MATHF-203 – Algèbre I

R. Petit

Année académique 2016 - 2017

Table des matières

1 Les groupes

1.1 Définitions

Définition 1.1. Un *groupe* $(G, *)$ est un ensemble non-vide G muni d'une loi de composition $* : G \times G \to G$ tels que :
- $*$ est associative ;
- G possède un élément neutre noté $e \in G$;
- chaque élément g de G possède un inverse noté g^{-1}.

Définition 1.2. Un ensemble non-vide M muni d'une loi de composition $* : M \times M \to M$ associative telle que M admet un neutre par $*$ est appelé un *monoïde*.

Définition 1.3. Un monoïde $(M, *)$ est dit *abélien* (ou *commutatif*) lorsque $*$ est commutative.

Remarque. Un groupe est un monoïde admettant un inverse pour chaque élément. Dès lors, les résultats et définitions sur les monoïdes s'appliquent également aux groupes.

Proposition 1.4. *Dans un groupe* $(G, *)$*, les équations :*

$$x * a = b, \tag{1}$$

et :

$$a * y = b \tag{2}$$

admettent une unique solution, i.e. :

$$(x, y) = (b * a^{-1}, a^{-1} * b) \in G^2.$$

Démonstration. G est un groupe, du coup a et b admettent un inverse. L'existence de la solution est donc triviale.

Soit x, solution de (1). On a alors :

$$x = x * e = x * a * a^{-1} = b * a^{-1}.$$

Similairement pour y, solution de (2), on a :

$$y = e * y = a^{-1} * a * y = a^{-1} * b.$$

□

Proposition 1.5. *Le neutre d'un groupe est unique, et l'inverse de tout élément l'est également.*

De plus :

$$\forall a, b, c, d \in G : \begin{cases} c * a = d * a \Rightarrow c = d, \\ a * c = a * d \Rightarrow c = d. \end{cases}$$

Démonstration. EXERCICE. □

Proposition 1.6. *Si* G *est un ensemble non-vide muni d'une loi de composition* $*$ *associative telle que* (1) *et* (2) *admettent une unique solution, alors* $(G, *)$ *est un groupe.*

Démonstration. Pour chaque élément $a \in G$, prenons e^L_a tel que $e^L_a * a = a$ et e^R_a tel que $a * e^R_a = a$. Ces deux équations admettent une unique solution par hypothèse. On trouve alors :

$$e^L_a * a = a = a * e^R_a,$$

d'où l'on déduit :

$$a * e^L_a * a = a * a = a * e^R_a * a,$$

et donc $e^L_a = e^R_a$ en multipliant à gauche et à droite par a^{-1}. On en déduit l'unicité d'un neutre pour a et notons-le e_a. Montrons que ce neutre l'est pour tous les éléments de G. Prenons $(a, b) \in G^2$ et leur neutre respectif e_a et e_b. On peut écrire :

$$a * e_b * b = a * b = a * e_a * b,$$

d'où l'on déduit $e_a = e_b$ en multipliant à gauche par a^{-1} et à droite par b^{-1}. □

Définition 1.7. Si $|G| < \infty$, on peut définir la *table de multiplication* de $(G, *)$ par un tableau de dimensions $|G| \times |G|$ reprenant tous les résultats de $g * h$ pour $g, h \in G$.

1.2 Groupes de transformation

Définition 1.8. Soit S un ensemble non-vide. Soit G l'ensemble des bijections de S dans S. On définit la loi de composition :

$$\circ : G \times G \to G : (\psi, \varphi) \mapsto (\psi \circ \varphi),$$

tels que $\forall s \in S : (\psi \circ \varphi)(s) = \psi(\varphi(s))$.

Proposition 1.9. $(G, \circ)$ *est un groupe (de permutation sur* S*).*

Démonstration. Le neutre est donné par $\mathrm{Id} \in G$ où $\forall s \in S : \mathrm{Id}(s) = s$. La loi $\circ$ est trivialement associative, et l'inverse d'une fonction est bien définie sur les bijections. □

Exemple 1.1. L'ensemble $SO(3, \mathbb{R})$ des rotations axiales passant par $\mathcal{O}$ forme un groupe de transformations.

Remarque. Un groupe de transformation est composé de fonctions bijectives. L'ensemble G est donc un ensemble fonctionnel.

