IV . −Groupes quotients, théorème de LAGRANGE

IV.0 . −Introduction

On aura sans doute déjà entr'aperçu l'importance de l'étude des morphismes dans la compréhension des propriétés des groupes (et des autres structures algébriques d'ailleurs.) En « transportant » la structure de l'objet qu'on veut étudier à un objet connu, les morphismes permettent en effet de les comparer.

Or l'expérience montre que, dans bon nombre de situations, les morphismes sont construits par *passage au quotient*. La notion de *quotient* est donc fondamentale dans la manière qu'on a de faire de l'algèbre actuellement ; mais, bien plus encore que le quotient, c'est sa *propriété universelle* qui en fait l'intéreêt, puisqu'elle permet de le relier aux autres objes de la théorie.

Les notions de quotient (cf. III.1.7 ,) et de propriété universelle (cf. III.1.9 ,) ont déjà été introduites dans le cadre des ensembles sans aucune structure supplémentaire. On voudra, dans ce chapitre, aboutir à la notion correspondante de *groupe quotient* (cf. IV.2.2 ,) et de *factorisation des morphismes* ou de propriété universelle (ce qui est à peu près synonyme) (cf. IV.2.4 .)

Il s'agira donc de constater qu'on ne peut pas fixer arbitrairement une *relation d'équivalence* sur un groupe G, si l'on souhaite que l'ensemble quotient $G/\sim$ ait lui-même une structure de groupe ; et surtout qu'elle entretienne un quelconque rapport avec celle de G ; ce qui se traduit par le fait que la *surjection canonique* $\pi : G \to G/\sim$ (cf. la définition III.1.7 ,) soit un morphisme (cf. la proposition IV.2.1 .)

On est donc amené à donner les quelques définitions et propriétés suivantes :

Définition IV.0.1 (RElation d'équivalence compatible)

Étant donné un magma associatif $(M, *)$,

on dit qu'une relation d'équivalence $\sim$ sur l'ensemble M est *compatible à la loi* $*$ ou simplement compatible si

$$\forall (x, y, z, t) \in M \times M \times M \times M,\ \big(x \sim z \text{ et } y \sim t\big) \ \Rightarrow\ x * y \ \sim\ z * t\ .$$

Lemme IV.0.2 *Si $(M, *)$ est un magma associatif, et $\sim$ une relation d'équivalence compatible,*

i) il existe une unique structure de magma sur l'ensemble quotient $M/\sim$ (ensemble des classes d'équivalence pour la relation $\sim$,) telle que la surjection canonique $\pi : M \to M/\sim$ soit un morphisme.

***Démonstration** : (cf. la question 1 de l'exercice IV.4.1 .)*

ii) Le magma $M/\sim$ est alors associatif (resp. commutatif) (resp. possède un élément neutre) s'il en est ainsi pour $(M, *)$.

***Démonstration** : (cf. la question 2 de l'exercice IV.4.1 .)*

Définition IV.0.3 (Magma quotient) Avec les notations du lemme IV.0.2 , le magma $M/\sim$ est appelé *magma quotient* ou bien on dit que l'ensemble $M/\sim$ est muni de la *structure quotient*.

IV.1 . −Sous-groupes normaux

On pourrait tout à fait se passer, pour rédiger cette section (IV.1 ,) des résultats des section III , III.6 et III.5 c'est-à-dire de tout ce qui concerne les actions de groupes. Un certain nombre de vérification devront alors être faites. Dans toute cette section (IV.1 ,) $(G, *)$ est un groupe d'élément neutre e.

Il est légitime de se demander comment les exigences que nous avons formulées dans l'introduction (cf. IV.0 ;) à savoir de disposer de quotients $G/\sim$ qui reçoivent leur structure de G, conduit à l'étude des sous-groupes de G et plus précisément même à certains d'entre eux que nous appellerons sous-groupes *distingués* ou *normaux*. La relation entre ces objets, les « bonnes relations d'équivalence » d'une part, et les sous-groupes distingués d'autre part est complètement explicitée à la proposition IV.1.11 ; on peut cependant, d'ores et déjà faire la remarque suivante :

Remarque IV.1.0 Si $(G, *, e)$ est un groupe et $\sim$ une relation compatible sur le magma $(G, *)$ (cf. la définition IV.0.1 ,) alors la classe $\overline{e}$ de l'élément neutre ett un sous-groupe de G.

En effet, $e \in \overline{e}$; si bien que $\overline{e} \neq \emptyset$. De plus :

$$\begin{array}{lrcl} \forall (x,y) \in \overline{e} \times \overline{e}, & x \sim e, y \sim e & \text{et} & y^{-1} \sim y^{-1} \\ \Rightarrow & x \sim e & \wedge & e \sim y^{-1} \\ \Rightarrow & x \sim e & \wedge & y^{-1} \sim e \\ \Rightarrow & x * y^{-1} & \sim & e \\ \Rightarrow & x * y^{-1} & \in & \overline{e}\,; \end{array}$$

ce qui achève de prouver que $\overline{e}$ est un sous-groupe de G.

On va en revanche expliquer au long de ce paragraphe que cette condition n'est pas suffisante et qu'on va être amené à considérer une classe particulière de sous-groupes *i.e.* les sous-groupes distingués ou normaux.

Notation IV.1.1 Pour tout sous-groupe H de G, on définit comme à la notation III.5.4 $\sim_{H,g}$ (resp. comme au point iv de la remarque III.5.5 $\sim_{H,d}$) la relation binaire sur $G \times G$ par :

$$\begin{array}{c} \forall x \in G,\ \forall y \in G,\ \left(x \sim_{H,d} y \ \Leftrightarrow x^{-1} * y \in H\right) \\ \left(\text{resp.} \quad \forall x \in G,\ \forall y \in G,\ \left(x \sim_{H,g} y \ \Leftrightarrow\ y * x^{-1} \in H\right) \quad \right). \end{array} \qquad \text{IV.1.1.1}$$

On notera encore, :

$$\forall x \in G,\ x * H \ := \ \{x * y\ ;\ y \in H\} \ \left(\text{resp. } H * x \ := \ \{y * x\ ;\ y \in H\}\ .\right) \qquad \text{IV.1.1.2}$$

On écrira parfois simplement xH (resp. Hx) pour $x * H$ (resp. $H * x$.)

