Chapitre 2

Groupe

2.1 Lois de composition internes

Dans tout ce chapitre, E est un ensemble.

Définition 2.1. *On appelle loi de composition interne sur E (lci) toute application de $E \times E$ dans E.*

Définition 2.2. *On appelle magma tout couple constitué d'un ensemble et d'une lci.*

Exemple 2.3. *$(\mathbf{Z}, -)$ est un magma, mais pas $(\mathbf{N}, -)$, car $-4 \notin \mathbf{N}$.*

Dans toute la suite, $\star$ est une lci sur E.

2.1.1 Propriétés usuelles des lci

Définition 2.4. *Soit $(E, \star)$ un magma.*

On dit que E est associatif si pour tout $x, y, z \in E$, on a : $x \star (y \star z) = (x \star y) \star z$. L'élément $x \star (y \star z) = (x \star y) \star z$ est alors noté $x \star y \star z$.

On dit que E est commutatif si pour tout $x, y \in E$, on a : $x \star y = y \star x$.

Soit $\sharp$ une seconde lci sur E. On dit que dans E $\star$ est distributive par rapport à $\sharp$ si pour tout $x, y, z \in E$, on a :
- *$x \star (y \sharp z) = (x \star y) \sharp (x * z)$*
- *$(y \sharp z) \star x = (y \star x) \sharp (z \star x)$.*

Remarque 2.5. *On dit que dans $(E, \star)$ est distributive à gauche par rapport à $\sharp$ si pour tout $x, y, z \in E$, on a : $x \star (y \sharp z) = (x \star y) \sharp (x \star z)$. De même, on a la notion de distributivié à droite.*

Exemple 2.6.
1. *$\mathbf{C}$, $\mathbf{R}$, $\mathbf{Q}$, $\mathbf{Z}$, $\mathbf{N}$ avec $+$ ou $\times$ sont associatifs, mais pas $(\mathbf{Z}, -)$ car $1 - (2 - 3) \neq (1 - 2) - 3$.*
2. *$\mathbf{C}$, $\mathbf{R}$, $\mathbf{Q}$, $\mathbf{Z}$, $\mathbf{N}$ avec $+$ ou $\times$ sont commutatifs, mais pas $(\mathbf{Z}, -)$, ni $(\mathcal{F}(\mathbf{R}, \mathbf{R}), \circ)$.*
3. *Sur $\mathbf{C}, \mathbf{R}, \mathbf{Q}, \mathbf{Z}, \mathbf{N}$ $\times$ est distributive par rapport à $+$, et sur $\mathcal{P}(E)$, $\cap$ et $\cup$ sont distributives l'une par rapport à l'autre.*

Définition 2.7. *1. Soit $e \in E$. on dit que e est un élément neutre à gauche (resp. à droite) pour $\star$ si pour tout $x \in E$ on a $e \star x = x$ (resp. $x \star e = x$). On dit que e est un élément neutre pour $\star$ si c'est un élément neutre à gauche et à droite, i.e. pour tout $x \in E, e \star x = x \star e = x$.*

2. Soit e un neutre pour $\star$ et soit $x \in E$. On dit que x est inversible à gauche (resp. à droite) s'il existe un élément $y \in E$ tel que $y \star x = e$ (resp. $x \star y = e$). Un tel élément y s'appelle UN inverse à gauche (resp. à droite) de x. On dit que x est inversible s'il est inversible à gauche et à droite, i.e. il existe $y \in E$ tel que $y \star x = x \star y = e$. Dans ce cas y est UN inverse de x.

Exemple 2.8. — *0 est un élément neutre pour + dans* **R**, **C**, **Q**, **Z**, **N**.

