II Groupes

Sommaire

II.1 Structure de groupe 19
II.1.a Généralités 19
II.1.b Ordre d'un groupe 21
II.1.c Groupes produits 21
II.2 Sous-groupes 22
II.2.a Généralités 22
II.2.b Intersection de sous-groupes ; sous-groupe engendré 23
II.2.c Groupes cycliques 25
II.3 Morphismes de groupe 26
II.3.a Généralités 26
II.3.b Image directe et réciproque d'un sous-groupe . . . 27
II.3.c Automorphismes intérieurs 28
II.3.d Centre d'un groupe 29
II.3.e Sous-groupes distingués 30
II.4 Groupes quotient 31
II.4.a Relation d'équivalence dans les groupes 31
II.4.b Classes à gauche, à droite 32
II.4.c Indice de H dans G, thm de Lagrange 33
II.4.d Groupe quotient par un sous-groupe distingué . . . 35
II.4.e Exemple fondamental : groupes-quotients de $(\mathbb{Z}, +)$ 38
II.4.f Décomposition/factorisation canonique d'un morphisme 39
II.5 Groupes symétriques 42
II.5.a Généralités 42
II.5.b Orbite d'un élément 43
II.5.c Décomposition en cycles disjoints 44
II.5.d Transpositions 46
II.5.e Signature d'une permutation 47

II.1 Structure de groupe

II.1.a Généralités

Définition II.1.a.1 *Un **groupe (abélien)** est un monoïde (commutatif) dont tout élément est symétrisable.*

Un couple $(G, *)$ est donc un groupe ssi

(i) $*$ est une l.c.i. sur l'ensemble G $(* \in G^{G\times G})$,

(ii) $*$ est associative $(\forall x, y, z \in G : x * (y * z) = (x * y) * z)$,

(iii) $*$ admet un élément neutre $(\exists e \in G, \forall x \in G : x * e = x = e * x)$,

(iv) tout élément de G admet un symétrique pour $*$ (dans G)
$(\forall x \in G, \exists x' \in G : x * x' = e = x' * x)$;

et le groupe est abélien[1] (ou commmutatif) si de plus, $*$ est commutative.

Remarque II.1.a.2 *On préfère préciser la loi en parlant du groupe $(G, *)$, car sur un même ensemble on peut définir différents lois ; s'il n'y a aucune de confusion possible sur la l.c.i., on parle aussi simplement du groupe G.*

Remarque II.1.a.3 *Rappellons les notations multiplicatives ($x * y = x\,y$; $e = 1$; $x' = x^{-1}$; $x * \cdots * x = x^n$ $(n \in \mathbb{N}^*)$) et additives ($x * y = x + y$; $e = 0$; $x' = -x$; $x * y' = x - y$; $x * \cdots * x = n\,x$). La dernière est reservée au cas abélien, de même pour les écritures $\frac{x}{y} = x/y = x\,y'$ en notation multiplicative.*

Remarque II.1.a.4 *Dans la pratique, ne pas oublier de vérifier le (i) ; puis la commutativité (dans le cas échéant), car elle simplifie le (iii) et le (iv). Dans cette définition, le (i) et le « dans G » du (iii) paraissent tellement évidents qu'on pourrait presque les croire superflus ; dans la pratique, selon les cas étudiés, ces deux peuvent être les seuls points « intéressants » à vérifier (cf. exemples).*

Exemple II.1.a.5 *(i) $(\mathbb{Z}, +)$ est un groupe abélien. (Exercice : preuve ?)*

(ii) $\mathbb{R}^* = (\mathbb{R} \setminus \{0\}, \cdot)$ est un groupe abélien. Ici on pourrait admettre le (ii) et (iii) comme « connus » (avec $1 \neq 0$ donc $1 \in \mathbb{R}^*$), et il s'agit surtout de vérifier que $\cdot$ est une l.c.i. sur $\mathbb{R}^*$ (c'est-à-dire ?) et que le symétrique de tout élément est encore dans $\mathbb{R}^*$.)

[1] d'après Niels Hendrik Abel (5 août 1802 – 6 avril 1829), mathématicien Norvégien.

(iii) *Sur un singleton $\{a\}$ il n'y a qu'une seule façon de définir une l.c.i., on vérifie que c'est alors un groupe abélien d'élément neutre a qui est son propre symétrique.*

(iv) $(\mathbb{R},\cdot)$ *n'est* ***pas*** *un groupe, car* 0 *n'est pas inversible.*
Cependant, $(\{0\},\cdot)$ ***est*** *un groupe : il suffit de vérifier que* $\cdot$ *est une l.c.i. sur* $\{0\}$ *et d'appliquer ce qui précède. (On a en fait* $(\{0\},\cdot) = (\{0\},+)$*.)*

(v) *Soit E un ensemble non-vide. Les* ***permutations de*** *E, l'ensemble $\mathfrak{S}(E)$ des bijections de E dans E, muni de la composition $\circ$, $(\mathfrak{S}(E),\circ)$, est un groupe (exercice !), non-abélien dès que* $\operatorname{card} E > 2$.
Par contre, l'ensemble $\mathcal{A}(E;E)$ des applications de E dans lui-même, muni de $\circ$, forme un monoïde, mais pas un groupe si $\operatorname{card} E > 1$.

(vi) *Les matrices inversibles d'ordre n forment le groupe linéaire $(GL_n(\mathbb{R}),\cdot)$, non abélien ssi $n \geq 2$.*

(vii) *L'ensemble des translations dans l'espace ordinaire forme un groupe abélien : se déplacer d'un mêtre vers le nord, puis de 2m vers l'est est équivalent à faire ces déplacements dans l'ordre inverse.*

(viii) *l'ensemble des rotations autour d'un centre choisi comme origine forme un groupe non-abélien : par exemple, une rotation de 90° (dans un sens à préciser) d'axe nord-sud suivi d'une rotation de 90° autour de l'axe est-ouest ne donne pas le même résultat que les mêmes opérations faites dans l'ordre inverse.*

Exercice II.1.a.6 *Montrer que l'ensemble des nombres complexes unimodulaires, $\mathcal{U} = \{\, z \in \mathbb{C} \mid |z| = 1 \,\}$, munis de la multiplication usuelle $\cdot$ dans $\mathbb{C}$, forment un groupe (appelé le groupe unitaire* $\mathrm{U}(1)$*).*

Remarque II.1.a.7 *Le symétrique x' d'un $x \in G$ étant unique [exercice !], on dispose de la fonction $x \mapsto \operatorname{sym}(x) = x'$.*

Remarque II.1.a.8 *Dans un groupe $(G,*)$, tout élément $x \in G$ est inversible, et donc toute puissance $x^m; m \in \mathbb{Z}$ est bien définie : pour $m \in \mathbb{N}^*$, on a $x^m = x * x * \cdots * x$ (m fois), pour $m = 0$, $x^m = e$, et pour $-m \in \mathbb{N}^*$, on pose $x^m = (x^{-1})^{-m}$.*
En notation additive, ceci devient $m\,x = x + x + \cdots + x$, $0\,x = e = 0$, et $m\,x = (-m)\,(-x)$. (Attention, il convient de se convaincre en détail des significations différentes des « 0 » et des « - » utilisés ici !)

Proposition II.1.a.9 *On a alors les règles de calcul suivantes :*

$$\forall x \in G,\ \forall m,n \in \mathbb{Z} : x^m * x^n = x^{(m+n)},\ (x^m)^n = x^{m\,n}.$$

Démonstration. Exercice (par récurrence). □

II.1.b Ordre d'un groupe

Un groupe peut être fini ou infini.

