III . −Groupes, morphismes, sous-groupes

III.1 . −Groupe

Définition III.1.1 (Groupe) Un *groupe* est un couple $(G, *)$ (le plus souvent simplement noté $G,$) où G est un ensemble et $* \ : \ G \times G \ \to \ G$ est une application appelée *loi de composition* vérifiant :

Gr_1) Pour tout triplet (x, y, z) d'éléments de G,

$$(x * y) * z \ = \ x * (y * z) \ ,$$

on dit que la loi interne $*$ est *associative*.

Gr_2) Il existe un élément $e \in G$ appelé *élément neutre* de G tel que, pour tout $x \in G$, $x*e \ = \ e*x \ = \ x$.

Gr_3) Pour tout élément $x \ \in \ G$, il existe un élément $x' \ \in \ G$ appelé *symétrique* de x et tel que $x * x' \ = \ x' * x \ = \ e$.

Il revient au même de dire que $(G, *)$ est un magma associatif possédant un élément neutre et dans lequel tout élément possède un symétrique au sens des définitions du paragraphe I.6.

Les formulations « $(G, *)$ est un groupe » ou « $*$ munit G d'une *structure de groupe* » sont synonymes.

Exemple III.1.2 a) L'axiome III.1.1.Gr_2) entraîne qu'il n'existe aucune structure de groupe sur l'ensemble vide $\emptyset$. Un groupe est donc un ensemble possédant au moins 1 élément.

b) On peut définir une unique loi de composition qui donne à l'ensemble $\{\emptyset\}$ à un élément une structure de groupe :

$$\emptyset * \emptyset \ := \ \emptyset \ .$$

c) (**Le groupe** $\mathcal{S}(X)$)

Un des premiers groupes qu'on peut introduire, au sens où sa définition ne nécessite guère plus que les premiers axiomes de la théorie des ensembles introduite au chapitre I, est le groupe $\mathcal{S}(E)$ des bijections d'un ensemble E muni de la loi $\circ$. C'est une partie du magma considéré dans l'exemple I.6.12, et précisément celle constituée des éléments qui ont un symétrique. Pour ne nécessiter que très peu de matériel pour être défini, ce groupe n'est cependant pas le plus aisé à étudier comme le montre le chapitre VI qui lui est entièrement consacré et encore seulement dans le cas où E est un ensemble fini. Pour tout ensemble E, l'ensemble $\mathcal{S}(E)$ des bijections de E dans lui-même muni de la loi $\circ$ de composition des applications est un groupe. En effet :

- si $f \mathrm{et}\, g \ : \ E \ \to \ E$ sont des bijections de E dans lui-même la composée $f \circ g$ est encore une bijection de E dans lui même, assurant que $\circ$ est bien une loi de composition (cf. I.6.1.)
- L'application identité de E (cf. I.2.6.a),) usuellement notée Id_E est un élément neutre pour $\circ$.
- Enfin pour toute bijection $f \ : \ E \ \to \ E$ son application réciproque f^{-1} est précisément un symétrique pour la composition $\circ$.

d) Si $\mathbb{K}$ est un corps et E un $\mathbb{K}$-espace vectoriel, l'ensemble $\mathrm{GL}(E)$ des applications linéaires bijectives de E dans lui-même (endomorphismes) est un groupe pour la loi de composition $\circ$. Si E est de dimension finie n, une base de E étant fixée, cette dernière définit un isomorphisme de $\mathbb{K}$-espace vectoriel $E \cong \mathbb{K}^n$ qui définit lui-même un isomorphisme de $\mathrm{GL}(E)$ sur le groupe $\mathrm{GL}_n(\mathbb{K})$ des matrices carrées $n \times n$ inversibles à coefficients dans $\mathbb{K}$.

Définition III.1.3 Étant donné un groupe $(G, *)$, si pour tout couple (x, y) d'éléments de G, $x * y = y * x$, on dira que G est *abélien* ou *commutatif*.

Dans ce cas on notera usuellement $+$ la loi interne et 0 l'élément neutre en référence au groupe abélien $(\mathbb{Z}, +)$ (cf. IV.)

