. Soient maintenant g et h deux élément de K. Alors $g, h \in H_\lambda$ pour tout λ et donc $gh^{-1} \in H_\lambda$ pour tout λ et donc $gh^{-1} \in K$. ■

Corollaire 1.3.7 Soit $E \subset G$ un sous-ensemble quelconque, alors il existe un plus petit sous-groupe K de G contenant E.

Preuve. Il suffit de prendre pour K l'intersection de tous les sous-groupes de G contenant E. ■

Définition 1.3.8 Soit G un groupe et $E \subset G$ un sous-ensemble de G.

— Le plus petit sous-groupe de G contenant E est appelé **sous-groupe de** G **engendré par** E et est noté $\langle E\rangle$.

— Si $E = \{g\}$ n'a qu'un seul élément, on note $\langle g\rangle = \langle E\rangle = \langle\{g\}\rangle$.

Remarque 1.3.9 En général, si H et K sont des sous-groupes de G, la réunion $H\cup K$ n'est pas un sous-groupe de G. Ainsi par exemple, $\mathbb{R}$ et $i\mathbb{R}$ sont des sous-groupes de $(\mathbb{C}, +)$ mais $R \cup i\mathbb{R}$ n'est pas un sous-groupe de $\mathbb{C}$. On a

$$\langle\mathbb{R}, i\mathbb{R}\rangle = \mathbb{C}$$

c'est-à-dire que le sous-groupe engendré par $\mathbb{R}$ et $i\mathbb{R}$ est $\mathbb{C}$ tout entier.

Proposition 1.3.10 Soit G un groupe et $g \in G$. Alors on a $\langle g\rangle = \{g^m \in G \mid m \in \mathbb{Z}\}$.

Preuve. Notons $H = \{g^m \in G \mid m \in \mathbb{Z}\}$. Montrons l'inclusion $H \subset \langle g\rangle$. Soit donc $m \in \mathbb{Z}$, il suffit de montrer que $g^m \in \langle g\rangle$. Si $m = 0$, alors $g^m = 1 \in \langle g\rangle$ car $\langle g\rangle$ est un sous-groupe de G. Si $m \geq 1$, alors comme $g \in \langle g\rangle$ et que $\langle g\rangle$ est un groupe donc stable par multiplication, on obtient par récurrence sur m que $g^m \in \langle g\rangle$. Si $m \leq -1$, on commence par remarque que $g^{-1} \in \langle g\rangle$ et on procède comme précedemment.

Réciproquement, montrons que $\langle g\rangle \subset H$. Comme $\langle g\rangle$ est le plus petit sous-groupe contenant g et que $g \in H$, il suffit de montrer que H est un sous-groupe de G. Comme $g \in H$, on a bien que H est non vide. Si $h, h' \in H$, alors $h = g^m$ et $h' = g^{m'}$ avec $m, m' \in \mathbb{Z}$. On a alors $h(h')^{-1} = g^m g^{-m'} = g^{m-m'} \in H$ donc H est un sous-groupe. ■

1.4. Ordre d'un élément

Définition 1.4.1 Soit G un groupe et soit $g \in G$. Le cardinal de $\langle g \rangle$ est appelé **ordre de** g dans G et est noté $\mathrm{ord}_G(g)$ ou $\mathrm{ord}(g)$ s'il n'y a pas de confusion possible sur le groupe G.

Remarque 1.4.2 Soit G un groupe et soit $g \in G$.

(i) L'ordre de g peut être infini.

(ii) On a $\mathrm{ord}(g) = 1$ si et seulement si $g = 1$ (en effet, on a alors que $\langle g \rangle$ est un groupe a un seul élément donc $\langle g \rangle = \{1\}$ mais comme $g \in \langle g \rangle$, on a bien $g = 1$).

Proposition 1.4.3 Soit G un groupe et soit $g \in G$ d'ordre fini.

(i) On a $\mathrm{ord}(g) = \min\{n \in \mathbb{N}^* \mid g^n = 1\}$.

(ii) Si n est un entier tel que $g^n = 1$, alors $\mathrm{ord}(g)$ divise n.

(iii) On a un ismorphisme $\langle g \rangle \simeq \mathbb{Z}/\mathrm{ord}(g)\mathbb{Z}$ donné par $g^m \mapsto [m]$ et de réciproque $[m] \mapsto g^m$.

