V . −Actions de groupes, groupes quotients

V.1 . −Actions de groupe

Pour tout ensemble E, on rappelle qu'on note $\mathcal{S}(E)$ le groupe des bijections de E défini en III.1.2.c) et pour toute bijection $f : E \to F$,

$$\mathcal{S}(f) : \mathcal{S}(E) \to \mathcal{S}(F)$$

l'isomorphisme de groupes qui s'en déduit (cf. III.2.6.)

Dans toute cette section (V.1,) $(G, *)$ est un groupe dont on notera e l'élément neutre.

Définition V.1.1 (Action de groupe) Étant donné un ensemble E et un groupe $(G, *)$ on dit que G *agit sur* (ou *opère sur*) E ou que E est muni d'une *action* de G, s'il existe un morphisme de groupe (cf. III.2.1,)

$$\phi : (G, *) \to (\mathcal{S}(E), \circ) .$$

On dira aussi que E est un *G-ensemble*.

Remarque V.1.2 Si l'on a une action $\phi : (G, *) \to (\mathcal{S}(E), \circ)$, cela signifie que

$$\forall g \in G, \ \forall h \in G, \ \phi(g * h) = \phi(g) \circ \phi(h)$$

et cela a pour conséquences que $\phi(e_G) = \mathrm{Id}_E$ (cf. III.2.9.i);) et $\forall g \in G, \ \phi(g^{-1}) = \phi(g)^{-1}$ (cf. III.2.9.ii).)

Notation V.1.3 Étant donnés un groupe G agissant sur un ensemble E il est usuel de noter

$$\forall g \in G, \ \forall x \in E, \ g \cdot x := \phi(g)(x) .$$

On a alors

$$\forall x \in E, \ e_G \cdot x = x \text{ et } \forall g \in G, \ \forall h \in G, \ (g * h) \cdot x = g \cdot (h \cdot x) .$$

Exemple V.1.4 a) Pour tout ensemble E, le groupe $\mathcal{S}(E)$ agit évidemment sur E, dans la mesure où $\mathrm{Id}_{\mathcal{S}(E)} : \mathcal{S}(E) \to \mathcal{S}(E)$ est un morphisme de groupes.

b) Étant donnés un groupe G agissant sur un ensemble E par $\phi : G \to \mathcal{S}(E)$ tout morphisme $f : H \to G$ définit une action $\phi \circ f$ de H sur E. En particulier si G agit sur E, tout sous-groupe H de G agit naturellement sur E à travers l'injection naturelle $H \hookrightarrow G$.

c) Si $f : E \to F$ est une bijection d'un ensemble E sur un ensemble F, l'isomorphisme

$$\mathcal{S}(f) : \mathcal{S}(E) \to \mathcal{S}(F)$$

défini en III.2.6, associe à toute action $\phi : G \to \mathcal{S}(E)$ d'un groupe G sur E, une action

$$\mathcal{S}(f) \circ \phi : G \to \mathcal{S}(F)$$

et l'on a de manière évidente :

$$\forall (g, x) \in G \times E, \ f(g \cdot x) = g \cdot f(x) .$$

Les exemples ci-dessus sont en quelque sorte tautologiques et ne mettent pas en évidence daction de groupes arbitraires (autre que le groupe $\mathcal{S}(E)$.) Or un des intérêts de la notion d'action de groupe est précisément de permettre l'étude d(d'un certain nombre de propriétés de groupes arbitraires à travers la manière dont ils peuvent agir. Donnons donc quelques exemples plus concrets qui sont cependant très loins d'épuiser la question :

Exemple V.1.5 a) Pour un $\mathbb{K}$-espace vectoriel V, le groupe linéaire $\mathrm{GL}(V)$ *i.e.* le groupe des applications linéaires bijectives de V dans lui-même agit sur V, puisque $\mathrm{GL}(V)$ est un sous-groupe de $\mathcal{S}(V)$.

Le groupe $\mathbb{K}^\times$ des éléments inversibles de $\mathbb{K}$ muni de la multiplication s'identifie au sous-groupe de $\mathrm{GL}(V)$ formé des homothéties bijectives et agit donc également sur V.

b) Dans le cas où V est un $\mathbb{K}$-espace vectoriel muni d'une structure euclidienne, il résulte de a) que les sous-groupes $\mathcal{O}(V)$ et $\mathcal{SO}(V)$ de $\mathrm{GL}(V)$ agissent également sur V. Il peut être plus intéressant encore de constater qu'ils agissent sur des parties remarquables de V (voir TD n° V, exercice B.)

c) Étant donné un $\mathbb{K}$-espace affine A, le groupe des translations, (resp. le groupe des isométries si A est euclidien) agit sur A [6].