Définition II.1.b.1 *On appelle* ***ordre*** *d'un groupe son cardinal, c-à-d. le nombre de ses éléments.*

Exemple II.1.b.2 *(i)* $(\{1,-1\},\cdot)$ *est un groupe d'ordre 2.*

(ii) Les racines n-ièmes de l'unité, $\left\{ e^{i\,2\,k\,\pi/n}; k=0,...,n-1 \right\}$*, muni de la multiplication de nombres complexes, forment un groupe d'ordre n.*

(iii) Les groupes $(\mathbb{Z},+)$*,* $(\mathbb{R},\cdot)$*,... sont infinis. (On ne s'intéresse ici pas au fait que* $\operatorname{card}\mathbb{Z} = \operatorname{card}\mathbb{Q} \neq \operatorname{card}\mathbb{R}$*...)*

II.1.c Groupes produits

Soient $(G_1,\cdot)$ et $(G_2,\cdot)$ deux groupes d'éléments neutres e_1 resp. e_2 ; et soit $G = G_1 \times G_2$ muni de la loi produit des lois de G_1 et G_2 (produit « par composante »), c'est-à-dire :

$$\forall (x_1,x_2),(y_1,y_2) \in G_1 \times G_2 :\ (x_1,x_2)\cdot(y_1,y_2) = (x_1\cdot y_1,\ x_2\cdot y_2)$$

Proposition II.1.c.1 *Avec les hypothèses ci-dessus, G est un groupe dont l'élément neutre est* (e_1,e_2)*.*

Démonstration. Exercice ! (Conséquence de la proposition suivante.) □

Exemple II.1.c.2 $\mathbb{R}^2 = (\mathbb{R},+)\times(\mathbb{R},+)$*, mais aussi* $(\mathbb{R},+)\times(\mathbb{R},\cdot)$ *: les deux groupes (et* a fortiori *les l.c.i.) sont en général différents.*

Définition II.1.c.3 *G est dit* ***groupe produit de*** $(G_1,\cdot)$ ***et*** $(G_2,\cdot)$*.*
Plus généralement, on définit le produit d'une famille de groupes $(G_i)_{i\in I}$*, de la façon suivante :*

Proposition II.1.c.4 *Soit* $((G_i,\cdot))_{i\in I}$ *une famille de groupes, et G le produit des ensembles sous-jacents.*
Le couple $(G,\cdot)$*, où "*$\cdot$*" est la loi-produit des lois des* G_i *:*

$$(x_i)_{i\in I}\cdot(y_i)_{i\in I} = (x_i\cdot y_i)_{i\in I}$$

est un groupe, dit groupe-produit des $(G_i,\cdot)$*.*
Le groupe produit est abélien ssi chacun des groupes donnés est abélien.

Démonstration. On vérifie failement toutes les propriétés requises en passant aux composantes : développer ceci en exercice. □

Exemple II.1.c.5 $\mathbb{R}^m = \mathbb{R} \times \cdots \times \mathbb{R}$ *est muni d'une structure de groupe additif en posant*

$$(x_1, \cdots, x_m) + (y_1, \cdots, y_m) = (x_1 + y_1, \cdots, x_m + y_m) \ .$$

II.2 Sous-groupes

II.2.a Généralités

Définition II.2.a.1 *Soit $(G, *)$ un groupe. Une partie H de G est un* ***sous-groupe*** *de G ssi H muni de la loi induite de $*$ est encore un groupe.*

Cela signifie en particulier que (la restriction à H de) $*$ doit être une loi interne sur H, donc à valeurs dans H, c'est-à-dire que H soit stable par $*$: $\forall h_1, h_2 \in H,\ h_1 * h_2 \in H$.

> La loi induite est généralement notée avec le même symbole que la loi sur G. Pour être rigoureux, il faut donc d'abord s'assurer que la restriction à $H \times H$ de $*$ est à valeurs dans H, puis composer cette restriction avec la fonction $i : G \to H;\ x \mapsto x$ pour $x \in H = D_i$ (domaine de i, qui n'est pas définie sur $G \setminus H$). Ainsi $i \circ *|_{H \times H}$ est en effet une l.c.i. sur H.

Exemple II.2.a.2 *(i) G est un sous-groupe de G ;*

(ii) $\{e\}$ (le singleton constitué de l'élément neutre) est un sous-groupe de G.

Exemple II.2.a.3 *Soit $G = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$, muni de la multiplication.*

(i) L'ensemble $\mathbb{R}_+^*$ des nombres > 0 est un sous-groupe de G.

(ii) L'ensemble $\{-1, 1\}$ est un sous-groupe de G.

(iii) G est un sous-groupe de $(\mathbb{C}^*, \cdot)$.

Exemple II.2.a.4 *$(n\,\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$.*

Exercice II.2.a.5 *Démontrer que tous les sous-groupes de $(\mathbb{Z}, +)$ sont exactement tous les $(n\,\mathbb{Z}, +)$, avec $n \in \mathbb{N}$.*

Solution : voir théorème II.4.e.1.

Théorème II.2.a.6 (caractérisation de sous–groupes) *Soit $(G, *)$ un groupe d'élément neutre e, et H une partie de G. Les assertions suivantes sont équivalentes :*

(i) H sous-groupe de G ;

(ii) H est stable pour $*$, $e \in H$, et $\forall x \in H : x^{-1} \in H$;

(iii) $H \neq \emptyset$ et $\forall x, y \in H : x * y^{-1} \in H$.

Démonstration. $(i) \Rightarrow (ii)$: H étant sous-groupe, $*$ est l.c.i., donc H stable pour $*$. $(H, *)$ étant groupe, H contient un élément neutre e' pour la loi induite $*$, qui vérifie $e'\,e' = e'$, d'où, en multipliant par $(e')^{-1}$ (dans G), $e' = e$, soit : $e \in H$. De même, tout $x \in H$ admet un symétrique $x' \in H$ tel que $x\,x' = e' = e$, d'où $x' = x^{-1}$ (dans G), et donc $x \in H \Rightarrow x^{-1} \in H$.

$(ii) \Rightarrow (iii)$: $e \in H \Rightarrow H \neq \emptyset$. Soient $x, y \in H$. Or, $y \in H \Rightarrow y^{-1} \in H$, et puisque H est stable pour le produit, on a $x \in H, y^{-1} \in H \Rightarrow x\,y^{-1} \in H$.

$(iii) \Rightarrow (i)$: Supposons $x, y \in H$. Alors $e = x\,x^{-1} \in H$, d'où $y^{-1} = e\,y^{-1} \in H$, donc $x\,y = x\,(y^{-1})^{-1} \in H$. Ainsi le produit est une l.c.i. sur H, qui est associative dans $H \subset G$ car elle l'est dans G. Etant donné $H \neq \emptyset$, il existe $x \in H$, d'après ce qui précède, on a donc $e \in H$ et cet élément neutre de G est bien sûr aussi élément neutre dans $(H, \cdot)$. D'autre part on a aussi $\forall y \in H : y^{-1} \in H$ qui est bien sûr aussi un symétrique de y dans $(H, \cdot)$. □

Remarque II.2.a.7 *Souvent on remplace $H \neq \emptyset$ par $e \in H$, ce qui est évidemment équivalent (sous réserve d'avoir l'autre condition), car $e \in H \Rightarrow H \neq \emptyset \Rightarrow \exists x \in H$ et $x \cdot x^{-1} = e \in H$).*

Remarque II.2.a.8 *Dans « $(i) \Rightarrow (ii)$ », il n'est pas évident que l'élément neutre de $(H, *|_H)$ soit l'élément neutre de G. Par exemple, la partie $\{0\}$ du monoïde $(\mathbb{R}, \cdot)$, muni de la loi induite qui est toujours la multiplication habituelle, est un groupe d'élément neutre 0, différent de l'élément neutre 1 (pourtant unique) de $(\mathbb{R}, \cdot)$. De même, 0 admet un symétrique dans $\{0\}$ muni de la loi induite, alors qu'il n'en a pas dans $(\mathbb{R}, \cdot)$.*

II.2.b Intersection de sous-groupes ; sous-groupe engendré

Cette section est encore en complète analogie avec ce qui a déjà été vu dans le cours d'algèbre linéaire concernant les sous-espaces vectoriels. Il sera instructif et donc tout à fait conseillé de comparer les théorèmes et définitions correspondantes.

