6. Groupes quotients

Soient G un groupe et H un sous-groupe de G. Comme sur tout ensemble, il existe en général une quantité de lois de groupes sur G/H, mais ces dernières n'ont en général aucun lien avec la structure du groupe G. Une bien meilleure question est la suivante : existe-t-il une loi de groupe sur G/H telle que la projection canonique $\pi : G \to G/H, g \mapsto gH$, est un morphisme de groupes ?

Observons d'abord que si une telle loi $\star$ existe, alors elle est unique. En effet, elle satisfait, $(gH) \star (g'H) = \pi(g) \star \pi(g') = \pi(gg') = gg'H$ pour tout $g, g' \in G$. En outre, le neutre de $\star$ doit être l'image du neutre de G par π, c'est donc $\pi(1) = H$. En particulier, le noyau du morphisme π est

$$\pi^{-1}(H) = \{g \in G,\ gH = H\} = H.$$

Il se trouve que les noyau des morphismes de groupes ne sont pas des sous-groupes quelconques : ce sont des sous-groupes *distingués*.

Proposition-Définition 6.1. *Un sous-groupe H du groupe G est dit* distingué, *ou* normal, *si l'une des propriétés équivalentes suivantes est satisfaite :*
(i) $gHg^{-1} \subset H$ pour tout $g \in G$,
(ii) $gHg^{-1} = H$ pour tout $g \in G$,
(iii) $gH = Hg$ pour tout $g \in G$.

Démonstration — L'équivalence (ii) $\Leftrightarrow$ (iii) est évidente, ainsi que (ii) $\Rightarrow$ (i). Supposons (i). Soit $g \in G$. On a $gHg^{-1} \subset H$ par (i), ainsi que $g^{-1}Hg \subset H$ encore par (i) appliquée à g^{-1}, ce qui équivaut à $H \subset gHg^{-1}$, et au final $gHg^{-1} = H$. $\square$

On note en général $H \lhd G$ pour dire « *H est un sous-groupe distingué du groupe G* ». Les sous-groupes évidents $\{1\}$ et G sont trivialement distingués. Ajoutons que pour $g \in G$ fixé, et pour un sous-groupe $H \subset G$ infini, il est possible d'avoir une inclusion stricte $gHg^{-1} \subsetneq H$ (voir l'Exercice 2.30). Si G est abélien, noter que *tous ses sous-groupes sont (trivialement) distingués.* La réciproque est fausse :

Exemple 6.2. (Le groupe H_8) *Considérons les éléments*

$$I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix},\quad J = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ et } K := IJ = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

de $\mathrm{GL}_2(\mathbb{C})$*. On a clairement $I^2 = -1$, $J^2 = -1$ et $JIJ^{-1} = -I$, i.e. $IJ = -JI$, puis*

$$I^2 = J^2 = K^2 = -1,\ IJ = K,\ JK = I,\ KI = J \text{ et } JI = -K,\ KJ = -I,\ IK = -J.$$

Ainsi $\mathrm{H}_8 := \langle I, J\rangle = \{\pm 1, \pm I \pm J, \pm K\}$ *est un sous-groupe de* $\mathrm{GL}_2(\mathbb{C})$ *d'ordre* 8*, appelé* groupe des quaternions d'ordre 8*. Les relations ci-dessus montrent que ses sous-groupes sont* $1, \langle -1\rangle, \langle I\rangle, \langle J\rangle, \langle K\rangle$ *et* H_8*, et qu'ils sont tous distingués.* [8]

Toutefois, nous verrons par la suite que les sous-groupes d'un groupe non abélien sont en général rarement distingués. Indiquons quelques moyens de construire des sous-groupes distingués.

---

8. Comme nous le verrons au Chapitre 2, le sous-$\mathbb{R}$-espace vectoriel $\mathbb{H}$ de $\mathrm{M}_2(\mathbb{C})$ engendré par H_8 est un sous-anneau à division (non commutatif), dont le groupe multiplicatif contient H_8. Cela montre aussi que le Théorème 5.1 ne s'étend pas aux corps gauches (car H_8 n'est pas cyclique).