— *1 est un élément neutre pour $\times$ dans* **R**, **C**, **Q**.
— *1_E est un élément neutre pour dans $\mathcal{F}(E, E)$, et les bijections sont tous les éléments inversibles de cet ensemble.*

Remarque 2.9. *1. Être inversible d'un seul côté ne suffit pas pour être inversible tout court.*

2. Un neutre est toujours inversible et est son propre inverse.

Proposition 2.10. *Si $\star$ admet un neutre, alors ce neutre est unique.*

Preuve:
Soient e et e' deux neutres. Alors $e \star e' = e$ et $e \star e' = e'$, donc $e = e'$. □

Proposition 2.11. *On suppose la loi $\star$ associative, et admettant un neutre e. Si un élément est inversible, alors il a un seul inverse.*

Preuve:
Soient y et y' deux inverses de $x \in E$. Alors $y \star x = e$ et $x \star y' = e$. Donc $y \star (x \star y') = y \star e = y$ et $(y \star x) \star y' = e \star y' = y'$, d'où $y = y'$. □

Remarque 2.12. *On utilise souvent les notations additives et multiplicatives.*

1. *En notation additive, $\star$ est en général notée $+$, $x + x + \cdots + x$ ($n-$fois(se note nx, et si x est inversible, son inverse se note $-x$. On l'appelle alors plutôt l'opposé de x. De même, on notera le neutre d'une telle structure 0, ou 0_E.*
2. *En notation multiplicative, $\star$ est en général remplacée par $\times$ (et ce symbole est même souvent omis), $x \times x \times \cdots \times x$ ($n-$fois) se note x^n et si x est inversible, son inverse se note x^{-1}. De même, on notera le neutre d'une telle structure 1, ou 1_E.*

Pour éviter toute erreur, on essaiera au maximum de n'utiliser la notation additive que pour des lois qui ont les mêmes propriétés que la loi + sur **R**.
Par exemple, noter + une lci non commutative peut-être déroutant, ainsi que pour une lci pour laquelle tous les éléments ne sont pas inversibles. La notation + est en général réservée à des lci commutatives et pour lesquelles les éléments sont tous inversibles.
Ce n'est pas le cas pour la notation multiplicative, qui est la plus couramment utilisée pour des lois associatives, mais sans plus. Par exemple il est fréquent d'utiliser $\times$

même pour une lci non commutative et pour laquelle les éléments ne sont pas tous inversibles. Donc faites attention, par défaut on aura $xy \neq yx$, et x^{-1} n'existera pas forcément !
Dans toute la suite, on adoptera la notation multiplicative, et on suppose que E a un neutre noté 1.

Proposition 2.13. *On suppose la loi $\star$ associative. Soient $x, y, z \in E$.*

1. *Simplification par un inversible : si x est inversible, alors $x \star y = x \star z \Leftrightarrow y = z$.*
2. *Inverse d'un produit : si x et y sont inversibles alors $x \star y$ l'est aussi et $(x \star y)^{-1} = y^{-1} \star x^{-1}$.* **Attention : l'inverse de $x \star y$ n'a aucune raison d'être $x^{-1} \star y^{-1}$.**
3. *Puissances négatives : si x est inversible, on pose pour $n \in \mathbf{N}^*$, $x^{-n} = (x^{-1})^n$. Alors $x^{-n} = (x^n)^{-1}$.*
4. *Inverse d'un inverse : si x est inversible, x^{-1} l'est aussi et $(x^{-1})^{-1} = x$.*

Preuve:

(3) Par récurrence. Vrai si $n = 0$ ou 1. Si vrai pour n, alors $x^{n+1} \star x^{-n-1} = x^n \star x \star x^{-1} \star x^{-n} = x^n \star e \star x^{-n} = x^n \star x^{-n} = e$.
(4) Vrai par unicité de l'inverse. □

Définition 2.14. *Soit $(E, \star)$ un magma et F une partie de E. On dit que F est une partie stable (de E par $\star$) si pour tous $x, y \in F, x \star y \in F$.*

Exemple 2.15. *$\{-1, 1\}$ est une partie stable de $(\mathbf{R}, \times)$, mais pas $\{-2, 2\}$.*

2.2 Structure de groupe

2.2.1 Définition et exemples

Définition 2.16. *On appelle groupe tout magma associatif, ayant un neutre, et dont tout élément est inversible. Si un groupe est commutatif (ce qui signifie en fait que sa loi est commutative), il est dit abélien. Par défaut on utilise la notation multiplicative pour un groupe, sauf pour les groupes abéliens pour lesquels on utilise la notation additive.*

