Cours d'Algèbre 6
Filière SMA

Mme F. ERRAJI, Pr.
Département de Mathématiques
Faculté des Sciences de Meknès

15 mars 2021

Table des matières

Chapitre 1

Groupes

I Rappels

I.1 Factorisation d'une Application

Définitions I.1.1. *1. Soit R une relation binaire sur un ensemble E. R est dite une relation d'équivalence sur E si les propriétés suivantes sont vérifiées :*

- *R est reflexive i.e. $\forall x \in E : \quad xRx$*
- *R est symétrique i.e. $\forall x, y \in E : \quad xRy \Longrightarrow yRx$*
- *R est transitive i.e. $\forall x, y, z \in E : \quad xRy \ \ et \ \ yRz \Longrightarrow xRz$*

2. Soit R une relation d'équivalence sur l'ensemble non vide E.

- *Pour tout élément x de E, l'ensemble $\{y \in E / xRy\}$ est appelé classe d'équivalence de x suivant R. On la note $\bar{x}$ (ou $\dot{x}$ ou encore $cl(x)$) et le sous-ensemble de $P(E)$, constitué par les classes d'équivalence suivant R s'appelle ensemble quotient de E par R, on le note E/R.*

Proposition I.1.1. *Soit E un ensemble non vide et R une relation d'équivalence sur E, alors :*

- *(i) $\bar{x} \neq \emptyset$, $\forall x \in E$,*
- *(ii) $\forall x, y \in E, \bar{x} = \bar{y} \Longleftrightarrow x \in \bar{y} \Longleftrightarrow y \in \bar{x} \Longleftrightarrow xRy$,*
- *(iii) l'ensemble quotient E/R est une partition de E.*

Preuve. 1. (iii)

- $\forall x \in E, \quad \overline{x} \neq \emptyset$ (D'après la réflexivité de R)
- $\forall x, y \in E$, si $z \in \overline{x} \cap \overline{y}$ alors xRz et zRy, d'où xRy, et d'après (ii), $\overline{x} = \overline{y}$; ainsi, $\overline{x} \cap \overline{y} \neq \emptyset \Rightarrow \overline{x} = \overline{y}$

— $\forall x \in E, x \in \overline{x}$, d'où $E = \bigcup_{\overline{x} \in E/R} \overline{x}$.

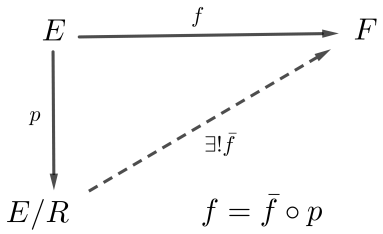
□

Soit R une relation d'équivalence sur E, d'après ce qui précède pour tout $x \in E$, il existe un élément X unique de E/R tel que $x \in X$, X n'est autre que la classe de x suivant R. On pose $X = \overline{x}$. L'application

$$\begin{array}{rccc} p: & E & \longrightarrow & E/R \\ & x & \longmapsto & \overline{x} \end{array}$$

s'appelle l'application (ou la projection) canonique.

Proposition I.1.2. *Soit R une relation d'équivalence sur l'ensemble non vide E et $p : E \to E/R$ l'application canonique. Si $f : E \to F$ est une application telle que f est constante sur les classes d'équivalence suivant R, alors il existe une application $\overline{f} : E/R \to F$ unique telle que : $\overline{f} \circ p = f$.*

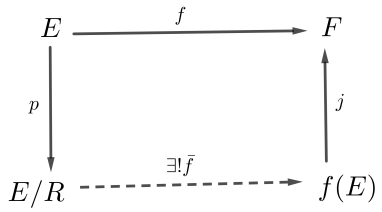


Preuve. Soit $\overline{x} \in E/R$, comme f est constante sur les classes, $\forall y \in \overline{x}, \quad f(y) = f(x)$. On considère alors

$$\begin{array}{rccc} \overline{f} & : & E/R & \to & F \\ & & \overline{x} & \mapsto & \overline{f}(\overline{x}) = f(x) \end{array}$$

La valeur $f(x)$ ne dépend que de $\overline{x}$ et non du représentant particulier x de $\overline{x}$. Ainsi, $\overline{f}$ est bien définie et par construction on a $\overline{f} \circ p = f$. Pour l'unicité : si g est une application de $E/R \to F$ telle que $g \circ p = f$ alors $\forall x \in E, \quad g \circ p(x) = f(x) = \overline{f} \circ p(x)$ d'où $\overline{f}(\overline{x}) = g(\overline{x}), \quad \forall \overline{x} \in E/R.$ □

Proposition I.1.3. *Soit $f : E \to F$ une application et R la relation binaire sur E définie par $xRy \iff f(x) = f(y)$ alors R est une relation d'équivalence sur E ; Si $j : f(E) \to F$ désigne l'injection canonique il existe une application unique $\overline{f} : E/R \to f(E)$ telle que $j \circ \overline{f} \circ p = f$, de plus $\overline{f}$ est bijective. La décomposition $f = j \circ \overline{f} \circ p$ s'appelle la décomposition (ou la factorisation) canonique de f.*



Preuve.

$$\begin{array}{rccc} \text{Soit} \quad f_1 & : & E & \to & f(E) \\ & & x & \mapsto & f_1(x) = f(x) \end{array}$$

f_1 est une application constante sur les classes d'équivalence suivant R. D'après la proposition précédente, il existe une application unique $\overline{f} : E/R \to f(E)$ telle que $\overline{f} \circ p = f_1$, et par suite $j \circ \overline{f} \circ p = j \circ f_1 = f$.

Il reste à montrer que $\overline{f}$ est bijective. Soit $y \in f(E)$, il existe donc $x \in E$ tel que $y = f(x)$. Or, $\overline{f}(\overline{x}) = f(x) = y$, ce qui prouve que $\overline{f}$ est surjective. Soit $\overline{x}, \overline{y} \in E/R$ tel que $\overline{f}(\overline{x}) = \overline{f}(\overline{y})$ d'où $f(x) = f(y)$ et donc xRy. Ainsi, $\overline{x} = \overline{y}$, donc $\overline{f}$ est injective. □

I.2 Lois de Composition Interne sur un Ensemble

Définitions et Propriétés I.2.1. *1. Une loi de composition interne sur un ensemble E est une application de $E \times E$ dans E. On la note souvent $+$ ou $\cdot$ ou $*$ ou $\top$ ou $\bot$.*

Soit $*$ une loi de composition interne sur E, l'image de (x, y) par $*$ sera désignée par $x * y$ et appelé le composé de x et y par $*$.

2. Soit $*$ une loi de composition interne sur un ensemble E et F une partie de E. On dit que F est stable par la loi $*$ si $\forall (x, y) \in F \times F, x * y \in F$. Dans ce cas, la restriction de l'application $*$ à F, notée $*/F$:

$$\begin{array}{rccc} */F & : & F \times F & \to & F \\ & & (x, y) & \mapsto & x * y \end{array}$$

est une loi de composition interne sur F appelée loi induite par $*$ sur F.

3. Soit $*$ une loi de composition interne sur un ensemble E et R une relation d'équivalence sur E. La relation R est dite compatible avec la loi $*$ si $\forall x, y, x', y' \in E$:

$$(xRx' \quad et \quad yRy') \Rightarrow x * y \, R \, x' * y'$$

Dans ce cas, la correspondance $\overline{*} : E/R \times E/R \to E/R$ définie par $\overline{x} \,\overline{*}\, \overline{y} = \overline{x * y}$ est une loi de composition interne sur E/R, appelée loi quotient sur E/R, induite par celle de E.

En effet, soit $(\overline{x},\overline{y}),(\overline{x'},\overline{y'}) \in E/R \times E/R$ *; si* $(\overline{x},\overline{y}) = (\overline{x'},\overline{y'})$ *alors* $\overline{x} = \overline{x'}$ *et* $\overline{y} = \overline{y'}$ *et donc* xRx' *et* yRy' *et d'après la compatibilité de* R *avec la loi on obtient* $x*y\,R\,x'*y'$ *et donc* $\overline{x*y} = \overline{x'*y'}$ *i.e.* $\overline{x}*\overline{y} = \overline{x'}*\overline{y'}$.

4. *Soit* $*$ *une loi de composition interne (L.C.I.) sur* E.

   — $*$ *est dite commutative si* $\forall x,y \in E, \quad x*y = y*x$

   — $*$ *est dite associative si* $\forall x,y,z \in E, \quad (x*y)*z = x*(y*z)$

   — *un élément* e *de* E *est dit neutre à droite (resp. à gauche) pour la loi* $*$ *si* $\forall x \in E, \quad x*e = x$ *(resp.* $\forall x \in E, \quad e*x = x$*).* e *est dit neutre pour* $*$ *s'il est à la fois neutre à gauche et à droite pour* $*$*, i.e.* $\forall x \in E, \quad x*e = x = e*x$.

   Remarque. *Si* e *est un élément neutre de* E *pour* $*$ *alors* e *est l'unique élément neutre. En effet, si* e' *est un autre élément neutre on aura :* $e*e' = e$*, mais aussi* $e*e' = e'$ *d'où* $e = e'$.

   — *Soit* $*$ *une L.C.I. sur* E *et* e *l'élément neutre de* E *pour* $*$*. Soit* $x \in E$*. On appelle symétrique à gauche (resp. à droite) de* x*, tout élément* $x' \in E$ *tel que :* $x'*x = e$ *(resp.* $x*x' = e$*) et on appelle symétrique de* x *tout élément* $x' \in E$ *qui est symétrique à gauche et à droite de* x*. Un élément* $x \in E$ *est dit symétrisable s'il admet un symétrique par rapport à* $*$*, i.e.* $\exists x' \in E$ *tel que* $x*x' = x'*x = e$*. Un élément est dit idempotent si* $x*x = x$.