Preuve. 1. Comme $\mathrm{ord}(g)$ est fini, l'application $\mathbb{Z} \to \langle g \rangle$, $m \mapsto g^m$ ne peut être injective. Il existe donc des entiers m et n distincts tels que $g^m = g^n$. On peut supposer par exemple que $m < n$. On a alors $g^{n-m} = 1$. L'ensemble $\{n \in \mathbb{N}^* \mid g^n = 1\}$ est donc non vide. Notons $n_0 = \min\{n \in \mathbb{N}^* \mid g^n = 1\}$ et montrons que $\langle g \rangle = \{g^r \mid r \in [0, n_0 - 1]\}$. On aura alors $\mathrm{ord}(g) = |\langle g \rangle| = n_0$.

On a l'inclusion $\{g^r \mid r \in [0, n_0 - 1]\} \subset \langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$ donc il suffit de montrer l'autre inclusion. Soit $m \in \mathbb{Z}$. On fait la division euclidienne de m par n_0 et on a $m = qn_0 + r$ avec $r \in [0, n_0 - 1]$. On a alors $g^m = g^{qn_0+r} = (g^{n_0})^q g^r = 1^q g^r = g^r \in H$ ce qui montre le résultat.

2. Soit n tel que $g^n = 1$. Montrons que $n_0 = \mathrm{ord}(g)$ divise n. On fait la division euclidienne de n par n_0 et on a $n = qn_0 + r$ avec $r \in [0, n_0 - 1]$. Par ailleurs, on a $1 = g^n = g^{qn_0+r} = (g_0^n)^q g^r = 1^q g^r = g^r$. Donc $g^r = 1$ avec $r \in [0, n_0 - 1]$. Par minimalité de n_0, on obtient $r = 0$ et $\mathrm{ord}(g) = n_0$ divise n.

3. On commence par vérifier que les deux applications sont bien définies. Commençons par $\varphi : \langle g \rangle \to \mathbb{Z}/\mathrm{ord}(g)\mathbb{Z}$ avec $\varphi(g^m) = [m]$. Il faut vérifier que si m et n sont tels que $g^m = g^n$, alors $[m] = \varphi(g^m) = \varphi(g^n) = [n]$. Mais on a $g^{m-n} = 1$ et $\mathrm{ord}(g)$ divise $m - n$ donc $[m] = [n]$.

Vérifions que $\psi : \mathbb{Z}/\mathrm{ord}(g)\mathbb{Z} \to \langle g \rangle$ avec $\psi([m]) = g^m$ est bien définie. Il faut vérifier que si $[m] = [n]$, alors $g^m = g^n$. Mais si $[m] = [n]$, alors $\mathrm{ord}(g)$ divise $m - n$ donc $m - n = d\mathrm{ord}(g)$ pour un $d \in \mathbb{Z}$. On a alors $g^{m-n} = g^{d\mathrm{ord}(g)} = (g^{\mathrm{ord}(g)})^d = 1^d = 1$. Donc $g^m = g^n$.

Les deux applications φ et ψ sont donc bien définies et inverses l'une de l'autre. Il reste à montrer que φ (ou ψ) est un morphisme de groupes. On a $\varphi(g^m \cdot g^n) = \varphi(g^{m+n}) = [m + n] = [m] + [n] = \varphi(g^m) + \varphi(g^n)$. ∎

Exemple 1.4.4 Un groupe infini peut avoir des éléments d'ordre fini. Ainsi par exemple $-1 \in \mathbb{R}^*$ est d'ordre 2.

Proposition 1.4.5 Si G est un groupe et $g \in G$ est d'ordre infini, alors $\langle g \rangle$ est isomorphe à $\mathbb{Z}$ via $g^m \leftrightarrow m$.

En particulier, il n'existe pas d'entier n non nul tel que $g^n = 1$.

Preuve. Commençons par montrer qu'il n'existe pas d'entier non nul n tel que $g^n = 1$. En remplaçant g par g^{-1}, on peut supposer $n > 0$. Montrons que si un tel n existe alors, pour tout $m \in \mathbb{Z}$, on a $g^m = g^r$ avec $r \in [0, n-1]$. Ceci étant impossible (car alors $\langle g \rangle$ est fini de cardinal au plus n), on aura terminé. On fait la division euclidienne de m par n. On a $m = qn + r$ avec $r \in [0, n-1]$. On a donc $g^m = g^{qn+r} = (g^n)^q g^r = 1^q g^r = g^r$ ce qu'on voulait démontrer.