Définition V.1.6 (Applications invariantes/G-morphismes) Étant donnés un groupe G et deux ensembles E et F munis d'actions

$$\phi_E(\text{resp. } \phi_F) \ : \ G \ \to \ \mathcal{S}(E)(\text{resp. } \mathcal{S}(F))$$

de G, on dit qu'une application $f \ : \ E \ \to \ F$ de E dans F est *invariante* si

$$\forall g \in G, \ f \ \circ \phi_E(g) \ = \ \phi_F(g) \ \circ \ f$$

ce qui s'écrit encore

$$\forall (g, x) \in G \times E, \ f(g \cdot_E x) \ = \ g \cdot_F f(x) \ .$$

Le terme de *morphisme de G-ensembles* est synonyme d'application invariante.

Exemple V.1.7 On a vu un exemple d'application invariante en V.1.4.c) mais c'est loin d'être le plus intéressant.

Toute application linéaire $V_1 \ \to \ V_2$ est invariante pour l'action par homothétie (cf. V.1.5.a).)

Proposition V.1.8 *Étant donnés un groupe G agissant sur un ensemble E, la relation $\sim$ définie sur E par*

$$\forall x \in E, \ \forall y \in E, \ x \ \sim \ y \ \Leftrightarrow \ \exists g \in G, \ y \ = \ g \cdot x$$

est une relation d'équivalence (cf. I.2.2.v),) sur E.

Preuve *: Voir l'exercice V.7.1.*

6. On conseille de reconsidérer cet exemple à la lumière du cours de géométrie.

Définition V.1.9 (Orbite) Étant donnés un groupe G agissant sur un ensemble E, *i.e.* un G-ensemble E :

i) (**orbite**)

Les classes déquivalence pour la relation définie par la proposition V.1.8 sont appelées *orbites*. Plus précisément pour tout $x \in E$, la classe de x est appelée *orbite de x sous l'action* de G. On la note usuellement $O_G(x)$ (ou simplement $O(x)$ s'il n'en résulte aucune ambiguîté) et l'on a :

$$O(x) = \{g \cdot x \, , \, g \in G\} \, .$$

ii) (**point fixe**)

Pour $x \in E$, de manière équivalente, $O(x) = \{x\}$, $O(x)$ est un singleton, $\forall g \in G, \; g \cdot x = x$. On dit alors que x est un *point fixe pour l'action* de G sur E. On dit aussi que l'orbite de x est *triviale*.

Exemple V.1.10 Pour laction de $\mathbb{K}^\times$ sur V par homothétie (cf. V.1.5.a),) les orbites sont, d'une part l'origine 0_V de V et d'autre part les droites de V privées de l'origine.

Lemme V.1.11 *Étant donné un G-ensemble E, les assertions suivantes sont équivalentes :*

a) Il y a une seule orbite sous l'action de G.

b)

$$\forall x \in E, \; O_G(x) = E \, .$$

c)

$$\forall (x, y) \in E \times E, \; \exists g \in G, \; y = g \cdot x \, .$$

***Preuve** : Voir l'exercice V.7.2.*

Définition V.1.12 (Action transitive) Si un G-ensemble E vérifie les assertions équivalentes du lemme V.1.11, on dit que l'action de G sur E est *transitive* ou encore que G agit/opère *transitivement* sur E.

Exemple V.1.13 Si E est un G-ensemble, pour tout $x \in E$, G agit transitivement sur l'orbite $O(x)$ de x.

Proposition V.1.14 (Stabilisateur d'un élément) *Étant donnée une action d'un groupe G sur un ensemble E, pour tout $x \in E$, l'ensemble :*

$$\mathrm{Stab}_G(x) := \{g \in G \, ; \, g \cdot x = x\} \qquad \textit{V.1.14.1}$$

est un sous-groupe de G.

***Preuve** : Voir l'exercice V.7.3 et le TD n° V, exercice E, question 3), a) dans le cas particulier de l'action par conjugaison.*

Définition V.1.15 (Stabilisateur) Étant donnée une action d'un groupe G sur un ensemble E, pour tout $x \in E$, le sous-groupe $\mathrm{Stab}_G(x)$ défini par la proposition V.1.14.1 est appelé *stabilisateur* de x.

Proposition V.1.16 *Étant donné un G-ensemble E, pour tout $x \in E$, notons $\mathrm{Stab}_G(x)$ le stabilisateur de x pour l'action de G, et*

$$p : G \to O(x) , g \mapsto g \cdot x .$$

Alors :

i) L'ensemble des $p^{-1}(\{y\})$ pour $y \in O(x)$, forme une partition de G.

***Preuve** : Voir l'exercice V.7.4.*

ii) Pour tout $g \in G$,

$$p^{-1}(\{g \cdot x\}) = g * \mathrm{Stab}_G(x) = \{g * h , h \in \mathrm{Stab}_G(x)\} .$$

***Preuve** : Pour tout $g \in G$ et tout $h \in p^{-1}(\{g \cdot x\})$ si et seulement si $p(h) = g \cdot x$ i.e.*

$$h \cdot x = g \cdot x \Leftrightarrow (g^{-1} * h) \cdot x = x \Leftrightarrow g^{-1} * h \in \mathrm{Stab}_G(x) \Leftrightarrow h \in g * \mathrm{Stab}_G(x) .$$

Corollaire V.1.17 *Sous les hypothèses de la proposition V.1.16, si l'on suppose de plus que G est un groupe fini alors :*