1.3 Sous-groupes

Définition 1.10. Soit $(G, *)$ un groupe, et soit $S \subset G$. Si $(S, *)$ est un groupe, alors on dit que $(S, *)$ est un *sous-groupe* de $(G, *)$.

Proposition 1.11. *Soit* $(G, *)$ *un groupe.* $S \subseteq G$ *est un sous-groupe de* G *si et seulement si :*

$$\forall a, b \in S : a * b^{-1} \in S.$$

Démonstration. $\boxed{\Rightarrow}$ Trivial car S est un groupe.

$\boxed{\Leftarrow}$ S est non-vide, donc $e \in S$ car si $a \in S$, alors par hypothèse $e = a * a^{-1} \in S$. De même, soit $a \in S$. On sait que $a^{-1} = e * a^{-1} \in S$. Et S est stable par $*$ car si $a, b \in S$, on sait que $b^{-1} \in S$, et donc $a * \left(b^{-1}\right)^{-1} \in S$. □

Proposition 1.12. *Si* $\{S_\alpha$ *t.q.* $\alpha \in I\}$ *est une famille de sous-groupes de* $(G, *)$*, alors* $S \coloneqq \bigcap_{\alpha \in I} S_\alpha$ *est un sous-groupe de* $(G, *)$ *également.*

<u>*Démonstration*</u>. On sait que $e \in S$ car $e \in S_\alpha$ pour tout $\alpha \in I$. Donc $S \neq \emptyset$. Prenons $a, b \in S$. On sait que $a, b \in S_\alpha$ pour tout $\alpha \in I$. Donc b^{-1} et $a * b^{-1}$ sont dans S_α pour tout $\alpha \in I$ également. Donc $a * b^{-1} \in S$. □

Définition 1.13. Soit $(G, *)$ un groupe et soit $P \subseteq G$. On appelle le *sous-groupe de* G *engendré par* P le plus petit sous-groupe de G contenant P. On le note $\langle P \rangle$

Définition 1.14. Soit $(G, *)$ un groupe et soit $g \in G$. On appelle *ordre de* g le plus petit $n \in \mathbb{N}^*$ tel que $g^n = e$. On le note $\mathrm{ord}(e)$.

L'ordre de $(G, *)$ est$|G|$.

Définition 1.15. Un groupe $(G, *)$ est dit *cyclique* lorsqu'il existe $g \in G$ tel que $G = \langle g \rangle \coloneqq \langle \{g\} \rangle$.

1.4 Isomorphismes

Définition 1.16. Un *isomorphisme* entre deux groupes $(G, *)$ et $(H, \star)$ est une bijection $\phi : G \to H$ telle que :

$$\forall g_1, g_2 \in G : \phi(g_1 * g_2) = \phi(g_1) \star \phi(g_2).$$

Remarque. La relation « *être isomorphe* » dans l'ensemble des groupes est une relation d'équivalence.

De plus, sis G et H sont deux groupes finis, $\phi : G \to H$ est un isomorphisme si et seulement si ϕ est bijective, et la table de multiplication de H par $\phi(G)$ est l'image de la table de multiplication de G par G.

Proposition 1.17. *Soit* $\phi : (G, *) \to (H, \star)$ *un isomorphisme de groupes. Alors :*

- $\phi(e_G) = e_H$;
- $\forall g \in G : \phi(g)^1 = \phi(g^{-1})$.

<u>*Démonstration*</u>. On sait que $\phi(e_G) = \phi(e_G * e_G) = \phi(e_G) \star \phi(e_G)$. Dès lors, il est évident que $\phi(e_G)$ est le neutre de H.

Soit $g \in G$. On sait également que $e_H = \phi(e_G) = \phi(g * g^{-1}) = \phi(g) \star \phi(g^{-1})$. On a donc bien, en multipliant par $\phi(g)^{-1}$ à gauche que $\phi(g)^{-1} = \phi(g^{-1})$. □

Théorème 1.18. *Tout groupe est isomorphe à un groupe de transformation.*

<u>*Démonstration*</u>. Soit $(G, *)$ un groupe, et soit $g \in G$. On définit $\phi : G \to \{\ell_g$ t.q. $g \in G\}$, où $\ell_g : G \to G : h \mapsto g * h$.

Pour $g \in G$, montrons que ℓ_g est bijective :

- il est évident que $\forall g, h, h' \in G : g * h = g * h' \iff h = h'$ par les règles de simplification ;
- $\forall h \in G : \ell_g(g^{-1} * h) = g * g^{-1} * h = h$.