Théorème II.2.b.1 *L'intersection d'une famille de sous-groupes d'un groupe G est un sous-groupe de G.*

Démonstration. Soit $(H_i)_{i\in I}$ la famille de sous-groupes et $H = \bigcap_{i\in I} H_i = \{ x \in G \mid \forall i \in I : x \in H_i \}$ leur intersection.
$\forall i \in I,\ e \in H_i \Rightarrow e \in \bigcap_{i\in I} H_i = H$.
$\forall i \in I,\ \forall (x,y) \in H_i^2,\ xy^{-1} \in H_i \Rightarrow \forall (x,y) \in H\ ,\ xy^{-1} \in H$. □

Remarque II.2.b.2 *D'après la définition de H en début de la démonstration, $H = G$ si I est vide : c'est une convention habituelle que l'intersection d'une famille vide est égale à tout « l'univers » considéré, en l'occurrence ici le groupe G en entier. Si on considère ceci comme pathologique, on peut se restreindre à une famille non-vide.*

Sous-groupe engendré par une partie

Soit A une partie d'un groupe G. Il existe des sous-groupes de G contenant A, G lui-même par exemple. L'intersection de tous ces sous-groupes est (d'après le théorème précédent), un sous-groupe de G contenant A. D'autre part, c'est le plus petit, au sens de l'inclusion : en effet, par définition de l'intersection, elle est contenue dans chaque partie considérée. Ainsi la définition suivante a bien un sens :

Définition II.2.b.3 *Soit A une partie d'un groupe G. On appelle* ***sous-groupe de*** *G* ***engendré par*** *A, et on note $\langle A \rangle$, l'intersection de tous les sous-groupes de G contenant A. Si $\langle A \rangle = G$, on dit que A est une* ***partie génératrice*** *de G. On étend de façon naturelle ces définitions aux* familles $\mathbf{a} = (a_i)_{i\in I}$ *d'éléments de G, en posant $\langle \mathbf{a} \rangle = \langle \{ a_i ; i \in I \} \rangle$.*

Remarque II.2.b.4 *Si $A = \emptyset$, on a $\langle A \rangle = \{ e \}$; c'est en effet le plus petit sous-groupe de G, et il contient bien A.*

Cherchons une caractérisation plus « constructive » du sous-groupe engendré par une partie.

Proposition II.2.b.5 *Soit A une partie (ou famille) non vide d'éléments d'un groupe G. Le sous-groupe $\langle A \rangle$ est l'ensemble des produits finis d'éléments de A et de leurs puissances :*

$$\langle A \rangle = \{ x \in G \mid \exists n \in \mathbb{N},\ \exists m_1, ..., m_n \in \mathbb{Z},\ \exists a_1, ..., a_n \in A : x = a_1^{m_1} \cdots a_n^{m_n} \}\ .$$

(La notation x^m étant définie sur page 20.)

Remarque II.2.b.6 *Ici encore, on peut permettre le cas d'une partie A vide si on admet la convention qu'un produit vide est égal à l'élément neutre e (c'est-à-dire $n = 0$, $x = \prod_{i\in\emptyset} a_i^{m_i} = e$).*

Démonstration. Il est clair que $\langle A\rangle$ doit contenir l'ensemble H des éléments de la forme $a_1^{m_1} a_{m_2}^{m_2} \cdots a_n^{m_n}$. Par ailleurs $e \in H$ d'où $H \neq \emptyset$, de plus H est stable (le produit de deux produits de cette forme en est encore un) et le symétrique d'un tel élément est $a_n^{-m_n}\, a_{n-1}^{-m_{n-1}} \cdots a_1^{-m_1} \in H'$ (en utilisant les règles II.1.a.9). En conclusion H est un sous-groupe de G contenu dans $\langle A\rangle$ et contenant A, donc $H = \langle A\rangle$. □

II.2.c Groupes cycliques

Définition II.2.c.1 *On dit qu'un groupe est* ***monogène*** *s'il est engendré par une partie réduite à un élément ; un tel élément est appelé* **générateur** *du groupe.*

Soient $(G, \cdot)$ un groupe et $a \in G$, alors $\langle a\rangle = \{\, a^n \,;\, n \in \mathbb{Z}\,\}$, resp., en notation additive pour un groupe abélien $(G, +)$, $\langle a\rangle = \{\, n\,a \,;\, n \in \mathbb{Z}\,\}$.

Il est clair que tout groupe monogène est abélien, car tout élément est de la forme $x = a^m$ et

$$a^m \cdot a^n = a^{m+n} = a^n \cdot a^m \ .$$

Exemple II.2.c.2 $(\mathbb{Z}, +) = \langle 1\rangle$ *et* $(m\mathbb{Z}, +) = \langle m\rangle$ *sont monogènes.*

Définition II.2.c.3 *(i) On appelle* **ordre d'un élément** $a \in G$ *et on note* $|a|$ *ou* $o(a)$*, le cardinal du groupe engendré par* a *:*

$$|a| = o(a) = |\,\langle a\rangle\,| = \operatorname{card}\langle a\rangle$$

(ii) On appelle groupe ***cyclique*** *tout groupe monogène fini.*

Exemple II.2.c.4 *Le groupe des n-ièmes racines de l'unité est cyclique : c'est de cet exemple (représentation graphique sur le cercle unité dans le plan complexe) que vient l'appelation des groupes cycliques.*

Proposition II.2.c.5 *On a* $|a| = \inf\left\{\, k \in \mathbb{N}^* \mid a^k = e \,\right\}$ *(avec* $\inf\emptyset = \infty$*).*

Démonstration. On suppose $K = \inf\left\{ k \in \mathbb{N}^* \mid a^k = e \right\}$ fini, et on considère $A = \left\{ a^0 = e,\ a^1 = a,\ a^2, ..., a^{K-1} \right\}$. Evidemment $A \subset \langle a \rangle$. Réciproquement, on a $\langle a \rangle \subset A$ car pour tout $a^n \in A$, on a par division eudlidienne $q \in \mathbb{Z}, r \in \mathbb{N}, r < K$ t.q. $n = K \cdot q + r$, donc $a^n = a^{K\,q}\, a^r = (a^K)^q\, a^r = e^q\, a^r = a^r \in A$.
D'autre part, évidemment $A \subset \langle a \rangle$, donc égalité. Il reste à m.q. $\operatorname{card} A = K$, c-à-d. $0 \leq \ell < m < K \Rightarrow a^\ell \neq a^m$. En effet, si on avait $a^\ell = a^m$, alors $a^{m-\ell} = e$ avec $m - \ell < K$ en contradiction avec la définition de K. □

II.3 Morphismes de groupe

II.3.a Généralités

Définition II.3.a.1 *Soient $(G, \cdot)$ et $(G', *)$ deux groupes. Un morphisme de groupes (de G dans G') est un morphisme de magmas $f : G \to G'$, c'est-à-dire une application de G dans G' telle que*

$$\forall x, y \in G : f(x \cdot y) = f(x) * f(y)\ .$$

On utilisera aussi les notions d'endo-, iso-, automorphisme, définies dans le cadre général des magmas.

Exemple II.3.a.2 *Soit $G = \prod_{i \in I} G_i$ un groupe produit. Alors chaque projection $p_i : G \to G_i,\ (g_i)_{i \in I} \mapsto g_i$, est un morphisme surjectif de groupes.*

Proposition II.3.a.3 *Soient G et G' deux groupes d'éléments neutres respectifs e et e', et f un morphisme de G dans G'. Alors :*

(i) $f(e) = e'$,

(ii) $\forall x \in G,\ f(x^{-1}) = [\, f(x)\,]^{-1}$,

(iii) $\forall x \in G, \forall n \in \mathbb{Z},\ f(x^n) = [\, f(x)\,]^n$.