Un groupe n'étant rien de plus (ni de moins d'ailleurs) qu'un magma associatif possédant un élément neutre et dans lequel tout élément possède un symétrique, la proposition I.6.13 vaut encore ici mutatis mutandis.

Proposition III.1.4 (Propriétés) *Soient $(G, *)$ un grouepe.*

i) Si ϵ et ϵ' sont des éléments neutres de $(G, *)$ alors $\epsilon = \epsilon'$.

ii) Si y et z éléments de E sont des symétriques pour $x \in E$, $y = z$.

***Preuve** : Voir l'exercice III.5.1.*

Remarque III.1.5 On pourra donc parler de L'élément neutre d'un groupe et du symétrique d'un élément dans un groupe.

L'élément neutre est souvent noté 1 et même 0 dans le cas des groupes abéliens par analogie avec le groupe $(\mathbb{Z}, +)$. Le symétrique d'un élément x est usuellement noté x^{-1} et appelé *inverse* de x, voire $-x$ dans le cas d'un groupe abélien et appelé alors *opposé* de x.

De même la proposition I.6.20 a son pendant pour les groupes :

Proposition III.1.6 *Étant donnés un groupe $(G, *)$ et un ensemble E, l'ensemble G^E des applications de E dans G muni de la loi induite (cf. I.6.21,) est un groupe (abélien si G l'est.)*

III.2 . −Morphisme

Définition III.2.1 (Morphisme de groupes) Étant donnés des groupes

$$(G, *) \text{ et } (H, \cdot),$$

un *morphisme de groupes* (ou *homomorphisme de groupes*) est une application $f : G \to H$ telle que pour tout couple (x, y) d'éléments de G,

$$f(x * y) = f(x) \cdot f(y) .$$

On notera $\mathrm{Hom}_{\mathbf{Gr}}(G, H)$ (ou simplement $\mathrm{Hom}(G, H)$ si le contexte ne prête pas à confusion) l'ensemble des morphismes de G dans H.

Remarque III.2.2 On constate que dans la définition ci-dessus aucune condition supplémentaire n'est exigée par rapport à un morphisme de magma (cf. I.6.2.)

On a l'exact analogue du lemme I.6.3 :

Lemme III.2.3 *i) Pour tout groupe $(G,*)$ l'identité Id_G est un morphisme du groupe G dans lui-même.*

ii) Pour $(G,*_G)$, $(H,*_H)$ et $(K,*_K)$ des groupes, $f : G \to H$ et $g : H \to K$ des morphismes, le composé $g \circ f$ est un morphisme.

On peut donc donner une définition analogue à la définition I.6.4 :

Définition III.2.4 Étant donnés deux groupes $(G,*)$ et $(H,\cdot)$, un morphisme $f : G \to H$ est un *isomorphisme* s'il existe un morphisme $g : H \to G$ tel que

$$g \circ f = \mathrm{Id}_G \text{ et } f \circ g = \mathrm{Id}_H .$$

On notera $\mathrm{Isom}_{\mathbf{Gr}}(G,H)$ (ou simplement $\mathrm{Isom}(G,h)$ si le contexte est clair) l'ensemble des isomorphismes de $(G,*)$ dans $(H,\cdot)$.

On a encore, san surprise puisqu'en fait l'axiomatique n'est pas vraiement différente, un analogue de la proposition I.6.5 :

Proposition III.2.5 *Étant donnés deux groupes $(G,*)$ et $(H,\cdot)$, une application $f : G \to H$ est un isomorphisme si et seulement si c'est un morphisme bijectif.*

Preuve *: Il n'y a rien de plus à montrer que dans la preuve de la proposition I.6.5.*

Exemple III.2.6 Soit E et F deux ensembles. On rappelle (cf. III.1.2.c),) que

$$(\mathcal{S}(E),\circ) \text{ (resp. } (\mathcal{S}(F),\circ) \text{)}$$

est le groupe des bijections de E (resp. F,) dans lui-même.

Soit $u : E \to F$ une bijection de E dans F. L'application

$$\mathcal{S}(u) : \mathcal{S}(E) \to \mathcal{S}(F) , \ f \mapsto u \circ f \circ u^{-1}$$

est un isomorphisme de groupes.