Considérons maintenant l'application $\psi : \mathbb{Z} \to \langle g \rangle$ définie par $\psi(m) = g^m$. C'est une application surjective. Montrons qu'elle est injective. Si $\psi(m) = \psi(n)$ avec $m \neq n$, alors $g^m = g^n$ et donc $g^{m-n} = 1$ ce qui est impossible par ce qu'on vient de montrer.

Il reste à vérifier que ψ est un morphisme de groupes. On a $\psi(m+n) = g^{m+n} = g^m g^n = \psi(m)\psi(n)$. ∎

1.5. Noyau et image

Proposition 1.5.1 Soit $\varphi : G \to G'$ un morphisme de groupes et soient $H \subset G$ et $H' \subset G'$ des sous-groupes. On a

(i) l'image $\varphi(H)$ de H est un sous-groupe de G' ;

(ii) l'image réciproque $\varphi^{-1}(H')$ de H' est un sous-groupe de G.

Preuve. 1. On a $1 \in H$ donc $1 = \varphi(1) \in \varphi(H)$. De plus, si $g, h \in H$, alors on a $gh^{-1} \in H$. On a donc $\varphi(g)\varphi(h)^{-1} = \varphi(gh^{-1}) \in \varphi(H)$.

2. On a $\varphi(1) = 1 \in H'$ donc $1 \in \varphi^{-1}(H')$. De plus, si $g, h \in \varphi^{-1}(H')$, alors $\varphi(g), \varphi(h) \in H'$ donc $\varphi(g)\varphi(h)^{-1} \in H'$. On a donc $\varphi(gh^{-1}) = \varphi(g)\varphi(h)^{-1} \in H'$ et $gh^{-1} \in \varphi^{-1}(H')$. ∎

Définition 1.5.2 Soit $\varphi : G \to G'$ un morphisme de groupe, les sous-groupes $\varphi(G) \subset G'$ et $\varphi^{-1}(1) \subset G$ son appelés **image** et **noyau**. On les note $\mathrm{Im}(\varphi)$ et $\mathrm{Ker}(\varphi)$.

Exemple 1.5.3

(i) On a $\mathrm{SL}_n(\mathbb{R}) = \mathrm{Ker}(\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*)$. Ainsi $\mathrm{SL}_n(\mathbb{R})$ est un sous-grope de $\mathrm{GL}_n(\mathbb{R})$. L'image de det est $\mathbb{R}^*$ (det est surjectif).

(ii) L'application $|\cdot| : \mathbb{C}^* \to \mathbb{R}^*$, $z \mapsto |z|$ est un morphisme de groupe. Son noyau $\mathrm{Ker}(|\cdot|) = \mathrm{S}^1 = \mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ est un sous-groupe de $\mathbb{C}^*$. Son image $\mathrm{Im}(|\cdot|) = \mathbb{R}_+^*$ est un sous-groupe de $\mathbb{R}^*$.

(iii) Si n est un entier plus grand que 1, l'application $p_n : \mathbb{C}^* \to \mathbb{C}^*$, $z \mapsto z^n$ est un morphisme de groupes. Son noyau $\mathrm{Ker}(p_n) = \mu_n = \{z \in \mathbb{C}^* \mid z^n = 1\}$ est le sous-groupe des **racines n-ièmes de l'unité** de $\mathbb{C}^*$. Son image est $\mathrm{Im}(p_n) = \mathbb{C}^*$.

(iv) La signature $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ est un morphisme de groupe surjectif. Son noyau est le **sous-groupe alterné** $\mathrm{Ker}(\varepsilon) = \mathfrak{A}_n$.

Proposition 1.5.4 Soit $\varphi : G \to G'$ un morphisme de groupes. Alors φ est injectif si et seulement si $\mathrm{Ker}(\varphi) = \{1\}$.

Preuve. Si φ est injectif et si $g \in \mathrm{Ker}(\varphi)$, alors $\varphi(g) = 1 = \varphi(1)$ donc $g = 1$. Réciproquement, supposons que l'on ait l'égalité $\mathrm{Ker}(\varphi) = \{1\}$. Soient $g, h \in G$ tels que $\varphi(g) = \varphi(h)$. Alors $1 = \varphi(g)\varphi(h)^{-1} = \varphi(gh^{-1})$ donc $gh^{-1} \in \mathrm{Ker}(\varphi)$ et $gh^{-1} = 1$. On obtient $g = h$. ∎

1.6. produit

Proposition 1.6.1 Soit $(G_i)_{i\in[1,n]}$ une famille de groupes. Alors le produit $G_1 \times \cdots \times G_n$ muni de la loi $(g_1, \cdots, g_n)(h_1, \cdots, h_n) = (g_1h_1, \cdots, g_nh_n)$ est un groupe.

