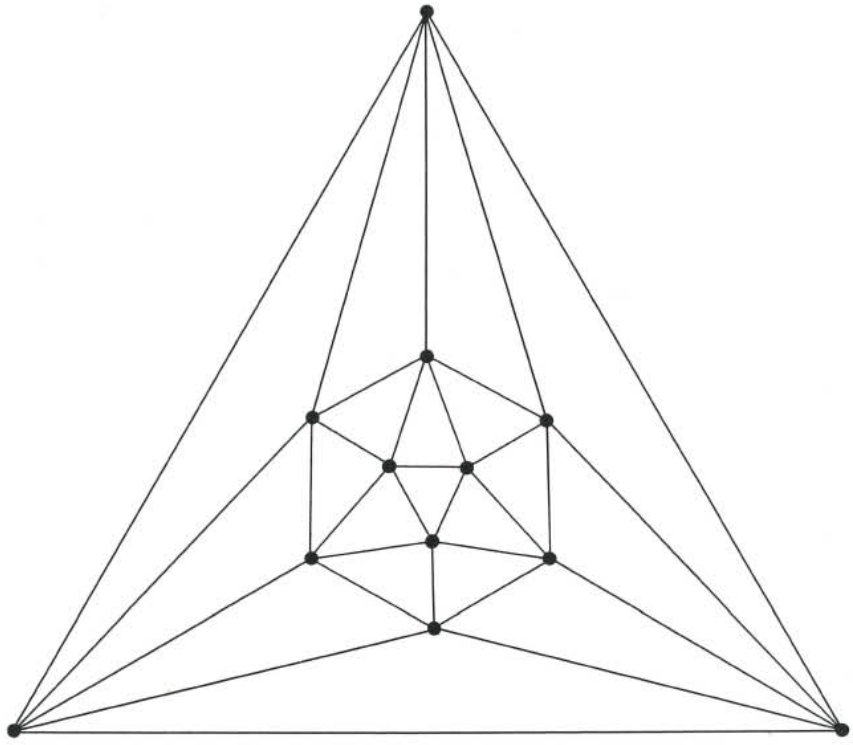
GROUPES, ALGÈBRES ET GÉOMÉTRIE

Tome 1



Jean-Marie ARNAUDIÈS
José BERTIN

ellipses

Chapitre I

Groupes

I.1 Introduction

Nous supposerons acquises les notions élémentaires de base concernant les groupes : Notion de groupe; sous-groupes d'un groupe; homomorphismes de groupes, isomorphismes, automorphismes d'un groupe. Noyau et image d'un homomorphisme. Groupe produit d'une famille de groupes. Famille génératrice d'un groupe. Notion de groupe monogène. Notion de groupe abélien. (Exemple : tout groupe monogène est abélien). Sauf mention contraire, les groupes dont il sera question ci-dessous seront notés : multiplicativement, pour la plupart d'entre eux; et, s'il s'agit de groupes abéliens , soit multiplicativement, soit additivement, selon le cas. S'il y a ambiguité, dans l'abréviation qui désigne un groupe, on peut faire figurer une loi de composition de ce groupe. Par exemple, étant donné le grand nombre de structures dont on peut doter $\mathbf{R}$, il pourra parfois être commode de noter $(\mathbf{R}, +)$ le *groupe additif* de $\mathbf{R}$, pour bien expliciter "l'oubli" de toutes autres structures sur $\mathbf{R}$.

Les groupes fondamentaux, qui servent à construire un grand nombre d'autres groupes, sont : $\mathbb{Z}$ additif ; $(\mathbb{Q}, +)$; $(\mathbb{Q}^*, \times)$; $(\mathbb{Q}_+^*, \times)$, $\mathbf{R}$ additif ; $(\mathbf{R}^*, \times)$; $(\mathbf{R}_+^*, \times)$; $\mathbf{C}$ additif ; $(\mathbb{C}^*, \times)$; $\mathbb{U}$ (= groupe des nombres complexes de module 1, pour la multiplication) ; si E est un ensemble non vide quelconque, $\mathfrak{S}_E$ désignera le *groupe des permutations* de E (la loi de composition étant la composition des applications) ; lorsque $E = [\![1, n]\!]$, où $n \in \mathbb{N}^*$, $\mathfrak{S}_E$ sera plutôt noté $\mathfrak{S}_n$; si G est un groupe, l'ensemble des automorphismes du groupe G est un sous-groupe de $\mathfrak{S}_G$, qui sera souvent noté $\mathrm{Aut}(G)$.