Des définitions analogues à I.6.6 peuvent donc être données :

Définition III.2.7 Soit $(G,*)$ un groupe.

i) (**Endomorphismes**)

Un morphisme $f : G \to G$ de G dans lui-même est appelé *endomorphisme*. On note $\mathrm{End}_{\mathbf{Gr}}(G)$ (ou simplement $\mathrm{End}(G)$,) l'ensemble des endomorphismes de G.

ii) (**Automorphisme**)

Un morphisme $f : G \to G$ est un *automorphisme* si c'est à la fois un isomorphisme et un endomorphisme. Il revient au même, grâce à la proposition III.2.5, de dire que f est un endomorphisme bijectif. On note $\mathrm{Aut}_{\mathbf{Gr}}(G)$ (ou simplement $\mathrm{Aut}(G)$) l'ensemble des automorphismes de G.

Exemple III.2.8 Pour un groupe G, l'identité Id_G est un automorphisme.

Proposition III.2.9 (Propriétés des morphismes) *Étant donné un morphisme de groupe*

$$f : (G, *) \to (H, \cdot) \text{ avec } e_G(\text{resp. } e_H) \text{ l'élément neutre de } G(\text{resp. } H :)$$

i) $f(e_G) = e_H$;

ii) pour tout $x \in G$, *si* $y \in G$ *est sont symétrique,* $f(y)$ *est le symétrique de* $f(x)$ *dans* H.

Preuve *: Voir l'exercice III.5.3.*

III.3 . −Sous-groupe

Définition III.3.1 (Sous-groupe) Une partie H d'un groupe $(G, *)$ est un *sous-groupe* si la restriction de $*$ à $H \times H$ donne à H une structure de groupe.

Remarque III.3.2 i) Il ne suffit pas pour que H soit un sous-groupe de G que H soit un sous-magma de G comme le montre l'exercice I.8.15.question 2). Il faut en effet exiger en plus que H possède un élément neutre (cf. III.1.1.Gr_2)e)t que tout élément de H possède un symétrique (cf. III.1.1.Gr_3).)

ii) La définition de sous-groupe donnée ci-dessus n'est peut-être pas celle qu'on a été habitué à rencontrer qui est parfois plutôt la caractérisation donnée à la proposition III.3.4.b). On ne peut cependant se contenter de cette dernière en l'état puisqu'aux termes stricts de cet énoncé on ne saurait même pas qu'un sous-groupe est lui-même un groupe, ce qui avouons-le devra à tout le moins être établi, si l'on veut bénéficier d'une théorie utilisable. L'énoncé clef est en fait l'équivalence entre III.3.4.a) et III.3.4.b).

Le lemme technique suivant est un ingrédient permettant d'établir l'équivalence entre les diverses caractérisations des sous-groupes.

Lemme III.3.3 *Soit* $(G, *)$ *un groupe d'élément neutre* ϵ_G *et* H *un sous-groupe de* G *au sens de la définition III.3.1. Notons* $*_H$ *la restriction de* $*$ *à* $H \times H$.

i) L'élément neutre ϵ_H *de* H *est l'élément neutre* ϵ_G *de* G.

Preuve : *Si ϵ_H est l'élément neutre de H, pour tout $x \in H$, $x *_H \epsilon_H = x$. Cependant, x et ϵ_H étant en particulier des éléments de G, on peut encore écrire, $x * \epsilon_H = x$. D'autre part, $x * \epsilon_G = x$. Notons x^{-1} le symétrique de x dans G. On a alors :*

$$x * \epsilon_H = x * \epsilon_G \Rightarrow x^{-1} * x * \epsilon_H = x^{-1} * x * \epsilon_G \Rightarrow \epsilon_H = \epsilon_G$$

c'est-à-dire que l'élément neutre de H est celui de G.

ii) Pour tout $x \in H$, l'inverse ${x^{-1}}_H$ de x dans H est aussi son inverse dans G.