Preuve. On a $(1, \cdots, 1)(g_1, \cdots, g_n) = (g_1, \cdots, g_n)(1, \cdots, 1) = (g_1, \cdots, g_n)$ donc $(1, \cdots, 1)$ est l'unité.

On a $(g_1, \cdots, g_n)((g_1^{-1}, \cdots, g_n^{-1}) = (g_1^{-1}, \cdots, g_n^{-1})(g_1, \cdots, g_n) = (1, \cdots, 1)$ donc $(g_1^{-1}, \cdots, g_n^{-1})$ est l'inverse de $(g_1, \cdots, g_n)$

Enfin, on a les égalités

$$\begin{aligned}[(g_1, \cdots, g_n)(h_1, \cdots, h_n)](k_1, \cdots, k_n) &= (g_1h_1, \cdots, g_nh_n)(k_1, \cdots, k_n)\\ &= (g_1h_1k_1, \cdots, g_nh_nk_n)\\ &= (g_1, \cdots, g_n)(h_1k_1, \cdots, h_nk_n)\\ &= (g_1, \cdots, g_n)[(h_1, \cdots, h_n)(k_1, \cdots, k_n)],\end{aligned}$$

la loi est donc associative. ∎

Définition 1.6.2 Soit $(G_i)_{i\in[1,n]}$ une famille de groupes. La loi de groupe définie sur le produit $G_1 \times \cdots \times G_n$ par $(g_1, \cdots, g_n)(h_1, \cdots, h_n) = (g_1h_1, \cdots, g_nh_n)$ est appelée **loi de groupe produit** et la structure de groupe ainsi définie s'appelle **groupe produit**.

Proposition 1.6.3 Soit $(G_i)_{i\in[1,n]}$ une famille de groupes, on muni le produit $G_1 \times \cdots \times G_n$ de la loi de groupe produit. Alors la projection $p_i : G_1 \times \cdots \times G_n \to G_i$, $(g_1, \cdots, g_n) \mapsto g_i$ est un morphisme de groupes.

Preuve. On a

$$\begin{aligned} p_i((g_1,\cdots,g_n)(h_1,\cdots,h_n)) &= p_i(g_1h_1,\cdots,g_nh_n) \\ &= g_ih_i \\ &= p_i(g_1,\cdots,g_n)p_i(h_1,\cdots,h_n), \end{aligned}$$

ce qui montre le résultat. ∎

Proposition 1.6.4 (Propriété universelle du produit) Soit $(G_i)_{i\in[1,n]}$ une famille de groupes, on muni le produit $G_1 \times \cdots \times G_n$ de la loi de groupe produit.

Si G est un groupe tel qu'il existe des morphismes de groupes $f_i : G \to G_i$ pour tout $i \in [1,n]$, alors il existe un unique morphisme de groupe $fG \to G_1 \times \cdots G_n$ tel que $f_i = p_i \circ f$ pour tout $i \in [1,n]$.

Preuve. Si f existe, alors la condition $f_i = p_i \circ f$ pour tout $i \in [1,n]$ impose que l'on a $f(g) = (f_1(g),\cdots,f_n(g))$ donc f est unique. Montrons que c'est un morphisme de groupes. On a

$$\begin{aligned} f(gh) &= (f_1(gh),\cdots,f_n(gh)) \\ &= (f_1(g)f_1(h),\cdots,f_n(g)f_n(h)) \\ &= (f_1(g),\cdots,f_n(g))(f_1(h),\cdots,f_n(h)) \\ &= f(g)f(h), \end{aligned}$$

ce qui termine la preuve. ∎

1.7. Conjugaison et centre

Définition 1.7.1 Soit G un groupe.

(i) Soit $g \in G$. On définit l'application $\mathrm{Int}_g : G \to G$ par $\mathrm{Int}_g(h) = ghg^{-1}$. Cette application est appelée **conjugaison par l'élément** g

(ii) On définit le **centre** de G par

$$Z(G) = \{g \in G \mid hg = gh \text{ pour tout } h \in G\}.$$

Proposition 1.7.2 Soit G un groupe.

(i) L'application $\mathrm{Int}_g : G \to G$ est un automorphisme du groupe G.

(ii) L'application $\mathrm{Int} : G \to \mathrm{Aut}(G)$, $g \mapsto \mathrm{Int}_g$ est un morphisme de groupe.