Soit $(G_i)_{i \in I}$ une famille de groupes : le groupe produit des G_i se note $\prod_{i \in I} G_i$; lorsque tous les G_i sont égaux à un même groupe G, ce produit sera noté aussi G^I ; c'est l'ensemble des applications : $I \to G$, muni de la loi de composition "point par point"; si tous les G_i sont abéliens, de façon claire le groupe $\prod_{i \in I} G_i$ l'est encore.

Supposons tous les G_i abéliens et notés additivement ; dans le groupe $\prod_{i \in I} G_i$, le sous-ensemble formé des familles $x = (x_i)_{i \in I}$ à *support fini* (i.e. telles que le *support* $S_x = \{i \in I / x_i \neq 0_{G_i}\}$ soit un ensemble fini) , forme un sous groupe, noté $\biguplus_{i \in I} G_i$ et appelé *somme directe des groupes abéliens* G_i. Lorsque tous les G_i sont égaux à un même groupe G, cette somme directe sera notée aussi $G^{(I)}$.
Etant donnés deux groupes G et H, l'ensemble des homomorphismes de groupe de G dans H sera noté $\mathrm{Hom}_{\mathrm{Gr}}(G, H)$. Ce n'est en général pas un sous-groupe de H^G ; mais

si H est abélien, alors $\mathrm{Hom}_{\mathrm{Gr}}(G,H)$ est un sous-groupe de H^G.

Soit $(G_i)_{i\in I}$ une famille de groupes ; notons G le groupe produit $\prod_{i\in I} G_i$ et $\pi_i : G \to G_i$ $(i \in I)$ les projections naturelles. Le groupe G vérifie la *propriété universelle* suivante :

1. **Pour tout groupe H et pour toute famille (ξ_i) d'homomorphismes de groupes $\xi_i : H \to G_i$ $(i \in I)$, il existe un et un seul homomorphisme de groupes $\xi : H \to G$ tel que $\xi_i = \pi_i \circ \xi$ pour tout $i \in I$.**

En conséquence de (1), on voit que l'application

2.
$$\mathrm{Hom}_{\mathrm{Gr}}(H,G) \to \prod_{i\in I} \mathrm{Hom}_{\mathrm{Gr}}(H,G_i)$$
$$\xi \longmapsto (\pi_i \circ \xi)_{i\in I}$$

est, pour tout groupe H, une *bijection* entre ensembles.

Supposons maintenant tous les G_i abéliens (et notés additivement). Notons S le groupe somme directe $\biguplus_{i\in I} G_i$. Pour chaque $i \in I$, soit $J_i : G_i \to S$ l'homomorphisme (injectif) qui envoie $x \in G_i$ sur l'élément $x = (x_j)_{j\in I}$ tel que $x_i = x$ et $x_j = 0_{G_j}$ pour tout $j \neq i$. on a alors la *propriété universelle* suivante :

3. **Pour tout groupe abélien H, et pour toute famille (ξ_i) d'homomorphismes de groupes $\xi_i : G_i \to H$ $(i \in I)$, il existe un et un seul homomorphisme de groupes $\xi : S \to H$ tel que $\xi \circ J_i = \xi_i$ pour tout $i \in I$.**

En conséquence de (3), on voit que l'application :

4.
$$\mathrm{Hom}_{\mathrm{Gr}}(S,H) \to \prod_{i\in I} \mathrm{Hom}_{\mathrm{Gr}}(G_i,H),$$
$$\xi \longmapsto (\xi \circ J_i)_{i\in I}$$

est, pour tout groupe *abélien* H, une bijection entre ensembles.
Mieux : si on munit $\mathrm{Hom}_{\mathrm{Gr}}(S,H)$ de sa structure de groupe naturelle (sous-groupe de H^S) et $\prod_{i\in I} \mathrm{Hom}_{\mathrm{Gr}}(G_i,H)$ de la structure de groupe produit des groupes $\mathrm{Hom}_{\mathrm{Gr}}(G_i,H)$, alors les bijections (2) et (4) sont des *isomorphismes de groupes abéliens.*

Pour clore cette introduction, précisons que l'élément neutre d'un groupe G sera noté, en général, e_G, ou e (resp. 0_G , *ou* 0) si G est noté multiplicativement (resp. additivement). L'inverse de $x \in G$ sera noté x^{-1} (resp. $-x$).