Exemple 2.17. 1. *$\mathbf{C}, \mathbf{R}, \mathbf{Q}, \mathbf{Z}$ sont des groupes pour la loi $+$, mais pas pour la loi $\times$.*

2. *Pour* $n \in \mathbf{N}^*$, $\mathbf{C}^n$, $\mathbf{R}^n$, $\mathbf{Q}^n$, $\mathbf{Z}^n$ *sont des groupes pour la loi* $+$.
3. $\mathbf{C}^*, \mathbf{R}^*, \mathbf{Q}^*$, *sont des groupes pour la loi* $\times$.
4. $\mathbf{N}$ *n'est un groupe ni avec la loi* $+$ *ni pour la loi* $\times$.

Définition 2.18. *Soit X un ensemble non vide. On appelle groupe des permutations de X l'ensemble des bijections de X dans X. Comme son nom l'indique, c'est un groupe, si on le munit de la loi de composition $\circ$. On le note $\mathcal{S}_X$.*

2.2.2 Sous-groupes

Dans toute la suite, $(G, \star)$ est un groupe de neutre e. On adopte la notation multiplicative

Définition 2.19. *On appelle sous-groupe de G tout ensemble H vérifiant les propriétés suivantes :*

1. $H \subset G$;
2. $e \in H$;
3. *Stabilité par produit :* $\forall x, y \in H, x \star y \in H$;
4. *Stabilité par passage à l'inverse :* $\forall x \in H$, *on a* $x^{-1} \in H$.

Exemple 2.20. *Sont des sous-groupes :*

1. $\{e\}$ *et* G *dans* $(G, \star)$.

2. $\mathcal{U}$ *dans* $(\mathbf{C}^*, \times)$.

3. $n\mathbf{Z}$ *dans* $(\mathbf{Z}, +)$**.**

4. $H = \{f \in \mathcal{S}_{\mathbf{R}} \mid f(0) = 0\}$ *dans* $(\mathcal{S}_{\mathbf{R}}, \circ)$**.**

Proposition 2.21. *Un ensemble* H *est un sous groupe de* G *si et seulement si* H *est un sous-ensemble non vide de* G *et pour tout* $(x, y) \in H^2$*, on a* $x^{-1} \star y \in H$*.*

Preuve:

□

Remarque 2.22. *On obtient une proposition vraie également en remplaçant ci-dessus la condition* $x^{-1} \star y \in H$ *par* $x \star y^{-1} \in H$*.*

Théorème 2.23. *Un sous-groupe muni de la loi induite du groupe est lui-même un groupe.*

Preuve:

□

Remarque 2.24. *Il est plus facile de montrer qu'un ensemble est un sous-groupe que de montrer que c'est un groupe (pas besoin de redémontrer l'associativité, etc.). Par exemple $(\mathcal{U}, \times)$ est un groupe, vu comme sous-groupe de $(\mathbf{C}^*, \times)$.*
À chaque fois que l'on essaiera de montrer qu'un ensemble est muni d'une structure de groupe, on tentera de le voir comme un sous-groupe d'un groupe bien connu.

Remarque 2.25. *La réciproque de ce théorème est également vraie (bien que moins utilisée) : si H est un sous-ensemble de G tel que, muni de la loi induite par celle de G, H soit un groupe, alors H est un sous-groupe de G.*

Exemple 2.26. *Si $n \in \mathbf{N}^*$, $\mathcal{U}_n$ est un sous-groupe de $(\mathcal{U}, \times)$, donc $(\mathcal{U}_n, \times)$ est un groupe.*

2.2.3 Morphismes de groupes

Définition 2.27. *Soient $(G, \star)$ et $(G', \sharp)$ deux groupes et $\varphi : G \to G'$.*

1. *On dit que φ est un morphisme du groupe $(G, \star)$ dans le groupe $(G', \sharp)$, si*

$$\forall x, y \in G, \qquad \varphi(x \star y) = \varphi(x) \sharp \varphi(y).$$