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

***Preuve** : C'est une conséquence immédiate de la proposition V.1.16.*

Proposition V.1.18 *Soit E un G-ensemble. Pour tout $x \in E$ et tout $g \in G$,*

$$\mathrm{Stab}_G(g \cdot x) = g * \mathrm{Stab}_G(X) * g^{-1} := \{g * h * g^{-1} , h \in \mathrm{Stab}_G(x)\} .$$

***Preuve** : (Voir aussi le V.7.5.)*

Pour tout $(x, g, h) \in E \times G \times G$, $h \in \mathrm{Stab}_G(g \cdot x)$ si et seulement si $h \cdot (g \cdot x) = g \cdot x$ si et seulement si

$$g^{-1} \cdot (h \cdot (g \cdot x)) = x \Leftrightarrow (g^{-1} * h * g) \cdot x = x \Leftrightarrow g^{-1} * h * g \in \mathrm{Stab}_G(x)$$

c'est-à-dire qu'il existe $k \in \mathrm{Stab}_G(x)$ tel que $g^{-1} * h * g = k$ i.e. $h = g * k * g^{-1}$ c'est-à-dire finalement que

$$h \in g * \mathrm{Stab}_G(x) * g^{-1} .$$

Les définitions qui suivent sont données pour compléter la présentation des actions de groupe mais il est probable qu'on n'en fera assez peu usage.

Définition V.1.19 Soit E un G-ensemble.

i) (**Action libre**)
On dit que l'action de G sur E est *libre* (ou encore que G agit/opère *librement*) si pour tout $x \in E$,

$$\mathrm{Stab}_G(x) = \{e\} .$$

ii) (**Action fidèle**)
On dit que l'action de G sur E est *fidèle* (ou encore que G agit/opère *fidèlement*) si l'intersection de touts les stabilisateurs des éléments de E est $\{e\}$ ce qui équivaut à dire que le morphisme $G \to \mathcal{S}(E)$ définissant l'action est injectif.

iii) (**ACtion simplement transitive**)
Laction est *simplement transitive* si elle est libre et transitive (cf. V.1.12.)

V.2 . −Action par translation à gauche

Dans ce paragraphe $(G, *)$ est un groupe (noté seulement G si aucune confusion n'en résulte) et l'on note e son élément neutre.

Lemme V.2.1 *Soit $(G, *)$ un groupe. L'application de $G \times G$ dans G définie par $g \cdot x := g * x$ est une action de G sur lui-même.*

***Preuve** : On constate d'abord que pour tout $g \in G$, l'application de G dans lui-même donée par $x \mapsto g * x$ est bien une bijection de G dans lui-même (i.e. un élément de $\mathcal{S}(G)$,) de bijection réciproque $x \mapsto g^{-1} * x$.*
En outre

$$\forall (g, h) \in G \times G,\ (g * h) \cdot x = (g * h) * x = g * (h * x) = g \cdot (h * x) = g \cdot (h \cdot x)$$

ce qui assure qu'on a bien une action.

Définition V.2.2 (Translation à gauche) Étant donné un groupe G, l'action de G sur lui-même définie par le lemme V.2.1 est appelée *action par translation à gauche*.

Il résulte de V.1.4.b) que tout sous-groupe H de G agit encore sur G à travers l'action de G sur lui-même par translation à gauche. Cette action de H sur G est encore appelée *action par translation à gauche de H sur G*.

Remarque V.2.3 Si $P \subset G$, est une partie de G (*i.e.*

$$P \in \mathcal{P}(G) \text{ pas nécessairement un sous-groupe },)$$

notons

$$\forall g \in G,\ g * P := \{g * x\ ,\ x \in P\}\ .$$

Alors l'application $G \times \mathcal{P}(G) \to \mathcal{P}(G)$ définie par $(g, P) \mapsto g \cdot P := g * P$ est une action de G sur l'ensemble de ses parties, qu'on apellera encore action par translation à gauche. Elle induit encore une action par translation à gauche de tout sous-groupe H de G sur $\mathcal{P}(G)$.

Notation V.2.4 On a vu en V.1.8 que, dès que E est un G-ensemble, l'action de G sur E induit une relation d'équivalence $\sim$. Dans le cas de l'action de H sur G par translation à gauche on notera parfois $\sim_{H,g}$ cette relation. Elle prend une forme suffisamment particulière dans ce cas pour qu'on l'explicite :

$$\begin{array}{lrcl} \forall (x,y) \in G \times G, & x & \sim_{H,g} & y \\ \Leftrightarrow & \exists h \in H,\ y & = & h \cdot x \\ \Leftrightarrow & y & = & h * x \\ \Leftrightarrow & y * x^{-1} & \in & H \\ \Leftrightarrow & x * y^{-1} & \in & H\ . \end{array}$$

Remarque V.2.5 Soit $(G, *)$ un groupe.

i) L'application de $G \times G$ dans G définie par $g \cdot x := x * g$ est une *action à droite* de G sur lui-même. Elle est appelée *action par translation à droite*.