On a donc que ℓ_g est bien bijective pour tout $g \in G$.

Montrons maintenant que $\phi : g \mapsto \ell_g$ est un isomorphisme de groupes :

- ϕ est surjective par définition.
- soient $g, h \in G$. $\ell_g = \ell_h$ si et seulement si pour tout $\gamma \in G$, on a $g * \gamma = h * \gamma$, et donc si et seulement si on a $g = h$. ϕ est donc injective.
- Soient $g, h, \gamma \in G$. $\phi(g * h)(\gamma) = g * h * \gamma = g * \ell_h(\gamma) = (\ell_g \circ \ell_h)(\gamma)$.

□

Théorème 1.19. *Tout groupe cyclique est déterminé, à isomorphisme près, par l'ordre d'un élément* g *qui l'engendre.*

Plus précisément, si $(G, *)$ *est un groupe engendré par un élément* g *d'ordre* $\mathrm{ord}(g)$ *fini, alors* $G \cong (\mathbb{Z}_{\mathrm{ord}(g)}, +)$ *; et si* g *est d'ordre infini, alors* $(G, *) \cong (\mathbb{Z}, +)$*.*

Démonstration. S'il existe $g \in G$ tel que $G = \langle g \rangle$ et $\mathrm{ord}(g) \lneqq +\infty$, alors $G = \{e, g, \ldots, g^{\mathrm{ord}(g)-1}\}$.

Soit $\phi : \mathbb{Z}_{\mathrm{ord}(g)} \to G : k \mapsto g^k$. ϕ est trivialement bijective, et on observe :

$$\phi(k + l) = g^{k+l} = g^k * g^l = \phi(k) * \phi(l).$$

Supposons maintenant qu'il existe $g \in G$ tel que $\mathrm{ord}(g) = +\infty$ et $\langle g \rangle = G$. On pose :

$$\forall p \in \mathbb{N}^* : g^{-p} \coloneqq g^{-1} * g^{1-p}.$$

Puisque $\mathrm{ord}(g) = +\infty$, si $g^x = g^y$ pour $x, y \in \mathbb{Z}$, alors $x = y$. En reprenant le même ϕ étendu à $\mathbb{Z}$, on a bien, à nouveau, un isomorphisme de groupes. □

Corollaire 1.20. *Tout groupe cyclique est commutatif.*

Démonstration. Étant isomorphe à $\mathbb{Z}_n$ pour un certain $n \in \mathbb{N}$ ou à $\mathbb{Z}$, par passage à l'isomorphisme, la propriété d'additivité est conservée. □

Proposition 1.21. *Si* $(G, *)$ *est un groupe cyclique, tout sous-groupe* S *de* G *est cyclique.*

Démonstration. Prenons $a \in G$ tel que $G = \langle a \rangle$. Posons $N \coloneqq \{n \in \mathbb{Z} \text{ t.q. } a^n \in S\}$. Dans le cas fini, prenons $\underline{n}$, le plus petit entier positif de N. Supposons par l'absurde que $a^t \in S$ ne soit pas une puissance entière de $a^{\underline{n}}$. Par Euclide, on a :

$$\exists (q, r) \in \mathbb{Z} \times \mathbb{N} \text{ t.q. } t = q\underline{n} + r,$$

et donc :

$$a^t = a^{q\underline{n}} * a^r,$$

avec $0 \lneqq r \lneqq \underline{n}$. On sait que $a^t \in S$, et $a^{q\underline{n}} \in S$ (donc $a^{-q\underline{n}} \in S$). Dès lors, $a^r \in S$. Or $\underline{n}$ est le plus petit entier positif tel que $a^{\underline{n}} \in S$. Il y a donc contradiction, et a^t est une puissance entière de $a^{\underline{n}}$. Dès lors, $S = \langle a^{\underline{n}} \rangle$. □

1.5 Classes latérales et théorème de Lagrange

Dans cette sous-section, considérons que $(G, *)$ est un groupe, et que S est un sous-groupe de G.
Définition 1.22. Soient $(G, *)$ un groupe, et S un sous-groupe de G. On appelle *classe latérale gauche de S par* $a \in G$ l'ensemble :

$$a * S \coloneqq \left\{ a * s \text{ t.q. } s \in S \right\}.$$

Similairement, une classe latérale droite est sous la forme :

$$S * a \coloneqq \left\{ s * a \text{ t.q. } s \in S \right\},$$

pour un certain $a \in G$.