Remarque IV.1.2 La relation $\sim_{H,g}$, (resp. $\sim_{H,d}$,) est la relation d'équivalence induite par l'action de H sur G par translation à gauche (resp. par translation à droite) C'est donc une relation d'équivalence dont les classes sont les orbites de l'action (cf. III.3.2. i .)

Si toutefois on ne veut pas tenir compte de ces résultas on peut montrer directement la proposition suivante :

Proposition IV.1.3 *i) Les relations binaires définies IV.1.1.1 sont des relations d'équivalence .*

Démonstration *: Montrons que la relation $\sim_{H,d}$ est une relation d'équivalence . Pour tout $x \in G$, $x^{-1} * x = e \in H$; car H est un sous-groupe de G, i.e. $x \sim_{H,d} x$ c'est-à-dire que la relation $\sim_{H,d}$ est réflexive.*

Par ailleurs :

$$\begin{array}{lrcl} \forall x \in G,\ \forall y \in G,\ \big(& x & \sim_{H,d} & y \\ \Rightarrow & x^{-1} * y & \in & H \\ \Rightarrow & y^{-1} * x \ = \ (x^{-1} * y)^{-1} & \in & H \\ \Rightarrow & y & \sim_{H,d} & x \big) \end{array}$$

la relation $\sim_{H,d}$ est donc symétrique.

Enfin :

$$\begin{array}{lrcl} \forall x \in G,\ \forall y \in G,\ \forall z \in G,\ \big(& x \sim_{H,d} y & \text{et} & y \sim_{H,d} z \\ \Rightarrow & x^{-1} * y \in H & \text{et} & y^{-1} * z \in H \\ \Rightarrow & x^{-1} * y * y^{-1} * z & \in & H \\ \Rightarrow & x^{-1} * z & \in & H \\ \Rightarrow & x & \sim_{H,d} & z \big) \end{array}$$

c'est-à-dire que la relation $\sim_{H,d}$ est transitive.

Un argument analogue vaut également pour $\sim_{H,g}$.

ii) L'ensemble $G/\sim_{g,H}$ (resp. $G/\sim_{d,H}$) des classes d'équivalence pour la relation $\sim_{g,H}$ (resp. $\sim_{d,H}$) s'identifie à $\{x * H\ ;\ x \in G\}$, (resp. $\{H * x\ ;\ x \in G\}$.)

Plus précisément :

$$\forall x \in G,\ \mathrm{cl}_g(x) \ = \ \{y \ \in \ G\ ;\ x \sim_{g,H} y\} \ = \ x * H \ \big(\text{resp. } \mathrm{cl}_d(x) \ = \ \{y \ \in \ G\ ;\ x \sim_{d,H} y\} \ = \ H * x\ .\big) \quad 1$$

Démonstration *: Pour tout $x \ \in \ G$, un élément y de G appartient à la classe de x modulo $\sim_{H,d}$ si et seulement si*

$$\big((x^{-1} * y \in H) \ \Leftrightarrow \ (\exists z \in H,\ (x^{-1} * y \ = \ z) \ \Leftrightarrow \ y \ \in \ x * H)\big)\ .$$

iii) Toute classe d'équivalence pour la relation $\sim_{g,H}$ (resp. $\sim_{d,H}$) est en bijection avec H.

Démonstration *: Pour tout $x \in G$, l'application*

$$G \ \to \ G\ ,\ z \ \mapsto \ x * z$$

induit par restriction une application $H \ \to \ x * H$ dont la bijection réciproque est

$$G \ \to \ G\ ,\ z \ \mapsto \ x^{-1} * z\ .$$

iv) L'application $x * H \ \mapsto \ H * x$ pour $x \ \in \ G$, induit une bijection de l'ensemble $G/\sim_{H,d}$ des classes selon $\sim_{H,d}$ dans l'ensemble $G/\sim_{H,g}$ des classes selon $\sim_{H,g}$.

Proposition IV.1.4 (Sous-groupe normal) *Pour tout sous-groupe $H \ \subset \ G$, les assertions suivantes sont équivalentes :*

a) La relations $\sim_{H,d}$ est compatible à la loi de groupe (cf. la définition IV.0.1 ,) i.e.

$$\forall (x,y,z,t) \in G \times G \times G \times G,\ \big(x \sim_{H,d} z \text{ et } y \sim_{H,d} t\big) \Rightarrow \ x * y \sim_{H,d} z * t\ .$$

b) La relations $\sim_{H,g}$ est compatible à la loi de groupe.

c) Les relations $\sim_{H,g}$ et $\sim_{H,d}$ sont égales.

d)
$$\forall x \in G,\ \left(x * H \ = \ H * x\right) .$$

e)
$$\forall x \in G,\ \left(H \ = \ x * H * x^{-1}\right) .$$

f)
$$\forall x \in G,\ \left(x * H * x^{-1} \ \subset \ H\right) .$$

Démonstration : *On montre l'équivalence f $\Leftrightarrow$ b . Pour d'avantage de détails (cf. l'exercice IV.4.3 :)*

Remarquons que, pour tout $y \in H$, $y \sim_{H,g} e$, et que, pour tout $x \in G$, $x \sim_{H,g} x$. Il en résulte donc, si l'on suppose l'assertion b vérifiée, que pour tout $y \in H$ et tout $x \in G$, $x * y \sim_{H,g} x$ c'est-à-dire précisément $x * y * x^{-1} \in H$. L'assertion b entraîne donc l'assertion f .