Preuve : *Tout $x \in H$ possède un inverse ${x^{-1}}_H$ tel que*

$$x *_H {x^{-1}}_H = {x^{-1}}_H *_H x = \epsilon_H = \epsilon_G$$

en utilisant le point i). Or x et ${x^{-1}}_H$ étant en particulier des éléments de G, on peut encore écrire,

$$x * {x^{-1}}_H = {x^{-1}}_H * x = \epsilon_G$$

c'est-à-dire que ${x^{-1}}_H$ est l'inverse x^{-1} de x dans G puisque ce dernier est unique (cf. III.1.4.i).)

Proposition III.3.4 (Caractérisation des sous-groupes) *Étant donnés un groupe $(G, *)$ et $H \subset G$ une partie de G, les assertions suivantes sont équivalentes :*

a) H est un sous-groupe au sens de la définition III.3.1.

b) H est non vide et pour tout couple (x, y) d'éléments de H, $x * y^{-1} \in H$.

c) La restriction

$$\mathrm{Id}_{G|H} : H \to G$$

de l'identité Id_G à H est un morphisme de groupes. Ceci signifie implicitement que H possède une structure de groupe.

Preuve :

*i) **(a) $\Rightarrow$ b))***
Si H est un sous-groupe de G, en particulier H est un groupe et il est donc non vide (cf. III.1.2.a).)
Pour tout couple (x, y) d'éléments de H, x et y^{-1} sont encore des éléments de H (cf. III.3.3.ii).)
Dire que la restriction $*_H$ de $*$ à $H \times H$ donne à H une structure de groupe signifie, en particulier, qu'elle est à valeurs dans H, ce qui prouve que

$$x * y^{-1} = x *_H y^{-1} \in H .$$

ii) ***(b)*** $\Rightarrow$ ***a))***

Réciproquement, supposons donnée une partie non vide H de G telle que pour tout couple (x, y) d'éléments de H, $x * y^{-1} \in H$.

Si H est non vide il existe en particulier un élément $x \in H$, et, dès lors, $\epsilon_G = x * x^{-1} \in H$. Il est clair que ϵ_G est alors un élément neutre pour H.

De plus, pour tout $x \in H$, puisque $\epsilon_G \in H$, $\epsilon_G * x^{-1} = x^{-1} \in H$ c'est-à-dire que tout élément de H possède un inverse dans H.

Enfin, pour tout couple (x, y) d'éléments de H, $y^{-1} \in H$ et

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

c'est-à-dire que la restriction de $*$ à $H \times H$ est bien à valeurs dans H.

La partie H de G est donc bien un sous-groupe.

Exemple III.3.5 Étant donné un groupe $(G, *)$ d'élément neutre ϵ, les ensembles $\{\epsilon\}$ et G lui-même sont des sous-groupes de G.

Proposition III.3.6 *Soient G un groupe, H et K des sous-groupes de G.*

i) $H \cap K$ est un sous-groupe de G.

***Preuve** : (cf. TD n° III, exercice D.)*

ii) Plus généralement, pour $\mathcal{H}$ un ensemble non vide de sous-groupes de G, $\bigcap_{H \in \mathcal{H}} H$ est un sous-groupe de G.

***Preuve** : Voir l'exercice III.5.6.*

iii) $H \cup K$ est un sous-groupe de G si et seulement si

$$H \subset K \text{ ou } K \subset H .$$

***Preuve** : (cf. TD n° III, exercice E.)*

iv) Si $(H_n)_{,n\in\mathbb{N}}$ est une suite de sous-groupes de G telle que

$$\forall (p, q) \in \mathbb{N} \times \mathbb{N},\ \exists r \in \mathbb{N},\ H_p \subset H_r \text{ et } H_q \subset H_r,$$

alors $\bigcup_{H \in \mathbb{N}} n$ est un sous-groupe de G.

***Preuve** : Voir l'exercice III.5.7 ou le TD n° III, exercice F.*

Proposition III.3.7 (Image directe/réciproque) *Soit $f : G \to H$ un morphisme de groupes.*

*i) (**Image directe**)*
Pour tout sous-groupe G' de G, l'image directe de G'

$$f(G') = \{y \in H \,;\, \exists x \in G',\ ,\ y = f(x)\}$$

est un sous-groupe de H.

*ii) (**Image réciproque**)*
Pour tout sous-groupe H' de H, l'image réciproque

$$f^{-1}(H') = \{x \in G \,;\, f(x) \in H'\}$$

est un sous-groupe de G.