Proposition 1.23. *Deux classes latérales gauches* $a * S$ *et* $b * S$ *sont identiques ou sont d'intersection nulle.*

Démonstration. Soient deux telles classes d'équivalences, telles que $a * S \cap b * S \neq \emptyset$. On sait alors qu'il existe $c \in a * S \cap b * S$. On en déduit $u, v \in S$ tels que $a * u = c = b * v$. On a alors, pour $s \in S$:

$$b * s = c * v^{-1} * s = a * u * v^{-1} * s.$$

Or u et v^{-1} sont dans S. Donc $b * S \subseteq a * S$.

Par un raisonnement similaire, on a $a * S \subseteq b * S$, et donc $a * S = b * S$. □

Proposition 1.24. *Deux éléments* $a, b \in G$ *ont la même classe latérale gauche, i.e.* $a * S = b * S$ *si et seulement si* $a^{-1} * b \in S$.

Démonstration. $\boxed{\Rightarrow}$ $a * S = b * S = a * a^{-1} * b * S$. Donc $a^{-1} * b \in S$.

$\boxed{\Leftarrow}$ On sait $S = e * S = s * S$ pour tout $s \in S$. Or $a^{-1} * b \in S$. Donc $S = a^{-1} * b * S$, ou encore $a * S = b * S$. □

Définition 1.25. On appelle *indice* d'un sous-groupe S de G le « nombre » de classes latérales gauches distinctes de S dans G.

Proposition 1.26. *Il existe une bijection entre un sous-groupe* S *et chacune de ses classes latérales.*

Démonstration. Soit $a \in G$. On considère $\phi : S \to a * S : s \mapsto a * s$.

ϕ est surjective par définition, et est trivialement injective. □

Corollaire 1.27. *Il existe une bijection entre tout groupe* $(G, *)$ *et l'ensemble* $S \times T$, *pour* S, *un sous-groupe de* G *et* T *l'ensemble des classes latérales gauches distinctes de* S *dans* G.

Théorème 1.28 (Théorème de Lagrange)**.** *Soient* $(G, *)$ *un groupe fini, et* S *un sous-groupe de* G. *L'ordre de* G *est un multiple de l'ordre de* S.

Démonstration. Trivial par le corollaire précédent. □

Corollaire 1.29. *Si* p *est un nombre premier, tout groupe* $(G, *)$ *à* p *éléments est isomorphe à* $(\mathbb{Z}_p, +)$.

Démonstration. p est premier, donc $|G| \geqslant 2$. Soit g tel que $\mathrm{ord}(g) > 1$ (c-à-d $g \neq e$). $S \coloneqq \langle g \rangle$ est un sous-groupe de G, on en déduit par Lagrange que $|\langle g \rangle|$ divise $|G|$. Donc $|S| \in \{1, p\}$. Et comme $e, g \in S$ pour $g \neq e$, on a $|S| \geqslant 2$, et donc $|S| = p$. □

Corollaire 1.30. *Si* G *est un groupe d'ordre fini* n, *pour tout* $g \in G$, *on a* $\mathrm{ord}(g)$ *divise* n.

Corollaire 1.31. *Il n'existe, à isomorphisme près, que deux groupes d'ordre 4, à savoir* $\mathbb{Z}_4$ *et* $V_4 \coloneqq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Corollaire 1.32. *Tout groupe d'ordre fini* $n \leqslant 5$ *est commutatif.*

1.6 Sous-groupes normaux et homomorphismes

Définition 1.33. Un sous-groupe N d'un groupe $(G, *)$ est dit *normal* lorsque ses classes latérales gauches sont des classes latérales droites, i.e. :

$$\forall a \in G : a * N = N * a.$$

Proposition 1.34. *Soit* N, *un sous-groupe d'un groupe* $(G, *)$. *Les assertions suivantes sont équivalentes :*

1. N *est normal ;*
2. $\forall a \in G : a * N = N * a$ *;*
3. $\forall a \in G : a * N \subseteq N * a$ *;*
4. $\forall a \in G : a * N * a^{-1} \subseteq N$.

Démonstration. On sait, par définition, que $1 \iff 2$, et $2 \Rightarrow 3$. En multipliant par a^{-1} à droite, on a $3 \iff 4$.