La notion d'action à droite ne sera pass développée ni utilisée dans ce qui suit. Disons simplement que la formule

$$(g * h) \cdot x = g \cdot (h \cdot x)$$

qui caractérise les actions à gauches est remplacée par

$$(g * h) \cdot x = h \cdot (g \cdot x)\ .$$

ii) Il résulte de V.1.4.b) que tout sous-groupe H de G agit encore sur G à travers l'action de G sur lui-même par translation à droite. Cette action de H sur G est encore appelée *action par translation à droite de H sur G*.

iii) Si $P \subset G$, est une partie de G (*i.e.* $P \in \mathcal{P}(G)$ pas nécessairement un sous-groupe,) notons

$$\forall g \in G,\ P * g := \{x * g\ ,\ x \in P\}\ .$$

Alors l'application $G \times \mathcal{P}(G) \to \mathcal{P}(G)$ définie par $(g, P) \mapsto g \cdot P := P * g$ est une action à droite de G sur l'ensemble de ses parties, qu'on apellera encore action par translation à droite. Elle induit encore une action par translation à droite de tout sous-groupe H de G sur $\mathcal{P}(G)$.

iv) On a vu en V.1.8 que, dès que E est un G-ensemble, l'action de G sur E induit une relation d'équivalence $\sim$. Dans le cas de l'action de H sur G par translation à droite on notera parfois $\sim_{H,d}$ cette relation. Elle prend une forme suffisamment particulière dans ce cas pour qu'on l'explicite :

$$\begin{array}{lrcl} \forall (x,y) \in G \times G, & x & \sim_{H,d} & y \\ \Leftrightarrow & \exists h \in H,\ y & = & h \cdot x \\ \Leftrightarrow & y & = & x * h \\ \Leftrightarrow & x^{-1} * y & \in & H \\ \Leftrightarrow & y^{-1} * x & \in & H\ . \end{array}$$

Définition V.2.6 (Classes à gauche/droite) Étant donnés un groupe G et un sous-groupe H de G, les classes d'équivalence pour la relation $\sim_{H,g}$, (cf. V.2.4,) qui sont aussi les orbites (cf. V.1.9,) pour l'action par translation à gauche, sont appelées *classes à gauche*. L'ensemble de ses classes est noté $G/\sim_{H,g}$.

On a une définition analogue de *classes à droite* en utilisant la relation $\sim_{H,d}$ (cf. V.2.5.iv),) dont l'ensemble est noté $G/\sim_{H,d}$.

Proposition V.2.7 *Soit G un groupe et H un sous-groupe de g. On considère l'action de H sur G par translation à gauche. Alors :*

i) Dans le cas où G est abélien, la relations d'équivalence $\sim_{H,g}$ associée à l'action de H est la même qe celle définie en VII.7.3.

***Preuve** : Est une vérification immédiate.*

ii) Pour tout $x \in G$, l'application

$$p\ :\ H\ \to\ O(x)\ ,\ g\ \mapsto\ g \cdot x$$

définie comme dans la proposition V.1.16 est bijective.

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

$$p\ :\ H\ \to\ O(x)\ ,\ g\ \mapsto\ g \cdot x$$

comme à la proposition V.1.16. Il résulte alors de V.1.16.ii) que

$$\forall y \in O(x),\ p^{-1}(\{y\})\ \cong\ \mathrm{Stab}_H(x)\ .$$

Or $g \in \mathrm{Stab}_H(x)$ si et seulement si $g \cdot x = x$, si et seulement si $g * x = x$ si et seulement si $g = e$. Le sous-groupe $\mathrm{Stab}_H(x)$ de H est donc un singleton. Ainsi en va-t-il donc aussi de $p^{-1}(\{y\})$ c'est-à-dire que $p\ :\ H\ \to\ O(x)$ est bijective.

iii) H est l'orbite de l'élément neutre e et la seule qui soit un sous-groupe de G.

***Preuve** : En effet*

$$O(e) \;=\; \{h\cdot e\,,\; h\;\in\; H\} \;=\; \{h*e\,,\; h\;\in\; H\} \;=\; \{h\in H\} \;=\; H\,.$$

Pour $x\;\in\; G$, si $O(x)$ est un sous-groupe $e\;\in\; O(x)$ et par conséquent $O(x)\;=\; O(e)$.

iv) Il existe une bijection entre l'ensemble $G/\!\sim_{H,g}$ des classes à gauche et l'ensemble $G/\!\sim_{H,d}$ des classes à droite.

***Preuve** : V.4.3.*

Remarque V.2.8 Le point V.2.7.ii) pourrait se reformuler en disant que l'action par translation à gauche (resp. à droite) est libre (cf. V.1.19.i).)

Définition V.2.9 (Indice d'un sous-groupe) Étant donnés un groupe G et un sous-groupe H de G, si l'ensemble $G/\!\sim_{H,g}$, est fini (cf. II.4.1,) son cardinal, qui est aussi celui de $G/\!\sim_{H,d}$, est appelé *indice de H dans G*.