Démonstration. (i) On a $f(e) = f(e\,e) = f(e)\, f(e)$. En multipliant les deux membres par l'inverse de $f(e)$:

$$\begin{aligned} f(e)^{-1}\, f(e) &= f(e)^{-1}\, f(e)\, f(e) \\ e' &= f(e) \end{aligned}$$

(ii) $\forall x \in G,\ f(x)\, f(x^{-1}) = f(x\, x^{-1}) = f(e) = e'$, d'où $f(x^{-1}) = f(x)^{-1}$.
(iii) Pour $n \in \mathbb{N}$, cela s'établit par récurrence : pour $n = 0$, il s'agit de l'égalité

$f(e) = e'$ déjà démontrée. En supposant la propriété vraie au rang n, on obtient au rang $n+1$:

$$f(x^{n+1}) = f(x^n)\, f(x) = [\, f(x)\,]^n\, f(x) = [\, f(x)\,]^{n+1} \ .$$

Pour $n < 0$, on utilise la définition de $x^n = (x^{-1})^{(-n)}$; $(-n)$ étant positif, on peut utiliser ce qui précède :

$$f((x^{-1})^{(-n)}) \overset{\text{(iii)}}{=} f((x^{-1}))^{(-n)} \overset{\text{(ii)}}{=} (f(x)^{-1})^{(-n)} = f(x)^n \ .$$

□

Remarque II.3.a.4 *Avec la notation additive (employée pour les groupes abéliens), la proposition précédente s'écrit :*

$$f(0) = 0 \ ; \quad f(-x) = -f(x) \ ; \quad f(n\,x) = n\, f(x) \ .$$

II.3.b Image directe et réciproque d'un sous-groupe

Théorème II.3.b.1 *Soit $f : G \to G'$ un morphisme de groupes, alors :*

(i) l'image par f d'un sous-groupe de G est un sous-groupe de G',

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

Démonstration. Si H est sous-groupe de G, $e \in H \Rightarrow e' = f(e) \in f(H)$ et $x', y' \in f(H) \Rightarrow \exists x, y \in H : x' = f(x),\ y' = f(y) \Rightarrow x'\,(y')^{-1} = f(x)\, f(y)^{-1} = f(x\,y^{-1}) \in f(H)$, donc $f(H)$ sous-groupe.
H' étant sous-groupe, $f(e) = e' \in H' \Rightarrow e \in f^{-1}(H')$ et $x, y \in f^{-1}(H') \iff f(x), f(y) \in H' \Rightarrow f(x\,y^{-1}) = f(x)\, f(y)^{-1} \in H' \Rightarrow x\,y^{-1} \in f^{-1}(H')$, donc $f^{-1}(H')$ sous-groupe. □

Les deux cas particuliers suivants sont les plus importants :

Définition II.3.b.2 *Soit $f : G \to G'$ un morphisme de groupes. On appelle* ***image de*** *f le sous-groupe*

$$\operatorname{im} f = f(G) = \{\, f(x);\ x \in G \,\} \ ,$$

et on appelle ***noyau de*** *f le sous-groupe*

$$\ker f = f^{-1}(\{\, e' \,\}) = \{\, x \in G \mid f(x) = e' \,\} \ ,$$

où e' est l'élément neutre de G'.

Ce sont en effet des sous-groupes car image (réciproque) des sous-groupes G et $\{ e' \}$.

Théorème II.3.b.3 *Soit $f : G \to G'$ un morphisme de groupes, alors*

$$\begin{aligned} f \text{ surjectif} &\iff \operatorname{im} f = G' \\ f \text{ injectif} &\iff \ker f = \{e\} \end{aligned}$$

Démonstration. La première partie n'est que la définition de la surjectivité. Pour la deuxième partie, on utilise $f(x) = f(y) \iff f(x)f(y)^{-1} = e \iff f(x)f(y^{-1}) = e \iff f(x\,y^{-1}) = e \iff x\,y^{-1} \in \ker f$. Si $\ker f = \{ e \}$, c'est $\iff x\,y^{-1} = e \iff x = y$ donc f injectif ; si f injectif, c'est $\iff x = y \iff x\,y^{-1} = e$ donc $\ker f = \{ e \}$. □

II.3.c Automorphismes intérieurs

Rappellons que les automorphismes d'un groupe G sont des morphismes bijectifs de G dans G, et qu'ils forment un groupe pour la composition d'application, noté $(\operatorname{Aut} G, \circ)$.

Proposition II.3.c.1 *Soit G un groupe. Pour tout $g \in G$, l'application $\varphi_g : G \to G$ définie par :*

$$\begin{aligned} \varphi_g : \ & G \to G \\ & x \mapsto g\,x\,g^{-1} \end{aligned}$$

est un automorphisme de G.

Pour en faire la démonstration, établissons d'abord le

Lemme II.3.c.2 *On a $\varphi_e = \mathrm{id}_G$, $\varphi_{gh} = \varphi_g \circ \varphi_h$, $\varphi_{g^{-1}} = \varphi_g^{-1}$.*

Démonstration. Exercice facile. (Pour la dernière propriété, utiliser les deux précédentes.) □

Dém. de la Proposition. Montrons que φ_g est un endomorphisme bijectif de G.
(i) φ_g est un morphisme car : $\forall (x, y) \in G$,

$$\begin{aligned} \varphi_g(x \cdot y) &= g \cdot x \cdot y \cdot g^{-1} \\ &= g \cdot x \cdot g^{-1} \cdot g \cdot y \cdot g^{-1} \\ &= \varphi_g(x) \cdot \varphi_g(y) \end{aligned}$$

(ii) En utilisant le Lemme, tout φ_a admet l'application réciproque $\varphi_a^{-1} = \varphi_{a^{-1}}$, telle que

$$\varphi_a \circ \varphi_{a^{-1}} = \mathrm{id}_G = \varphi_{a^{-1}} \circ \varphi_a \ ,$$

c'est donc une bijection. □

Définition II.3.c.3 *L'application φ_g est appelée automorphisme intérieur de G défini par g ;*
l'ensemble des automorphismes intérieurs de G se note $\mathrm{Int}(G)$.

Proposition II.3.c.4 $\mathrm{Int}(G)$ *est un sous-groupe de* $\mathrm{Aut}\, G$*, ensemble des automorphismes de G.*

Démonstration. Soit l'application Φ de $(G, \cdot)$ dans $(\mathrm{Aut}\, G, \circ)$ définie par :

$$\begin{aligned} \Phi : (G, \cdot) &\longrightarrow (\mathrm{Aut}\, G, \circ) \\ a &\longmapsto \varphi_a \end{aligned}$$

D'après le Lemme, Φ est un morphisme. $\mathrm{Int}(G)$, image de G par Φ, est donc un sous-groupe de $\mathrm{Aut}\, G$ □

II.3.d Centre d'un groupe

Définition II.3.d.1 *On appelle centre d'un groupe G et on note $Z(G)$, l'ensemble des éléments de G qui permutent avec chacun des éléments de G.*

Proposition II.3.d.2 *Le noyau de Φ est le sous-groupe $Z(G)$ de G.*

Démonstration.

$$\begin{aligned} \ker \Phi &= \{\ a \in G \mid \varphi_a = \mathrm{id}\ \} \\ &= \{\ a \in G \mid \forall x \in G,\ axa^{-1} = x\ \} \\ &= \{\ a \in G \mid \forall x \in G,\ ax = xa\ \} \\ &= Z(G) \end{aligned}$$

L'ensemble $Z(G)$, noyau d'un morphisme de G dans $\mathrm{Aut}\, G$, est un sous-groupe de G. □

II.3.e Sous-groupes distingués

Définition II.3.e.1 *On appelle sous-groupe distingué (ou : invariant) d'un groupe G, tout sous-groupe H de G qui est stable par tout automorphisme intérieur de G, i.e. :*

$$\forall a \in G,\ \ a\,H\,a^{-1} \subset H \ \text{, soit :}\ \ \forall a \in G, \forall h \in H,\ \ a\,h\,a^{-1} \in H,$$

on note ceci $H \lhd G$.