Réciproquement, étant donné un quadruplet (x, z, y, t) d'éléments de G, si $y \sim_{H,g} t$, $y * t^{-1} \in H$. Si l'on suppose l'assertion f vérifiée, $x * y * t^{-1} * x^{-1} \in H$. Mais $x \sim_{H,g} z$ entraîne que $x * z^{-1} \in H$; ce qui entraîne, puisque H est un sous-groupe de G, que

$$x * y * (z * t)^{-1} \ = \ x * y * t^{-1} * z^{-1} \ = \ x * y * t^{-1} * x^{-1} * x * z^{-1} \ \in \ H$$

c'est-à-dire que $x * y \sim_{H,g} z * t$. On a donc montré que l'assertion f entraîne l'assertion b .

Définition IV.1.5 (Sous-groupes normaux/distingués) Un sous-groupe H de G est dit *normal* ou *distingué*, s'il vérifie l'une des conditions équivalentes de la proposition IV.1.4 .

Remarque IV.1.6 On peut reformuler la définition ci-dessus en termes d'actions par conjugaison (cf. III.6 ,) un sous-groupe distingué n'étant rien d'autre qu'un point fixe pour l'action de G par conjugaison sur ses sous-groupes (cf. III.6.5 .) On dira donc parfois que H est *invariant par conjugaison* ou même simplement *invariant*.

Notation IV.1.7 Le point c de la proposition IV.1.4 autorise à noter, pour un sous-groupe distingué H de G, simplement $\sim_H$ indifféremment $\sim_{H,g}$ et $\sim_{H,d}$ qui sont égales. De plus il résulte du point b de la proposition IV.1.4 (ou indifféremment du point a de la proposition IV.1.4) que $\sim_H$ est compatible à la loi de groupe sur G (cf. IV.0.1 .) L'ensemble quotient

$$G/\sim_H \ = \ G/\sim_{H,d} \ = \ G/\sim_{H,g},$$

sera usuellement noté G/H et bénéficie de propriétés tout à fait intéressantes qui seront étudiées en détail dans la section IV.2 .

Définition IV.1.8 Pour tout sous-groupe distingué H de G, on appellera *classes modulo H* ou *classes selon H* les classes d'équivalence pour la relation $\sim_H$. Cette dernière étant compatible, pour tout couple (α, β) de classes, tout x, x' dans α tout y, y' dans β, on a $x * y \ \sim_H \ x' * y'$ c'est-à-dire que $x * y$ et $x' * y'$ définissent la même classe selon H. On peut donc poser

$$\alpha * \beta \ = \ \overline{x} * \overline{y} \ := \ \overline{x * y} \qquad \text{IV.1.8.1}$$

la classe de $x * y$ pour n'importe quel représentant x de α et n'importe quel représentant y de β.

On note désormais G/H, l'ensemble des classes selon H muni de la loi de composition définie ci-dessus.

Exemple IV.1.9 a) Les sous-groupes $\{e\}$ et G de G sont toujours distingués dans G.

b) Si G est un groupe abélien ($(\mathbb{Z}, +)$ par exemple,) tout sous-groupe est distingué.

Proposition IV.1.10 (Image réciproque/directe) *Pour tout morphisme de groupes $f : G \to H$ (cf. II.2.1 ,) l'image réciproque $f^{-1}(L)$ de tout sous-groupe distingué L de H est un sous-groupe distingué de G.*

En particulier, $\mathrm{Ker}\, f = f^{-1}(\{e_H\})$ est un sous-groupe distingué de G.

En revanche, il n'est pas vrai en général que l'image $f(K)$ d'un sous-groupe distingué K de G est un sous-groupe distingué de H. C'est cependant le cas si f est surjectif.

Démonstration : *(cf. l'exercice IV.4.4 .)*

Proposition IV.1.11 (Relations d'équivalence compatibles) *i) Une relation d'équivalence $\sim$ sur G est compatible si et seulement si pour tout $(x, y) \in G \times G$,*

$$x \sim y \Leftrightarrow x^{-1} * y \sim e\,.$$

Démonstration : *Si $\sim$ est une relation d'équivalence compatible sur G, comme $\sim$ est réflexive, pour tout $x \in G$, $x^{-1} \sim x^{-1}$. Comme $\sim$ est compatible, si $y \sim x$,*

$$x^{-1} * y \sim x^{-1} * x = e\,.$$

Réciproquement, si x et y dans G sont tels que $x^{-1} * y \sim e$, comme $x \sim x$ et que $\sim$ est compatible,

$$y = x * x^{-1} * y \sim x * e = x\,.$$

ii) La classe $\overline{e}$ de l'élément neutre e pour une relation d'équivalence compatible est un sous-groupe distingué de G.

Démonstration : *Par définition même d'une classe d'équivalence , $e \in \overline{e}$. Si $x \in \overline{e}$, comme $x^{-1} \sim x^{-1}$, (par réflexivité de $\sim$,)*

$$e = x^{-1} * x \sim x^{-1} * e = x^{-1}\,,$$

(par compatibilité ;) i.e. $x^{-1} \in \overline{e}$. Enfin si $(x, y) \in \overline{e} \times \overline{e}$,

$$x * y \sim e * e = e\,,$$

(par compatibilité ;) i.e. $x * y \in \overline{e}$. D'après la proposition II.3.5 , $\overline{e}$ est donc un sous groupe de G.