V.3 . −Action par conjugaison

Dans cette section $(G,*)$ (le plus souvent abrégé en G) est un groupe dont on note e l'élément neutre.

Lemme V.3.1 *Étant donné un groupe G, pour tout $g\;\in\; G$, l'application $x\;\mapsto\; g*x*g^{-1}$ est un automorphisme de groupe de G (cf. III.2.7.ii).)*

***Preuve** : Tout d'abord*

$$\forall (g,x,y)\in G\times G\times G,\; g*x*y*g^{-1}\;=\; g*x*g^{-1}\;*\; g*y*g^{-1}$$

si bien que $x\;\mapsto\; g*x*g^{-1}$ est bien un morphisme de G dans luie-même (on pourrait dire un endomorphisme de G.)

Par ailleurs,

$$\forall (g,x)\in G\times G,\; (g^{-1})*g*x*g^{-1}*(g^{-1})^{-1}\;=\; x$$

si bien que $x\;\mapsto\; (g^{-1})*x*(g^{-1})^{-1}$ est l'application réciproque de $x\;\mapsto\; g*x*g^{-1}$ cette dernière étant donc bijective donc un isomorphisme et finalement un automorphisme (isomorphisme et endomorphisme.)

Lemme V.3.2 *L'application de $G \times G$ dans G donnée par $(g, x) \mapsto g \cdot x := g * x * g^{-1}$ définit une action de G sur lui-même.*

***Preuve** : On a vu au lemme V.3.1 que $x \mapsto g * x * g^{-1}$ est un automorphisme de G donc en particulier une bijection de G sur lui-même i.e. un élément de $\mathcal{S}(G)$ (cf. III.1.2.c).)*

De plus

$$\begin{array}{rcl} \forall (g,h,x) \in G \times G \times G, \quad (g * h) \cdot x & = & g * h * x * g * h^{-1} \\ & = & g * h * x * h^{-1} * g^{-1} \\ & = & g \cdot (h * x * h^{-1}) \\ & = & g \cdot (h \cdot x) \end{array}$$

ce qui prouve qu'on a bien défini une action.

Définition V.3.3 (Action par conjugaison) Soit G un groupe :

i) L'action de G sur lui-même définie par le lemme V.3.2 s'appelle *action par conjugaison* de G sur lui-même.

ii) Les orbites (cf. V.1.9,) pour l'action par conjugaison sont usuellement appelées *classes de conjugaison*.

iii) Deux élément appartenant à la même orbite, ou de manière équivalente, en relation par la relation $\sim$ (cf. V.1.8,) sont dits *conjugués*. Ainsi explicitement, $(x, y) \in G \times G$ sont conjugués s'il existe z (appartenant à G ou à un sous-groupe selon l'action considérée,) tel que $y = z * x * z^{-1}$.

iv) Il résulte de V.1.4.b) que tout sous-groupe H de G agit encore sur G à travers l'action de G sur lui-même par conjugaison. Cette action de H sur G est encore appelée *action par conjugaison de H sur G*.

Remarque V.3.4 Si $P \subset G$, est une partie de G,
(*i.e.* $P \in \mathcal{P}(G)$, pas nécessairement un sous-groupe,) notons

$$\forall g \in G,\ g * P * g^{-1} := \{g * x * g^{-1}\ ,\ x \in P\}\ .$$

Alors l'application $G \times \mathcal{P}(G) \to \mathcal{P}(G)$ définie par $(g, P) \mapsto g \cdot P := g * P * g^{-1}$ est une action de G sur l'ensemble de ses parties, qu'on apellera encore action par conjugaison. Elle induit encore une action par conjugaison de tout sous-groupe H de G sur $\mathcal{P}(G)$.

Proposition V.3.5 *Étant donné un groupe $(G, *)$ on note $\mathcal{G}$ l'ensemble de ses sous-groupes. Pour tout $g \in G$, et $H \in \mathcal{G}$ on note :*

$$g * H * g^{-1} := \{g * x * g^{-1}\ ,\ x \in H\}\ . \qquad \textit{V.3.5.1}$$

Alors :

i) Pour tout $H \in \mathcal{G}$ $g * H * g^{-1}$ est un sous-groupe de G i.e. un élément de $\mathcal{G}$.

***Preuve** : Étant donné un sous-groupe H de G et $g \in G$, $g * H * g^{-1}$ n'est autre que l'image de H par l'application $x \mapsto g * x * g^{-1}$ dont on a montré au lemme V.3.1 que c'est un morphisme de groupe. L'ensemble $g * H * g^{-1}$ est donc un groupe.*

ii) L'application

$$G \times \mathcal{G} \to \mathcal{G}\ ,\ (g, H) \mapsto g * H * g^{-1}$$

est une action de G sur $\mathcal{G}$ qui sera encore apppelée action par conjugaison.

***Preuve** : Voir l'exercice V.7.8.*

V.4 . −Sous-groupes normaux

On pourrait tout à fait se passer, pour rédiger cette section (V.4,) des résultats des section V.1, V.3 et V.2 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 (V.4,) $(G, *)$ est un groupe d'élément neutre e.