Montrons donc que $3 \Rightarrow 2$. En particulier, c'est vrai pour a^{-1}, et donc $a^{-1} * N \subseteq N * a^{-1}$, ou encore $N * a \subseteq a * N$. Avec 3, cela implique que $a * N = N * a$. □

Définition 1.35. Un *homomorphisme* d'un groupe $(G, *)$ dans un groupe $(H, \star)$ est une application $f : G \to H$ telle que :

$$\forall g_1, g_2 \in G : f(g_1 * g_2) = f(g_1) \star f(g_2).$$

Proposition 1.36. *Si* f *est un homomorphisme de* $(G, *)$ *dans* $(H, \star)$, *alors l'image du neutre par* f *est le neutre de* H, *et l'inverse* g^{-1} *d'un élément* $g \in G$ *est envoyé sur* $f(g)^{-1} \in H$.

Démonstration. Voir preuve de la Proposition 1.17. □

Proposition 1.37. *Si* f *est un homomorphisme de* $(G, *)$ *dans* $(H, \star)$, *alors :*

1. $\operatorname{Im} f \coloneqq \{f(g) \text{ t.q. } g \in G\} \eqqcolon f(G)$ *est un sous-groupe de* H *;*
2. $\operatorname{Ker} f \coloneqq \{g \in G \text{ t.q. } f(g) = e_H\}$ *est un sous-groupe* ***normal*** *de* H.

Démonstration. Montrons d'abord que $\operatorname{Im} f \leqslant H$. Prenons donc $g, g' \in G$. On a alors $f(g) \star f(g')^{-1} = f(g * g'^{-1}) \in \operatorname{Im} f$ car f est un homomorphisme.

Montrons ensuite que $\operatorname{Ker} f \leqslant G$. Prenons $g_1, g_2 \in \operatorname{Ker} f$. On sait donc que :

$$f(g_1 * g_2^{-1}) = f(g_1) \star f(g_2)^{-1} = e_H \star e_H^{-1} = e_H.$$

On en déduit que $g_1 * g_2^{-1} \in \operatorname{Ker} f$.

Montrons alors que pour tout $a \in G$, on a $a * \operatorname{Ker}(f) * a^{-1} \subseteq \operatorname{Ker} f$. Soit $g \in \operatorname{Ker} f$. On calcule :

$$f\left(a * g * a^{-1}\right) = f(a) * e_H * f(a)^{-1} = f(a) * f(a)^{-1} = e_H,$$

et donc $a * g * a^{-1} \in \operatorname{Ker} f$, ou encore $a * \operatorname{Ker}(f) * a^{-1} \subseteq \operatorname{Ker} f$. $\operatorname{Ker} f$ est donc bien un sous-groupe normal de G. □

Remarque. Un isomorphisme est un homomorphisme tel que $\operatorname{Ker} f = \{e_G\}$ et $\operatorname{Im} f = H$ car f est respectivement injective et surjective.

Définition 1.38. Un homomorphisme d'un groupe $(G, *)$ dans lui-même est appelé un *automorphisme*.

Définition 1.39. Pour tout $g \in G$, on définit la *conjugaison par* g comme la fonction :

$$c(g) : G \to G : h \mapsto g * h * g^{-1}.$$

Proposition 1.40. *Pour* $g \in G$*, la conjugaison par* g *est un automorphisme.*

Démonstration. $c(g)$ est injective par les règles de simplification, et est surjective car pour tout $\gamma \in G$, on a :

$$c(g)^{-1}(\gamma) = g^{-1} * \gamma * g,$$

en effet :

$$c(g)(g^{-1} * \gamma * g) = g * \left(g^{-1} * \gamma * g\right) * g^{-1} = \gamma.$$

Donc $c(g)$ est bien surjective.

Et puisque $c(g)$ va de G dans G, c'est bien un automorphisme. $\square$

Proposition 1.41. *L'application* $C : G \to \mathrm{Aut}(G) \subset G^G : g \mapsto c(g)$ *est un homomorphisme.*

Démonstration. Soient $g, h, \gamma \in G$. On calcule :

$$\begin{aligned} C(g * h)(\gamma) &= c(g * h)(\gamma) = (g * h) * \gamma * (g * h)^{-1} = g * h * \gamma * h^{-1} * g^{-1} = c(g)(h * \gamma * h^{-1}) \\ &= c(g)\left(c(h)(\gamma)\right) = \left(c(g) \circ c(h)\right)(\gamma). \end{aligned}$$