Exemple 6.3. *Si $f : G \to G'$ est un morphisme de groupes, on a* $\ker f \triangleleft G$. En effet, si $f(h) = 1$ et $g \in G$ alors $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)f(g)^{-1} = 1$ et donc $ghg^{-1} \in \ker f$.

Exemple 6.4. Plus généralement, *si $f : G \to G'$ est un morphisme de groupes on vérifie immédiatement que si $H' \triangleleft G'$ alors $f^{-1}(H') \triangleleft G$, et si f est surjective, que l'on a aussi $H \triangleleft G$ alors $f(H) \triangleleft G'$.*

Exemple 6.5. *Un sous-groupe H d'indice* 2 *dans G est nécessairement distingué.* En effet, pour $g \notin H$ on a à la fois $G = H \coprod Hg$ et $G = H \coprod gH$ (car $x \mapsto x^{-1}$ est une bijection des classes à droites sur les classes à gauche), donc $Hg = gH = G \setminus H$.

Exemple 6.6. (Normalisateur) Si H est un sous-groupe d'un groupe G, le *normalisateur de H dans G* est le sous-groupe de G défini par $\mathrm{N}_G(H) = \{g \in G \mid gHg^{-1} = H\}$. C'est manifestement *le plus grand sous-groupe de G dans lequel H est distingué.* En particulier, on a $H \triangleleft G \iff \mathrm{N}_G(H) = G$.

Le théorème principal concernant les groupes quotients est le suivant.

Théorème 6.7. *Soit H un sous-groupe d'un groupe G.*

(i) Il existe au plus une loi de groupe sur G/H telle que la projection canonique $G \to G/H$ est un morphisme de groupes.

(ii) Une telle loi existe si, et seulement si, on a $H \triangleleft G$, auquel cas elle coïncide avec la loi sur G/H induite par $\bullet$ sur $\mathrm{P}(G)$.

Démonstration — Le (i) a déjà été démontré, ainsi que le fait que si la loi existe on a $H \triangleleft G$. Supposons donc $H \triangleleft G$. Pour $g, g' \in H$ on a

$$(gH)(g'H) = g(Hg')H = g(g'H)H = gg'HH = gg'H$$

(associativité de $\bullet$ sur $\mathrm{P}(G)$, propriété (iii) des sous-groupes distingués et Lemme 4.1). Cela montre que G/H est stable par $\bullet$, et donc que $\bullet$ est une loi associative sur G/H (car sur $\mathrm{P}(G)$), et aussi que la projection canonique $\pi : G \to G/H$ vérifie $\pi(g)\pi(g') = \pi(gg')$ pour tout $g, g' \in G$. Le fait que $(G/H, \bullet)$ est un groupe se déduit alors formellement du fait que G est un groupe et que π est surjective. On peut le vérifier directement : l'élément H est un neutre car on a $H(gH) = gHH = gH$ pour tout $g \in G$, et pour tout $g \in G$ on a $(gH)(g^{-1}H) = gg^{-1}H = H$ et de même $(g^{-1}H)(gH) = H$, donc gH est inversible d'inverse $g^{-1}H$. □

Proposition-Définition 6.8. *Si H est un sous-groupe distingué de G, le* groupe quotient *G/H est la donnée de l'ensemble G/H muni de son unique loi de groupe telle que la projection canonique $\pi : G \to G/H$ est un morphisme de groupes.*

Le neutre de G/H est H, l'inverse de l'élément gH, pour $g \in G$, est $g^{-1}H = Hg^{-1} = (gH)^{-1}$, et pour tout $g, g' \in G$ on a $(gH)(g'H) = gg'H = (gH) \bullet (g'H)$. On a aussi déjà dit que le noyau du morphisme $\pi : G \to G/H$ est H. En particulier, on a démontré que tout sous-groupe distingué est le noyau d'un morphisme.

Remarque 6.9. (i) Pour de nombreuses questions, il n'est pas nécessaire de savoir que la loi de groupe quotient $\star$ sur G/H est induite par la multiplication des parties dans $\mathrm{P}(G)$, mais simplement qu'elle satisfait $(gH)\star(g'H) = gg'H$ pour tout $g, g' \in G$.