   Si $*$ *est une L.C.I. sur* E *associative et* e *l'élément neutre et si* $x \in E$ *admet un symétrique* y *à gauche* $(y*x = e)$ *et un symétrique* z *à droite* $(x*z = e)$ *alors* $y = z$ *car* $y = y*e = y*(x*z) = (y*x)*z = e*z = z$*. Cet élément* $y \in E$ *vérifie donc* $y*x = x*y = e$ *et il est le seul à les vérifier. Donc,* x *admet un symétrique et un seul (qui est aussi l'unique symétrique à gauche et l'unique symétrique à droite).*

I.3 Notion de Groupe

Définitions I.3.1. *Soit* G *un ensemble non vide muni d'une L.C.I. notée* T*. On dit que* (G,T)*, (par abus que* G*), est un groupe si on a les propriétés suivantes :*

— T *est associative*

— *il existe dans* G *un élément neutre* e *pour* T

— *tout élément de* G *est symétrisable.*

Si de plus la loi T *est commutative, le groupe* (G,T) *est dit abélien ou commutatif. Lorsque le cardinal de l'ensemble* G *est fini et égal à* n*, on dit que le groupe* (G,T) *est fini d'ordre* n*, noté* $|G| = n$.

Remarques. — *Si* (G,T) *est un groupe, le symétrique d'un élément quelconque de* G *est unique et l'application :*

$$\begin{array}{ccc} G & \to & G \\ x & \mapsto & x^{-1} \end{array} \quad \textit{est bijective.}$$

— *Si* G *est un ensemble non vide muni d'une L.C.I. associative notée* T*, alors :* (G,T) *est un groupe*

$$\iff \begin{array}{llll} (i)- & \exists e \in G & / \quad \forall x \in G & : \quad xTe = x \\ (ii)- & \forall x \in G, & \exists x' \in G & : \quad xTx' = e \end{array}$$

de même (G,T) *est un groupe* $\iff$ $\begin{array}{llll} (i)- & \exists e \in G & / \quad \forall x \in G & : \quad eTx = x \\ (ii)- & \forall x \in G, & \exists x' \in G & : \quad x'Tx = e \end{array}$

(à montrer !)

Exemples. 1. *Les ensembles* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *munis de l'addition usuelle sont des groupes abéliens. Il en est de même pour* $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ *munis de la multiplication.*

2. *Soit* E *un ensemble non vide. L'ensemble des bijections de* E *sur* E *muni de la composition usuelle des applications est un groupe.*

   Lorsque $E = \{1, 2, \cdots, n\}$ *ce groupe est noté* $(S_n, \circ)$ *ou* $(S_n, \cdot)$ *et* $|S_n| = n!$*. Si* $n \geq 3$*,* S_n *n'est pas abélien.*

3. *Soit* X *un ensemble non vide et* (G,T) *un groupe. On munit l'ensemble* G^X *des applications de* X *dans* G *de la loi* $*$ *définie par :*

$$(f * g)(x) = f(x)Tg(x), \quad \forall x \in X$$

   $(G^X, *)$ *est un groupe.*

4. *Pour tout* $n \geq 1$*, l'ensemble* $GL_n(\mathbb{K})$ *(*$\mathbb{K} = \mathbb{R}$ *ou* $\mathbb{C}$*) des matrices carrées d'ordre* n *inversibles à coefficients dans* $\mathbb{K}$ *muni de la multiplication est un groupe.*

Conventions de Notations et Propriétés

On convient généralement de noter la loi de composition interne d'un groupe G quelconque soit multiplicativement soit additivement. On réserve la notation additive aux groupes abéliens.

Dans le premier cas, le composé de deux éléments x et y est noté $x \cdot y$ ou tout simplement xy et appelé *produit* de x et y.

Le symétrique d'un élément $x \in G$ est appelé son *inverse* et noté x^{-1}. On a la propriété :

$$\forall x, y \in G, \quad (x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$$

Soit $n \in \mathbb{Z}$ et $x \in G$. On définit x^n par :

$$x^n = \underbrace{x \cdot x \cdots x}_{n\, fois} = xx^{n-1} \qquad \text{si} \quad n \geq 1$$

et par convention :

$$x^0 = e, \quad x^n = (x^{-1})^{-n} = (x^{-n})^{-1} \quad \forall n \leq -1$$

Dans le cas additif, le composé de deux éléments de G est noté $x + y$ et appelé *somme* de x et y. L'élément neutre de G est noté 0. Le symétrique d'un élément $x \in G$ s'appelle son opposé et est noté $-x$.

Soit $n \in \mathbb{Z}$ et $x \in G$. De façon analogue, on définit nx par :

$$nx = \underbrace{x + x + \cdots + x}_{n\ fois} \text{ si } \quad n \geq 1$$

et par convention $0x = 0$ et $nx = (-n)(-x) = -(-nx), \qquad \forall n \leq -1.$

Propriété I.3.1. *Soit $(G, \cdot)$ un groupe et $a \in G$. On note τ_a (resp. δ_b) la translation à gauche (resp. à droite) par a, l'application de $G \to G$ définie par : $\tau_a(x) = ax$ (resp. $\delta_a(x) = xa$) pour tout $x \in G$. On a alors :*

- *(i) $\forall a, b \in G, \quad \tau_a \circ \tau_b = \tau_{ab}$ et $\delta_a \circ \delta_b = \delta_{ba}$,*
- *(ii) $\forall a \in G, \quad \tau_a$ et δ_a sont bijectives,*
- *(iii) tout élément de G est régulier,*
- *(iv) l'élément neutre est le seul élément idempotent de G.*

Preuve.

- (i) Soit $a, b \in G$. $\forall x \in G$, $\tau_a \circ \tau_b(x) = \tau_a(\tau_b(x)) = \tau_a(bx) = a(bx) = (ab)x = \tau_{ab}(x)$ et $\delta_a \circ \delta_b(x) = (xb)a = x(ba) = \delta_{ba}(x)$
- (ii) Soit $a \in G$. D'après (i), on a

  $$\tau_a \circ \tau_{a^{-1}} = \tau_{aa^{-1}} = Id_G \text{ et } \quad \tau_{a^{-1}} \circ \tau_a = \tau_{a^{-1}a} = Id_G,$$

  donc τ_a est bijective et $(\tau_a)^{-1} = \tau_{a^{-1}}$. De même, on a $(\delta_a)^{-1} = \delta_{a^{-1}}$.
- (iii) Soit $a \in G$. D'après l'injectivité de τ_a et δ_a on a $\forall x, y \in G$:

  $$\begin{array}{ccc} (\tau_a(x) = \tau_a(y) \Rightarrow x = y) & \text{et} & (\delta_a(x) = \delta_a(y) \Rightarrow x = y) \\ \text{i.e. } (ax = ay \Rightarrow x = y) & \text{et} & (xa = ya \Rightarrow x = y) \end{array}$$

  donc a est régulier.
- (iv) En particulier, pour tout $x \in G \quad : \quad x \cdot x = x \Leftrightarrow x \cdot x = x \cdot e \Rightarrow x = e.$

□

I.4 Homomorphismes de Groupes

Définitions I.4.1. *Soit G et G' deux groupes. On appelle homomorphisme de G dans G', une application f de G dans G', telle que :*

$$\forall x, y \in G,\ f(xy) = f(x)f(y)$$

On note $Hom(G, G')$ l'ensemble des homomorphismes de G dans G'.

Si $f \in Hom(G, G')$ et f est surjective (resp. f est injective), f est dite un épimorphisme (resp. monomorphisme).

On dit que $f \in Hom(G, G')$ est un isomorphisme de groupes si f est bijective.

S'il existe un isomorphisme de G sur G', on dit que les groupes G et G' sont isomorphes et on note $G \cong G'$.

Un homomorphisme de G dans lui-même est appelé endomorphisme de G. On note $End(G)$ l'ensemble des endomorphismes de G.

On appelle un automorphisme de G, un isomorphisme de G sur lui-même. L'ensemble des automorphismes est noté $Aut(G)$.

Propriétés I.4.1. *Soit G et G' deux groupes d'éléments neutres e et e'. Si f est un homomorphisme de G vers G' alors :*

- *(1) $f(e) = e'$*
- *(2) $f(x^{-1}) = (f(x))^{-1}, \quad \forall x \in G$*
- *(3) $\forall k \in \mathbb{Z}, \forall x \in G, \quad f(x^k) = (f(x))^k$*
- *(4) Si de plus f est bijective, i.e. si f est un isomorphisme de G dans G' alors f^{-1} la réciproque de f est aussi un isomorphisme de G' dans G. En effet, $\forall x, y \in G$:*

$$\begin{aligned} f^{-1}(xy) &= f^{-1}(f \circ f^{-1}(x) \cdot f \circ f^{-1}(y)) = f^{-1}(f(f^{-1}(x)) \cdot f(f^{-1}(y))) \\ &= f^{-1}(f(f^{-1}(x) \cdot f^{-1}(y))) = f^{-1} \circ f(f^{-1}(x) \cdot f^{-1}(y)) \\ &= f^{-1}(x) \cdot f^{-1}(y) \end{aligned}$$

Exemples. — *Soit G et G' deux groupes d'éléments neutres e et e' respectivement.*

$$\begin{array}{rccc} f_0 : & G & \longrightarrow & G' \\ & x & \longmapsto & e' \end{array}$$

est un homomorphisme appelé homomorphisme nul.