$\square$

Proposition 1.42. *Soit* f *un homomorphisme de groupe de* $(G, *)$ *dans* $(H, \star)$*. Deux éléments* $x, y \in G$ *ont la même image par* f *si et seulement si ils appartiennent à la même classe latérale de* $\mathrm{Ker}\, f$ *dans* G*.*

Démonstration. Soient x et y tels que $f(x) = f(y)$. On calcule :

$$f(x * y^{-1}) = f(x) \star f(y^{-1}) = f(y) \star f(y)^{-1} = e_H.$$

Donc $x * y^{-1} \in \mathrm{Ker}\, f$, et donc $x * \mathrm{Ker}\, f = y * \mathrm{Ker}\, f$ par la Proposition 1.24. $\square$

1.7 Groupes quotients

Soit $f : (G, *) \to (H, \star)$ un homomorphisme surjectif. Si $x' \in H$, alors il existe $x \in G$ tel que $f(x) = x'$. On a alors :

$$f^{-1}(\{x'\}) = x * \mathrm{Ker}\, f.$$

Si $|\mathrm{Ker}\, f| \geqslant 2$, prenons également $y' \in H$ et donc $y \in G$ tel que $f^{-1}(\{y'\}) = y * \mathrm{Ker}\, f$.

On peut ensuite calculer :

$$x' \star y' = f(x) \star f(y) = f(x * y),$$

d'où l'on déduit :

$$f^{-1}(\{x' * y'\}) = x * y * \mathrm{Ker}\, f.$$

Définition 1.43. Soit N un sous-groupe normal du groupe $(G, *)$. On désigne par G/N l'ensemble des classes latérales de N dans G. Cela se lit G *quotienté* N.

Proposition 1.44. *Soient* $x * N$ *et* $y * N$ *deux éléments de* G/N. *Si* $x' \in x * N$ *et* $y' \in y * N$, *alors :*

$$x' * y' \in x * y * N.$$

Démonstration. On sait qu'il existe $m, n \in N$ tels que $x' = x * n$ et $y' = y * m$. Par normalité de N, on sait qu'il existe $m' \in N$ tel que $y' = n * y = y * n'$. Dès lors :

$$x' * y' = x * n * y * n' * m.$$

Or, $n' * m \in N$. Donc :

$$x' * y' \in x * y * N.$$

□

Définition 1.45. On définit le produit $\bar{*} : G/N \times G/N \to G/N : (x * N, y * N) \mapsto (x * N)\bar{*}(y * N) := x * y * N$.

Théorème 1.46. *Soient* $(G, *)$ *un groupe et* N *un sous-groupe normal de* G. *Alors* $(G/N, \bar{*})$ *est un groupe.*

Démonstration. $\bar{*}$ est interne par définition et par la proposition précédente, et est associative par associativité de $*$.

$(G/N, \bar{*})$ admet pour neutre $e * N = N$.

Soit $g * N \in G/N$. Il admet pour inverse $g^{-1} * N$ car $(g * N)\bar{*}(g^{-1} * N) = e * N = N$. □

Définition 1.47. Le groupe $(G/N, \bar{*})$ est appelé le *groupe quotient de* G *par* N.

Définition 1.48. Soient $(G, *)$ un groupe, et $N \leqslant G$. La projection $\pi_N : G \to G/N : g \mapsto g * N$ est appelée la *projection canonique*.

Proposition 1.49. $\pi_N : (G, *) \to (G/N, \bar{*})$ *est un homomorphisme.*

Démonstration. Soient $g, h \in G$. $\pi_N(g * h) = g * h * N = (g * N)\bar{*}(h * N) = \pi_N(g)\bar{*}\pi_N(h)$. □

Proposition 1.50. *Si* $(G, *)$ *et* $(H, \star)$ *sont deux groupes,* $f : G \to H$ *est un homomorphisme, et si* N *est un sous-groupe normal de* G *contenu dans* $\operatorname{Ker} f$, *alors il existe un homomorphisme* $\overline{f} : G/N \to H$ *avec* $\overline{f}(g * N) = f(g)$. *De plus :*

$$\operatorname{Im} \overline{f} = \operatorname{Im} f \qquad \textit{et} \qquad \operatorname{Ker} \overline{f} = \operatorname{Ker}(f)/N.$$

Démonstration. $\overline{f}$ est bien définie. Soient $g, g' \in G$. On calcule :

$$\overline{f}((g * N)\bar{*}(g' * N)) = \overline{f}(g * g' * N) = f(g * g').$$

Par propriétés de morphismes de f, on trouve donc :

$$\overline{g}((g * N)\bar{*}(g' * N)) = f(g) \star f(g') = \overline{f}(g * N) \star \overline{f}(g' * N).$$

$\operatorname{Im} f = \operatorname{Im} \overline{f}$ de manière triviale.