Définition III.3.8 (Noyau/image) Étant donné un morphisme de groupes $f : G \to H$, ϵ_H étant l'élément neutre de H, on appelle

i) (**Noyau**)
noyau de f le sous-ensemble

$$\operatorname{Ker} f := f^{-1}(\{\epsilon\}_H) = \{x \in G \,;\, f(x) = \epsilon_H\},$$

ii) (**Image**)
image de f l'ensemble

$$\operatorname{Im} f := f(G) = \{y \in H \,;\, \exists x \in G,\ ,\ y = f(x)\}\,.$$

Corollaire III.3.9 *Pour un morphisme de groupes $f : G \to H$, le noyau (resp. l'image) de f est un sous-groupe de G (resp. H.)*

Proposition III.3.10 *Un morphisme de groupes $f : G \to H$ est injectif (resp. surjectif) si et seulement si* $\operatorname{Ker} f = \{\epsilon_G\}$ *(resp.* $\operatorname{Im} f = H$.)

Définition III.3.11 Si $i : H \to G$ est un morphisme de groupes injectif, il induit un isomorphisme $H \cong \operatorname{Im} i$; si bien que H est isomorphe à un sous-groupe de G. On dira parfois même par abus de langage que H est lui-même un sous-groupe de G.

$\frac{1}{2}$;

III.4 . −Partie génératrice

Dans tout ce paragraphe (III.4,) $(G, *)$ est un groupe dont lélément neutre est noté e et dans lequel l'inverse (symétrique) de toute élément x est noté x^{-1}.

Lemme III.4.1 *Étant donnée une partie $S \subset G$, notons $\mathcal{G}_S$ l'ensemble des sous-groupes de G contenant S. Alors*

$$< S > := \bigcap K \in \mathcal{G}_S K$$

est le plus petit élément (pour l'inclusion) de $\mathcal{G}_S$.

***Preuve** : On remarque d'abord que $\mathcal{G}_S$ est non vide puisque $G \in \mathcal{G}_S$. Or pour tout $K \in \mathcal{G}_S$, $S \subset K$, donc*

$$S \subset < S > .$$

Il s'ensuit en particulier que

$$< S > \neq \emptyset .$$

Pour tout $(x, y) \in < S > \times < S >$, par définition,

$$\forall K \in \mathcal{G}_S,\ x \in K \text{ et } y \in K$$

il s'ensuit (cf. III.3.4,) que

$$\forall K \in \mathcal{G}_S,\ x * y^{-1} \in K$$

ce qui entraîne que $x * y^{-1} \in < S >$ ce qui combiné au fait que $< S >$ est non vide assure que $< S >$ est un sous-groupe de G. On pourrait aussi déduire ce fait de la proposition III.3.6.ii).

Puisque, de plus $S \subset < S >$,

$$< S > \in \mathcal{G}_S .$$

Il est immédiat de montrer, et ce du fait même de la définition de $< S >$, que

$$\forall K \in \mathcal{G}_S,\ < S > \subset K$$

c'est-à-dire que $< S >$ est un minorant de $\mathcal{G}_S$ qui, étant de plus élément de $\mathcal{G}_S$ est son plus petit élément.

Définition III.4.2 Étant donné un groupe G et $S \subset G$ une partie de G :

i) (**sous-groupe engendré**)
le sous-groupe $< S >$ de G défini par le lemme III.4.1 s'appelle le *sous-groupe de G engendré par S*;

ii) (**partie génératrice**)
si $G = < S >$, on dit que G est *engendré* par S ou que S est une *partie génératrice* de G.

Exemple III.4.3 a) Pour tout groupe G d'élément neutre e,

$$< \emptyset >= \{e\} .$$

b) Pour tout groupe G, $G = < G >$.

Définition III.4.4 (Groupe monogène) Pour un groupe G et $x \in G$, si $< \{x\} >= G$ on dit que G est *monogène*.

Notation III.4.5 Pour deux sous-groupes H et K d'un groupe G, on note

$$HK := < (H \cup K) >$$

qui est le plus petit sous-groupe contenant à la fois H et K. Si G est abélien la notation

$$H + K := < (H \cup K) >$$

sera plutôt utilisée.