Notation V.4.1 Pour tout sous-groupe H de G, on définit comme en V.2.4 $\sim_{H,g}$ (resp. comme en V.2.5.iv) $\sim_{H,d}$) la relation binaire sur $G \times G$ par :

$$\begin{array}{rl} & \forall x \in G,\ \forall y \in G,\ \left(x \sim_{H,d} y \ \Leftrightarrow x^{-1} * y \in H\right) \\ \left(\text{resp.} \quad\right. & \left.\forall x \in G,\ \forall y \in G,\ \left(x \sim_{H,g} y \ \Leftrightarrow\ y * x^{-1} \in H\right) \quad\right)\ . \end{array} \qquad \text{V.4.1.1}$$

On notera encore, :

$$\forall x \in G,\ x * H \ := \ \{x * y\ ;\ y \in H\}\ \left(\text{resp. } H * x \ := \ \{y * x\ ;\ y \in H\}\ .\right) \qquad \text{V.4.1.2}$$

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

Remarque V.4.2 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. V.1.9.)

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

Proposition V.4.3 *i) Les relations binaires définies en V.4.1.1 sont des relations d'équivalence.*

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

Plus précisément :

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

Preuve : *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 $\sim_{H,g}$ (resp. $\sim_{H,d}$) est en bijection avec H.

Preuve : *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 V.4.4 *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. I.6.17,) 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)

$$\forall x \in G,\ \big(x * H\ =\ H * x\big)\ .$$

e)

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

f)

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

***Preuve** : On montre l'équivalence e) $\Leftrightarrow$ b) :*

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 a) 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 e).

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 e) 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 e) entraîne l'assertion b).

Définition V.4.5 (Sous-groupes normaux/distingués) Un sous-groupe H de G est dit *normal* ou *distingué*, s'il vérifie les conditions équivalentes de la proposition V.4.4.

Remarque V.4.6 On peut reformuler la définition ci-dessus en termes d'actions par conjugaison (cf. V.3,) 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. V.3.5.) On dira donc parfois que H est *invariant par conjugaison* ou même simplement *invariant*.

Notation V.4.7 Le point V.4.4.c) 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 de V.4.4.b) (ou indifféremment de V.4.4.a)) que $\sim_H$ est compatible à la loi de groupe sur G (cf. I.6.17.) 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 V.5.

Définition V.4.8 Pour tout sous-groupe distingué H de G, on appellera *classes modulo H* ou *classes selon H* les classes d'équivalences 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

$$\alpha * \beta \ = \ \overline{x} * \overline{y} \ := \ \overline{x * y} \qquad \text{V.4.8.1}$$

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 V.4.9 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 de G est distingué.

c) Pour $n \ \in \ \mathbb{N}$, si $\mathcal{S}_n$ est le groupe symétrique, le groupe alterné $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$ (cf. VI.4).

d) Si E est un $\mathbb{R}$-espace vectoriel euclidien, le groupe spécial orthogonal $\mathcal{SO}(E)$ est un sous-groupe distingué du groupe orthogonal $\mathcal{O}(E)$.

Proposition V.4.10 *Pour tout morphisme de groupes $f \ : \ G \ \to \ H$ (cf. III.2.1,) l'image réciproque $f^{-1}(H')$ de tout sous-groupe distingué H' 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 $f(G')$ d'un sous-groupe distingué G' de G est un sous-groupe distingué de H. C'est cependant le cas si f est surjectif.

Preuve *: Voir l'exercice V.7.10.*

Proposition V.4.11 (Relations d'équivalences compatibles) *i) Une relation d'équivalence $\sim$ sur G est compatible si et seulement si pour tout $(x, y) \in G \times G$,*

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

Preuve *: 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.

***Preuve** : 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 III.3.4, $\overline{e}$ 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 V.4.4.e), 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 $\overline{e} = H$.

***Preuve** : 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 V.4.12 *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)

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

***Preuve** :*

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 V.4.11.i)

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

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.

V.5 . −Groupe quotient, factorisation des morphismes

Dans toute cette section (V.5,) $(G, *)$ est un groupe d'élément neutre e.

Proposition V.5.1 *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 $\overline{x^{-1}}$.*

Preuve *:*

i) S'il existe une structure de groupe $\dagger$ *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*

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

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

Comme π *est surjective, la structure* $\dagger$ *est nécessairement unique.*

ii) Comme $\sim_H$ *est compatible à* $(G, *)$ *(cf. V.4.4,)*

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

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* $\dagger$*.*

Définition V.5.2 (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 V.5.3 Nous avons remarqué (cf. V.4.9.b),) que dans un groupe abélien, et en particulier dans $(\mathbb{Z}, +)$, tout sous-groupe est distingué. Nous avons aussi établi (cf. IV.5.5,) qu'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 TD n° IV, exercice B. 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 V.5.4 (Factorisation des morphismes) *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* $H = \mathrm{Ker}\, f$, *(rsp.* f *est surjectif.)*

***Preuve** :*

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* $x * x'^{-1} \in \mathrm{Ker}\, f$ *si l'on suppose que* $H \subset \mathrm{Ker}\, f$, *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. V.4.8.1,)*

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

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

iv) Un élément $u \in H$ *appartient à* $\mathrm{Im}\, \overline{f}$ *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,*

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

ce qui établit (cf. III.3.10,) 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. III.3.10.) 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 V.5.5 *Étant donné un morphisme de groupes $f : G \to K$ il existe un unique isomorphisme de groupes*

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

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.