Exemple II.3.e.2 *(i) On a toujours $\{\,e\,\} \lhd G$ et $G \lhd G$.*
(ii) On a aussi $Z(G) \lhd G$.

Démonstration. $\forall y \in G,\ \forall x \in Z(G) : x\,y = y\,x$ par définition du centre, c'est-à-dire $\forall y \in G,\ \forall x \in Z(G) : y\,x\,y^{-1} = x \in Z(G)$. □

Remarque II.3.e.3 *Attention, la relation $\lhd$ n'est pas transitive ! En effet, $K \lhd H$ et $H \lhd G$ n'implique pas $K \lhd G$.*

Proposition II.3.e.4 *Soit G un groupe et H un sous-groupe de G, les assertions suivantes sont équivalentes :*
(i) H est distingué dans G,
(ii) $\forall x \in G,\ \ xH \subset Hx$,
(iii) $\forall x \in G,\ \ xH = Hx$.

Démonstration. (i) $\Rightarrow$ (ii) :

$$\begin{aligned}\forall x \in G, \forall y \in H,\ \ xyx^{-1} \in H &\Rightarrow \forall x \in G, \forall y \in H, \exists y_1 \in H\ \ xyx^{-1} = y_1\\ &\Rightarrow \forall x \in G, \forall y \in H, \exists y_1 \in H\ \ xy = y_1 x\\ &\Rightarrow \forall x \in G,\ xH \subset Hx\end{aligned}$$

$(ii) \Rightarrow (iii)$ Soit $x \in G$, il suffit de m.q. $Hx \subset xH \iff \forall h \in H : h\,x \in xH$.
Or $x^{-1} \in G$, donc $x^{-1}\,H \subset H\,x^{-1}$, c'est-à-dire $\forall h \in H : \exists h' \in H :$

$$x^{-1}\,h = h'\,x^{-1} \iff h = x\,h'\,x^{-1} \Rightarrow H \subset xHx^{-1} \Rightarrow Hx \subset xH.$$

$(iii) \Rightarrow (i) : \forall x \in G,\ \forall h \in H,\ \exists h' \in H :\ x\,h = h'\,x$
$\Rightarrow \forall x \in G,\ \forall h \in H,\ \exists h' \in H :\ x\,h\,x^{-1} = h' \in H$
$\Rightarrow H \lhd G.$ □

Théorème II.3.e.5 *Soit $f : G \to G'$ morphisme de groupes.*
Alors $H' \lhd G' \Rightarrow f^{-1}(H') \lhd G$, et $H \lhd G \Rightarrow f(H) \lhd f(G)$.

Démonstration. On a $g\,f^{-1}(H')\,g^{-1} \subset f^{-1}(f(g))\,f^{-1}(H')\,f^{-1}(f(g^{-1})) \subset f^{-1}(f(g)\,H'\,f(g)^{-1}) \subset f^{-1}(H')$, où l'on a utilisé que $f^{-1}(A)f^{-1}(B) \subset f^{-1}(A\,B)$ (car $f(\,f^{-1}(A)\,f^{-1}(B)\,) \subset f(f^{-1}(A))\,f(f^{-1}(B)) \subset A\,B$) et que $H' \lhd G' \supset f(G)$. D'autre part, $f(g)\,f(H)\,f(g)^{-1} = f(g\,H\,g^{-1}) \subset f(H)$. □

Remarque II.3.e.6 (Contre-exemple) *Attention, on ne peut remplacer $f(H) \lhd f(G)$ par $f(H) \lhd G'$ (comme pour l'image réciproque) : par exemple,*

$$f : (\mathbb{R}, +) \to (\mathrm{GL}_2(\mathbb{R}), \cdot)\ , \quad x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

est un morphisme, et pour tout $H \lhd \mathbb{R}$: $f(H) \lhd f(\mathbb{R})$ (groupe abélien car image d'un groupe abélien), mais $f(H) \lhd \mathrm{GL}_2(\mathbb{R})$ seulement pour $H = \{\,0\,\}$: pour $x \neq 0$, on a par exemple

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \notin f(\mathbb{R})$$

(Exercice : montrer que $\forall M \in \mathrm{GL}_2(\mathbb{R}) : M\,f(x)\,M^{-1} = I + x\,M'$, en explicitant la matrice M' em fonction de M.)

Corollaire II.3.e.7 (fondamental)
Si $f : G \to G'$ est morphisme de groupes, $\ker f \lhd G$.

En effet, $\ker f$ est image réciproque de $\{\,e'\,\} \lhd G'$.

II.4 Groupes quotient

II.4.a Relation d'équivalence dans les groupes

Définition II.4.a.1 *Soit $\Re$ une relation d'équivalence sur un magma $(G, \cdot)$ (par exemple un groupe). On dit que $\Re$ est compatible à gauche (resp. à droite) avec la loi de G ssi*

$$\forall x, y, z \in G,\ x\,\Re\,y \Rightarrow zx\,\Re\,zy \quad \textit{(resp. } xz\,\Re\,yz\ \textit{).}$$

Théorème II.4.a.2 *Soit $(G, \cdot)$ un groupe. Toute relation d'équivalence sur G compatible à gauche (resp. à droite) avec la loi de G est de la forme*

$$\forall x, y \in G : x\,\Re\,y \iff x^{-1} \cdot y \in H\ (\iff y \in x \cdot H = \underset{\Re}{cl}(x)\ )\quad (*)$$

$$\textit{(resp. } \forall x, y \in G : x\,\Re\,y \iff y \cdot x^{-1} \in H \iff y \in H \cdot x = \underset{\Re}{cl}(x)\ )\ ,$$

où H est un sous-groupe de G.
Réciproquement toute relation de ce type est une relation d'équivalence compatible à gauche (resp. à droite) avec la loi de G.

Démonstration. Soit $\Re$ une relation d'équivalence sur G, compatible à gauche avec $\cdot$. Soit $H = c\ell_{\Re}(e)$ la classe de l'élément neutre de G.
Montrons qu'on a $(*)$: la compatibilité de $\Re$ à gauche permet d'écrire

$$x \,\Re\, y \iff x^{-1} \cdot x \,\Re\, x^{-1} \cdot y \iff e \,\Re\, x^{-1} \cdot y \iff x^{-1} \cdot y \in H \ .$$

Montrons que H est un sous-groupe de G : par définition de H, on a $e \in H$.
Soient $x, y \in H$, donc $e \,\Re\, x \wedge y \,\Re\, e$. La compatibilité (à gauche) permet de multiplier la seconde relation par $x \cdot y^{-1}$, d'où $e \,\Re\, x \wedge x \,\Re\, x \cdot y^{-1}$; d'où, par transitivité, $e \,\Re\, x \cdot y^{-1}$, soit : $x \cdot y^{-1} \in H$.
Réciproquement, soit H un sous-groupe de G, et $\Re$ définie par $(*)$. On a pour tout $x \in H$, $x^{-1}x = e \in H$, d'où la réflexivité.
$\Re$ est symétrique, car si $x^{-1}y \in H$, H étant un groupe, $(x^{-1}y)^{-1} = y^{-1}x \in H$.
Elle est transitive car si $x^{-1}y \in H$ et $y^{-1}z \in H$, il en est de même du produit $(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$.
Le même raisonnement d'applique au cas de la compatibilité à droite. □

II.4.b Classes à gauche, à droite

Définition II.4.b.1 *Soit G un groupe, H un sous-groupe, a un élément de G. Les ensembles*

$$a \cdot H = \{\, a \cdot h; h \in H \,\} \quad \text{et} \quad H \cdot a = \{\, h \cdot a;\ h \in H \,\}$$

sont dits classes à gauche et à droite de a, suivant H. Ce sont les classes d'équivalence de a pour les relations d'équivalence $\Re_g$ et $\Re_d$ définies par :

$$\forall x, y \in G : x \,\Re_g\, y \iff x^{-1} \cdot y \in H \iff y \in x \cdot H = \underset{\Re_g}{c\ell}(x) \iff x \in y \cdot H \ .$$

$$\forall x, y \in G : x \,\Re_d\, y \iff y \cdot x^{-1} \in H \iff y \in H \cdot x = \underset{\Re_d}{c\ell}(x) \iff x \in H \cdot y \ .$$

(La dernière équivalence s'obtient de $y = x \cdot h \iff x = y \cdot h^{-1} \in y \cdot H$.)