Pour tout $x \in \overline{e}$, et tout $y \in G$,

$$\begin{array}{rrcl} & x & \sim & e \\ \Rightarrow & y * x & \sim & y \\ \Rightarrow & y * x * y^{-1} & \sim & y * y^{-1} \\ \Rightarrow & y * x * y^{-1} & \sim & e\,; \end{array}$$

c'est-à-dire que pour tout $y \in G$,

$$y * \overline{e} * y^{-1} \subset \overline{e}\,;$$

i.e. , d'après la caractérisation proposition IV.1.4, point f , des sous-groupes distingués, $\overline{e}$ est un sous-groupe distingué de G.

iii) Étant donné un sous-groupe distingué H de G, la relation $\sim_H$ compatible définie ci-dessus est la seule relation d'équivalence compatible $\sim$ sur G telle que $\overline{e} = H$.

***Démonstration** : Il est clair que la classe de e selon $\sim_H$ pour tout sous-groupe distingué H de G s'identifie à H. L'unicité de $\sim_H$ découle alors du lemme plus général :*

Lemme IV.1.12 *Étant donné un groupe G et deux relations d'équivalence $\sim_1$ et $\sim_2$ compatibles sur G, on note $\overline{x}_1$ (resp. $\overline{x}_2$) la classe d'un élément x de G selon $\sim_1$ (resp. $\sim_2$.)*
Alors les assertions suivantes sont équivalentes :

a) Les relations $\sim_1$ et $\sim_2$ sont égale c'est-à-dire que pour tout $(x, y) \in G \times G$,

$$x \sim_1 y \Leftrightarrow x \sim_2 y\ .$$

b) Pour tout $x \in G$

$$\overline{x}_1 = \overline{x}_2\ .$$

c) Il existe $g \in G$ tel que

$$\overline{g}_1 = \overline{g}_2\ .$$

d)

$$\overline{e}_1 = \overline{e}_2\ .$$

***Démonstration** :*

*i) (**a** $\Leftrightarrow$ **b**)*
est pour ainsi dire tautologique.

*ii) (**b** $\Rightarrow$ **c**)*
est immédiat.

*iii) (**c** $\Rightarrow$ **d**)*
Soit donné $g \in G$, tel que $\overline{g}_1 = \overline{g}_2$. Pour tout

$$\begin{array}{rrcl} & x & \in & \overline{e}_1 \\ \Rightarrow & x & \sim_1 & e \\ \Rightarrow & x * g & \sim_1 & g \\ \Rightarrow & x * g & \in & \overline{g}_1 \\ \Rightarrow & x * g & \in & \overline{g}_2 \\ \Rightarrow & x * g & \sim_2 & g \\ \Rightarrow & x * g * g^{-1} & \sim_2 & g * g^{-1} = e \\ \Rightarrow & x & \sim_2 & e\ . \end{array}$$

On vient donc de montrer que $\overline{e}_1 \subset \overline{e}_2$. Le raisonnement étant parfaitement symétrique, on peut montrer, de la même manière, l'inclusion réciproque.

iv) ***(d $\Rightarrow$ a)***
Pour tout $(x, y) \in G$, si $x \sim_1 y$, alors, d'après le point i de la proposition IV.1.11

$$\begin{array}{rrcl} & x^{-1} * y & \sim_1 & e \\ \Rightarrow & x^{-1} * y & \in & \overline{e}_1 \\ \Rightarrow & x^{-1} * y & \in & \overline{e}_2 \\ \Rightarrow & x & \sim_2 & y\,. \end{array}$$

Le raisonnement étant évidemment symétrique, on montrerait, exactement de la même manière que si $x \sim_2 y$ alors $x \sim_1 y$; ce qui termine la preuve.

IV.2 . −Groupe quotient, factorisation des morphismes, propriété universelle

Dans toute cette section (IV.2 ,) $(G, *)$ est un groupe d'élément neutre e.

Proposition IV.2.1 (Existence de quotients) *Pour $(G, *)$ un groupe et H un sous-groupe distingué, la relation $\sim_H$ est compatible à la loi $*$ si bien qu'il existe une unique structyure de groupe sur l'ensemble G/H des classes pour la relation $\sim_H$ telle que la surjection canonique $\pi : G \to G/H$ soit un morphisme de groupe. Alors l'élément neutre de G/H est $\overline{e} = H$ et l'inverse de tout élément $\overline{x}$ est $\overline{x^{-1}}$.*

***Démonstration** :*

i) S'il existe une structure de groupe † sur l'ensemble $G/\sim_H$ des classes d'équivalence selon $\sim_H$, telle que π est un morphisme, alors nécessairement, pour tout quadruplet (x, x', y, y') d'éléments de G tel que

$$x \sim_H x' \text{ et } y \sim_H y'\,,$$

$$\begin{array}{rcl} \pi(x * y) & = & \pi(x) \dagger \pi(y) \\ & = & \pi(x') \dagger \pi(y') \\ & = & \pi(x' * y')\,. \end{array}$$

Comme π est surjective, la structure † est nécessairement unique.

ii) Comme $\sim_H$ est compatible à $(G, *)$ (cf. IV.1.4 ,)

$$\begin{array}{rcl} \pi(x * y) & = & \overline{x * y} \\ & = & \overline{x' * y'} \\ & = & \pi_H(x' * y')\,; \end{array}$$

on peut donc poser, pour tout $(\overline{x}, \overline{y}) \in G/\sim_H \times G/\sim_H$,

$$\overline{x} \dagger \overline{y} := \overline{u * v}$$

pour n'importe quel élément $u \in \overline{x}$ (resp. $v \in \overline{y}$;) ce qui prouve l'existence de la structure †.

Définition IV.2.2 (Groupe quotient) Le groupe

$$G/H \text{ ou même le couple } \big(G/H, \pi \,:\, G \,\to\, G/H\big)$$

est appelé *groupe quotient*. On dit encore que l'ensemble $G/\sim_H$ est muni de la *structure quotient*.