I.2 Ordre d'un élément

Rappelons sans démonstration le théorème fondamental :

THEOREME I.1 *L'application qui, à tout entier naturel a, associe le sous-groupe $a\mathbb{Z}$ de $\mathbb{Z}$ (additif), est une bijection de $\mathbb{N}$ sur l'ensemble des sous-groupes de $\mathbb{Z}$.*

Soit alors G un groupe et a un élément de G. L'application $\psi_a : \mathbb{Z} \to G$, $m \mapsto a^m$, où

$$a^m = \begin{cases} e_G & \text{si } m = 0 \\ \textit{le produit de } m \textit{ fois } a & \text{si } m \geq 1 \\ (a^{-m})^{-1} & \text{si } m \leq -1 \end{cases}$$

est un homomorphisme de groupes.
En appliquant le théorème I.1, on voit qu'il y a un unique $\omega_a \in \mathbb{N}$ tel que : $\mathrm{Ker}(\psi_a) = \omega_a\mathbb{Z}$. Par définition, si $\omega_a \geq 1$, a est dit d'*ordre fini*, et l'entier ω_a est alors appelé son *ordre*. Et si $\omega_a = 0$, l'élément a est dit *d'ordre infini*. (Il est clair que l'ordre d'un élément $a \in G$ ainsi défini est invariant par tout isomorphisme de groupes).
L'image $\mathrm{Im}(\psi_a)$ est le *groupe engendré par a dans G*, noté aussi $\mathrm{Gr}(a)$.
Si a est d'ordre infini, ψ_a est injectif, et réciproquement. Dans ce cas, ψ_a définit un isomorphisme de $(\mathbb{Z}, +)$ sur $\mathrm{Gr}(a)$; (en particulier $\mathrm{Gr}(a)$ est infini). Si a est d'ordre fini, la restriction de ψ_a à $[\![0, \omega_a - 1]\!]$ définit une bijection de $[\![0, \omega_a - 1]\!]$ sur $\mathrm{Gr}(a)$; donc dans ce cas, $\mathrm{Gr}(a)$ est fini, de cardinal ω_a. De plus, pour tout $n \in \mathbb{Z}$, les relations "$a^n = e_G$" et "$n \in \omega_a\mathbb{Z}$" sont *équivalentes.*

Nous supposerons acquise la définition du groupe additif des classes de $\mathbb{Z}$ modulo un entier naturel donné N. Ce groupe se note $\mathbb{Z}/N\mathbb{Z}$, notation qui sera justifiée plus loin. Si $N = 0$, $\mathbb{Z}/N\mathbb{Z}$ est de façon naturelle isomorphe à $\mathbb{Z}$ additif et si $N \geq 1$, $\mathbb{Z}/N\mathbb{Z}$ est fini, de cardinal N, engendré par la classe de 1.

Revenant à l'élément a du groupe G, et supposé d'ordre fini $\omega_a \geq 1$, notons J la bijection $[\![0, \omega_a - 1]\!] \to \mathbb{Z}/\omega_a\mathbb{Z}$ qui associe, à tout $k \in [\![0, \omega_a - 1]\!]$ sa classe mod (ω_a). Alors l'application $\mathbb{Z}/\omega_a\mathbb{Z} \to \mathrm{Gr}(a)$, $x \mapsto \psi_a \circ J^{<-1>}(x)$, est un isomorphisme de groupes.

Soit maintenant H un groupe ; H est dit *monogène* ssi $\exists\, a \in G \mid H = \mathrm{Gr}(a)$; dans ce cas, tout $a \in H$ que $H = \mathrm{Gr}(a)$ est appelé un *générateur* de H.