— *Soit G un groupe et $a \in G$. L'application :*

$$\begin{array}{rccc} \sigma_a : & G & \longrightarrow & G \\ & x & \longmapsto & axa^{-1} \end{array}$$

est un automorphisme de G appelé automorphisme intérieur déterminé par a. $(\sigma_a)^{-1} = \sigma_{a^{-1}}$. En effet, on remarque que $\sigma_a = \tau_a \circ \delta_a$ donc, σ_a est bijective. C'est un homomorphisme car :

$\forall x, y \in G, \quad \sigma_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = axa^{-1}aya^{-1} = \sigma_a(x)\sigma_a(y)$

— *On considère le groupe $(\mathbb{Z}, +)$ et un groupe G noté multiplicativement d'élément neutre e. Soit $x \in G$. L'application :*

$$\begin{array}{rccc} f : & \mathbb{Z} & \longrightarrow & G \\ & k & \longmapsto & x^k \end{array}$$

f est un homomorphisme de groupes (voir TD).

Proposition I.4.1. *Soit G, G' et G'' trois groupes. Si $f : G \longrightarrow G'$ et $g : G' \longrightarrow G''$ sont deux homomorphismes alors la composée $g \circ f : G \longrightarrow G''$ est un homomorphisme.*

Corollaire I.1. *L'ensemble des automorphismes d'un groupe G, muni de la composition est un groupe.*

Preuve. On sait que la composition est une L.C.I. sur l'ensemble des applications de G dans G qui est associative et admet Id_G comme élément neutre. Il résulte de la proposition précédente et du fait que la composition de deux bijections est une bijection que $Aut(G)$ est stable par la composition, et par suite, la composition sur l'ensemble des automorphismes est une L.C.I., associative et admet Id_G comme élément neutre car $Id_G \in Aut(G)$. Finalement, d'après la propriété I.4.1 précédente, pour tout $f \in Aut(G)$ on a $f^{-1} \in Aut(G)$ donc tout élément de $Aut(G)$ est symétrisable. □

I.5 Groupes Quotients

Proposition et Définition I.5.1. *Soit G un groupe noté multiplicativement et d'élément neutre e. Soit R une relation d'équivalence sur G compatible avec la loi " $\cdot$ " de G. L'ensemble quotient G/R muni de la loi "$\dot{\cdot}$" définie par : $\overline{x} \dot{\cdot} \overline{y} = \overline{x \cdot y}, \forall \overline{x}, \overline{y} \in G/R$ a alors la structure d'un groupe appelé groupe quotient.*

Preuve. D'après §2., il résulte du fait que "$\cdot$" est une L.C.I. sur G et R est une relation d'équivalence sur G compatible avec la loi "$\cdot$", que "$\dot{\cdot}$" est une L.C.I. sur G/R.
Les autres propriétés de la loi quotient de G/R découlent de celles vérifiées par la loi de G. □

Remarque. — *La loi quotient induite par celle de G est l'unique L.C.I sur G/R telle que la surjection canonique $p : G \longrightarrow G/R$ soit un homomorphisme de groupes.*

— *Si G est abélien alors G/R l'est aussi.*

Exemple. On considère le groupe $(\mathbb{Z}, +)$. Soit $n \in \mathbb{N}^*$ et R la relation de congruence modulo n sur $\mathbb{Z}$ (on rappelle que x est congru à y modulo n et on écrit $x \equiv y[n]$ si $x - y$ est divisible par n, autrement dit si $x - y \in n\mathbb{Z}$), alors $\mathbb{Z}/R$ muni de la loi $\overline{+}$ est un groupe abélien qu'on note $\mathbb{Z}/n\mathbb{Z}$.

Exercice 1. *Montrer que $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$. En conclure que le groupe $(\mathbb{Z}/n\mathbb{Z}, \overline{+})$ est d'ordre n.*

Dans la suite on utilisera la même notation pour la loi quotient ($\overline{\cdot}$) induite par la loi de G et la loi de G.

I.6 Produit Direct de Groupes

Proposition I.6.1. *Soit $(G_1, \cdot)$ et $(G_2, \cdot)$ deux groupes. On définit sur l'ensemble $G_1 \times G_2$ la loi :*

$$\forall (x_1, x_2), (y_1, y_2) \in G_1 \times G_2 \quad : \quad (x_1, x_2) \cdot (y_1, y_2) = (x_1 \cdot y_1, x_2 \cdot y_2)$$

On a alors :

— *(i) $(G_1 \times G_2, \cdot)$ est un groupe appelé groupe produit direct de G_1 et G_2,*

— *(ii) les projections canoniques :*

$$p_1 : \begin{array}{ccc} G_1 \times G_2 & \longrightarrow & G_1 \\ (x_1, x_2) & \longmapsto & x_1 \end{array} \quad et \quad p_2 : \begin{array}{ccc} G_1 \times G_2 & \longrightarrow & G_2 \\ (x_1, x_2) & \longmapsto & x_2 \end{array}$$

sont des épimorphismes de groupes.

Preuve. — (i) La loi "$\cdot$" est une L.C.I. sur $G_1 \times G_2$

— (ii) l'associativité de la loi de $G_1 \times G_2$ découle de l'associativité de la loi de G_1 et de celle de G_2.

On vérifie aisément que (e_1, e_2) est l'élément neutre de $G_1 \times G_2$ pour la loi et que tout élément $(x_1, x_2) \in G_1 \times G_2$ est symétrisable : $(x_1, x_2)^{-1} = (x_1^{-1}, x_2^{-1})$. □

Remarque. — *$G_1 \times G_2$ est abélien si et seulement si G_1 et G_2 le sont,*

— *le produit direct $G_1 \times G_2$ est isomorphe au groupe produit direct $G_2 \times G_1$,*

— *plus généralement : si* $(G_i)_{i\in I}$ *est une famille de groupes, l'ensemble*

$$\prod_{i\in I} G_i = \{(x_i)_{i\in I} \quad / \quad \forall i \in I,\, x_i \in G_i\}$$

muni de la loi :

$$(x_i)\cdot(y_i) = (x_i y_i) \quad \forall (x_i),(y_i) \in \prod_{i\in I} G_i$$

alors, $(\prod_{i\in I} G_i, \cdot)$ *est un groupe appelé groupe produit.*

I.7 Sous-groupes

Définition I.7.1. *Soit* H *une partie non vide d'un groupe* G*.* H *est dit sous-groupe de* G *et noté* $H \prec G$ *si* H *est stable par la loi de* G *et si* H *muni de la loi induite par celle de* G *est un groupe.*

Exemples. — $\mathbb{Z}$ *est un sous-groupe de* $(\mathbb{R}, +)$*.*

— $Aut(G) \prec B(G)$ *où* G *est un groupe.*

— $\mathbb{Q}^*$ *est un sous-groupe de* $(\mathbb{R}^*, \cdot)$

Proposition I.7.1. *Soit* H *une partie d'un groupe* G*.* H *est un sous-groupe si et seulement si :*

— *(i)* $H \neq \emptyset$*,*

— *(ii)* $\forall x, y \in H, \quad xy \in H$

— *(iii)* $\forall x \in H, \quad x^{-1} \in H$*.*

Remarque. — *(i) et (ii)* $\Leftrightarrow \forall x, y \in H, \quad xy^{-1} \in H$*,*

— *Tout groupe admet toujours au moins pour sous-groupes* $\{e\}$ *et* G*,*

— *Tout sous-groupe d'un groupe abélien est lui-même abélien,*

— *Si* H *est un sous-groupe de* G *et si* K *est un sous-groupe de* H *alors* K *est un sous-groupe de* G*.*

— *Soit* H *et* K *deux sous-groupes de* G*.*

L'intersection de H *et* K*,* $H \cap K$*, est un sous-groupe de* G*. D'une manière générale, si* $(H_i)_{i\in I}$ *est une famille quelconque de sous-groupes de* G*, alors* $\bigcap_{i\in I} H_i$ *est un sous-groupe de* G*.*

$H \cup K$ *est un sous-groupe de* G *si et seulement si* $H \subset K$ *ou* $K \subset H$*.*

On désigne par HK *le sous-ensemble de* G *formé des éléments qui s'écrivent comme le produit d'un élément de* H *par un élément de* K *:* $HK = \{hk \quad / h \in H, k \in K\}$*.* HK *est un sous-groupe de* G *si et seulement si* $HK = KH$*.* ***(à montrer !)****.*

Exercice 2. *Montrer que tout sous-groupe de* $\mathbb{Z}$ *est de la forme* $n\mathbb{Z}$ *où* $n \in \mathbb{N}$.

Proposition I.7.2. *Soit* G *et* G' *deux groupes d'éléments neutres* e *et* e' *respectivement. Soit* f *un homomorphisme de* G *dans* G'.

- *(i) Si* H *est un sous-groupe de* G *alors* $f(H)$ *est un sous-groupe de* G'. *En particulier,* $f(G)$ *est un sous-groupe de* G *appelé image de* f *et noté* $Im(f)$.
- *(ii) Si* H' *est un sous-groupe de* G' *alors* $f^{-1}(H')$ *est un sous-groupe de* G. *En particulier,* $f^{-1}(\{e'\})$ *est un sous-groupe de* G.

$$f^{-1}(\{e'\}) = \{x \in G \,/ \quad f(x) = e'\}$$

  est appelé noyau de f *et noté* $Ker(f)$.
- *(iii)* f *est injectif* $\Leftrightarrow Ker(f) = \{e\}$

Preuve. Exercice ! □

Exercice 3. *Soit* G *et* G' *deux groupes. Soit* $f \in Hom(G, G')$ *et* A *une partie de* G. *Montrer que*

$$\begin{aligned} f^{-1}(f(A)) &= AKer(f) = Ker(f)A \qquad \textit{en notation multiplicative} \\ &= A + Ker(f) = Ker(f) + A \qquad \textit{en notation additive} \end{aligned}$$

Proposition I.7.3. *Soit* $f : G \to G'$ *un homomorphisme de groupes et* R *la relation d'équivalence sur* G *définie par* $xRy \iff f(x) = f(y)$ *alors* R *est compatible avec la loi de* G *et l'ensemble quotient* G/R *muni de la loi quotient est un groupe ; Si* $j : f(G) \to G'$ *désigne l'injection canonique et* $p : G \to G/R$ *la surjection canonique, il existe un homomorphisme unique* $\overline{f} : G/R \to Im(f)$ *tel que* $j \circ \overline{f} \circ p = f$, *de plus* $\overline{f}$ *est bijective (*$\overline{f}$ *est un isomorphisme de groupes).*

Preuve. R est une relation d'équivalence compatible avec la loi de G, d'après l'homomorphisme de f, et par suite G/R muni de la loi quotient est un groupe. Par ailleurs, d'après la décomposition de l'application f, il existe une application unique $\overline{f} : G/R \to Im(f)$ tel que $j \circ \overline{f} \circ p = f$. De plus $\overline{f}$ est bijective.