Exemple IV.2.3 (Groupes quotients) Nous avons remarqué (cf. IV.1.9. b ,) que dans un groupe abélien, et en particulier dans $(\mathbb{Z}, +)$, tout sous-groupe est distingué. De plus une partie H de $\mathbb{Z}$ est un sous-groupe si et seulement s'il existe un entier $d \geq 0$ tel que $H \,=\, d\mathbb{Z}$.

On constate alors, que pour deux entiers x et y, $x \sim_H y$ si $y - x \in H$, c'est-à-dire si et seulement si $d|y - x$. La relation $\sim_H$ n'est autre, dans ce cas, que la relation de congruence modulo d.

Nous retrouvons dans ce cas particulier, grâce aux résultats de cette section, que la relation de congruence est compatible, fait que nous avions déjà établi dans le exercice IV.4.2 . L'ensemble des classes modulo d que nous avions noté $\mathbb{Z}/d\mathbb{Z}$ s'identifie en tant que groupe, au groupe quotient $\mathbb{Z}/H \,=\, \mathbb{Z}/d\mathbb{Z}$.

Proposition IV.2.4 (Factorisation des morphismespropriété universelle) *Pour tout morphisme de groupes*

$$f \,:\, G \,\to\, K \text{ et tout sous-groupe distingué } H \,\subset\, G,$$

les assertions suivantes sont équivalentes :

a) $H \,\subset\, \operatorname{Ker} f$.

b) Il existe un unique morphisme $\overline{f} \,:\, G/H \,\to\, K$ *tel que* $\overline{f} \,\circ\, \pi \,=\, f$.
De plus, $\overline{f}$ *est injectif (resp. surjectif) si et seulement si* $H \,=\, \operatorname{Ker} f$, *(rsp.* f *est surjectif.)*

Démonstration *:*

i) Le fait même qu'on demande que, pour tout $x \in G$,

$$\overline{f}(\overline{x}) \,=\, f(x)\,,$$

assure tautologiquement l'unicité de $\overline{f}$.

ii) Pour tout x, x' *dans* G, *si* $x \sim_H x'$, $x * x'^{-1} \,\in\, H$ *ce qui implique que* $x * x'^{-1} \in \operatorname{Ker} f$ *si l'on suppose que* $H \subset \operatorname{Ker} f$, *c'est-à-dire que* $f(x * x'^{-1}) \,=\, e_H$ *ou encore que* $f(x) \,=\, f(x')$. *On peut donc définir* $\overline{f}(\overline{x})$ *par* $f(x)$ *pour n'importe quel représentant* x *de* $\overline{x}$. *Ceci assure donc l'existence de* $\overline{f}$.

iii) Pour tout couple (α, β) *d'éléments de* G/H, *tout* $x \,\in\, \alpha$, *tout* $y \,\in\, \beta$, *étant donné la définition de la loi de composition sur* G/H *(cf. IV.1.8.1 ,)*

$$\begin{aligned}
\overline{f}(\alpha * \beta) \;&=\; \overline{f}(\overline{x * y}) \\
&=\; f(x * y) \\
&=\; f(x) *_H f(y) \\
&=\; \overline{f}(\alpha) *_H \overline{f}(\beta)
\end{aligned}$$

c'est-à-dire que $\overline{f}$ *est un morphisme de groupes.*

iv) Un élément $u \,\in\, H$ *appartient à* $\operatorname{Im} \overline{f}$ *si et seulement s'il existe un élément* $\overline{x} \in G/H$ *tel que* $\overline{f}(\overline{x}) \,=\, u$ *c'est-à-dire si et seulement s'il existe* $x \,\in\, G$ *tel que* $u \,=\, f(x)$. *Autrement dit,*

$$\operatorname{Im} \overline{f} \,=\, \operatorname{Im} f$$

ce qui établit (cf. II.3.11 ,) que f *est surjectif si et seulement si* $\overline{f}$ *l'est.*

v) Enfin, $\overline{f}$ est injective si et seulement si

$$\mathrm{Ker}\,\overline{f} \;=\; e_{G/H} \;=\; H$$

(cf. II.3.11 .) Ceci signifie exactement que $\overline{f}(\overline{x}) \;=\; e_H$ si et seulement si $\overline{x} \;=\; H$, ou encore $f(x) \;=\; e_H$ si et seulement si $x \;\in\; H$ c'est-à-dire si et seulement si

$$H \;=\; \mathrm{Ker}\, f\ .$$

Corollaire IV.2.5 *Étant donné un morphisme de groupes $f \;:\; G \;\to\; K$ il existe un unique isomorphisme de groupes*

$$\overline{f} \;:\; G/\mathrm{Ker}\, f \;\cong\; \mathrm{Im}\, f \;\; \textit{tel que} \;\; f \;=\; \overline{f} \circ \pi$$

où $\pi \;:\; G \;\to\; G/\mathrm{Ker}\, f$ est la surjection canonique. En particulier si f est surjectif

$$\overline{f} \;:\; G/\mathrm{Ker}\, f \;\cong\; K$$

est un isomorphisme.

Démonstration *: Il suffit d'appliquer la proposition IV.2.4 à $H \;:=\; \mathrm{Ker}\, f$.*

Corollaire IV.2.6 *Étant donné un morphisme surjectif de groupes $p \;:\; G \;\to\; Q$, il existe un unique isomorphisme de groupes*

$$\phi \;:\; G/\mathrm{Ker}\, p \;\to\; Q \;\; \textit{tel que} \;\; p \;=\; \phi \circ \pi \;\textit{où}\; \pi \;:\; G \;\to\; G/\mathrm{Ker}\, p \;\textit{est la surjection canonique}\,.$$

Démonstration *: C'est une conséquence immédiate du corollaire IV.2.5 puisque $\mathrm{Im}\, p \;=\; Q$.*

Proposition IV.2.7 *Étant donné un groupe $(G, *)$, les données suivantes sont équivalentes, au sens où la donnée de l'une d'entre elles permet de construire canoniquement les autres :*

a) Un sous-groupe distingué K de G.

b) Une relation d'équivalence $\sim$ compatible sur G.

c) Un morphisme de groupes surjectif $p \;:\; G \;\to\; Q$.