***Preuve** : Il suffit d'appliquer la proposition V.5.4 à $H := \mathrm{Ker}\, f$.*

Corollaire V.5.6 *Étant donné un morphisme surjectif de groupes $p : G \to Q$, il existe un unique isomorphisme de groupes*

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

***Preuve** : C'est une conséquence immédiate du corollaire V.5.5 puisque $\mathrm{Im}\, p = Q$.*

Proposition V.5.7 *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 $p : G \to Q$.

***Preuve** :*

i) On a vu, grâce à la proposition V.4.11, 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 V.5.1, 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. V.4.10.)

Le corollaire V.5.6 établit qu'en fait, les procédés ii) et iii) "inverses" l'un de l'autre, en un certain sens.

La proposition suivante V.5.8 étend au cas des groupes les constructions donées dans la proposition II.5.4.

Proposition V.5.8 *Étant donnés un entier* $n \in \mathbb{N}^*$, $(G_k, *_k)_{,1\leq k\leq n}$ *des groupes*

$$\forall 1 \leq k \leq n,\ p_k \ :\ \prod_{i=1}^{n} G_i \ \to\ G_k \text{ les projections}$$

(cf. II.5.1.ii),) Alors :

i) Il existe une unique loi de composition $*$ *sur* $\prod_{k=1}^{n} G_k$ *telle que pour tout* $1 \leq k \leq n$, p_k *soit un morphisme de groupes ; la loi* $*$ *est donnée par*

$$\forall\big((x_1,\dots,x_n),(y_1,\dots,x_n)\big) \in \prod_{k=1}^{n} G_k \times \prod_{k=1}^{n} G_K,$$
$$(x_1,\dots,x_n)\ *\ (y_1,\dots,y_n)\ =\ (x_1 *_1 y_1,\dots,x_n *_n y_n)\ .$$

ii) La loi $*$ *étant définie sur* $\prod_{k=1}^{n} G_K$ *comme ci-dessus, si*

a) pour tout $1 \leq k \leq n$, e_k *est l'élément neutre de* G_k, $(e_1,\dots,e_n)$ *est l'élément neutre pour* $*$;

b) $x \in \prod_{k=1}^{n} G_k$ *est tel que pour tout* $1 \leq k \leq n$, $y_k \in G_k$ *est le symétrique de* $p_k(x)$, *alors* $(y_1,\dots,y_n)$ *est le symétrique de* x *dans* $\prod_{k=1}^{n} G_k$.

iii) Si pour tout $1 \leq k \leq n$, $(G_k, *_k)$ *est un groupe abélien,* $\big(\prod_{k=1}^{n} G_k, *\big)$ *est un groupe abélien.*

iv) Pour tout n*-uplet de morphismes de groupes*

$$f_k\ :\ H\ \to\ G_k\ ,_{1\leq k\leq n}\ ,$$

il existe un unique morphisme de groupe

$$f\ :\ H\ \to\ \prod_{k=1}^{n} G_k \text{ tel que } \forall 1 \leq k \leq n,\ f_k\ =\ p_k\ \circ\ f\ .$$

v) Dans le cas où il existe G tel que $\forall 1 \leq k \leq n,\ G_k = G$, la bijection $\phi : G^{[1;n]} \cong \prod_{k=1}^{n} G$ définie par la proposition II.5.1.iv) est un isomorphisme, pour peu que $G^{[1;n]}$ soit muni de la structure définie par la proposition I.6.20.

vi) Pour $(G_1, *_1), (G_2, *_2)$ des groupes d'élément neutre respectif ϵ_1 et ϵ_2, on définit les applications

$$i_1 : G_1 \to G_1 \times G_2 ,\ x \mapsto (x, \epsilon_2) \text{ et } i_2 : G_2 \to G_1 \times G_2 ,\ x \mapsto (\epsilon_1, x) .$$

Alors :

a) les applications i_1 et i_2 sont des morphismes injectifs de groupes ;

b)

$$p_1 \circ i_1 = \mathrm{Id}_{G_1} \text{ et } p_2 \circ i_2 = \mathrm{Id}_{G_2} ;$$

c)

$$\mathrm{Ker}\, p_1 = \mathrm{Im}\, i_2 \text{ et } \mathrm{Ker}\, p_2 = \mathrm{Im}\, i_1 .$$

***Preuve** : Voir le Examen partiel du 24 octobre 2018 , exercice B.*

Définition V.5.9 (Groupe produit) Avec les notations de la proposition V.5.8, la loi $*$ définie sur $\prod_{k=1}^{n} G_k$ comme en V.5.8.i) est appelée *loi produit* et le couple

$$(\prod_{k=1}^{n} G_k, *)$$

groupe produit.