(iii) Le noyau de Int est $Z(G)$.

Preuve. 1. et 2. On a $\mathrm{Int}_g(hk) = ghkg^{-1} = ghg^{-1}gkg^{-1} = \mathrm{Int}_g(h)\mathrm{Int}_g(k)$ donc Int_g est un morphisme de groupes. Montrons que $\mathrm{Int}_g \circ \mathrm{Int}_h = \mathrm{Int}_{gh}$ c'est-à-dire que Int est un morphisme de groupes. On a

$$\mathrm{Int}_g \circ \mathrm{Int}_h(k) = \mathrm{Int}_g(hkh^{-1}) = ghkh^{-1}g^{-1} = (gh)k(gh)^{-1} = \mathrm{Int}_{gh}(k).$$

En particulier, on a $\mathrm{Int}_g \circ \mathrm{Int}_{g^{-1}} = \mathrm{Int}_{g^{-1}} \circ \mathrm{Int}_g = \mathrm{Int}_1 = \mathrm{Id}_G$ donc Int_g est bijective.

3. Le noyau de Int est l'ensemble des éléments g tels que $\mathrm{Int}_g = \mathrm{Id}_G$ c'est-à-dire l'ensemble des éléments $g \in G$ tels que $ghg^{-1} = h$ pour tout $h \in G$ soit $gh = hg$ pour tout $h \in H$. C'est bien le centre de G. ∎

1.8. Les groupes $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, les groupes monogènes et cycliques

On considèrera que les groupes $(\mathbb{Z}, +)$ et $(\mathbb{Z}/n\mathbb{Z}, +)$ sont connus.

Proposition 1.8.1 Les sous-groupes de $\mathbb{Z}$ sont les sous-ensembles $d\mathbb{Z}$ pour $d \in \mathbb{Z}$.

Preuve. On vérifie aisément que $d\mathbb{Z}$ est bien un sous-groupe de $\mathbb{Z}$. Réciproquement, soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Sinon, il existe un élément $n \in H$ non nul. Si $n < 0$, l'élément $-n$ est encore dans H donc on peut supposer que H contient au moins un élément strictement positif. Soit alors $d = \min\{m \in H \mid m > 0\}$. On montre que $H = d\mathbb{Z}$. Comme $d \in H$ et que H est un groupe, on a $d\mathbb{Z} \subset H$. Soit maintenant $m \in H$. On fait la division euclidienne de m par d. On a $m = dq + r$ avec $r \in [0, d-1]$. Mais $d, m \in H$ donc $r = m - qd \in H$. Par minimalité de d, on doit avoir $r = 0$ donc d divise m et $m \in d\mathbb{Z}$. ∎

La preuve à peu près évidente de la proposition suivante est laissée au lecteur.

Proposition 1.8.2 Le groupe $\mathbb{Z}$ est engendré par l'élément 1 : $\mathbb{Z} = \langle 1 \rangle$. Le groupe $d\mathbb{Z}$ est engendré par l'élément d : $d\mathbb{Z} = \langle d \rangle$.

Corollaire 1.8.3 Les groupes $\mathbb{Z}$ et $d\mathbb{Z}$ sont monogènes non cycliques.

Lemme 1.8.4 L'application $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $m \mapsto [m]$, où $[m]$ désigne la classe de m modulo n, est un morphisme de groupes surjectif. □

Preuve. Le fait que π_n est surjectif provient du fait tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ représentent les classes modulo n des éléments de $\mathbb{Z}$. Le fait que π_n est un morphisme de groupe provient de la définition de l'addition dans $\mathbb{Z}/n\mathbb{Z}$: $\pi_n(x+y) = [x+y] = [x] + [y] = \pi_n(x) + \pi_n(y)$. ∎

Notons $d\mathbb{Z}/n\mathbb{Z}$ le sous ensemble de $\mathbb{Z}/n\mathbb{Z}$ obtenu comme image par π_n de $d\mathbb{Z}$:

$$d\mathbb{Z}/n\mathbb{Z} = \pi_n(d\mathbb{Z}) = \left\{ [m] \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; m \in d\mathbb{Z} \right\} = \left\{ [m] \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; d \text{ divise } m \right\}.$$

Proposition 1.8.5 Soit n un entier non nul.

(i) Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$ pour d un diviseur de n.

(ii) Si d divise n, le sous-groupe $d\mathbb{Z}/n\mathbb{Z}$ est d'ordre $\frac{n}{d}$ et est engendré par $[d]$.