$g * N \in \operatorname{Ker} \overline{f}$ si et seulement si $g \in \operatorname{Ker} f$. On a alors bien $\operatorname{Ker} \overline{f} = \{h * N \text{ t.q. } h \in \operatorname{Ker} f\} = \operatorname{Ker}(f)/N$. □

1.8 Théorèmes d'isomorphisme

1.8.1 Premier théorème d'isomorphisme

Théorème 1.51. *Si* $f : (G, *) \to (H, \star)$ *est un homomorphisme de groupes, il induit un isomorphisme :*

$$G/\operatorname{Ker}(f) \cong \operatorname{Im} f.$$

Démonstration. $(\operatorname{Im} f, \star)$ est un groupe car $\operatorname{Im} f$ est un sous-groupe de H. $f : G \to \operatorname{Im} f$ est un homomorphisme.

Considérons $N = \operatorname{Ker} f$. $\bar{f} : G/\operatorname{Ker}(f) \to \operatorname{Im} f$ est surjectif car $\operatorname{Im} f = \operatorname{Im} \bar{f}$ et est injectif car $\operatorname{Ker}(\bar{f}) = \operatorname{Ker}(f)/\operatorname{Ker}(f) = \{e * \operatorname{Ker} f\} = \{e\}$. $\bar{f}$ est donc un homomorphisme bijectif, ou encore, un isomorphisme. □

1.8.2 Deuxième théorème d'isomorphisme

Théorème 1.52. *Si* K, N *sont des sous-groupes de* $(G, *)$, *alors* $K/(N \cap K) \cong (N * K)/N$, *où on définit :*

$$N * K := \left\{ n * k \text{ } \textit{t.q.} \text{ } (n, k) \in N \times K \right\}.$$

Démonstration. Montrons que $N * K$ est un sous-groupe de G, i.e. $\forall x, y \in N * K : x * y^{-1} \in N * K$. Prenons donc $(x, y) \in (N * K)^2$. Il existe $n_x, n_y \in N$ et $k_x, k_y \in K$ tels que $(x, y) = (n_x * k_x, n_y * k_y)$. On a alors :

$$x * y^{-1} = n_x * k_x * k_y^{-1} * n_y^{-1}.$$

En posant $k := k_x * k_y^{-1} \in K$ (car K est un sous-groupe), on trouve :

$$x * y^{-1} = n_x * k * n_y.$$

Par normalité de N on sait qu'il existe $n \in N$ tel que $k * n_y = n * k$. On trouve alors :

$$x * y^{-1} = n_x * n * k = (n_x * n) * k \in N * K.$$

On observe maintenant que si N est normal dans G, alors il l'est dans $N * K$.

L'application $f : K \to (N*K)/N : k \mapsto k*N$ est un homomorphisme. Son noyau est $\operatorname{Ker} f = \{k \in K \text{ t.q. } k*N = N\} = K \cap N$. $K \cap N$ est donc un sous-groupe normal de K. Par le théorème précédent, on a :

$$K/\operatorname{Ker}(f) \cong \operatorname{Im} f = (N * K)/N.$$

□

1.8.3 Troisième théorème d'isomorphisme

Théorème 1.53. *Si* K *et* N *sont deux sous-groupes normaux de* $(G, *)$ *tels que* $K \subseteq N$, *alors* N/K *est normal dans* G/K *et :*

$$\left(G/K\right) / \left(N/K\right) \cong G/N.$$

<u>Démonstration</u>. Prenons $\pi_N : G \to G/N$ l'homomorphisme canonique. On a $K \subset \operatorname{Ker} \pi = N$. Par le théorème précédent, il existe un homomorphisme $\overline{\pi} : G/K \to G/N : g * K \mapsto g * N$ surjectif de noyau $\operatorname{Ker} \overline{\pi} = N/K$.

Puisque l'on en déduit G/K normal dans N/K, en appliquant le premier théorème d'isomorphisme à $\overline{\pi}$, on trouve :

$$\left(G/K\right) / \left(N/K\right) \cong G/N.$$

$\square$