Il reste à montrer que $\overline{f}$ est un homomorphisme, sachant que j, p et f sont des homomorphismes de groupes. Soit $\overline{x}, \overline{y} \in G/R$.

$$\begin{aligned} j \circ \overline{f}(\overline{x}\,\overline{y}) = j \circ \overline{f}(\overline{xy}) &= j \circ \overline{f} \circ p(xy) = f(xy) \\ &= f(x)f(y) = j \circ \overline{f} \circ p(x) \cdot j \circ \overline{f} \circ p(y) \\ &= j \circ \overline{f}(\overline{x}) \cdot j \circ \overline{f}(\overline{y}) = j(\overline{f}(\overline{x})) \cdot j(\overline{f}(\overline{y})) \\ &= j(\overline{f}(\overline{x})\overline{f}(\overline{y})) \end{aligned}$$

Et d'après l'injectivité de j, on conclut que $\overline{f}(\overline{x}\,\overline{y}) = \overline{f}(\overline{x})\overline{f}(\overline{y})$. □

Corollaire I.2. *Soit $f : G \to G'$ un homomorphisme de groupes et R la relation binaire sur G définie par $xRy \iff xy^{-1} \in Ker(f)$ alors R est une relation d'équivalence compatible avec la loi de G et l'ensemble quotient G/R noté $G/Ker(f)$ muni de la loi quotient est un groupe isomorphe à $Im(f)$.*

Produit Direct de deux Sous-groupes

Définition I.7.2. *Soit G un groupe, H et K deux sous-groupes de G. On dit que G est le produit direct (interne) de H par K lorsque les trois conditions suivantes sont vérifiées :*

$$(1) : G = HK \quad ; \quad (2) : H \cap K = \{e\} \quad ; \quad (3) : \forall h \in H, \forall k \in K, hk = kh.$$

Il est clair qu'alors, on a aussi $G = KH$ et que G est donc le produit direct de K par H.

Exemple. *Soit* $G = \{\begin{pmatrix} 1 & 0 & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \ / \ b, c \in \mathbb{R}\}$, $H = \{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \ / \ b \in \mathbb{R}\}$,

$K = \{\begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \ / \ c \in \mathbb{R}\}$

G est un sous-groupe de $GL_3(\mathbb{R})$, H et K sont des sous-groupes de G, et G est le produit direct de H par K.

Remarques. *Soit G un groupe et H, K deux sous-groupes de G.*

- *(a) Si $H \cap K = \{e\}$, tout élément de HK s'écrit de façon unique sous la forme hk avec $h \in H, k \in K$.*
- *(b) Si $H \cap K = \{e\}$ et si H et K sont finis alors HK est fini et $card(HK) = |H||K|$.*
- *(c) Si G est le produit direct interne de H par K alors G est isomorphe au groupe produit $H \times K$.*

En effet, (a) : si $h_1k_1 = h_2k_2$ avec $h_1, h_2 \in H_1$ et $k_1, k_2 \in K_2$, on a $h_2^{-1}h_1 = k_2k_1^{-1}$. Le premier produit est dans H puisque H est un sous-groupe, et le second est dans K puisque K est un sous-groupe. Donc $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K$, c'est-à-dire $h_2^{-1}h_1 = k_2k_1^{-1} = e$, et donc $h_2 = h_1$ et $k_2 = k_1$.

(b) : il résulte du point précédent que $H \times K$ est alors équipotent à HK, par la bijection $(h, k) \mapsto hk$.

Proposition I.7.4. *Soit G_1 et G_2 deux groupes d'élément neutre e_1 et e_2 respectivement, et $G = G_1 \times G_2$ leur produit direct. On pose : $H = G_1 \times \{e_2\}$ et $K = \{e_1\} \times G_2$. Alors, H est un sous-groupe de G isomorphe à G_1, K est un sous-groupe de G isomorphe à G_2, et G est le produit direct interne de ces sous-groupes, H et K.*

Les notions de produit direct de deux groupes et de produit direct interne de deux sous-groupes d'un groupe sont en fait deux formulations d'une même notion.

Sous-groupe Engendré par une Partie

Définition I.7.3. *Soit A une partie d'un groupe G. L'intersection de tous les sous-groupes de G qui contiennent A est appelée le sous-groupe engendré par A dans G et noté $< A >$.*

Si $A = \{a_1, a_2, \cdots, a_n\}$ est une partie finie de G, on note $< A >=< a_1, a_2, \cdots, a_n >$ et on dit que c'est un sous-groupe de type fini.

Soit $a \in G$. Le sous-groupe engendré par le singleton $\{a\}$, noté $< a >$, s'appelle sous groupe monogène ou cyclique engendré par a.

Exemple. $< \emptyset >= \{e\}$; $< G >= G$

Proposition I.7.5. *Soit G un groupe et A une partie de G. Le sous-groupe engendré par A est le plus petit sous-groupe (pour l'inclusion) de G contenant A.*

Preuve. Soit $\mathcal{C}$ l'ensemble des sous-groupes de G contenant A, on a $< A >= \bigcap_{H \in \mathcal{C}} H$, donc $A \subset < A >$ et $< A > \in \mathcal{C}$. Par ailleurs, $\forall H \in \mathcal{C} :< A > \subset H$. Donc $< A >$ est le plus petit sous-groupe de G contenant A. □

Proposition I.7.6. *Soit G un groupe et A une partie non vide de G. Alors,*

$$< A >= \left\{ x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n} \quad / \quad n \in \mathbb{N}^*, \forall i \in \{1, 2, \cdots, n\}, \quad x_i \in A \ \ et \, \epsilon_i = \pm 1 \right\}$$

En particulier, $< a >= \{a^k \quad / \quad k \in \mathbb{Z}\}$.

Remarque. *L'égalité ci-dessus peut s'écrire aussi :*

$< A >= \left\{ x_1 x_2 \cdots x_n \quad / \quad n \in \mathbb{N}^*, \forall i \in \{1, 2, \cdots, n\}, \quad x_i \in A \cup A^{-1} \right\}$ *où* $A^{-1} = \left\{ x^{-1} \quad / \quad x \in A \right\}$.

Preuve. On pose

$$H = \left\{ x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n} \quad / \quad n \in \mathbb{N}^*, \forall i \in \{1, 2, \cdots, n\}, \quad x_i \in A \ \text{ et } \ \epsilon_i = \pm 1 \right\}$$

On montre que H est un sous-groupe de G contenant A.

A est non vide, soit alors $x \in A$, $e = xx^{-1} \in H$ d'où $H \neq \emptyset$.

Soit $h_1, h_2 \in H$,

$h_1 = \prod\limits_{1 \leq i \leq n} x_i^{\epsilon_i}$ où $n \in \mathbb{N}^*, \forall i \in \{1, 2, \cdots, n\}, \quad x_i \in A$ et $\epsilon_i = \pm 1$

$h_2 = \prod\limits_{1 \leq j \leq m} y_j^{\alpha_j}$ où $m \in \mathbb{N}^*, \forall j \in \{1, 2, \cdots, m\}, \quad y_j \in A$ et $\alpha_j = \pm 1$

On a alors, d'une part :

$$h_1 h_2 = \prod_{1 \leq i \leq n} x_i^{\epsilon_i} \prod_{1 \leq j \leq m} y_j^{\alpha_j} \in H \text{ , par définition de } \quad H.$$

D'autre part,

$$h_1^{-1} = \left(\prod_{1\leq i\leq n} x_i^{\epsilon_i}\right)^{-1} = \left(x_1^{\epsilon_1}x_2^{\epsilon_2}\cdots x_n^{\epsilon_n}\right)^{-1} = x_n^{-\epsilon_n}x_{n-1}^{-\epsilon_{n-1}}\cdots x_2^{-\epsilon_2}x_1^{-\epsilon_1} \in H$$

Ainsi, H est un sous-groupe de G. Et $\forall x \in A, \quad x = x^1 \in H$ d'où $A \subset H$, donc H est un sous-groupe de G contenant A et par conséquent $< A > \subset H$.

Inversement, soit $h \in H$ donc $\exists n \in \mathbb{N}^*, \quad \exists x_1, \cdots, x_n \in A$ tel que $h = \prod_{i=1}^n x_i^{\epsilon_i}$ avec $\epsilon_i = \pm 1$. Comme $A \subset < A >$ donc $\forall i \in \{1, \cdots, n\}, \quad x_i \in < A >$ et d'après la stabilité de $< A >$ par la loi et par l'inverse, on conclut que $h \in < A >$ d'où $H \subset < A >$. Conclusion $H = < A >$. □

Remarques. — $< e >= \{e\}$

— *si H_1 et H_2 sont deux sous-groupes de G,*

$$< H_1 \cup H_2 >= \left\{x_1x_2\cdots x_n / \quad n \in \mathbb{N}^*, \forall i \in \{1, \cdots, n\}, \quad x_i \in H_1 \cup H_2\right\}$$

Si de plus $H_1 H_2 = H_2 H_1$ alors $< H_1 \cup H_2 >= H_1H_2$.