Preuve. 1. Comme $d\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, son image est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. Soit maintenant $H \subset \mathbb{Z}/n\mathbb{Z}$ un sous-groupe. Alors $\pi_n^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$ donc $\pi_n^{-1}(H) = d\mathbb{Z}$ pour un certain entier d. De plus, $n\mathbb{Z} = \pi_n^{-1}(\{0\}) \subset \pi_n^{-1}(H) = d\mathbb{Z}$ donc $n \in d\mathbb{Z}$ donc d divise n. Comme pi_n est surjectif, on obtient que $H = \pi_n(\pi_n^{-1}(H)) = \pi_n(d\mathbb{Z}) = d\mathbb{Z}/n\mathbb{Z}$ avec d un diviseur de n.

2. Soit $H = \pi_n(d\mathbb{Z}) = d\mathbb{Z}/n\mathbb{Z}$ avec d un diviseur de n. Comme $d\mathbb{Z}$ est engendré par d, son image $\pi_n(d\mathbb{Z})$ est engendré par $\pi_n(d) = [d]$ donc H est engendré par $[d]$. Écrivons $n = kd$. On a

$$\langle [d] \rangle = \{ m[d] \mid m \in \mathbb{Z} \} = \{ [0], [d], [2d], \cdots, [(k-1)d] \}$$

donc $d\mathbb{Z}/n\mathbb{Z}$ est d'ordre $k = \frac{n}{d}$. ∎

Une autre formulation de la proposition précédente est la suivante.

Corollaire 1.8.6 Pour chaque diviseur d de n, il existe un unique sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$: le sous-groupe $\langle \left[\frac{n}{d}\right] \rangle$ engendré par $\left[\frac{n}{d}\right]$

Proposition 1.8.7 Soit $[m] \in \mathbb{Z}/n\mathbb{Z}$.

(i) Alors $\mathrm{ord}(m) = \frac{n}{\mathrm{pgcd}(m,n)}$.

(ii) En particulier, on a les équivalences

$$\begin{aligned} m \text{ est premier avec } n &\Leftrightarrow [m] \text{ est un générateur de } \mathbb{Z}/n\mathbb{Z} \\ &\Leftrightarrow \langle [m] \rangle = \mathbb{Z}/n\mathbb{Z}. \end{aligned}$$

Preuve. 1. Posons $d = \mathrm{pgcd}(m, n)$. Il existe des entiers a et b tels que $m = ad$ et $n = bd$ avec $\mathrm{pgcd}(a, b) = 1$.

Rappelons que $\mathrm{ord}(m) = \min\{k \in \mathbb{N}^* \mid k[m] = [0]\}$. On a donc $\mathrm{ord}(m) = \min\{k \in \mathbb{N}^* \mid km \text{ est divisible par } n\}$. Montrons que ce minimum doit être $\frac{n}{\mathrm{pgcd}(m,n)} = \frac{n}{d} = b$.

Soit k tel que $k[m] = [0]$. Alors il existe un entier r tel que $km = rn$. On obtient $kad = rbd$ et donc $ka = rb$. On obtient que b divise ka et comme a et b sont premiers entre eux, on a que b divise k.

Réciproquement, montrons que $b[m] = [0]$. On a $b[m] = \left[\frac{mn}{d}\right]$ et comme $m/d = a \in \mathbb{Z}$, on obtient $b[m] = \left[\frac{mn}{d}\right] = [an] = [0]$. Ainsi $b = \min\{k \in \mathbb{N}^* \mid k[m] = [0]\} = \mathrm{ord}([m])$.

2. Découle directement de 1. ∎

Exemple 1.8.8 Dans $\mathbb{Z}/6\mathbb{Z}$ les ordres des éléments sont les suivants

x	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$\mathrm{ord}(x)$	1	6	3	2	3	6

Définition 1.8.9 Soit G un groupe.

(i) Le groupe G est dit **monogène** s'il existe un élément $g \in G$ tel que $G = \langle g \rangle$.

(ii) Le groupe G est dit **cyclique** s'il est monogène et fini.

Proposition 1.8.10 Soit G un groupe monogène.

(i) Si G est infini, alors $G \simeq \mathbb{Z}$.

(ii) Si G est cyclique d'ordre n, alors $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Preuve. Soit g un générateur du groupe c'est-à-dire un élément $g \in G$ tel que $G = \langle g \rangle$. Considérons l'application $\varphi : \mathbb{Z} \to G$, $m \mapsto g^m$.