Si H est monogène infini, il est isomorphe à $\mathbb{Z}$ additif et il n'a donc que deux générateurs : si g est l'un d'eux, l'autre est g^{-1}.

Si H est monogène fini et si a est l'un de ses générateurs, alors a est d'ordre fini, égal à $N = \mathrm{card}(H)$. Dans ce cas, le nombre des générateurs est le même que le nombre des générateurs du groupe $\mathbb{Z}/N\mathbb{Z}$; ce nombre est donc fini, compris entre 1 et N et ne dépend que de N : on l'appelle l'*indicateur d'Euler de N* et on le note $\phi(N)$. Un groupe monogène fini est appelé un groupe *cyclique.*

Concernant l'ordre d'un élément, nous ne donnerons que deux propriétés du reste bien connues, résumées dans le Théorème suivant :

THEOREME I.2 *Soit G un groupe et $a \in G, b \in G$;*

(a) Supposons a d'ordre fini n ; alors pour tout $k \in \mathbb{Z}$, a^k est d'ordre fini et l'ordre de a^k est $n/pgcd(k, n)$

(b) Supposons $ab = ba$, a et b d'ordres finis, respectivement égaux à m et n et $pgcd(m, n) = 1$.
Alors $c = ab$ est d'ordre fini, cet ordre étant égal à mn.

Démonstration (abrégée)

(a) Soit $d = \text{pgcd}(k,n)$. Posant $k' = k/d, n' = n/d$, on sait que $\text{pgcd}(k',n') = 1$. On a d'abord : $(a^k)^{n'} = a^{k'dn'} = (a^n)^{k'} = e_G$, donc a^k est d'ordre fini et son ordre ω divise n' ; si d'autre part $m \in \mathbb{Z}$ vérifie : $(a^k)^m = e_G$, alors $km \in n\mathbb{Z}$, donc $k'm \in n'\mathbb{Z}$ et puisque $\text{pgcd}(k',n') = 1$, cela entraîne : $m \in n'\mathbb{Z}$. Donc $n' \mid \omega$ et $\omega \mid n'$ et par suite $\omega = n'$.

(b) Puisque $ab = ba$, on a : $(ab)^{mn} = a^{nm}b^{nm} = (a^m)^n(b^n)^m = e_G$; donc $c = ab$ est d'ordre fini ω et $\omega \mid mn$. Soit $k \in \mathbb{Z}$ tel que $c^k = e_G$. Alors $c^{kn} = e_G = a^{kn}b^{kn} = a^{kn}$, donc $kn \in m\mathbb{Z}$, d'où $k \in m\mathbb{Z}$ parce que $\text{pgcd}(m,n) = 1$. On voit de même que $k \in n\mathbb{Z}$; et à nouveau du fait que $\text{pgcd}(m,n) = 1$, on en déduit que $k \in mn\mathbb{Z}$. Ainsi $mn \mid \omega$ et $\omega \mid mn$, d'où $\omega = mn$. □

Une importante conséquence du Théorème I.2 est : si $a \in G$ est d'ordre fini n et si $k \in \mathbb{Z}$, alors l'ordre de a^k est n ssi $\text{pgcd}(k,n) = 1$. En particulier, si G est cyclique et si a est un générateur de G, alors tout générateur de G s'écrit de manière unique sous la forme a^k, avec $k \in [\![0, n-1]\!]$, $(n = \text{card}(G))$ et $\text{pgcd}(k,n) = 1$. En particulier, *l'indicateur d'Euler* $\phi(N)$ *est le nombre des entiers* $k \in [\![0, N-1]\!]$ *qui sont premiers avec* N.

I.3 Classes, indice

Soit G un groupe et H un sous-groupe de G. On associe à H deux relations d'équivalence R_s et R_d sur G : pour $(x,y) \in G^2$: $xR_sy \in H$ ssi $x^{-1}y \in H$ et xR_dy ssi $xy^{-1} \in H$.
Les classes de R_s (resp. de R_d) sont appelées les *classes à gauche de* G *modulo* H *(resp. les classes à droite de* G *modulo* H*).*

L'ensemble des classes à gauche (resp. à droite) sera noté $(G/H)_s$ (resp. $(G/H)_d$). [Notons que si G est abélien, alors $R_s = R_d$, donc $(G/H)_s = (G/H)_d$]. L'application naturelle $G \to (G/H)_s$ n'est autre que $x \mapsto xH$. De même, l'application naturelle $G \to (G/H)_d$ est $x \mapsto Hx$.
Pour tout $x \in G$, l'application $H \to xH$, $t \mapsto xt$ est bijective et de même $H \to Hx$, $t \mapsto tx$, est bijective : toutes les classes à droite ou à gauche mod(H) sont donc équipotentes à H.