(ii) Pour montrer l'existence de $\star$ nous aurions aussi pu nous passer de $\bullet$ et remarquer que comme H est distingué dans G, si $a, a', b, b' \in G$ sont tels que $aH = a'H$ et $bH = b'H$, alors on a aussi $abH = a'b'H$: on peut « multiplier les congruences modulo H ». Cela montre qu'il y a un sens à poser sans ambiguité $aH \star bH := abH$, *i.e.* que l'application $G \times G \to G/H, (a, b) \mapsto abH$ passe au quotient $G/H \times G/H \to G/H, (aH, bH) \mapsto abH$. C'est l'approche suivie traditionnellement pour définir l'addition sur $\mathbb{Z}/n\mathbb{Z}$!

Exemple 6.10. (*Retour sur* $\mathbb{Z}/n\mathbb{Z}$) Le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est (comme on s'en doutait !) le groupe quotient de $\mathbb{Z}$ par son sous-groupe $n\mathbb{Z}$. En effet, la loi d'addition sur $\mathbb{Z}/n\mathbb{Z}$ satisfait $\overline{k} + \overline{k'} = \overline{k + k'}$ pour tout $k, k' \in \mathbb{Z}$, mais cela signifie exactement que la projection canonique $\mathbb{Z} \mapsto \mathbb{Z}/n\mathbb{Z}, k \mapsto \overline{k}$, est un morphisme de groupes.

Donnons une application aux carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$. Soit p premier impair. Écrivons $(\mathbb{Z}/p\mathbb{Z})^\times = \mathrm{C}_p \coprod \mathrm{N}_p$ où C_p est l'ensemble des carrés. On a vu que C_p est un sous-groupe d'indice 2. Ainsi, le groupe quotient $(\mathbb{Z}/p\mathbb{Z})^\times/\mathrm{C}_p = \{\mathrm{C}_p, \mathrm{N}_p\}$ a deux éléments, et il est de neutre C_p. Il est donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$ (ou à $\{\pm 1\}$) et on a

$$\mathrm{C}_p\mathrm{C}_p = \mathrm{C}_p,\ \mathrm{C}_p\mathrm{N}_p = \mathrm{N}_p \text{ et } \mathrm{N}_p\mathrm{N}_p = \mathrm{C}_p. \tag{8}$$

Cette dernière égalité dit par exemple que le produit de deux non-carrés est un carré ! Suivant Legendre, pour $x \in \mathbb{Z}/p\mathbb{Z}$ on pose $(\frac{x}{p}) = 1$ si x est un carré non nul, $(\frac{0}{p}) = 0$, et $(\frac{x}{p}) = -1$ si x n'est pas un carré. En particulier, $x \mapsto (\frac{x}{p})$ n'est rien d'autre que la composée des morphismes naturels $(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times/\mathrm{C}_p$ et $(\mathbb{Z}/p\mathbb{Z})^\times/\mathrm{C}_p \simeq \{\pm 1\}$. Le fait que c'est un morphisme, ou les égalités (8), se reformulent en :

Corollaire 6.11. (*Multiplicativité du symbole de Legendre*) *Pour p premier impair et $x, y \in (\mathbb{Z}/p\mathbb{Z})^\times$ on a $(\frac{xy}{p}) = (\frac{x}{p})(\frac{y}{p})$.*

Cette multiplicativité ramène l'étude de $(\frac{q}{p})$, avec $q \in \mathbb{Z}$, aux cas $q = -1$ et q premier. On a déjà vu $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$ (Exemple 5.8). Le cas q premier est l'objet de la fameuse *loi de réciprocité quadratique* (conjecturée par Euler, formulée ainsi par Legendre, et démontrée par Gauss), pour laquelle nous renvoyons aux exercices.

Remarque 6.12. Le symbole de Legendre définit donc un morphisme de groupes $(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}, x \mapsto (\frac{x}{p})$. On peut y penser comme un analogue du morphisme *signe* : $\mathbb{R}^\times \to \{\pm 1\}$, $x \mapsto \frac{x}{|x|}$. Plus généralement, pour tout sous-groupe H d'indice 2 d'un groupe G (automatiquement distingué par l'Exemple 6.5), il existe un unique morphisme $\epsilon_H : G \to \{\pm 1\}$ de noyau H.