Proposition II.4.b.2 *Avec les hypothèses de la définition précédente, l'ensemble des inverses des éléments de $a \cdot H$ n'est autre que $H \cdot a^{-1}$. Il en résulte une bijection de $G \,/\, \Re_g$ sur $G \,/\, \Re_d$ en associant à toute classe à gauche la classe à droite constituée par les inverses de ses éléments.*

Démonstration. L'inverse d'un élément de la forme $a \cdot h \in a \cdot H$ est $h^{-1} \cdot a^{-1} \in H \cdot a^{-1}$, H étant sous-groupe. Or l'application $h \mapsto h^{-1}$ est une bijection (elle est sa propre réciproque), donc surjective et ainsi $\{ x^{-1} \ ; \ x \in a \cdot H \} = H \cdot a^{-1}$. De même, $x \mapsto x^{-1}$ est une bijection de G dans G, et

$$x \, \Re_g y \iff x^{-1} \cdot y \in H \iff y^{-1} \cdot x \in H \iff x^{-1} \, \Re_d y^{-1}$$

Ainsi, l'ensemble des inverses d'une classe à gauche est dans une même classe à droite et réciproquement :

$$\begin{aligned} G/\Re_g = \{ x \cdot H \ ; \ x \in G \} &\overset{\bar{x} \mapsto \bar{x}^{-1}}{\longleftrightarrow} \{ H \cdot x^{-1} \ ; \ x \in G \} \\ &= \{ H \cdot x \ ; \ x \in G \} = G/\Re_d \end{aligned}$$

□

II.4.c Indice de H dans G, thm de Lagrange

Etant donnée la bijection $x \mapsto x^{-1}$ entre les classes à droite et les classes à gauche, si l'un des ensembles $G \,/\, \Re_g$ ou $G \,/\, \Re_d$ est fini, il en est de même pour l'autre et ils ont même cardinal.

Définition II.4.c.1 *Le cardinal commun de $G \,/\, \Re_g$ et $G \,/\, \Re_d$ est appelé* ***indice*** *de H dans G et noté $[G : H]$.*

Théorème II.4.c.2 (de Lagrange) *Si G est fini alors pour tout sous-groupe H de G, on a*

$$|G| = [G : H] \cdot |H| \ .$$

En particulier, l'ordre et l'indice des sous-groupes de G divisent l'ordre de G.

Démonstration. $\forall a \in G$, l'application $\left\{ \begin{array}{ccc} H & \mapsto & a \cdot H \\ x & \mapsto & a \cdot x \end{array} \right.$ est bijective, sa réciproque étant $y \mapsto a^{-1} \cdot y$. D'où

$$\forall x \in G : \mathrm{card}(x \cdot H) = \mathrm{card}(H) \ .$$

Ces classes sont au nombre de $[G : H]$ et réalisent une partition de G (Prop. I.2.f.2), il en résulte le théorème. □

Corollaire II.4.c.3 *Dans un groupe G d'ordre premier les seuls sous-groupes sont G et $\{e\}$.*

Exercice II.4.c.4 *Existe-t-il un sous-groupe d'ordre* 7 *d'un groupe d'ordre* 225 *?*

Corollaire II.4.c.5 *Si G est d'ordre fini, l'ordre de tout élément divise l'ordre de G.*

Démonstration. Par définition $o(x) = \text{card}\,\langle x\rangle$ et c'est un sous-groupe □

Proposition II.4.c.6 *Tout groupe fini d'ordre premier est cyclique.*

Démonstration. $|G|$ étant premier, G a au moins deux éléments.
Soit donc $a \in G$, $a \neq e$, on a alors $o(a)$ qui divise $|G|$ avec $o(a) \geq 2$. $|G|$ étant premier, $|G| = o(a)$. D'où $G = \langle a\rangle$. □

Exemple II.4.c.7 *On appelle* ***groupe dihédral*** D_n*, le groupe des isométries planes laissant globalement invariant un polygone régulier à n côtés.*
Pour $n = 3$, D_3 est un groupe non abélien d'ordre 6.

$$\begin{array}{ccc} & C & \\ & / \quad o \quad \backslash & \\ A & --- & B \end{array}$$

$$D_3 = \{\ \sigma_0, \sigma_1,\ \sigma_2, , \tau_1, \tau_2, \tau_3, \}$$

où les σ_i et les τ_i sont définis comme suit :

$$\begin{array}{cc} \sigma_0 = \text{id} & \tau_1 = sym(AO) \\ \sigma_1 = rot(O, 2\pi/3) & \tau_2 = sym(BO) \\ \sigma_2 = rot(O, 4\pi/3) & \tau_3 = sym(CO) \end{array}$$

On vérifie que $H = \{\ \sigma_0, \sigma_1, \sigma_2\}$ est un sous-groupe d'ordre 3 *de D_3.*

$\circ$	σ_0	σ_1	σ_2
σ_0	σ_0	σ_1	σ_2
σ_1	σ_1	σ_2	σ_0
σ_2	σ_2	σ_0	σ_1

Les classes à gauche de H sont :

$$\begin{array}{cc} \sigma_0 H = \{\ \sigma_0, \sigma_1, \sigma_2\ \} & \tau_1 H = \{\ \tau_1, \tau_2, \tau_3\ \} \\ \sigma_1 H = \{\ \sigma_1, \sigma_2, \sigma_0\ \} & \tau_2 H = \{\ \tau_2, \tau_3, \tau_1\ \} \\ \sigma_2 H = \{\ \sigma_2, \sigma_0, \sigma_1\ \} & \tau_3 H = \{\ \tau_3, \tau_1, \tau_2\ \} \end{array}$$

On a donc

$$G \,/\, \Re_g = \{\ \overline{\sigma_0}, \overline{\tau_1}\ \}\ ,$$

d'où

$$[G : H] = 2\ .$$

On retrouve le résultat du théorème de Lagrange :

$$|G| = [G : H] \times |H| = 2 \times 3 = 6\ .$$

II.4.d Groupe quotient par un sous-groupe distingué

Si l'on veut que l'ensemble quotient d'un groupe G par une relation d'équivalence hérite encore structure de groupe, il faut que la relation soit compatible (ce qui signifie compatible à la fois à gauche et à droite) avec la loi de G.

Proposition II.4.d.1 *Soit $\Re$ une relation d'équivalence définie sur un groupe G. Si $\Re$ est compatible avec la loi de G, alors il existe un sous-groupe H **distingué** dans G tel que :*

$$\forall x, y \in G,\ \ x \,\Re\, y \iff xy^{-1} \in H.$$

*Réciproquement, si H est un sous-groupe **distingué** de G, la relation définie ci-dessus est une relation d'équivalence compatible avec la loi de G. On dit que H et $\Re$ sont **associés**.*

Démonstration. On a déjà vu que la compatibilité à droite implique que $H = c\ell(e)$ est un sous-groupe et que $x \,\Re\, y \iff y \in H\,x = c\ell_{\Re}(x)$. De même, la compatibilité à gauche donne $c\ell_{\Re}(x) = x\,H$; ainsi, pour tout $x \in G : x\,H = H\,x$, soit : $H \lhd G$.
De même pour la réciproque : la relation définie ainsi est une relation d'équivalence compatible à droite ($x \Re y \iff xy^{-1} \in H \iff x \in Hy \iff y \in Hx$ comme avant) mais puisque $\forall x : Hx = xH$, elle est aussi compatible à gauche avec la loi de G. □

Exercice II.4.d.2 *Démontrer la proposition directement sans utiliser les résultats du paragraphe précédent.*