L'involution $x \mapsto x^{-1}$ de G induit une bijection de $(G/H)_s$ sur $(G/H)_d$ et de $(G/H)_d$ sur $(G/H)_s$, ces bijections étant réciproques l'une de l'autre.
En particulier, les ensembles $(G/H)_s$ et $(G/H)_d$ sont finis ou infinis en même temps et sont toujours équipotents. Quand ils sont finis, ils ont donc même cardinal. On pose :

DEFINITION I.1 *Soit* H *un sous-groupe d'un groupe* G.
On dit que H *est d'indice fini dans* G *ssi les ensembles* $(G/H)_s$ *et* $(G/H)_d$ *sont finis. Dans ce cas, leur cardinal commun est appelé* indice de H dans G *et noté* $[G : H]$. *Si les ensembles* $(G/H_s$ *et* $(G/H)_d$ *sont infinis, on dit que* H *est* d'indice infini *dans* G *et on convient d'écrire* $[G : H] = \infty$.

La propriété de base de l'indice est fournie par le théorème suivant :

THEOREME I.3 *(Transitivité des indices)*
Soit G *un groupe et* H, K *deux sous-groupes de* G *tels que* $K \subset H$ *(on dit que* $K \subset$

$H \subset G$ est une "tour de groupes").
Alors les ensembles $(G/K)_s$ et $(G/H)_s \times (H/K)_s$ sont équipotents. En particulier, $[G : K]$ est fini ssi $[G : H]$ et $[H : K]$ le sont et dans ce cas, on a :

$$[G : K] = [G : H][H : K]$$

Démonstration : Soit $\mathcal{H}$(resp. $\mathcal{K}$) une partie de G (resp. de H) telles que les applications $\mathcal{H} \to (G/H)_s$, $x \mapsto xH$ et $\mathcal{K} \to (H/K)_s$, $y \mapsto yK$ soient bijectives.
Notons Φ l'application :

$$\mathcal{H} \times \mathcal{K} \to (G/K)_s,\ (x, y) \mapsto xyK.$$

On prouve facilement que Φ est bijective, ce qui établit l'ensemble du théorème. En effet :

- Φ est injective, car de $xyK = x'y'K$ on déduit : $x'^{-1}xH \supset x'^{-1}xyK = y'K \subset H$, donc $x'^{-1}xH = H$ (car deux classes à gauche de G mod H sont disjointes ou égales), donc $xH = x'H$, donc $x = x'$, donc $yK = y'K$, donc $y = y'$ (car $x \in \mathcal{H}$, $x' \in \mathcal{H}$ et $y \in \mathcal{K}$, $y' \in \mathcal{K}$).

- Φ est surjective, car si $z \in G$, on a d'abord un $x \in \mathcal{H}$ tel que $zH = xH$ d'où $x^{-1}zH = H$ d'où $x^{-1}z \in H$. Puis on a un $y \in \mathcal{K}$ tel que $x^{-1}zK = yK$ d'où : $zK = xyK = \Phi(x, y)$. □

Si H est le sous-groupe $\{e_G\}$ de G, il est clair que $(G/H)_s$ et $(G/H)_d$ peuvent être identifiés à G. En particulier dire que G est fini équivaut à dire que l'indice $[G : \{e_G\}]$ est fini ; cet indice étant alors le cardinal de G. Dans ce cas, on notera $[G]$ ce cardinal.

En prenant $K = \{e\}$ dans le Théorème I.3, on obtient :

COROLLAIRE I.1 *Soit H un sous-groupe d'un groupe fini G.*
(Alors $[G : H]$ est évidemment fini, ainsi que H). On a :

$$[G] = [G : H] \times [H]$$

Ce corollaire donne non seulement le fait, bien connu, que $[H]$ divise $[G]$, mais aussi l'interprétation du quotient $[G]/[H] := [G : H]$.