2. *Tout morphisme d'un groupe dans lui-même est appelé endomorphisme.*
3. *Tout morphisme de G dans G' qui est une bijection est appelé isomorphisme de G sur G'. Dans ce cas on dit que G et G' sont isomorphes. Un morphisme qui est à la fois un isomorphisme et un endomorphisme est appelé automorphisme.*

Exemple 2.28. *1. $(\mathbf{Z}, +) \to (\mathbf{Z}, +), x \mapsto 2x$ est un morphisme, mais pas un isomorphisme.*

2. $(\mathbf{C}^*, \times) \to (\mathbf{R}^*, \times), z \mapsto |z|$*, est un morphisme, mais pas un isomorphisme.*

3. $(\mathbf{R}, +) \to (\mathbf{C}^*, \times), x \mapsto e^{ix}$*, est un morphisme, mais pas un isomorphisme.*

4. $(\mathbf{R}, +) \to (\mathbf{R}_+^*, \times), x \mapsto e^x$ *est un isomorphisme de réciproque* ln*, qui est aussi un isomorphisme.*

Exemple 2.29. *Etudions les applications suivantes*

1. Si $n \in \mathbf{N}^*$*,*

$$\begin{array}{rccccc} \varphi_n & : & (\mathbf{C}^*, \times) & \to & (\mathbf{C}^*, \times) \\ & & z & \mapsto & z^n \end{array}$$

2. Si $n \in \mathbf{N}^*$ *et* $a_1, \ldots, a_n \in \mathbf{K}^n$*, l'application*

$$\begin{array}{rccc} \varphi_n & : & (\mathbf{K}^n, +) & \to & (\mathbf{K}, +) \\ & & (x_1, \ldots, x_n) & \mapsto & a_1x_1 + \cdots + a_nx_n \end{array}$$

Dans toute la suite, $(G, \star)$ et $(G', \sharp)$ sont deux groupes de neutres e et e', on adopte une notation muliplicative, et $\varphi : G \to G'$ est un morphisme.

Théorème 2.30. *Soit* φ *un morphisme de* G *sur* G'*, on a,* e *et* e' *désignant les neutres de* G *et* G' *:*

1. $\varphi(e) = e'$ *;*

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

Preuve:

□

Corollaire 2.31. *Sous les mêmes hypothèses, on a*

$$\forall x \in G \qquad \forall k \in \mathbf{Z} \qquad \varphi(x^k) = \varphi(x)^k.$$

Preuve:
Soit $x \in G$. D'après le théorème ci-dessus, on a

$$\varphi(x^0) = \varphi(e) = e' = \varphi(x)^0.$$

On peut alors démontrer par récurrence que pour tout $n \in \mathbf{N}$, on a $\varphi(x^n) = \varphi(x)^n$ (l'hérédité résulte directement de la définition de morphisme).
D'après le théorème ci-dessus, pour tout $n \in \mathbf{N}$,

$$\varphi(x^{-n}) = \varphi(xn)^{-1}$$

d'où $\varphi(x^{-n}) = \varphi(x)^{-n}$. On en déduit le résultat. □

Exemple 2.32. *1.* $\mathbf{C}^* \to \mathbf{R}^*, z \mapsto |z|$ *est un morphisme de* $(\mathbf{C}^*, \times)$ *dans* $(\mathbf{R}^*, \times)$*, donc pour tout* $z \in \mathbf{C}^*$*, on a*

$$| \frac{1}{z} | = \frac{1}{| z |}$$

2. exp est un morphisme de $(\mathbf{C}, +)$ *dans* $(\mathbf{C}^*, \times)$*, donc pour tout* $z \in \mathbf{C}$*,* $e^{-z} = \frac{1}{e^z}$.