— *si G est un groupe dont la loi est additive, $\forall x \in G, \quad < x >= \{kx \quad / k \in \mathbb{Z}\}$.*
On considère le groupe $(\mathbb{Z}, +)$, on a alors $\forall p \in \mathbb{Z}^*, \quad < p >= \{kp \quad / k \in \mathbb{Z}\} = |p|\mathbb{Z}$.

Proposition I.7.7. *Soit $f : G \to G'$ un homomorphisme de groupes. Si A est une partie non vide de G alors $f(< A >) =< f(A) >$. En particulier, si A est de type fini, alors $f(< A >)$ est un sous-groupe de type fini. L'image d'un groupe de type fini par un homomorphisme de groupes est un groupe de type fini.*

Preuve. $< f(A) > \subset f(< A >)$ car $A \subset < A >$ et $< f(A) >$ est le plus petit sous-groupe contenant $f(A)$. Réciproquement, soit $y \in f(< A >)$, $\exists x \in < A >$ tel que $y = f(x)$, donc, $\exists n \in \mathbb{N}^*, \exists x_1, \cdots, x_n \in A$ tel que $x = \prod_{i=1}^n x_i^{\epsilon_i}$ où $\epsilon_i = \pm 1$ et $y = f(\prod_{i=1}^n x_i^{\epsilon_i})$.
Il résulte de l'homomorphisme de f que $y = \prod_{i=1}^n f(x_i)^{\epsilon_i}$ avec $f(x_i) \in f(A)$ et $\epsilon_i = \pm 1$, $\forall 1 \leq i \leq n$. Ce qui prouve que $y \in < f(A) >$. □

II Ordre d'un Elément et Groupe Cyclique

II.1 Ordre d'un Elément

Définition II.1.1. *Soit G un groupe et a un élément de G.*

— *(i) On dit que a est d'ordre infini dans G si le sous-groupe de G engendré par a, $< a >$, est infini.*

— *(ii) Si $< a >$ est fini, on dit que a est d'ordre fini et $| < a > |$, i.e. le cardinal de $< a >$ s'appelle l'ordre de a et on le note $o(a)$.*

Exemple. *1.* $o(e) = 1$ *et* e *est l'unique élément de* G *d'ordre* 1.

2. Dans $(\mathbb{Z}, +)$, $\forall p \in \mathbb{Z}^*$, p *est d'ordre infini.*

Remarques. $\forall a, b \in G$, $o(a) = o(a^{-1})$, $o(bab^{-1}) = o(a)$, $o(ab) = o(ba)$.

Exercice 4. *Montrer que si* a *est l'unique élément d'ordre* 2 *d'un groupe* G, *alors* a *appartient au centre de* G, $Z(G)$.

Théorème II.1. *Soit* G *un groupe et* a *un élément de* G. *Soit l'homomorphisme*

$$\begin{aligned} f : \mathbb{Z} &\to G \\ p &\mapsto a^p \end{aligned}$$

On a alors

1. *Si* f *est injectif,* a *est d'ordre infini.*
2. *Sinon,* a *est d'ordre fini et son ordre est l'entier* n *strictement positif tel que* $Ker(f) = n\mathbb{Z}$.

Preuve. On a $Im(f) =< a >$ donc f est un homomorphisme surjectif de $\mathbb{Z}$ sur $< a >$.

1. Si f est injectif alors f est un isomorphisme de $\mathbb{Z}$ sur $< a >$, ainsi a est d'ordre infini.
2. Si f n'est pas injectif alors $Ker(f)$ est un sous-groupe non nul de $\mathbb{Z}$. Dans ce cas, il existe $n \in \mathbb{N}^*$ tel que $Ker(f) = n\mathbb{Z}$ et par factorisation de f à travers son noyau $n\mathbb{Z}$, on obtient $\mathbb{Z}/n\mathbb{Z} \cong < a >$, par suite a est d'ordre fini et $o(a) = n$.

□

Corollaire II.1. *Soit* G *un groupe et* $a \in G$.

$$\begin{aligned} a \text{ est d'ordre infini} &\iff \forall k \in \mathbb{Z}^*, \quad a^k \neq e \\ &\iff \forall k \in \mathbb{Z}, \quad a^k = e \Leftrightarrow k = 0 \end{aligned}$$

Soit $m \in \mathbb{N}^*$.

$$\begin{aligned} o(a) = m &\iff m \text{ est le plus petit entier strictement positif tel que } a^m = e \\ &\iff (\forall k \in \mathbb{Z},\ a^k = e \iff m \text{ divise } k). \end{aligned}$$

Preuve. La preuve se déduit du fait que $Ker(f) = \{k \in \mathbb{Z} : a^k = e\}$ et du théorème. □

Corollaire II.2. *Soit* G *un groupe et* $a \in G$.

1. *Si a est d'ordre infini, les éléments de $< a >$ sont distincts deux à deux.*
2. *Si $o(a) = m$ où $m \in \mathbb{N}^*$ alors $< a >= \{e, a, \cdots, a^{m-1}\}$.*

Preuve. 1. Si a est d'ordre infini, f est injectif, donc $\forall k, k' \in \mathbb{Z},\ k \neq k' \Longrightarrow a^k \neq a^{k'}$.

2. $o(a) = m \Longleftrightarrow Ker(f) = m\mathbb{Z}$, et d'après la factorisation de f,

$$\begin{array}{rcl} \overline{f} : \mathbb{Z}/m\mathbb{Z} & \longrightarrow & < a > \\ \overline{p} & \longmapsto & \overline{f}(\overline{p}) = f(p) = a^p \end{array}$$

est un isomorphisme de groupes. D'où
$< a >= \{\overline{f}(\overline{p}) \quad / \quad \overline{0} \leq \overline{p} \leq \overline{m-1}\} = \{e, a, a^2, \cdots, a^{m-1}\}$.

□

Proposition II.1.1. *Soit G un groupe et a un élément de G d'ordre m. Alors :*
$\forall k \in \mathbb{Z}, \quad o(a^k) = \frac{m}{pgcd(m,k)}$

Preuve. Soit $k \in \mathbb{Z}$. On pose $d = pgcd(m, k)$, donc $\exists m', k' \in \mathbb{Z}$ tels que $m = dm'$, $k = dk'$ et $pgcd(m', k') = 1$. On a $(a^k)^{m'} = a^{km'} = a^{k'dm'} = a^{k'm} = e$.

Et, $\forall p \in \mathbb{N}^*, \quad (a^k)^p = e \Longleftrightarrow a^{kp} = e \Longleftrightarrow m/kp \Longleftrightarrow m'/k'p \Longleftrightarrow m'/p$, donc
$o(a^k) = m' = \frac{m}{d} = \frac{m}{pgcd(m,k)}$. □

Proposition II.1.2. *Soit G un groupe et a, b deux éléments de G d'ordres respectifs m et n. On suppose $ab = ba$. On a alors : $o(ab) = mn \Longleftrightarrow pgcd(m, n) = 1$.*

Preuve. On suppose $o(ab) = mn$. Soit $d = pgcd(m, n)$, alors $m = dm'$ et $n = dn'$, d'où $(ab)^{dm'n'} = (a^{dm'})^{n'}(b^{dn'})^{m'} = e$. Il résulte alors de l'hypothèse que $mn/dm'n'$ donc $dm'dn'/dm'n'$ ce qui donne $d/1$ d'où $d = 1$.

Réciproquement, on suppose que $pgcd(m, n) = 1$.

— On a $(ab)^{mn} = (a^m)^n(b^n)^m = e$.

— Soit $k \in \mathbb{N}^*$,

$$\begin{array}{rcl} (ab)^k = e & \Longleftrightarrow & a^k b^k = e \ (\text{car} \quad ab = ba) \\ & \Longleftrightarrow & a^k = b^{-k} \Rightarrow b^{-k} = a^k \in < a > \cap < b > . \end{array}$$

On pose $c = b^{-k} = a^k$. Par hypothèse, m et n sont premiers entre eux, donc d'après le théorème de Bézout, $\exists u, v \in \mathbb{Z}$ tel que $mu + nv = 1$ on a alors $c = c^1 = c^{mu+nv} = c^{mu}c^{nv} = (a^m)^{ku}(b^n)^{-kv} = e$ d'où $a^k = b^{-k} = e$. Par suite, m/k et n/k et il résulte de l'hypothèse que mn/k.

□

Proposition II.1.3. *Soit G, G' deux groupes et a, b deux éléments de G, G' respectivement, d'ordre fini. Alors l'élément $(a, b) \in G \times G'$ est d'ordre fini et $o(a, b) = ppcm(o(a), o(b))$.*

Preuve. Soit $m = o(a), n = o(b)$. On note $\mu = ppcm(m, n)$ donc, $\exists m', n' \in \mathbb{N}$ tel que $\mu = mm'$ et $\mu = nn'$, d'où $(a, b)^\mu = (a^\mu, b^\mu) = ((a^m)^{m'}, (b^n)^{n'}) = (e, e')$.

Soit $p \in \mathbb{N}^*$:

$$\begin{aligned} (a,b)^p = (e,e') &\iff (a^p, b^p) = (e, e') \\ &\iff (a^p = e \text{ et } b^p = e') \\ &\iff (o(a)/p \text{ et } o(b)/p) \iff ppcm(o(a), o(b))/p \end{aligned}$$

donc le plus petit entier strictement positif tel que $(a, b)^p = (e, e')$ est le $ppcm(o(a), o(b))$.