COROLLAIRE I.2 *: ("Théorème de Lagrange").*
Soit G un groupe fini, de cardinal N. Pour tout $x \in G$, on a : $x^N = e_G$.

Démonstration : On considère le sous-groupe $H = Gr(x)$ de G. Notant $\omega = [H]$, on sait que $x^\omega = e_G$. Puisque $\omega \mid N$ à cause du cor. 1 ci-dessus), a fortiori $x^N = e_G$. □

Exemple de base : "petit" Thérorème de Fermat.
Soit p un nombre premier et soit $a \in \mathbb{Z}$ un nombre non divisible par p. Notons $\bar{x}$ la classe *mod*(p) d'un élément quelconque $x \in \mathbb{Z}$. Alors $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^* = (\mathbb{Z}/p\mathbb{Z})\backslash\{\bar{0}\}$.
Le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ est de cardinal $p-1$. D'après le Théorème de Lagrange, $\bar{a}^{p-1} = \bar{1}$. Ce qui signifie :
$a^{p-1} \equiv 1 \bmod (p)$. On retrouve le célèbre "petit" théorème de Fermat, propriété dont il a été donné à ce jour plus de *cent* démonstrations différentes. □

I.4 Groupes quotients

Soit G un groupe. Pour tout $\tau \in G$, on vérifie sans peine que l'application $I_\tau : G \to G$, $x \mapsto \tau x \tau^{-1}$ est un *automorphisme* de G; ce type d'automorphisme est appelé un *automorphisme intérieur* de G.

L'application $I : G \to \mathrm{Aut}(G)$, $\tau \mapsto I_\tau$ est un homomorphisme de groupes, dont l'image est appelée le *groupe des automorphismes intérieurs* de G et noté ici $\mathrm{Int}(G)$. On laisse à la vérification du lecteur la proposition suivante:

PROPOSITION I.1 *Soit H un sous-groupe de G. Les propriétés suivantes sont équivalentes :*

(a) $\forall \tau \in G, I_\tau(H) = H$;

(b) $\forall \tau \in G, \tau H = H\tau$;

(c) $\forall (s,t) \in G^2$, *stH ne dépend que de sH et tH;*

(d) $\forall (s,t) \in G^2$, *Hst ne dépend que de Hs et Ht.*

DEFINITION I.2 *Avec les notations de la Prop. I.1, le sous-groupe H de G est dit* distingué *(ou* invariant *ou* normal *) ssi les conditions (a),(b), (c),(d) de cette proposition sont satisfaites. Si c'est le cas on écrit :*

$$H \lhd G$$

- On a toujours : $\{e_G\} \lhd G$ et $G \lhd G$;
- Si $f : G_1 \to G_2$ est un homomorphisme d'un groupe G_1 dans un groupe G_2 et si H_i est un sous-groupe de $G_i (i \in \{1,2\})$, alors :
  si $H_2 \lhd G_2$, on a : $f^{-1}(H_2) \lhd G_1$; si $H_1 \lhd G_1$ et *si f est surjectif*, on a $f(H_1) \lhd G_2$.
  En particulier, on a toujours : $\mathrm{Ker}(f) \lhd G_1$ (et cette propriété sert fréquemment à prouver qu'un sous-groupe est distingué dans un autre).
- Si $K \subset H \subset G$ est une tour de groupes et si $K \lhd G$, alors $K \lhd H$ (mais attention ! $K \lhd H$ et $H \lhd G$ *n'entraîne pas* $K \lhd G$).
- Toute intersection de sous-groupes distingués de G est un sous-groupe distingué de G.
- Soit $(G_i)_i \in I$ une famille de groupes, et pour tout $i \in I$, soit $H_i \lhd G_i$; alors $\prod_{i \in I} H_i \lhd \prod_{i \in I} G_i$.
- Si G est abélien, de façon évidente tout sous-groupe de G est distingué. (A noter que la réciproque de cette propriété est fausse, un groupe non abélien pouvant très bien n'avoir que des sous-groupes distingués. L'exemple le plus simple d'un tel groupe est le groupe *quaternionique*, (cf. [1], Exercice 12, § V.7, page 200).
- Si $H \lhd G$, la propriété (c) de la Proposition I.1 montre que $(G/H)_s = (G/H)_d$. On notera alors tout simplement G/H cet ensemble, qui sera alors appelé *ensemble des classes de G* mod (H).
  Un groupe G, est dit *simple* ssi : les seuls sous-groupes distingués de G sont $\{e_G\}$ et G, et $G \neq \{e_G\}$. Les exemples les plus élémentaires de groupes simples sont les groupes additifs $\mathbb{Z}/p\mathbb{Z}$, p premier. D'après le Théorème I.3, corollaire I.1, un