Démonstration *:*

i) On a vu, grâce à la proposition IV.1.11 , qu'à toute relation compatible $\sim$ on associe canoniquement un sous-groupe distingué $H \;:=\; \overline{e}$ et que, réciproquement, à tout sous-groupe distingué H on associe une unique relation compatible telle que $\overline{e} \;=\; H$.

ii) On a vu également, grâce à la proposition IV.2.1 , qu'à tout sous-groupe distingué (ou de manière équivalente à toute relation d'équivalence compatible) on associe une surjection $\pi \;:\; G \;\to\; G/H$ qui est un morphisme de groupes.

iii) Réciproquement, à tout morphisme surjectif $p \;:\; G \;\to\; Q$, on peut associer le sous-groupe distingué $H \;:=\; \mathrm{Ker}\, p$ (cf. IV.1.10 .)

Le corollaire IV.2.6 établit qu'en fait, les procédés ii et iii "inverses" l'un de l'autre, en un certain sens.

IV.3 . −Groupes finis : théorème de LAGRANGE

Définition IV.3.1 (Groupe fini) Un groupe $(G, *)$ est un *groupe fini* si G est un ensemble fini .

Exemple IV.3.2 Pour $n \in \mathbb{N}^*$, le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe fini (cf. l'exercice IV.4.2 .)

Proposition IV.3.3 *Si $(G, *)$ est un groupe fini, une partie H de G munie de la loi de composition $*$ est un sous-groupe de G si et seulement si H est non-vide et pour tout $(x, y) \in H \times H$, $x * y \in H$.*

Démonstration : *(cf. l'exercice IV.4.5 .)*

Proposition IV.3.4 *Si G est un groupe fini et H un sous-groupe de G, la relation d'équivalence $\sim_{H,g}$ (resp. $\sim_{H,d}$) étant définie comme à la notation III.5.4 , (resp. remarque III.5.5, point iv ,)*

$$\#(G) \;=\; \#(H) * \#\big(G/\!\sim_{H,g}\big) \;=\; \#(H) * \#\big(G/\!\sim_{H,d}\big)$$

d'où il résulte en particulier que

$$\#(H) | \#(G) \text{ (cf. le point iv de la proposition III.5.7 .)}$$

Démonstration : *Puisque les orbites sous l'action de H (aussibien à gauche qu'à droite,) sont des classes d'équivalence , elles réalisent une partition de G. Si G est fini, les orbites sont donc toutes des sous-ensembles finis ($H = O(e)$ (cf. III.5.7. ii ,) en particulier) et en nombre fini i.e. $G/\sim$ est aussi un ensemble fini (où $\sim$ désigne aussibien $\sim_{H,g}$, que $\sim_{H,d}$.)*

En posant $\#(G/\sim) = k \in \mathbb{N}$, choisissons $(x_i)_{1 \leq i \leq k}$ des éléments de G tels que

$$\forall (i,j) \in [1;k] \times [1;k],\; i \neq j \;\Rightarrow\; O(x_i) \cap O(x_j) = \emptyset$$

autrement dit un représentant par orbite. On a alors :

$$G \;=\; \bigcap_{1 \leq i \leq k} O(x_i)$$

ce qui entraîne

$$\#(G) \;=\; \sum_{i=1}^{k} \#(O(x_i))\,.$$

Or il découle du point i de la proposition III.5.7 que $\forall 1 \leq i \leq k,\ \#(O(x_i)) = \#(H)$ d'où il résulte finalement que

$$\#(G) \;=\; k * \#(H) \;=\; \#(G/\sim) \;*\; \#(H)\,.$$

Corollaire IV.3.5 *Si G est un groupe fini et H un sous-groupe, le cardinal de G est le produit de l'indice de H dans G (cf. III.5.9 p)ar le cardinal de H.*

Corollaire IV.3.6 (théorème de LAGRANGE) *Si G est un groupe fini pour tout sous-groupe H de G, le cardinal de H divise le cardinal de G.*

Corollaire IV.3.7 *Le corollaire IV.3.5 ci-dessus et le corollaire IV.2.5 on pour conséquence que, pour tout morphisme de groupes $f : G \to H$, avec G groupe fini,*

$$\#(G) = \#\big(\mathrm{Ker}\, f\big) * \#\big(\mathrm{Im}\, f\big) .$$

Proposition IV.3.8 *Étant donné un groupe $(G, *)$ pour tout $x \in G$:*

i) Le sous-groupe $< \{x\} >$ engendré par $\{x\}$ (cf. II.4.2 ,) de G est l'image du morphisme

$$\epsilon_x : \mathbb{Z} \to G\ ,\ n \mapsto x^n$$

Démonstration *: (cf. l'exercice IV.4.6 .)*

ii) a) Soit le noyau de ϵ_x est réduit à $\{0\}$ au quel cas

$$< \{x\} > \cong \mathbb{Z}\ ;$$

b) Soit il existe $d \in \mathbb{N}^*$ tel que $\mathrm{Ker}\, \epsilon_X = d\mathbb{Z}$ et

$$< \{x\} > \cong \mathbb{Z}/\mathrm{Ker}\, \epsilon_x \cong \mathbb{Z}/d\mathbb{Z} .$$

Démonstration *: Le noyau du morphisme ϵ_x est un sous-groupe de $\mathbb{Z}$ il existe donc $d \in \mathbb{N}$ tel que $\mathrm{Ker}\, \epsilon_x = d\mathbb{Z}$. Or $d = 0$ si et seulement si ϵ_x est un morphisme injectif si et seulement si*

$$\mathbb{Z} \cong \mathrm{Im}\, \epsilon_x \cong < \{x\} >$$

ce qui correspond à la situation du point a .