3. $\ln$ *est un morphisme de* $(\mathbf{R}_+^*, \times)$ *dans* $(\mathbf{R}, +)$*, donc pour tout* $x \in \mathbf{R}_+^*$*, on a* $\ln(\frac{1}{x}) = -\ln(x)$*.*

Théorème 2.33. *1. La composée de deux morphismes de groupes est un morphisme de groupe. Plus précisément, soit* $(G_1, \star_1)$*,* $(G_2, \star_2)$ *et* $(G_3, \star_3)$ *trois groupes,* φ *un morphisme de* G_1 *dans* G_2 *et* φ *un morphisme de* G_2 *dans* G_3*. Alors* $\psi \circ \varphi$ *est un morphisme de* G_1 *dans* G_3*.*

2. La fonction réciproque d'un isomorphisme (en tant qu'application bijective) est un isomorphisme. Plus précisément, soit $(G_1, \star_1)$ *et* $(G_2, \star_2)$ *deux groupes et* φ *un isomorphisme de* G_1 *sur* G_2*. Alors* φ^{-1} *est un isomorphisme de* G_2 *sur* G_1*.*

Preuve:

□

Théorème 2.34. *1. L'image d'un sous-groupe par un morphisme de groupes est un sous-groupe.*

2. L'image réciproque d'un sous-groupe par un morphisme est un sous-groupe.

Preuve:

□

Remarque 2.35. *lorsque l'on veut montrer qu'un ensemble est muni d'une structure de groupe, on commence toujours par essayer de l'identifier comme image réciproque (ou directe) d'un sous-groupe d'un groupe bien connu par un morphisme.*

Définition 2.36. *1. On appelle noyau de φ, noté* $\operatorname{Ker}\varphi$*, l'image réciproque de $\{e'\}$ par φ, autrement dit l'ensemble des antécédents de e' par φ*

$$\operatorname{Ker}\varphi = \{x \in G \mid \varphi(x) = e'\}.$$

2. On appelle image de φ notée $\operatorname{Im}\varphi$*, l'image directe de G par φ. Autrement dit*

$$\operatorname{Im}\varphi = \{\varphi(x) \mid x \in G\}.$$

Théorème 2.37. *Les noyaux et les images sont des sous-groupes respectivement de G et G'.*

Preuve:
Montrons que $\operatorname{Ker}\varphi$ est un sous-groupe de G :

1. On a évidemment $\operatorname{Ker}\varphi \subset G$ et de plus $\varphi(e) = e'$ donc $\operatorname{Ker}\varphi$ est un sous-ensemble non vide de G.

2. Soit $x, y \in \operatorname{Ker}\varphi$. Alors on a successivement

$$\begin{aligned} \varphi(x \star y^{-1}) &= \varphi(x) \sharp \varphi(y)^{-1} \\ &= e' \sharp e'^{-1} \\ &= e' \end{aligned}$$

Donc $x \star y^{-1} \in Ker\varphi$.
Donc $\operatorname{Ker}\varphi$ est un sous-groupe de G.

□

Remarque 2.38. *lorsque l'on veut montrer qu'un ensemble est muni d'une structure de groupe, on commence toujours par essayer de l'identifier comme noyau ou image d'un morphisme.*

Exemple 2.39. *$\mathcal{U}$ est le noyau du morphisme « module », de $(\mathbf{C}^*, \times)$ dans $(\mathbf{R}^*, \times)$.*

Proposition 2.40. *Soit $\varphi : G \to G'$ un morphisme de groupes, soit $x, y \in G$. Alors $\varphi(x) = \varphi(y)$ si et seulement si $x \star y^{-1} \in \operatorname{Ker}\varphi$.*

Preuve:
$\varphi(x) = \varphi(y)$ si et seulement si $\varphi(x) \sharp \varphi(y)^{-1} = e'$ si et seulement si $\varphi(x \star y^{-1}) = e'$. □

Théorème 2.41. *1. φ injectif si et seulement si $\operatorname{Ker}\varphi = \{e\}$.*

2. φ surjectif si et seulement si $\operatorname{Im}\varphi = G'$.

Preuve:

□

Remarque 2.42. *Pour montrer qu'un morphisme est injectif, on utilisera TOUJOURS le noyau et JAMAIS (ou presque) la méthode classique pour des fonctions quelconques : c'est beaucoup plus rapide !*