Remarque III.4.6 On a vu en III.3.6.iii) que $H \cup K$ n'est pas en général un sous-groupe de G et c'est HK qui « joue alors le rôle » de $H \cup K$. Si le lecteur a quelques souvenirs de son cours d'algèbre linéaire il remarquera que c'est précisément la situation rencontrée pour les espaces vectoriels, ce qui n'a d'ailleurs rien d'étonnant, ces derniers étant en particuliers des groupes abéliens.

Proposition III.4.7 *Étant donnés un groupe G et une partie S de G, on note (comme au lemme III.4.1,) $\mathcal{G}_S$ l'ensemble des sous-groupes de G qui contiennent S. Alors pour toute partie H G, les assertions suivantes sont équivalentes :*

a) L'ensemble H est l'intersection de tous les sous-groupes de G contenant S :

$$H = \bigcap_{K \in \mathcal{G}_S} K ;$$

b)

$$H \in \mathcal{G}_S \text{ et } \forall K \in \mathcal{G}_S,\ H \subset K$$

autrement dit H est le plus petit élément de $\mathcal{G}_S$;

c) H est constitué des éléments $t_1 t_2 \dots t_r$ avec $r \geq 1$ où un élément t_i est dans S ou a son inverse dans S.

***Preuve** : Voir le TD n° III, exercice G.*

III.5 . −Exercices

Exercice III.5.1 [Unicité des éléments remarquables] Soit $(E, *)$ un ensemble muni d'une loi associative.

1) () (**Élément neutre**)
Montrer que si $(E, *)$ possède un élément neutre ϵ celui-ci est unique.

2) () (**Symétrique**)
Montrer que si $(E, *)$ possède un élément neutre ϵ, tout élément $x \in E$ possède au plus un symétrique.

Exercice III.5.2 Faire la preuve de la proposition III.1.6.

Exercice III.5.3 [Morphismes de groupes] Soit

$$f \ : \ (G, *, \epsilon_G) \ \to \ (H, \bullet, \epsilon_H)$$

un morphisme de groupes.

1) () (**Élément neutre**)
Montrer que $f(\epsilon_G) \ = \ \epsilon_H$.

2) () (**Symétrique**)
Montrer que pour tout $x \in G$, si y est son symétrique, $f(y)$ est le symétrique de $f(x)$.

3) () (**Image**)
Montrer que $\mathrm{Im}\, f$ est un sous-groupe de $(H, \bullet)$.

4) () (**Noyau**)
Montrer que $\mathrm{Ker}\, f$ est un sous-groupe de $(G, *)$.

5) () (**Isomorphisme**)
Montrer que si f est bijective et que g est son applications réciproque, alors g est un morphisme de groupe.

Exercice III.5.4 Faire la preuve de la proposition III.2.9 et comparer à la situation des magmas envisagée dans l'exercice I.8.13.

Exercice III.5.5 Compléter la preuve de la proposition III.3.4.

Exercice III.5.6 Faire la preuve de la proposition III.3.6.ii).

Exercice III.5.7 Faire la preuve de la proposition III.3.6.iv).

Exercice III.5.8 Faire la preuve de la proposition III.3.7.

Exercice III.5.9 **1)** () Étant donnés un groupe G et deux parties S et T de G, montrer que

$$< S \cup T > = < S > \ + \ < T > \ .$$

2) () Étant donné un groupe $(G, *)$ pour une partie $S \subset G < S >$ est l'ensemble des éléments $x \in G$ tels que :

$$\exists d \in \mathbb{N}^*,\ \exists s_i\ ,1\leq i\leq d \in S,\ \exists \alpha_i\ ,1\leq i\leq d \in \mathbb{Z},\ x = \prod_{i=1}^{d} s_i^{\alpha_i}\ , \qquad 1$$

en prenant garde que, dans le produit ci-dessus, l'ordre des facteurs n'est pas indifférent, dans la mesure où l'on ne suppose pas que G est abélien. Pour ne pas exclure le cas où $S = \emptyset$, on conviendra que, dans ce cas, le produit ci-dessus vaut e.