Le théorème d'existence des groupes quotients est le point de départ de la *stratégie de dévissage* pour étudier les groupes : étant donné G, on cherche un sous-groupe distingué nontrivial $H \subsetneq G$ (ou ce qui revient au même, un morphisme non trivial $G \to G'$) et on commence par étudier H et G/H, qui sont d'ordre plus petit. Les groupes G pour pour lesquels cette stratégie échoue sont dit simples.

DÉFINITION 6.13. *Un groupe G est dit simple si on a $G \neq 1$ et si les seuls sous-groupes distingués de G sont $\{1\}$ et G.*

EXEMPLE 6.14. *Les groupes abéliens simples sont les $\mathbb{Z}/p\mathbb{Z}$ avec p premier.* En effet, tout sous-groupe d'un groupe abélien est distingué, donc un groupe abélien simple est monogène. Il est cyclique car $2\mathbb{Z}$ est un sous-groupe distingué strict de $\mathbb{Z}$. On conclut car les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les diviseurs de n.

EXEMPLE 6.15. Si H et K sont deux groupes, alors $H' = H \times \{1\}$ est un sous-groupe distingué de $H \times K$, et on a $H' \simeq H$ et $(H \times K)/H' \simeq K$ (utiliser par exemple le Théorème 6.17 ci-dessous). En revanche, il n'est pas du tout vrai en général que pour $H \lhd G$, on a $G \simeq H \times (G/H)$. Par exemple le groupe abélien $G = \mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ alors qu'il quotient un sous-groupe H d'ordre 2, à savoir $\langle \overline{2} \rangle$, et donc $H \simeq G/H \simeq \mathbb{Z}/2\mathbb{Z}$. Pire, ce n'est pas parce que H et G/H sont abéliens que G l'est : voir l'Exercice 2.27.

Dégageons maintenant quelques propriétés générales des groupes quotients. Supposons $H \lhd G$ et soit $f : G/H \to G'$ un morphisme de groupes. La composée $g = f \circ \pi : G \to G'$, où $\pi : G \to G/H$ est la projection canonique, est un morphisme de groupes vérifiant $g(H) = f(\pi(H)) = f(H) = \{1\}$. Réciproquement :

PROPOSITION 6.16. *(Propriété universelle des groupes quotients) Soient H un sous-groupe distingué du groupe G et $f : G \to G'$ un morphisme de groupes vérifiant $H \subset \ker f$. Alors il existe un unique morphisme de groupes $\overline{f} : G/H \to G'$ envoyant gH sur $f(g)$ pour tout $g \in G$.*

Bien sûr, la propriété $\overline{f}(gH) = f(g)$ s'écrit aussi $f = \overline{f} \circ \pi$ avec $\pi : G \to G/H$ la projection canonique.

DÉMONSTRATION — L'unicité de $\overline{f} : G/H \to G'$ vérifiant $\overline{f}(gH) = f(g)$ est évidente (car π est surjective). Un tel $\overline{f}$ est automatiquement un morphisme de groupes : pour $g, g' \in G$ on a $\overline{f}(gHg'H) = \overline{f}(gg'H) = f(gg') = f(g)f(g') = \overline{f}(gH)\overline{f}(g'H)$. Il ne reste qu'à montrer l'existence de $\overline{f}$. Soient $g, g' \in G$ avec $g \sim_H g'$. On a $g' = gh$ avec $h \in H$ donc $f(g') = f(g)f(h) = f(g)$ car $H \subset \ker f$: l'existence de $\overline{f}$ découle de la Proposition 2.1. $\square$