1. Si $G = \langle g \rangle$ est infini, alors on a vu que φ est un ismorphisme.

2. Si $G = \langle g \rangle$ est fini d'ordre n, alors on a vu que $G = \langle g \rangle \simeq \mathbb{Z}/\mathrm{ord}(g)\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$. ∎

2. Quotient par un sous-groupe, groupe quotient

2.1. Relations d'équivalence

Nous rappelons la notion de relation d'équivalence et la partition qui est découle.

Définition 2.1.1 Soit E un ensemble.

(i) Une **relation** est une sous-partie R du produit $E \times E$ c'est-à-dire : $R \subset E \times E$.

(ii) Si $(x, y) \in R$, on dit que x **est en relation avec** y, on le note xRy.

(iii) Une relation est dite **réflexive** si tout Íément est en relation avec lui-même, c'est-à-dire si xRx est vrai pour tout $x \in E$.

(iv) Une relation est dite **symétrique** si on a l'implication $(xRy \Rightarrow yRx)$ pour toute paire $(x, y) \in E^2$.

(v) Une relation est dite **antisymétrique** si on a $(xRy$ et $yRx \Rightarrow x = y)$ pour toute paire $(x, y) \in E^2$.

(vi) Une relation est dite **transitive** si on a l'implication $(xRy$ et $yRz \Rightarrow xRz)$ pour tout triplet $(x, y, z) \in E^3$.

(vii) Une relation est appelée **relation d'équivalence** si elle est reflexive, symétrique et transitive.

(viii) Une relation est appelée **relation d'ordre** si elle est reflexive, antisymétrique et transitive.

Exemple 2.1.2 Soit E un ensemble.

(i) La relation d'égalité est une relation d'équivalence.

(ii) Si $E = \mathbb{Z}$ et $n \in \mathbb{Z}$ est un entier, la relation de congruence modulo n : $(\equiv \pmod{n})$ est une relation d'équivalence.

(iii) Si $E = \mathbb{Z}$, alors la relation $\leq$ est une relation d'ordre sur E. De même, la relation $\geq$ est une relation d'ordre sur E.

Définition 2.1.3 Soit E un ensemble, soit $x \in E$ et soit R une relation d'équivalence sur E. La **classe d'équivalence de** x **pour la relation** R, notée $[x]_R$ ou $[x]$ lorsque la relation R est claire est définie par

$$[x]_R = \{y \in E \mid xRy\}.$$

L'ensemble des classes d'équivalence pour la relation R est noté E/R.

Lemme 2.1.4 Soit E un ensemble, soit R une relation d'équivalence sur E et soient $x, y \in E$. Alors les classes déquivalence $[x]$ et $[y]$ de x et y pour la relation R sont soit égales : $[x] = [y]$, soit disjointes : $[x] \cap [y] = \emptyset$. □

Preuve. Soient x et y des élements de E. Nous devons montrer que l'alternative suivante est vraie : soit on a $[x] = [y]$, soit on a $[x] \cap [y] = \emptyset$. Supposons que $[x] \cap [y] \neq \emptyset$. Alors il existe $z \in [x] \cap [y]$. On a donc xRz et yRz. Par symétrie, on a xRz et zRy et par transitivité on obtient xRy (et yRx par symétrie).

Soit maintenant $t \in [x]$. Alors on a xRt et yRx. On a donc (transitivité) yRt et $t \in [y]$. On a donc $[x] \subset [y]$. On procède pour obtenir $[y] \subset [x]$ et donc $[x] = [y]$. ■

Définition 2.1.5 Soit E un ensemble et $(E_i)_{i \in I}$ une famille de sous-ensembles de E. On dit que cette famille forme une **partition** de E si les propriétés suivantes sont satisfaites :

(i) on a $E_i \cap E_j = \emptyset$ pour $i \neq j$;

(ii) on a $E = \cup_{i \in I} E_i$.

Proposition 2.1.6 Soit E un ensemble et R une relation d'équivalence sur E. Alors les classes déquivalence pour la relation R forment une partition de E.

Preuve. Le lemme précédent montre que la première condition pour avoir une partition est satisfaite. Montrons maintenant que les classes d'équivalence recouvrent E.

Soit E/R l'ensemble des classes d'équivalence. On a clairement l'inclusion $\cup_{[x] \in E/R}[x] \subset E$. Réciproquement, soit $x \in E$, alors par réflexivité, on a xRx et donc $x \in [x]$ d'où l'inclusion $E \subset \cup_{[x] \in E/R}[x]$. ■

Exemple 2.1.7 Si $E = \mathbb{Z}$ et R est la relation de congruence modulo un entier n. Alors les classes d'équivalence pour la relation R sont les ensembles

$$[m] = \{m + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\}.$$

L'ensemble des classes d'équivalences est $\mathbb{Z}/n\mathbb{Z}$.