□

II.2 Groupes Cycliques

Définition II.2.1. *Un groupe G est dit cyclique lorsqu'il est engendré par un de ses éléments, i.e. lorsqu'il existe un élément $x \in G$ tel que $G =< x >$.*

Exemple.

— *$\mathbb{Z} =< 1 >$ est un groupe cyclique infini.*

— *Pour $n \geq 2$, on a $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$, et $\forall \overline{k} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{k} = k\overline{1}$. Donc $\mathbb{Z}/n\mathbb{Z} =< \overline{1} >$ est un groupe cyclique fini.*

— *Tout sous-groupe $n\mathbb{Z}$ (où $n \in \mathbb{N}^*$) est un groupe cyclique infini, $n\mathbb{Z} = \{nk \quad k \in \mathbb{Z}\} =< n >$.*

— *Soit $n \in \mathbb{N}^*$, le sous-groupe $\mathbb{U}_n = \{z \in \mathbb{C}^* / z^n = 1\}$ de $\mathbb{C}^*$ est un groupe cyclique fini engendré par $e^{i2\pi/n}$.*

Théorème II.2. *Tout groupe cyclique infini est isomorphe à $\mathbb{Z}$, et tout groupe cyclique fini d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Preuve. Soit G un groupe cyclique, $\exists a \in G, G =< a >$. L'homomorphisme

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow G =< a > \\ k &\longmapsto a^k \end{aligned}$$

est surjectif et d'après la factorisation de f on a $\mathbb{Z}/Ker(f) \cong G$. Si G est infini, a est donc d'ordre infini et d'après le théorème II.1 f est alors injectif, i.e. $Ker(f) = \{0\}$, et par suite $G \cong \mathbb{Z}$. Si G est fini d'ordre n, a est d'ordre n et donc d'après le théorème II.1 $Ker(f) = n\mathbb{Z}$, et $G \cong \mathbb{Z}/n\mathbb{Z}$. □

Corollaire II.3. *Deux groupes cycliques finis sont isomorphes si et seulement si ils ont le même ordre.*

Preuve. Si G et G' sont isomorphes, ils ont le même cardinal. Réciproquement, si G et G' sont cycliques, $|G| = |G'| = n$, le théorème montre que G et G' sont isomorphes à $\mathbb{Z}/n\mathbb{Z}$. □

Proposition II.2.1. *1. (i) Tout sous-groupe d'un groupe cyclique est cyclique.*

2. *(ii) Soit G un groupe cyclique et $f : G \to G'$ un homomorphisme de groupes surjectif. Alors G' est cyclique.*

3. *(iii) Le groupe quotient d'un groupe cyclique est cyclique.*

Preuve. 1. (i) Soit H un sous-groupe d'un groupe cyclique $G =< a >$ avec $H \neq \{e\}$. Soit m le plus petit entier strictement positif tel que $a^m \in H$. On a alors $< a^m > \subset H$. Réciproquement, soit $a^p \in H$ avec $p \in \mathbb{N}^*$, la division euclidienne de p par m donne $p = mq + r$ avec $(q, r) \in \mathbb{N}^2$ et $0 \leq r < m$. $a^p = (a^m)^q \cdot a^r$ et par suite $a^r = a^p(a^m)^{-q} \in H$. Puisque $0 \leq r < m$ et m est le plus petit entier strictement positif tel que $a^m \in H$ on a alors $r = 0$ et il s'ensuit $a^p = (a^m)^q \in < a^m >$, donc $H \subset < a^m >$.

2. (ii) G est cyclique donc $\exists a \in G$ tel que $G =< a >$ et comme f est un homomorphisme de G dans G', il résulte de la proposition I.7.7 : $f(G) = f(< a >) =< f(a) >$ et finalement d'après la surjection de f, on obtient $G' =< f(a) >$.

3. (iii) G/R est l'image homomorphe de G par l'homomorphisme surjectif canonique $p : G \to G/R$ donc d'après ce qui précède G/R est cyclique.

□

Proposition II.2.2. *Soit G_1 et G_2 deux groupes finis d'ordres respectifs m et n. Le produit $G_1 \times G_2$ est cyclique si et seulement si G_1 et G_2 sont cycliques dont les ordres sont premiers entre eux.*

Preuve. Supposons que $G_1 \times G_2$ est cyclique et engendré par (a, b). La projection p_1 (resp. p_2) de G sur G_1 (resp. sur G_2) sont des homomorphismes surjectifs. D'après la proposition précédente, $G_1 = Im(p_1)$ et $G_2 = Im(p_2)$ sont cycliques engendrés par a et b, donc $m = |G_1| = o(a)$ et $n = |G_2| = o(b)$. Il s'ensuit alors, d'après la proposition II.1.3 que $o(a, b) = ppcm(m, n)$. D'autre part, et comme

$$o(a, b) = |G_1 \times G_2| = |G_1||G_2| = mn$$

On conclut alors que $ppcm(m, n) = mn$, ainsi m et n sont premiers entre eux.

Réciproquement, supposons que G_1 et G_2 sont cycliques, d'ordres m et n premiers entre eux. Soit a un générateur de G_1 et b un générateur de G_2, d'après la proposition II.1.3, $o(a, b) = ppcm(m, n) = mn = |G_1||G_2| = |G_1 \times G_2|$, donc $G_1 \times G_2 =< (a, b) >$. □

Corollaire II.4. *Soit $m, n \in \mathbb{N}^*$,* $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/nm\mathbb{Z} \iff pgcd(n, m) = 1$

Générateurs d'un Groupe Cyclique

Théorème II.3. — *(i)* 1 *et* -1 *sont les seuls générateurs du groupe cyclique* $(\mathbb{Z},+)$.

— *(ii)* $\forall \overline{k} \in \mathbb{Z}/n\mathbb{Z}, (où\ n \in \mathbb{N}^*)$: $\overline{k}$ *est un générateur de* $\mathbb{Z}/n\mathbb{Z} \Longleftrightarrow pgcd(k,n) = 1$.

Preuve. — (i) S'il existe $p \in \mathbb{Z} \setminus \{-1,1\}$ tel que $\mathbb{Z} =< p >$, on aura alors $1 \in < p >$, donc $\exists k \in \mathbb{Z}$ tel que $1 = kp$, ceci est impossible.

— (ii) Pour $n \geq 2$, $\forall \overline{k} \in \mathbb{Z}/n\mathbb{Z}$,

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} =< \overline{k} > &\iff \exists m \in \mathbb{Z} \quad / \quad \overline{1} = m\overline{k} \Longleftrightarrow \exists m,p \in \mathbb{Z} \quad / \quad mk - 1 = pn \\ &\iff \exists m,p \in \mathbb{Z} \quad / \quad mk + (-p)n = 1 \Longleftrightarrow pgcd(n,k) = 1. \end{aligned}$$

□

Définition II.2.2. *La fonction d'Euler (ou encore indicateur d'Euler) est l'application* $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ *définie par* $\varphi(1) = 1$ *et pour* $n \geq 2$, $\varphi(n)$ *est le cardinal de l'ensemble* $\{k \in \mathbb{N} \quad / 0 \leq k \leq n-1 \ \ et \ \ pgcd(k,n) = 1\}$

Exemple. $\varphi(2) = 1$, $\varphi(3) = 2, \varphi(4) = 2$, $\varphi(5) = 4, \varphi(6) = 2$, $\varphi(7) = 6$, *et* $\varphi(8) = 4$

Exercice 5. *Montrer que* $\varphi(p) = p - 1$ *si et seulement si* p *est premier.*

Remarque. $\varphi(n)$ *est le cardinal de l'ensemble des générateurs de* $(\mathbb{Z}/n\mathbb{Z},+)$.

On va généraliser ce résultat.

Théorème II.4. *Soit* $G =< a >$ *un groupe cyclique.*

— *(i) Si* G *est infini alors* a *et* a^{-1} *sont les seuls générateurs de* G.

— *(ii) Si* G *est fini d'ordre* n, $\forall 0 \leq k \leq n-1, a^k$ *est un générateur de* $G \Leftrightarrow pgcd(n,k) = 1$. *Il existe donc* $\varphi(n)$ *générateurs distincts de* G. *En particulier, si* n *est premier, tous les éléments de* G *distincts de* e *sont des générateurs de* G.

Preuve. — Si G est infini, alors $G \cong \mathbb{Z}$. Comme 1 et -1 sont les seuls générateurs de $\mathbb{Z}$, on a alors a et a^{-1} sont les seuls générateurs de G.

— Si $|G| = n$, alors $G \cong \mathbb{Z}/n\mathbb{Z}$, ainsi, a^k est un générateur de $G \Longleftrightarrow \overline{k}$ est un générateur de $\mathbb{Z}/n\mathbb{Z} \Longleftrightarrow pgcd(k,n) = 1$.

□

III Classes. Sous-groupes Distingués. Groupe Quotient

III.1 Classes à Droite et Classes à Gauche

Définition III.1.1. *Soit G un groupe et H un sous-groupe de G. On définit une relation d'équivalence R_g sur G par : $\forall x, y \in G \quad xR_g y \Leftrightarrow x^{-1}y \in H$. D'une manière similaire on définit aussi une relation d'équivalence R_d sur G par : $\forall x, y \in G \quad xR_d y \Leftrightarrow xy^{-1} \in H$.*

Soit $x \in G$. La classe d'équivalence suivant R_g de x est $\overline{x}^g = \{xh/ \quad h \in H\} = xH$, appelée classe à gauche modulo H. De même, la classe d'équivalence suivant R_d de x est $\overline{x}^d = \{hx/ \quad h \in H\} = Hx$, appelée classe à droite modulo H.