Si $d \neq 0$, Il existe un unique isomorphisme

$$\overline{\epsilon}_x : \mathbb{Z}/\mathrm{Ker}\, \epsilon_x = \mathbb{Z}/d\mathbb{Z} \to \mathrm{Im}\, \epsilon_x = < \{x\} > .$$

On peut en effet appliquer les résultats du paragraphe IV.2 et en particulier la proposition IV.2.4 .

Définition IV.3.9 (Ordre d'un élément) Pour $(G, *)$ un groupe et $x \in G$, avec les notations de la proposition IV.3.8 , si $< \{x\} > \cong \mathbb{Z}$, on dit que x est d'*ordre infini* sinon on dit que x est d'*ordre* d où d est l'entier défini de manière équivalente dans le point b du point ii de la proposition IV.3.8 par $\mathrm{Ker}\, \epsilon_x = d\mathbb{Z}$ ou $d = \#(\mathrm{Im}\, \epsilon_x)$.

Remarque IV.3.10 Il est immédiat de vérifier que pour tout élément x d'un groupe G, l'ordre de x défini comme à la définition IV.3.9 , est le plus petit (aussibien au sens de la relation d'ordre que de la relation de divisibilité sur $\mathbb{Z}$) entier $n \in \mathbb{N}^*$ tel que $x^n = e$.

Proposition IV.3.11 (Propriétés de l'ordre d'un éléments) *i) Soit $f : G \to h$ un morphisme de groupes et $x \in G$. Si x est d'ordre fini, $f(x)$ l'est aussi et l'ordre de $f(x)$ divise l'ordre de x.*

ii) Avec les notations du point i , si f est injectif, x et $f(x)$ ont même ordre.

iii) Dans un groupe g deux éléments conjugués (cf. III.6.3. iii ,) ont même ordre.

Théorème IV.3.12 (de Lagrange) *Pour G un groupe fini, l'ordre de tout élément x de G divise le cardinal de G.*

Démonstration *: Remarquons d'abord que si G est fini, on ne peut se trouver dans la situation du point a du point ii de la proposition IV.3.8 si bien que l"ordre d de x est bien un entier naturel. Or il résulte du point b du point ii de la proposition IV.3.8 que*

$$d \;=\; \#(\operatorname{Im}\epsilon_x) \;=\; \#(<\{x\}>)\,.$$

Puisque $<\{x\}>$ est un sous-ghroupe de G, il suffit d'appliquer le corollaire IV.3.6 .

Définition IV.3.13 Avec les notations de la proposition IV.3.8 ,

i) si le morphisme ϵ_x est surjectif, autrement dit si

$$G \;=\; \operatorname{Im}\epsilon_x \;=<\tilde{s}x>,$$

on dit que G est *monogène* ;

ii) si de plus on est dans la situation du point b du point ii de la proposition IV.3.8 , auqel cas $G \;\cong\; \mathbb{Z}/d\mathbb{Z}$, on dit que G est *cyclique*.

Corollaire IV.3.14 *Un groupe est cyclique si et seulement s'il est monogène et fini.*

Corollaire IV.3.15 *Si G est un groupe fini de cardinal p premier, G est isomorphe (non canoniquement) à $(\mathbb{Z}/p,+)$ et donc commutatif (abélien).*

IV.4 . −Exercices

Exercice IV.4.1 On suppose que E est munie d'une relation d'équivalence $\sim$ et d'une loi

$$\cdot \;:\; E\times E \;\to\; E\,.$$

On suppose que $\cdot$ et $\sim$ sont *compatibles* c'est-à-dire que

$$\forall(x,y,z,t)\in E\times E\times E,\;\big(x\sim y \;\wedge\; z\sim t \;\Rightarrow x\cdot z \;\sim\; y\cdot t\big)\,.$$

On note $\pi \;:\; E \;\to\; E/\sim$ la surjection canonique.

1) Montrer qu'il existe une unique loi $\dagger \;:\; E/\sim \times E/\sim \to\; E/\sim$ tel que π soit un morphisme c'est-à-dire que

$$\forall(x,y)\in E\times E,\;\big(\pi(x\cdot y) \;=\; \pi(x)\dagger\pi(y)\big)\,.$$

On parle alors de *structure quotient*.

2) Montrer que si $\cdot$ est associative, (resp. possède un élément neutre) (resp. est commutative) il en est de même de $\dagger$. Montrer que si $x \;\in\; E$ possède un symétrique y pour $\cdot$ alors $\pi(y)$ est le symétrique de $\pi(x)$ pour $\dagger$.

3) Donner des exemples déjà connus des constructions précédentes.

Exercice IV.4.2 (Congruence modulo n) **1)** Montrer que tout entier relatif divise 0 tandis que 0 ne divise que lui-même.

Pour tout entier naturel n on définit la *relation de congruence modulo* n sur $\mathbb{Z}$ par a congrue à b modulo n si n divise $b-a$ et l'on écrit

$$a \equiv b\,[n]\,.$$

2) Montrer que la relation de congruence modulo n est une relation d'équivalence .

On notera $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence pour la relation de congruence modulo n, qu'on abrègera en *Classes de congruence modulo* n.

Pour tout $a \in \mathbb{Z}$, on notera $\pi_n(a)$ ou $\overline{a}$ la classe de a modulo n .

3) **a)** Montrer que $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est une application surjective. On l'appelle usuellement *surjection canonique*.

b) Est-elle injective ?

4) Donner le cardinal de $\mathbb{Z}/n\mathbb{Z}$.

