1. Groupes

1.1 Rappels

Définition 1.1 (Groupe). *On rappelle qu'un groupe G est un ensemble muni d'une loi de composition $\star$ telle que :*

(i) *$\star$ est associative ;*

(ii) *il existe un élément neutre e pour la loi $\star$;*

(iii) *tout élément x admet un symétrique x^e.*

Le neutre est alors unique, ainsi que le symétrique d'un élément x donné.

Définition 1.2 (Groupe abélien ou commutatif). *On dit qu'un groupe $(G, \star)$ est abélien (ou commutatif) si la loi de G est commutative.*

Remarque 1.3 (Notation additive, notation multiplicative).

- *Dans le cas général, on utilise souvent une notation multiplicative. Ainsi, la loi est $\times$, le neutre est souvent noté 1, le signe opératoire peut être omis (ab désigne $a \times b$) et on désignera sous forme de puissance l'itération de la loi, ainsi que la prise de symétrique ($x^e = x^{-1}$, on parlera alors d'inverse).*
- *Dans le cas abélien, on peut trouver la notation additive $+$, avec les conventions usuelles : le neutre est souvent noté 0, l'itération est notée nx, le symétrique est noté $-x$ et est appelé opposé.*

Définition 1.4 (Homomorphisme de groupes). *Soit $(G, \star)$ et $(H, \circ)$ deux groupes.*

- *On dit qu'une application $f : G \to H$ est un homomorphisme de groupes (ou plus simplement morphisme de groupes) si pour tout $(x, y) \in G$, $f(x \star y) = f(x) \circ f(y)$.*
- *On note $\mathrm{Hom}(G, H)$ l'ensemble des homomorphismes de G dans H.*
- *Si $(G, \star) = (H, \circ)$, on dit que f est un endomorphisme de $(G, \star)$.*
- *Un homomorphisme bijectif est appelé isomorphisme.*
- *Un endomorphisme bijectif est appelé automorphisme. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.*

Proposition 1.5 (Image du neutre par un morphisme). *Soit $f : G \to H$ un morphisme de groupes. Alors $f(e_G) = e_H$.*

Proposition 1.6 (Image par un morphisme d'un inverse). *Soit G, H deux groupes (notés multiplicativement), et f un morphisme de G dans H. Alors $f(x^{-1}) = f(x)^{-1}$. On adaptera aisément cette propriété au cas ou l'un (ou les deux) groupe(s) est (sont) en notation additive.*

Éléments de preuve. Considérer $f(x)f(x^{-1})$. □

Proposition 1.7 (Composée et réciproque de morphismes). *Soit G, H et K trois groupes.*

(i) Si $f : G \to H$ et $g : H \to K$ sont deux morphismes de groupes, alors $g \circ f$ est aussi un morphisme de groupes.

(ii) Si $f : G \to H$ est un isomorphisme, alors $f^{-1} : H \to G$ est aussi un isomorphisme.

Éléments de preuve. Vérifications faciles pour la composée. Pour la réciproque, considérer $f^{-1}(f(f^{-1}(x)f^{-1}(y)))$. □

1.2 Sous-groupes

Définition 1.8 (Sous-groupe). *Soit $(G, \star)$ un groupe. Un sous-ensemble H de G est appelé* sous-groupe de G *si H est stable pour la loi de G et si la loi induite définit sur H une structure de groupe. Le neutre de H est alors nécessairement le même que celui de G.*

Théorème 1.9 (Caractérisation des sous-groupes). *Un sous-ensemble H d'un groupe $(G, \star)$ (de neutre e_G) est un sous-groupe de G si et seulement si :*

(i) H est non vide,

(ii) H est stable pour $* : \forall (x, y) \in H, x * y \in H$,

(iii) H est stable par prise de symétrique : $\forall x \in H, x^* \in H$.

Dans la pratique, pour montrer que H est non vide, on vérifie souvent que $e_G \in H$.

Théorème 1.10 (Caractérisation des sous-groupes, version condensée). *Un sous-ensemble H d'un groupe $(G, \star)$ (de neutre e_G) est un sous-groupe de G si et seulement si :*

(i) H est non vide,

(ii) $\forall (x, y) \in H^2, x * y^* \in H$.

On traduit cette dernière propriété dans les deux cas les plus fréquents :

- *pour un sous-groupe d'un groupe additif, la vérification de stabilité à faire est donc : $\forall (x, y) \in H^2, x - y \in H$;*
- *pour un sous-groupe d'un groupe multiplicatif, la vérification de stabilité à faire est donc : $\forall (x, y) \in H^2, xy^{-1} \in H$.*

Proposition 1.11 (Image directe et réciproque de sous-groupes par un homomorphisme). *Soit G et H deux groupes, et soit $f \in Hom(G, H)$ un morphisme de groupes.*

(i) Soit G' un sous-groupe de G. Alors $f(G')$ est un sous-groupe de H.

(ii) Soit H' un sous-groupe de H. Alors $f^{-1}(H')$ est un sous-groupe de G.

Définition 1.12 (Noyau). *Soit G et H deux groupes et $f \in Hom(G, H)$ un morphisme de groupes. Le noyau de f est le sous-groupe de G défini par :*

$$Ker(f) = f^{-1}(\{e_H\}) = \{y \in G \mid f(y) = e_H\}.$$

Théorème 1.13 (Caractérisation de l'injectivité). *Soit $f \in Hom(G, H)$. Le morphisme f est injectif si et seulement si $Ker(f) = \{e_G\}$.*