On désigne par $(G/H)_g$ et $(G/H)_d$ l'ensemble des classes à gauche et l'ensemble des classes à droite modulo H respectivement.

Remarque.
- *Si G est abélien, les relations R_g et R_d coincident,*
- *en général, aucune de ces relations n'est compatible avec la loi de G,*
- *la classe à gauche et la classe à droite de l'élément neutre de G est H,*
- *$\forall x \in G$, xH, Hx et H sont équipotents via la translation à gauche et la translation à droite, respectivement. Donc, si H est fini, on a $|H| = card(xH) = card(Hx)$, $\forall x \in G$.*

Proposition III.1.1.

$$\begin{array}{rccc} \text{Soit} \quad \varphi : & (G/H)_g & \longrightarrow & (G/H)_d \\ & \overline{x}^g = xH & \longmapsto & Hx^{-1} = \overline{x^{-1}}^d \end{array}$$

φ est une application bijective. En particulier, si $(G/H)_g$ est fini, alors $(G/H)_d$ est fini et ils ont même nombre d'éléments.

Preuve. Montrons que φ est bien définie et injective : $\forall \overline{x}^g, \overline{y}^g \in (G/H)_g$.

$$\overline{x}^g = \overline{y}^g \Leftrightarrow xR_g y \Leftrightarrow x^{-1}y \in H \Leftrightarrow x^{-1}(y^{-1})^{-1} \in H \Leftrightarrow x^{-1}R_d\, y^{-1}$$
$$\Leftrightarrow \overline{x^{-1}}^d = \overline{y^{-1}}^d \Leftrightarrow Hx^{-1} = Hy^{-1} \Leftrightarrow \varphi(\overline{x}^g) = \varphi(\overline{y}^g)$$

Il est clair que φ est surjective. □

Définition III.1.2. *Si $(G/H)_g$ est fini alors on note $[G : H] = card(G/H)_g, (= card(G/H)_d)$ et on l'appelle l'indice de H dans G.*

Théorème III.1. *(Théorème de Lagrange) Si G est un groupe fini et H un sous-groupe de G, on a $|G| = [G : H]|H|$. En particulier, $|H|/|G|$.*

Preuve. Comme l'ensemble des classes distinctes à gauche (resp. à droite) forme une partition de G et toutes les classes à gauche (resp. à droite) ont le même cardinal $|H|$, on a alors $|G| = m|H|$ où m est le nombre de classes distinctes à gauche (resp. à droite) i.e. $[G : H]$. □

Si l'ordre de $|G| = n$ et $d \in \mathbb{N}^*$ est un diviseur de n alors il n'existe pas nécessairement un sous-groupe de G dont l'ordre est d. Par contre, si G est cyclique d'ordre n, alors pour tout diviseur d de n, il existe un et un seul sous-groupe de G dont l'ordre est d. (voir TD.)

Corollaire III.1. *Soit G un groupe fini.*

- *(a) $\forall x \in G, \quad o(x)/|G|$ en particulier $x^{|G|} = e$.*
- *(b) Si H est un sous-groupe de G et K un sous-groupe de H, alors $[G : K] = [G : H]\cdot[H : K]$.*

Preuve.
- (a) Il résulte du théorème de Lagrange que

$$\forall x \in G, \quad |G| = [G :< x >]| < x > | = [G :< x >]o(x)$$

  donc $o(x)/|G|$ et, par suite, $x^{|G|} = e$.
- (b) H est un sous-groupe de G et K un sous-groupe de H ; donc,

$$|G| = [G : H]|H| \text{ et } |H| = [H : K]|K|.$$

  Or, on a : $|G| = [G : K]\cdot|K|$. Par conséquent, $[G : K] = [G : H][H : K]$.

□

Théorème III.2. *Soit H et K deux sous-groupes finis d'un groupe G. Alors, $card(HK) = \dfrac{|H||K|}{|H \cap K|}$.*

Preuve. Soit $L = H \cap K$. On a $[K : L] = \dfrac{|K|}{|L|} = n$ et $(Lk_i)_{1\leq i\leq n}$ est une partition de K, d'où $K = \bigcup_{i=1}^{n} Lk_i$ et par suite, $HK = \bigcup_{i=1}^{n} HLk_i = \bigcup_{i=1}^{n} Hk_i$ car $HL = H$. Comme $(Hk_i)_{1<i<n}$ sont disjoints deux-à-deux, (en effet, s'il existe $i \neq j$ tel que $Hk_i \cap Hk_j \neq \emptyset$, il existe $h, h' \in H$ tels que $hk_i = h'k_j$ d'où $h'^{-1}h = k_jk_i^{-1} \in H \cap K = L$ et par suite $k_j \in Lk_i$, ceci est contradictoire avec $Lk_i \cap Lk_j = \emptyset$), on a alors

$$card(HK) = \sum_{i=1}^{n} card(Hk_i) = n|H| = \frac{|H||K|}{|H \cap K|}.$$

□

III.2 Sous-groupes Distingués

Définition III.2.1. *Un sous-groupe H d'un groupe G est dit distingué ou normal si $\forall x \in G, \quad xHx^{-1} = H$. On notera $H \trianglelefteq G$.*

Remarque. — *Tout sous-groupe d'un groupe abélien est distingué.*

— *G et $\{e\}$ sont des sous-groupes distingués de G.*

Proposition III.2.1. *Soit H un sous-groupe d'un groupe G alors les conditions suivantes sont équivalentes :*

— *(i) $xH = Hx, \quad \forall x \in G$*

— *(ii) $xHx^{-1} \subset H, \quad \forall x \in G$*

— *(iii) $xHx^{-1} = H, \quad \forall x \in G$ i.e. $H \trianglelefteq G$.*

Preuve. — $(i) \Leftrightarrow (iii)$: les translations à gauche étant bijectives, $\forall x \in G$, $xH = Hx \Leftrightarrow xHx^{-1} = Hxx^{-1} \Leftrightarrow xHx^{-1} = H$

— $(ii) \Rightarrow (iii)$: on suppose que $xHx^{-1} \subset H, \quad \forall x \in G$.
Soit $h \in H$ et $x \in G$. $h = x(x^{-1}hx)x^{-1}$ avec $x^{-1}hx \in H$ d'après l'hypothèse, d'où $h \in xHx^{-1}$, ainsi, $H \subset xHx^{-1}, \quad \forall x \in G$.

□

Exercice 6. — $Z(G) \trianglelefteq G$.

— $Int(G) \trianglelefteq Aut(G)$.

— *Tout sous-groupe d'indice 2 d'un groupe G est distingué.*

Propriétés III.2.1. — *(a) Si H et K sont deux sous-groupes de G tel que $K \subset H$ et $K \trianglelefteq G$ alors $K \trianglelefteq H$.*

— *(b) Soit H et K deux sous-groupes de G. Si $H \trianglelefteq G$ (resp. $K \trianglelefteq G$) alors HK est un sous-groupe de G.*

— *(c) L'image réciproque d'un sous-groupe distingué par un homomorphisme de groupes est un sous-groupe distingué. En particulier, le noyau est un sous-groupe distingué.*

— *(d) L'image directe d'un sous-groupe distingué par un homomorphisme de groupes surjectif est un sous-groupe distingué.*

— *(e) Soit $(H_i)_{i\in I}$ une famille de sous-groupes distingués de G, $\bigcap_{i\in I} H_i$ et $< \bigcup_{i\in I} H_i >$ sont des sous-groupes distingués.*

Attention ! *Soit H et K deux sous-groupes de G tel que $K \subset H$: $K \trianglelefteq H$ et $H \trianglelefteq G$ $\not\Rightarrow K \trianglelefteq G$*

Il est clair que si $H \trianglelefteq G$ on a $R_g = R_d$, et par suite $(G/H)_g = (G/H)_d$. On notera alors $G/H = (G/H)_g = (G/H)_d$.

La proposition suivante est une caractérisation du groupe quotient.

Proposition III.2.2. *Soit H un sous-groupe de G. H est distingué de G si et seulement si l'ensemble $(G/H)_g$ est un groupe pour la loi : $\overline{x}\cdot\overline{y} = \overline{x\cdot y}$, $\forall \overline{x}, \overline{y} \in (G/H)_g$. Et dans ce cas, G/H est appelé groupe quotient et la surjection canonique $p : G \longrightarrow G/H$ est un homomorphisme de groupes.*

Preuve. On suppose que $H \trianglelefteq G$. Pour montrer que $\big((G/H)_g, \cdot\big)$ est un groupe il suffit de montrer que R_g est compatible avec la loi de G. $\forall x_1, x_2, y_1, y_2 \in G$ tel que $x_1 R_g y_1$ et $x_2 R_g y_2$, donc $x_1^{-1}y_1 \in H$ et $x_2^{-1}y_2 \in H$. Comme H est distingué, $x_2^{-1}(x_1^{-1}y_1)x_2 \in H$; et puisque H est stable par la loi, on a alors $(x_2^{-1}x_1^{-1}y_1x_2)(x_2^{-1}y_2) \in H$, donc $(x_1x_2)^{-1}y_1y_2 \in H$, i.e., $x_1x_2R_gy_1y_2$. Ainsi R_g est compatible avec la loi de G.

Et finalement, puisque H est distingué dans G, alors $(G/H)_g = (G/H)_d = G/H$.

On conclut alors que G/H est un groupe.