Solution : Soit $\Re$ une relation d'équivalence définie sur un groupe G telle que : $\forall x, y, z \in G$,

$$\begin{cases} x \,\Re\, y \Rightarrow zx \,\Re\, zy & \text{(i)} \\ x \,\Re\, y \Rightarrow xz \,\Re\, yz & \text{(ii)} \end{cases}\ .$$

Alors en prenant $z = y^{-1}$ dans (ii), on obtient :

$$\begin{aligned} x \,\Re\, y &\Rightarrow xy^{-1} \,\Re\, e \\ x \,\Re\, y &\Rightarrow xy^{-1} \in \bar{e} = H \end{aligned}$$

Inversement,

$$\begin{aligned} xy^{-1} &\in H \Rightarrow xy^{-1} \,\Re\, e \\ xy^{-1} &\in H \Rightarrow xy^{-1} y \Re\, y \quad \text{(compat. à droite)} \\ xy^{-1} &\in H \Rightarrow x \Re\, y. \end{aligned}$$

On a donc $\forall x, y \in G,\ \ x \,\Re\, y \Leftrightarrow xy^{-1} \in H$.
Montrons que $H = c\ell(e)$ est un sous-groupe distingué dans G si $\Re$ est compatible à droite et à gauche.
$\forall x \in G$, $\forall h \in H$,

$$\begin{aligned} h \Re e &\Rightarrow xh \Re x \quad \text{(compat. à gauche)} \\ xh \Re x &\Rightarrow xhx^{-1} \Re x x^{-1} \quad \text{(compat. à droite)} \\ \text{c'est-à-dire} \quad xh \Re x &\Rightarrow xhx^{-1} \Re e \end{aligned}$$

On a donc le résultat :

$$\forall x \in G, \forall h \in H, \quad xhx^{-1} \in H \quad (H \text{ sous-groupe distingué de } G).$$

Réciproquement, on suppose que la relation $\Re$ est définie par :

$$\forall x, y \in G,\ \ x \,\Re\, y \iff xy^{-1} \in H. \quad (\text{avec } H \lhd G)$$

Montrons que $\Re$ est une relation d'equivalence.
a)

$$e \in H \Rightarrow \forall x \in G,\ \ xx^{-1} \in H \Leftrightarrow \forall x \in G,\ \ x \,\Re\, x \quad \text{(réflexivité)}$$

b) $\forall x, y \in G$,

$$\begin{aligned} x \,\Re\, y \Leftrightarrow xy^{-1} \in H &\Rightarrow (xy^{-1})^{-1} = yx^{-1} \in H \ \ (\text{ car } H \text{ sous-groupe}) \\ &\Rightarrow yx^{-1} \in H \Rightarrow y \Re x \quad \text{(symétrie)} \end{aligned}$$

c) $\forall x, y, z \in G$,

$$\begin{aligned} x \,\Re\, y \wedge y \,\Re\, z &\Rightarrow xy^{-1} \in H \wedge yz^{-1} \in H \\ &\Rightarrow xy^{-1} yz^{-1} = xz^{-1} \in H \ \ (\text{car } H \text{ stable}) \\ &\Rightarrow x \,\Re\, z \quad \text{(transitivité)} \end{aligned}$$

Montrons que $\Re$ est compatible avec la loi de G :
$\forall x, y, z \in G$,

$$\begin{aligned} x \,\Re\, y &\iff xy^{-1} \in H \\ &\Rightarrow xzz^{-1}y^{-1} \in H \iff (xz)(yz)^{-1} \in H \\ &\Rightarrow xz \,\Re\, yz \quad \text{(compatibilité à droite)} \\ x \,\Re\, y &\iff xy^{-1} \in H \\ &\Rightarrow z(xy^{-1})z^{-1} \in H \quad \text{(car } H \text{ distingué)} \\ &\Rightarrow (zx)(zy)^{-1} \in H \\ &\Rightarrow zx \,\Re\, zy \quad \text{(compatibilité à gauche)} \end{aligned}$$

Définition II.4.d.3 *Soit G un groupe et H un sous-groupe distingué de G. On note G/H l'ensemble-quotient de G par la relation d'équivalence associée à H, et on l'appelle le* ***groupe-quotient*** *de G par H.*

On a donc $G/H = \{\, \bar{x} \;;\; x \in G \,\}$ avec $\bar{x} = x\,H = H\,x$.

Cette définition est justifiée par la proposition suivante :

Proposition II.4.d.4 *Soit $H \lhd G$. Alors la loi induite sur $\mathcal{P}(G)$ par celle de G,*

$$X \cdot Y = \{\, x \cdot y \;;\; x \in X,\, y \in Y \,\}$$

définit une l.c.i. sur G/H appelée la ***loi quotient****, pour laquelle*

$$\bar{x} \cdot \bar{y} = \overline{x \cdot y} \;;$$

muni de cette loi, l'ensemble G/H est un groupe.

Démonstration. Montrons que la loi induite est une l.c.i. bien définie sur G/H. Puisque $H \lhd G$, on peut écrire tout élément $X \in G/H$ indifféremment comme $X = \bar{x} = x\,H = H\,x$ pour un certain $x \in G$. On a

$$\forall \bar{x}, \bar{y} \in G/H : \bar{x}\,\bar{y} = x\,H\,y\,H = x\,y\,HH = x\,y\,H = \overline{x\,y} \;,$$

car $H\,y = y\,H$ et $H\,H = H$ (inclusion dans les 2 sens immédiate à vérifier). Ainsi c'est bien une l.c.i. sur G/H, et il est immédiat à vérifier que $\bar{e} = H$ est élément neutre :

$$\forall \bar{x} \in G/H : \bar{e}\,\bar{x} = \overline{e\,x} = \bar{x} = \overline{x\,e} = \bar{x}\,\bar{e} \;.$$

L'associativité est aussi conséquence immédiate de celle de la loi de G. Finalement, pour tout $\bar{x} \in G/H$, $\overline{x^{-1}}$ est son symétrique :

$$\bar{x}\,\overline{x^{-1}} = \overline{x\,x^{-1}} = \bar{e} \;.$$

(Notons que, en conséquence de la première vérification ci-dessus, c'est indépendant du choix du représentant x de $\bar{x}$; on obtient le même ensemble en prenant la classe de l'inverse d'un $x' \in \bar{x}$ quelconque. □

Remarque II.4.d.5 *Evidemment, si G est abélien, G/H est abélien. La réciproque est fausse en général ; pour le voir il suffit de considérer $H = G$, auquel cas $G/H = \{ G \} = \{ \bar{e} \}$, qui est bien sûr abélien quel que soit G.*

Exercice II.4.d.6 *Montrer que* ***surjection canonique*** $\varphi : G \to G/H;\ x \mapsto \bar{x}$ *est un morphisme de groupes.*

II.4.e Exemple fondamental : groupes-quotients de $(\mathbb{Z}, +)$

Théorème II.4.e.1 *Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\,\mathbb{Z}$, $n \in \mathbb{N}$.*

Démonstration. voir exercice II.4.e.2. □

Exercice II.4.e.2 *Montrer que les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\,\mathbb{Z}$, $n \in \mathbb{N}$.*

Solution : *D'abord, $n\mathbb{Z}$ est sous-groupe car $0 \in n\,\mathbb{Z}$ et si $n \cdot k$, $n \cdot k' \in n\mathbb{Z}$, alors $n \cdot k + (-n \cdot k) = n \cdot (k - k') \in n\,\mathbb{Z}$. Réciproquement, soit H un sous-groupe de $(\mathbb{Z}, +)$. Si $H = \{0\}$, alors on a $H = 0 \cdot \mathbb{Z} = n\,\mathbb{Z}$ pour $n = 0$.*
Sinon, soit $n = \min \{ x \in H \mid x > 0 \}$ le plus petit entier positif non nul de H. (Si H contient un élément non nul, il contient aussi son opposé et donc au moins un élément strictement positif).
Montrons que $H = n\,\mathbb{Z}$: D'une part, $n\mathbb{Z} \subset H$ car H sous-groupe (donc $0 \in H$ et $n \in H \Rightarrow -n \in H,\ n + n = 2\,n \in H,\ -2\,n \in H, \ldots$ donc $k\,n \in H$ pour tout $k \in \mathbb{Z}$). D'autre part, $H \subset n\mathbb{Z}$ car tout $x \in H$ s'écrit $x = q \cdot n + r$ avec $q, r \in \mathbb{Z}$ et $0 < r < n$ (reste de la division euclidienne de x par n), et on a $r = x - n \cdot q \in H$ (car sous-groupe et $x,\ q \cdot n \in H$). Or $0 \leq r < n$, la déf. de n implique donc $r = 0$, d'où $x \in n\mathbb{Z}$. Ainsi finalement $H = n\mathbb{Z}$.