tel groupe, en effet, n'admet pour sous- groupes que $\{0_{\mathbb{Z}/p\mathbb{Z}}\}$ et $\mathbb{Z}/p\mathbb{Z}$, donc a fortiori est simple, car $[\mathbb{Z}/p\mathbb{Z}] = p$ n'admet pour diviseurs que 1 et p. D'ailleurs les groupes $(\mathbb{Z}/p\mathbb{Z}, +)$, p premier, sont les seuls groupes abéliens simples car :

- Tous les sous-groupes d'un groupe abélien sont distingués;
- $(\mathbb{Z}, +)$ est non simple, donc un groupe abélien simple n'a pas d'élément d'ordre infini ;
- de plus un tel groupe est forcément monogène, donc en fin de compte il est cyclique, donc isomorphe à $(\mathbb{Z}/N\mathbb{Z}, +)$ pour un certain entier $N \geq 1$;
- et enfin, tout élément $\neq 0$ de $(\mathbb{Z}/p\mathbb{Z}, +)$ supposé simple doit engendrer le groupe, d'où $\phi(N) = N - 1$, ce qui implique à l'évidence que N est premier.

THEOREME I.4 *Soit G un groupe et H un sous-groupe distingué de G. Soit $\varpi : G \to G/H$ l'application canonique. Il existe sur G/H une et une seule loi de composition telle que* $(\forall (x,y) \in G_2)\ \varpi(xy) = \varpi(x)\varpi(y)$. *Cette loi de composition est une loi de groupe ; pour cette loi de groupe sur G/H, on a : $Ker(\varpi) = H$, $Im(\varpi) = G/H$; $e_{G/H} = H$.*

Démonstration (abrégée). L'existence de la loi de composition découle des propriétés (c) et (d) de la Prop. I.1. L'unicité de cette loi découle de façon évidente de la *surjectivité* de ϖ. C'est aussi cette surjectivité de ϖ qui permet de prouver que cette loi sur G/H est une loi de groupe : l'élément neutre de G/H est $H = \varpi(e_G)$, et si $X = \varpi(x) \in G/H$, l'inverse de X est $\varpi(x^{-1})$. Enfin ϖ est surjectif et si $x \in G, \varpi(x) = e_{G/H}$ signifie : $x \in H$, d'où $\mathrm{Ker}(\varpi) = H$. □

Par définition, si $H \lhd G$, la structure de groupe définie dans le Th. I.4 sur G/H est appelée *structure de groupe quotient* de celle de G par celle de H. Le groupe G/H ainsi défini est appelé *l'homomorphisme canonique* (ou : *naturel*) de G dans G/H (dit souvent *projection canonique*).

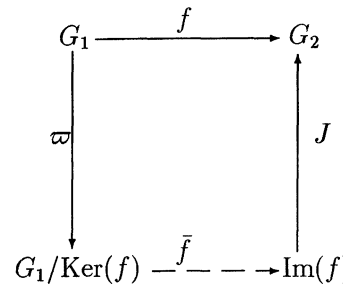
Exemple de base : Soit $m \in \mathbb{N}$. Le groupe quotient $\mathbb{Z}/m\mathbb{Z}$ peut être défini ($\mathbb{Z}$ étant abélien, n'a que des sous-groupes distingués). On vérifie que ce groupe quotient $\mathbb{Z}/m\mathbb{Z}$ n'est autre que le groupe additif des *classes modulo m* dans $\mathbb{Z}$, groupe que l'on avait convenu de noter $\mathbb{Z}/m\mathbb{Z}$. (Cette notation $\mathbb{Z}/m\mathbb{Z}$ se trouve donc à présent justifiée a posteriori).