Inversement, on suppose que $(G/H)_g$ est un groupe et donc que R_g est compatible avec la loi de G. Montrons que $H \trianglelefteq G$. Soit $x \in G$ et $h \in H$. On a xR_gx et hR_ge. Par hypothèse, xhR_gx i.e. $xhx^{-1} \in H$ donc H est distingué. □

Exemple. *$(\mathbb{Z}, +)$ est un groupe abélien, d'où tout sous-groupe $n\mathbb{Z}$ où $n \in \mathbb{N}$ de $\mathbb{Z}$ est distingué, et par suite $\mathbb{Z}/n\mathbb{Z}$ est un groupe abélien.*

Remarque.

1. *Si G est abélien alors G/H est abélien. Mais réciproquement, G/H peut être abélien sans que G le soit ! (cf. TD)*
2. *Si H est un sous-groupe distingué et d'indice fini dans G alors G/H est un groupe fini et $|G/H| = [G : H]$.*
3. *Si G est fini et H un sous-groupe distingué de G alors G/H est un groupe fini et $|G/H| = \dfrac{|G|}{|H|}$.*
   Attention ! *G/H peut être fini sans que ni G ni H le soient (exemple : $\mathbb{Z}/n\mathbb{Z}$ pour $n \geq 1$).*

Proposition III.2.3. *Soit H un sous-groupe d'un groupe G. H est distingué si et seulement si H est le noyau d'un homomorphisme de groupes.*

Preuve. Soit $H \trianglelefteq G$. On considère l'homomorphisme canonique surjectif

$$\begin{array}{rccc} p: & G & \longrightarrow & G/H \\ & x & \longmapsto & \overline{x} \end{array}$$

$\forall x \in G$, $x \in Ker(p) \Longleftrightarrow \overline{x} = \overline{e} \Longleftrightarrow x \in H$, donc $Ker(p) = H$.

Inversement, si $f : G \to G'$ est un homomorphisme de groupes, on a $Ker(f) \trianglelefteq G$, donc si $H = Ker(f), \quad H \trianglelefteq G.$ □

Définition III.2.2. *On dit qu'un groupe G est simple s'il ne contient aucun sous-groupe distingué non trivial (i.e. différent de G et $\{e\}$).*

Proposition III.2.4. *Un groupe G est d'ordre premier si et seulement si il est cyclique et simple.*

Preuve. Exercice ! □

Donc, les groupes $(\mathbb{Z}/p\mathbb{Z}, +)$ où p est un nombre premier, sont les seuls groupes commutatifs simples. On verra dans la suite (chapitre 2) que les groupes alternés A_n pour $n \neq 4$ sont simples.

Propriété Universelle du Groupe Quotient

Théorème III.3. *(Décomposition canonique d'un homomorphisme de groupes) Soit H un sous-groupe distingué d'un groupe G et p l'homomorphisme surjectif canonique de G vers G/H. Pour tout homomorphisme $f : G \longrightarrow G'$ tel que $H \subset Ker(f)$, il existe un unique homomorphisme de groupes $\overline{f} : G/H \longrightarrow G'$ tel que $\overline{f} \circ p = f, \quad Ker(\overline{f}) = p(Ker(f)) = Ker(f)/H$ et $Im(\overline{f}) = Im(f)$. $\overline{f}$ est un isomorphisme si et seulement si f est surjective et $Ker(\overline{f}) = H$.*

Preuve. Comme f est constante sur H de valeur l'élément neutre $e' \in G'$, on voit que f est constante sur toute classe $\overline{x} = xH$ modulo H. D'après la décomposition de l'application f, il existe une application $\overline{f}$ de G/H dans G', unique, tel que $\overline{f} \circ p = f$ et il est facile de vérifier que $\overline{f}$ est un homomorphisme.

On a $Im(\overline{f}) = Im(f)$ car $\overline{f}(\overline{x}) = f(x), \forall x \in G$. Et $\forall \overline{x} \in G/H$,

$$\overline{x} \in Ker(\overline{f}) \Leftrightarrow \overline{f}(\overline{x}) = e' \Leftrightarrow f(x) = e' \Leftrightarrow x \in Ker(f) \Leftrightarrow \overline{x} \in p(Ker(f))$$

Ce qui prouve que $Ker(\overline{f}) = p(Ker(f))$. □

On déduit du théorème précédent le résultat suivant qui, en raison de son importance et usage fréquent, a été montré précédemment. Ce résultat est connu sous le nom de "Premier théorème d'isomorphisme". Et de ce dernier vont découler deux autres théorèmes d'isomorphisme.

Corollaire III.2. *(Premier théorème d'isomorphisme) Soit $f : G \to G'$ un homomorphisme de groupes alors $G/Ker(f) \cong Im(f)$. Si de plus G et G' sont finis, $|f(G)|/|G|$ et $|f(G)|/|G'|$.*

Preuve. D'après le théorème précédent $H = Ker(f) \trianglelefteq G$, $Ker(\overline{f}) = p(H) = \{\overline{e}\}$ et $Im(\overline{f}) = Im(f)$. Donc $\overline{f}$ est un isomorphisme de $G/Ker(f)$ sur $Im(f)$. □

Exercice 7. *Montrer que* $G/Z(G) \cong Int\, G$.

Exercice 8. *Soit* G *un groupe. On suppose que* G *est le produit direct de deux sous-groupes* H *et* K. *Montrer alors que* $H \trianglelefteq G$ *et* $G/H \cong K$.

Théorème III.4. *(Deuxième théorème d'isomorphisme) Soit* H *un sous-groupe distingué d'un groupe* G. *Pour tout sous-groupe* K *de* G, *on a* $H \cap K \trianglelefteq K$, $\quad H \trianglelefteq HK$ *et* $K/H \cap K \cong HK/H$.

Preuve. On a $H \trianglelefteq G$ d'où HK est un sous-groupe de G et puisque $H \subset HK$ on a alors $H \trianglelefteq HK$ et par suite HK/H est un groupe.

$H \cap K \trianglelefteq K$, en effet, soit $h \in H \cap K$ et $x \in K$, on a $xhx^{-1} \in H$ puisque $H \trianglelefteq G$. On a aussi $xhx^{-1} \in K$ puisque $x, h \in K$. On conclut alors que $xhx^{-1} \in H \cap K$, donc $H \cap K \trianglelefteq K$ et par suite $K/H \cap K$ est un groupe.

$$\begin{array}{rccc} \text{Soit} \quad \varphi : & K & \longrightarrow & HK/H \\ & k & \longmapsto & \overline{k} = kH = Hk \end{array}$$

φ est un homomorphisme de groupes. D'après le Premier théorème d'isomorphisme, $K/Ker(\varphi) \cong Im(\varphi)$.

$\forall k \in K, \quad k \in Ker(\varphi) \iff \varphi(k) = \overline{e} \iff \overline{k} = \overline{e} \iff k \in H \Rightarrow k \in H \cap K$, donc $Ker(\varphi) = H \cap K$. Ainsi, φ est injectif. Soit maintenant $\overline{hk} \in HK/H$ avec $h \in H$ et $k \in K$. On a $\overline{hk} = \overline{h}\,\overline{k} = \overline{e}\overline{k} = \overline{k} = \varphi(k)$, donc, φ est surjectif, ainsi $Im(\varphi) = HK/H$. On conclut que $K/H \cap K \cong HK/H$. □

Remarque. *Lorsque* H *et* K *sont finis, on en déduit l'égalité suivante :* $|HK| = \dfrac{|H||K|}{|H \cap K|}$.

Exercice 9. *Soit* H *et* K *deux sous-groupes distingués d'un groupe fini* G. *On suppose que le* $pgcd(|H|, |K|) = 1$, *montrer que pour tout* $h \in H, k \in K$, $hk = kh$. *En déduire que* $H \times K \cong HK$.

Sous-groupe d'un Groupe Quotient et Troisième Théorème d'Isomorphisme

Proposition III.2.5. *Soit* G *un groupe et* H *un sous-groupe distingué dans* G. *L'ensemble des sous-groupes de* G/H *est en bijection avec l'ensemble des sous-groupes de* G *contenant* H. *En considérant* $p : G \to G/H$ *l'homomorphisme surjectif canonique, pour tout sous-groupe* $\overline{K}$ *de* G/H, *il existe un unique sous-groupe* K *de* G *contenant* H *tel que* $\overline{K} = p(K) = K/H$.

Preuve. Exercice ! □

Théorème III.5. *(Troisième théorème d'isomorphisme) Soit G un groupe et H, K deux sous-groupes de G tel que $K \subset H$, $H \trianglelefteq G$ et $K \trianglelefteq G$, alors*
$(H/K) \trianglelefteq (G/K)$ *et* $(G/K)/(H/K) \cong G/H$.

Preuve. Notons p_H (resp. p_K) l'homomorphisme surjectif canonique $G \to G/H$ (resp. $G \to G/K$). Il est clair que $H/K = p_K(H)$ est un sous-groupe distingué de G/K comme image par un homomorphisme surjectif d'un groupe distingué dans G. Donc, $(H/K) \trianglelefteq (G/K)$ et par suite, $(G/K)/(H/K)$ est un groupe.

Par ailleurs, en appliquant le théorème de la propriété universelle d'un groupe quotient (théorème III.3) à $p_H : G \to G/H$ puisque $Ker(p_H) = H \supset K$, il existe un homomorphisme $\overline{f} : G/K \to G/H$, unique, tel que $\overline{f} \circ p_K = p_H$ et

$$Ker(\overline{f}) = p_K(Ker(p_H)) = p_K(H) = H/K$$

Comme $\overline{f} \circ p_K = p_H$ est surjectif, on a $\overline{f}$ est surjectif, d'où : $Im(\overline{f}) = G/H$. On conclut d'après le Premier théorème d'isomorphisme que $G/K/Ker(\overline{f}) \cong Im(\overline{f})$ donc $(G/K)/(H/K) \cong G/H$. □