5) Un entier naturel n étant fixé, montrer que, pour tout quadruplet (a,b,c,d) d'entiers relatifs,

$$a \equiv c\,[n] \text{ et } b \equiv d\,[n] \Rightarrow a+b \equiv c+d\,[n]\,;$$

c'est-à-dire que la relation de congruence et la loi d'addition $+$ sont compatibles

Exercice IV.4.3 (Caractérisation des sous-groupes distingués) Compléter la preuve de la proposition IV.1.4 .

Exercice IV.4.4 (Image réciproque/directe) Faire la preuve de la proposition IV.1.10 .

Exercice IV.4.5 (Sous-groupe d'un groupe fini) Faire la preuve de la proposition IV.3.3 et comparer avec la proposition II.3.5 .

Exercice IV.4.6 Faire la preuve du point i de la proposition IV.3.8 .

Exercice IV.4.7 (Un sous-groupe de GL_3) **Soit $\mathbb{K}$ un corps commutatif. On considère l'ensemble U des matrices de $\mathrm{GL}_3(\mathbb{K})$ de la forme**

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \textbf{ pour } (a,b,c) \in \mathbb{K}\times\mathbb{K}\times\mathbb{K}\,.$$

1) Montrer que U est un sous-groupe de $\mathrm{GL}_3(\mathbb{K})$.

2) Le sous-groupe U est-il distingué dans $\mathrm{GL}_3(\mathbb{K})$?

Indication : *On pourra calculer* $T * A * T^{-1}$, *pour* $T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

Exercice IV.4.8 (Équation aux classes)

Soit $(G, *)$ **un groupe dont on note** e **l'élément neutre.**

Pour tout $(x, y) \in G \times G$, **on dit que** y **est *conjugué à*** x **s'il existe** $g \in G$ **tel que** $y = g^{-1} * x * g$. **On notera** $x \sim y$.

1) Montrer que la relation « est conjugué à » est une relation d'équivalence dite *relation de conjugaison* ce qui permettra de dire dorénavant x et y *sont conjugués*. On appellera *classe de conjugaison d'un élément* $x \in G$ et on notera $\overline{x}$ sa classe pour la relation de conjugaison.

2) On appelle *centre du groupe* G **qu'on note** $\mathcal{Z}(G)$ **le sous-ensemble**

$$\mathcal{Z}(G) := \{g \in G \,;\, \forall h \in G,\ g * h = h * g\} \subset G\,.$$

a) Montrer que $\mathcal{Z}(G)$ est un sous-groupe distingué de G.

b) À quellle condition nécessaire et suffisante sur $\mathcal{Z}(G)$ G est-il abélien ?

c) Caractériser les éléments de $\mathcal{Z}(G)$ à l'aide de leur classe de conjugaison.

d) Montrer que si $G/\mathcal{Z}(G)$ est monogène alors G est abélien.

Indication : *On pourra penser à écrire (en le justifiant bien entendu !) un élément* $x \in G$ *sous la forme*

$$x = z * g^n\ ,\ z \in \mathcal{Z}(G)\ ,\ \overline{g} \text{ générateur de } G/\mathcal{Z}(G)\ ,\ n \in \mathbb{N}\,.$$

3) Pour tout $x \in G$, **on appelle *stabilisateur de*** x **et on note** $\mathrm{Stab}_G(x)$ **l'ensemble**

$$\mathrm{Stab}_G(x) := \{g \in G \,;\, x = g^{-1} * x * g\} \subset G\,.$$

a) Montrer que, pour tout $x \in G$, $\mathrm{Stab}_G(x)$ est un sous-groupe de G.

b) Quelle sous-groupe remarquable de G est contenu dans $\mathrm{Stab}_G(x)$ pour tout $x \in G$, Que vaut

$$\bigcap_{x \in G} \mathrm{Stab}_G(x) \ ?$$

Pour tout $x \in G$, **tout** $(y, z) \in G \times G$, **on note** $z \sim_x y$ **si** $y * z^{-1} \in \mathrm{Stab}_G(x)$.

c) Rappeler pourquoi $\sim_x$ est une relation d'équivalence.

d) Montrer que, pour tout $x \in G$, on a une bijection

$$G/\sim_x \cong \overline{x}\ .$$

e) En déduire que si G est fini

$$\forall x \in G,\ \#(G) \ =\ \#(\overline{x}) \cdot\ \#(\mathrm{Stab}_G(x))\ .$$

4) Soit p un nombre premier et $r \in \mathbb{N}^*$. on suppose désormais que $\#(G) = p^r$.

a) Montrer que si $r = 1$, *i.e.* $\#(G) = p$ G est cyclique et par conséquent abélien.
On suppose maintenant que $r \in \mathbb{N}^*$ est quelconque.

b) Quelles valeurs peut prendre $\#(\overline{x})$ pour $x \in G$?

Notons $\mathcal{C}$ l'ensemble des classes de conjugaison de G,

$$\mathcal{C}_0 \ :=\ \{c \in \mathcal{C}\ ;\ \#(c) = 1\} \text{ et } \mathcal{C}_\infty \ :=\ \mathcal{C} \setminus \mathcal{C}_0\ .$$

c) Montrer que

$$\#(\mathcal{Z}(G)) \ =\ \#(G) - \sum_{c \in \mathcal{C}_\infty} \#(c)$$

et en déduire que $p|\#(\mathcal{Z}(G))$.

d) En déduire qu'il existe $k \in \mathbb{N}\ 1 \le k \le r$ tel que $\#(\mathcal{Z}(G)) = p^k$.

e) Déduire de ce qui précède que, si $\#(G) = p^2$, G est abélien.

Exercice IV.4.9 (Action d'un sous-groupe distingué) Soit H un sous-groupe distingué d'un groupe G qui agit transitivement sur un ensemble X.

Montrer que les orbites de l'action (induite de l'action de G) de H sur X ont toutes même cardinal.