V.6 . −Groupes finis : théorème de Lagrange

Définition V.6.1 (Groupe fini) Un groupe $(G, *)$ est un *groupe fini* si G est un ensemble fini au sens de la définition II.4.1.

Exemple V.6.2 Pour $n \in \mathbb{N}^*$, le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe fini (cf. TD n° IV, exercice B.)
D'autres exemples de groupes finis seront étudiés dans le chapitre VI.

Proposition V.6.3 *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 $(x, y) \in H \times H$, $x * y \in H$.*

***Preuve** : Voir le TD n° V, exercice A.*

Proposition V.6.4 *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 en V.2.4, (resp. V.2.5.iv),)*

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

d'où il résulte en particulier que

$$\#(H) | \#(G) \ .$$

Preuve *: 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. V.2.7.iii),) 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 de V.2.7.ii) que $\forall 1 \leq i \leq k, \ \#(O(x_i)) \ = \ \#(H)$ d'où il résulte finalement que

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

Corollaire V.6.5 *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. V.2.9p)ar le cardinal de H.*

Corollaire V.6.6 (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 V.6.7 *Le corollaire V.6.5 ci-dessus et le corollaire V.5.5 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 V.6.8 *Étant donné un groupe $(G,*)$ pour tout $x \ \in \ G$:*

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

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

(cf. Problème n° II, exercice A.)

Preuve *: Voir l'exercice V.7.12.*

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

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

***Preuve** : Le noyau du morphisme ϵ_x est un sous-groupe de $\mathbb{Z}$ il existe donc $d \in \mathbb{N}$ tel que $\mathrm{Ker}\, \epsilon_x = d\mathbb{Z}$ (cf. IV.5.5.) 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 V.5 et en particulier la proposition V.5.4.

Définition V.6.9 (Ordre d'un élément) Pour $(G, *)$ un groupe et $x \in G$, avec les notations de la proposition V.6.8, 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 la proposition V.6.8.ii).b) par $\mathrm{Ker}\, \epsilon_x = d\mathbb{Z}$ ou $d = \#(\mathrm{Im}\, \epsilon_x)$.

Remarque V.6.10 Il est immédiat de vérifier que pour tout élément x d'un groupe G, l'ordre de x défini comme en V.6.9, 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 V.6.11 (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. V.3.3.iii),) ont même ordre.

Théorème V.6.12 (de Lagrange) *Pour G un groupe fini, l'ordre de tout élément x de G divise le cardinal de G.*

***Preuve** : Remarquons d'abord que si G est fini, on ne peut se trouver dans la situation de V.6.8.ii).a) si bien que l"ordre d de x est bien un entier naturel. Or il résulte de V.6.8.ii).b) que*

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

Puisque $< \{x\} >$ est un sous-ghroupe de G, il suffit d'appliquer le corollaire V.6.6.

Définition V.6.13 Avec les notations de la proposition V.6.8,

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

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

on dit que G est *monogène* ;

ii) si de plus on est dans la situation de V.6.8.ii).b), auqel cas $G \;\cong\; \mathbb{Z}/d\mathbb{Z}$, on dit que G est *cyclique*.

Corollaire V.6.14 *Un groupe est cyclique si et seulement s'il est monogène et fini.*

Corollaire V.6.15 *Si G est un groupe fini de cardinal p premier, G est isomorphe (non canoniquement) à $(\mathbb{Z}/p, +)$ et donc commutatif (abélien).*

V.7 . −Exercices

Exercice V.7.1 Faire la preuve de la proposition V.1.8.

Exercice V.7.2 Faire la preuve du lemme V.1.11

Exercice V.7.3 Faire la preuve de la proposition V.1.14.

Exercice V.7.4 Faire la preuve de la proposition V.1.16.i).

Exercice V.7.5 [Stabilisateur]

Soit $(G, *)$ un groupe et E un ensemble muni d'une action de G notée $g \cdot x$ pour tout $(g, x) \in G \times E$.

Montrer que pour tout $(x, g) \in E \times G$,

$$\mathrm{Stab}_G(g \cdot x) \;=\; g \;*\; \mathrm{Stab}_G(x) \;*\; g^{-1}\,.$$

Exercice V.7.6 Considérons l'action par translation à gauche sur les parties de G définie en V.2.3.

1) Montrer que cette action ne se restreint pas en général en une action de G sur l'ensemble de ses sous-groupes.

2) Montrer que l'orbite $O(P)$ d'une partie $P \in \mathcal{P}(G)$ contient au plus un sous-groupe.

Exercice V.7.7 Faire les détails de la construction esquissée dans la remarque V.2.5.

Exercice V.7.8 Faire la preuve de la proposition V.3.5.ii).

Exercice V.7.9 Compléter la preuve de la proposition V.4.4.

Exercice V.7.10 Faire la preuve de la proposition V.4.10.

Exercice V.7.11 Faire la preuve de la proposition V.5.1.

Exercice V.7.12 Faire la preuve de la proposition V.6.8.i).