A la notion de groupe quotient, sont associés les *mécanismes* fondamentaux suivants :

A - *Décomposition canonique d'un homomorphisme de groupes :*

THEOREME I.5 *Soit G_1 et G_2 deux groupes et $f \in Hom_{Gr}(G_1, G_2)$. On sait que $Ker(f) \lhd G_1$. Notons $\varpi : G_1 \to G_1/Ker(f)$ la projection canonique et $J : Im(f) \to G_2$ l'injection canonique.*
Il existe alors une unique application $\bar{f} : G_1/Ker(f) \to Im(f)$ telle que $J \circ \bar{f} \circ \varpi = f$; cette application est un isomorphisme de groupes.

Ce théorème est illustré par le diagramme suivant :



(I.1)

et la relation $f = J \circ \bar{f} \circ \varpi$ se traduit en disant que ce *diagramme est commutatif.* On dit que $f = J \circ \bar{f} \circ \varpi$ est la *factorisation canonique* de f.

Démonstration (abrégée). L'unicité de $\bar{f}$ découle de la surjectivité de ϖ. L'existence de $\bar{f}$, du fait, presque évident, que f est *constante sur chaque classe de* G_1 mod $\mathrm{Ker}(f)$; on pose donc pour $X \in G_1/\mathrm{Ker}(f)$: $\bar{f}(X) =$ valeur constante de f sur les $x \in X$; et on vérifie que $J \circ \bar{f} \circ \varpi = f$. La vérification que $\bar{f}$ ainsi définie est un isomorphisme de groupes ne présente pas d'autre difficulté qu'un certain effet soporifique. □

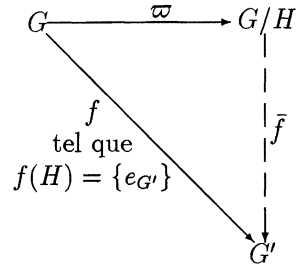
COROLLAIRE *Avec les notations du Th. I.5, supposons* G_1 *fini (ce qui entraîne évidemment que* $Im(f)$ *est fini). Alors* $[Ker(f)] \times [Im(f)] = [G_1]$.

Démonstration : D'après le Th. I.5, on a : $[\mathrm{Im}(f)] = [G_1/\mathrm{Ker}(f)]$.
Or $[G_1/\mathrm{Ker}(f)] = [G_1 : \mathrm{Ker}(f)]$ par les définitions mêmes et on conclut à l'aide du Cor. I.1 du Th. I.3.□

B - *Propriété universelle du quotient.*

THEOREME I.6 *Soit* G *un groupe,* H *un sous-groupe distingué de* G *et notons* $\varpi : G \to G/H$ *la projection canonique.*
Pour tout groupe G' *et pour tout* $f \in Hom_{Gr}(G, G')$ *tel que* $f(H) = \{e_{G'}\}$, *existe un unique* $\bar{f} \in Hom_{Gr}(G/H, G')$ *tel que* $\bar{f} \circ \varpi = f$.

Cette propriété universelle est illustrée par le diagramme suivant :



(I.2)

et la relation $\bar{f} \circ \varpi = f$ se traduit en disant que *ce diagramme est commutatif.*
Soit $\mathcal{E}_{G'}$, l'ensemble des $f \in \mathrm{Hom}_{\mathrm{Gr}}(G, G')$ tels que $f(H) = \{e_{G'}\}$.
Du Théorème I.6, on déduit que *l'application* $\mathrm{Hom}_{\mathrm{Gr}}(G/H, G') \to \mathcal{E}_{G'}$, $g \mapsto g \circ \varpi$, *est bijective.*

Démonstration du Th. I.6 . L'unicité de $\bar{f}$ (en tant qu'*application entre ensembles)* vient de la surjectivité de ϖ. L'existence de $\bar{f}$ en tant qu'application découle du fait que f (à cause de l'hypothèse $f(H) = \{e_{G'}\}$) est constante sur chaque classe de