Définition 2.1.8 Soit E un ensemble et R une relation d'équivalence sur E. L'application $\pi_R : E \to E/R$ définie par $\pi_R(x) = [x]_R$ est appelée **projection canonique**.

Exemple 2.1.9 Si $E = \mathbb{Z}$ et R est la relation de congruence modulo un entier n. Alors la projection canonique est l'application $\mathbb{Z} \to Z/n\mathbb{Z}$, $m \mapsto [m]$.

2.2. Classes à droite et à gauche

Définition 2.2.1 Soit G un groupe et H un sous-groupe. On définit la relation de congruence (à droite) modulo H par $x \sim y \Leftrightarrow y^{-1}x \in H$.

Lemme 2.2.2 Soit G un groupe et H un sous-groupe.

(i) La relation de congruence (à droite) modulo H est une relation d'équivalence.

(ii) La classe d'équivalence de g est $gH = \{gh \in G \mid h \in H\}$.

(iii) On a $x \sim y \Leftrightarrow x \in yH$. □

Preuve. 1. On a $x^{-1}x = e \in H$ donc $x \sim x$ et la relation est reflexive. Si $x \sim y$ alors $y^{-1}x \in H$ et donc son inverse est dans H aussi : $x^{-1}y = (y^{-1}x)^{-1} \in H$ donc $y \sim x$, la relation est symétrique. Enfin, si $x \sim y$ et $y \sim z$, alors $y^{-1}x \in H$ et $z^{-1}y \in H$ donc le produit est dans H : $z^{-1}x = z^{-1}yy^{-1}x \in H$ donc $x \sim z$, la relation est transitive.

2. Soit $[g]$ la classe d'équivalence de g. Soit $g' \in [g]$, alors $(g')^{-1}g \in H$ donc il existe $h \in H$ tel que $(g')^{-1}g = h$ et $g'h = g$ donc $g' = gh^{-1} \in gH$. Réciproquement, si $g' \in gH$, alors il existe $h \in H$ tel que $g' = gh$ et donc $(g')^{-1}g = h^{-1} \in H$ donc $g \sim g'$ et $g' \in [g]$. ■

Définition 2.2.3 Soit G un groupe et H un sous-groupe.

(i) Les classes d'équivalence pour la relation de congruence (à droite) modulo H sont appelées **classes à gauche suivant** H.

(ii) L'ensemble des classes à gauche est noté G/H.

(iii) La projection canonique est notée π_H ou $\pi : G \to G/H$.

Remarque 2.2.4 Soit G un groupe et H un sous-groupe. On peut définir la relation de congruence (à gauche) modulo H par $g \approx h \Leftrightarrow gh^{-1} \in H$. On a alors :

(i) La relation $\approx$ est une relation d'équivalence.

(ii) Les classes d'équivalence de la relation $\approx$ sont appelées les classes à droite et sont de la forme $Hg = \{hg \in G \mid h \in H\}$.

(iii) L'ensemble des classes d'équivalence est noté $H\backslash G$.

(iv) La projection canonique est $\pi : G \to G\backslash H$.

Lemme 2.2.5 Soit G un groupe et H un sous-groupe.

(i) Alors toutes les classes d'équivalence $gH \in G/H$ sont en bijection avec H.

(ii) En particulier, si H est fini, on a $|gH| = |H|$. □

Preuve. 2. Découle de 1. Pour 1., on a la bijection $H \to gH$, $h \mapsto gh$ de bijection réciproque $x \mapsto g^{-1}x$. ■

Corollaire 2.2.6 (Théorème de Lagrange) Soit G un groupe fini et H un sous-groupe.

(i) On a l'égalité $[G] = |H| \cdot |G/H|$.

(ii) En particulier, l'ordre de H divise celui de G.

Preuve. 2. Découle de 1. Pour 1., on rappelle que l'on a une partition

$$G = \coprod_{gH \in G/H} gH.$$

Mais pour tout g, on a $|gH| = |H|$ donc on obtient

$$|G| = \sum_{gH \in G/H} |gH| = \sum_{gH \in G/H} |H| = |H| \sum_{gH \in G/H} 1 = |H| \cdot |G/H|$$

ce qui démontre le résultat. ∎