On retiendra : « c'est la même chose de se donner un morphisme $G/H \to G'$ et un morphisme de $G \to G'$ trivial sur H ». De manière plus précise, pour tout groupe G' l'application $f \mapsto f \circ \pi$ est une bijection de $\mathrm{Hom}(G/H, G')$ sur $\{f \in \mathrm{Hom}(G, G') \mid f(H) = \{1\}\}$. Dans le cas $G = \mathbb{Z}$ et $H = n\mathbb{Z}$ (Exemple 6.10), on obtient par exemple que se donner un morphisme $\mathbb{Z}/n\mathbb{Z} \to G'$ est la même chose que se donner un morphisme de $f : \mathbb{Z} \to G'$, *i.e.* $f(1) = g \in G'$, tel que $f(n) = 1$, *i.e.* avec $g^n = 1$. Un corollaire particulièrement utile est le suivant, appelé parfois le *premier théorème d'isomorphisme.*

THÉORÈME 6.17. *Si $f : G \to G'$ est un morphisme de groupes, alors f induit par passage au quotient un isomorphisme de groupes $\overline{f} : G/\ker f \xrightarrow{\sim} \mathrm{Im}\, f$.*

DÉMONSTRATION — Quitte à remplacer G' par son sous-groupe $\mathrm{Im}\, f$, on peut supposer f surjective. La proposition 2.1 appliquée à $H = \ker f$ montre que f induit par passage au quotient un morphisme de groupes $\overline{f} : G/\ker f \to G'$, envoyant $g \ker f$

sur $f(g)$ pour tout $g \in G$. Le morphisme $\overline{f}$ est donc surjectif car f l'est. Son noyau est l'ensemble des $g \ker f \in G/\ker f$ tels que $f(g) = 1$, ce qui force $g \in \ker f$ et donc $g \ker f = \ker f$. Ainsi, $\overline{f}$ est également injective : c'est un isomorphisme. $\square$

Exemple 6.18. *L'application $z \mapsto e^{2\pi i z}$ définit des morphismes surjectifs $\mathbb{R} \to \mathbb{U}$ et $\mathbb{C} \to \mathbb{C}^\times$, de même noyau $\mathbb{Z}$. Elle induit donc des isomorphismes*

$$\mathbb{R}/\mathbb{Z} \simeq \mathbb{U} \text{ et } \mathbb{C}/\mathbb{Z} \simeq \mathbb{C}^\times.$$

Ainsi, tout morphisme de groupes $f : G \to G'$ se décompose naturellement comme composé de trois morphismes naturels : d'abord la projection canonique $G \to G/\ker f$, envoyant g sur $g \ker f$ (surjective), suivie de l'isomorphisme canonique $G/\ker f \xrightarrow{\sim} \operatorname{Im} f$ de l'énoncé, envoyant $g \ker f$ sur $f(g)$, et enfin le morphisme d'inclusion $\operatorname{Im} f \to G'$ (injectif). C'est le *dévissage canonique* d'un morphisme.

Terminons par une étude des sous-groupes et des quotients du groupe quotient G/H.

Proposition 6.19. *Soit H un sous-groupe distingué d'un groupe G.*

(i) L'application $K \mapsto K/H$ induit une bijection croissante entre sous-groupes K de G contenant H et sous-groupes de G/H.

(ii) Dans cette bijection, on a $K/H \lhd G/H \Leftrightarrow K \lhd G$, auquel cas le morphisme naturel $G/H \to G/K$ induit un isomorphisme $(G/H)/(K/H) \xrightarrow{\sim} G/K$.

L'isomorphisme du (ii) est parfois appelé *troisième théorème d'isomorphisme.*

Démonstration — Appliquons la Proposition 2.10 au morphisme surjectif $\pi : G \to G/H$. Le (i) s'en déduit car pour K un sous-groupe de G avec $H \subset K \subset G$, on constate $\pi(K) = K/H$. Le premier point du (ii) résulte de l'Exemple 6.4. Pour $g \in G$ on a $gHK = gK$ car $HK = K$ puisque H est inclus dans K. La multiplication à droite par K induit donc une application $\varphi : G/H \to G/K, gH \mapsto gK$, qui est manifestement surjective et un morphisme de groupes : c'est l'application sous-entendue dans l'énoncé. On a $\ker \varphi = \{gH \mid gK = K\} = K/H$, car pour $g \in G$ on a $gK = K \Leftrightarrow g \in K$. On conclut par le Théorème 6.17. $\square$