Théorème II.4.e.3 *Pour tout $n \in \mathbb{N}$, le groupe quotient $\mathbb{Z}_n := \mathbb{Z}\,/\,n\mathbb{Z}$ est appelé groupe des entiers naturels modulo n. Il est monogène. Si $n = 0$, il est isomorphe à $\mathbb{Z}$; si $n > 0$, il est d'ordre n (et donc cyclique).*

Démonstration. Soit $\varphi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ k \mapsto k + n\mathbb{Z}$ la surjection canonique.
On a alors :

$$\forall k \in \mathbb{Z} : \varphi_n(\bar{k}) = \varphi_n(k.\bar{1}) = k\varphi_n(\bar{1}).$$

(C'est en effet un morphisme de groupes.)
Ainsi, $\varphi_n(1)$ est générateur de $\mathbb{Z}/n\mathbb{Z}$, qui est donc un groupe monogène.
· Si $n = 0$, la relation d'équivalence selon le groupe $0\mathbb{Z}$ est l'égalité :

$$x - y \in 0\,\mathbb{Z} = \{ 0 \} \iff x - y = 0 \iff x = y\ ,$$

D'où

$$\forall x \in \mathbb{Z} : \bar{x} = \{x\} \text{ et } \mathbb{Z}/\{0\} \text{ est isomorphe à } \mathbb{Z}.$$

· Soit $n \geq 1$. Tout $X \in \mathbb{Z}\,/\,n\mathbb{Z}$ est l'image par φ_n d'un et un seul élément de l'ensemble $\{\,0, 1, \ldots, n-1\,\}$. Cet élément est le reste commun de la division par n des entiers qui constituent la classe X.
La restriction de φ_n à $\{\,0, 1, \ldots, n-1\,\}$ est ainsi une bijection ;
$\mathbb{Z}/\,n\mathbb{Z}$ a pour cardinal n et peut s'écrire $\left\{\,\bar{0}, \bar{1}, \ldots, \overline{n-1}\,\right\}$, en notant $\bar{x}$ pour $\varphi_n(x)$. □

Exercice II.4.e.4 *Déterminer la table d'addition de* $\mathbb{Z}\,/\,5\mathbb{Z}$.

Solution : Table d'addition de $\mathbb{Z}\,/\,5\mathbb{Z}$:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

II.4.f Décomposition/factorisation canonique d'un morphisme

Théorème II.4.f.1 *Un morphisme de groupes $f : G \to G'$ peut se factoriser de manière canonique, en :*

(i) un épimorphisme (morphisme surjectif) p de G sur $G/\ker f$,

(ii) un isomorphisme $\tilde{f}$ de $G/\ker f$ sur $\operatorname{im} f$,

(iii) un morphime injectif i de $\operatorname{im} f$ dans G',

d'après le schéma

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ p\ \downarrow & & \uparrow\ i \\ G/\ker f & \xrightarrow[\ \tilde{f}\ ]{} & \operatorname{im} f \end{array} \quad .$$

Démonstration. Tout d'abord, $\ker f$ est un sous-groupe distingué de G (d'après II.3.e.7), on peut donc considérer le groupe quotient de G par $\ker f$, sous-groupe distingué associé à la relation d'équivalence $\Re$ définie par :

$$x \,\Re\, y \iff x \cdot y^{-1} \in \ker f \ .$$

On définit alors la projection p (« surjection canonique »)

$$\begin{aligned} p : G &\to G/\ker f \\ x &\mapsto \bar{x} = x \cdot \ker f \end{aligned}$$

(par définition, $G/\ker f = \operatorname{im} p$), et l'application

$$\begin{aligned} \tilde{f} : G/\ker f &\to \operatorname{im} f \\ \bar{x} &\mapsto f(x) \ . \end{aligned}$$

En effet, $\tilde{f}$ est bien définie car si $x' \in \bar{x}$, alors

$$\begin{aligned} x' \cdot x^{-1} \in \ker f &\iff f(x' \cdot x^{-1}) = e' \text{ (él. neutre de } G') \\ &\iff f(x') \cdot f(x^{-1}) = e' \\ &\iff f(x') = f(x) \end{aligned}$$

Or, $\tilde{f}$ est un morphisme car $\forall \bar{x}, \bar{y} \in G/\ker f$,

$$\tilde{f}(\bar{x} \cdot \bar{y}) = \tilde{f}(\overline{x\,y}) = f(x\,y) = f(x) \cdot f(y) = \tilde{f}(\bar{x}) \cdot \tilde{f}(\bar{y})$$

D'autre part, $\tilde{f}$ est injectif (d'après II.3.b.3), car $\forall \bar{x} \in G/\ker f$,

$$\tilde{f}(\bar{x}) = e' \iff f(x) = e' \iff x \in \ker f \iff \bar{x} = \bar{e} \ ,$$

et $\tilde{f}$ est surjectif car

$$\forall y \in \operatorname{im} f, \ \exists x \in G : y = f(x) = \tilde{f}(\bar{x}) \in \operatorname{im} \tilde{f} \ .$$

Enfin, i est l'injection canonique de $\operatorname{im} f$ dans G' :

$$\begin{aligned} i : \operatorname{im} f &\to G' \\ y &\mapsto y \ . \end{aligned}$$

(L'injection canonique de $A \subset B$ dans B est la restriction de l'identité sur B à A, $i = \mathrm{id}_B\,|_A$; elle « ne fait rien » à part changer l'ensemble d'arrivée.)

On a donc $\forall x \in G$,

$$i \circ \tilde{f} \circ p(x) = i \circ \tilde{f}(\bar{x}) = i \circ f(x) = f(x) \ ,$$

c'est-à-dire

$$f = i \circ \tilde{f} \circ p \ .$$

□

Proposition II.4.f.2 *Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}_n$.*

Démonstration. Il suffit d'appliquer le Theorème à $f : \mathbb{Z} \to G = \langle a \rangle \ ; \ k \mapsto a^k$, a étant un générateur quelconque de G. C'est un morphisme ($f(k+\ell) = ...$) donc $\ker f$ est sous-groupe de $\mathbb{Z}$ dc de la forme $\ker f = m\mathbb{Z}$, $m \in \mathbb{N}$ (Thm II.4.e.1) ; d'après le Théorème on a donc l'isomorphisme $\tilde{f} : \mathbb{Z}/\ker f = \mathbb{Z}/m\mathbb{Z} \to \operatorname{im} f = \left\{ a^k ; k \in \mathbb{Z} \right\} = G, \bar{k} \mapsto a^k$. Ainsi $\mathbb{Z}_m \simeq G$ et ces deux étant donc de même cardinal on a $m = |G|$. □

Exemple II.4.f.3 *Pour $m \in \mathbb{N}^*$, $U_m = \{ z \in \mathbb{C} \mid z^m = 1 \}$ (ensemble des racines m-ièmes de l'unité) est un sous-groupe cyclique de $(\mathbb{C}^*, \cdot)$ ($e^{i\,2\pi/m}$ étant générateur), de cardinal m donc isomorphe à $\mathbb{Z}\,/\,m\mathbb{Z}$.*