Théorie des groupes

Table des matières

1. Groupes

Définition 1.1 (Groupe)**.** Soit G un ensemble et $\star : G \times G \to G$ une loi de composition interne. On dit que le couple $(G, \star)$ forme un *groupe* s'il vérifie les propriétes suivantes
(1) la loi $\star$ est associative, $\forall x, y, z \in G, (x \star y) \star z = x \star (y \star z)$,
(2) il existe un neutre $e_G \in G, \forall x \in G, x \star e_G = e_G \star x = x$,
(3) existence d'un inverse, $\forall x \in G, \exists x^{-1} \in G, x \star x^{-1} = x^{-1} \star x = e_G$.

Exemple 1.2. Le couple $(\mathbb{Z}, +)$ est un groupe, le neutre est 0 et pour $n \in \mathbb{Z}$ un inverse est $-n$. Le couple $(\mathbb{R}, \cdot)$ n'est pas un groupe, 0 n'admet pas d'inverses.

Proposition 1.3. Soit $(G, \star)$ un groupe. Alors
(1) le neutre e_G est unique,
(2) soit $x \in G$, alors son inverse x^{-1} est unique.

Démonstration.
(1) Soit $e \in G$ vérifiant $\forall x \in G, x \star e = e \star x = x$. Alors
$$e = e \star e_G = e_G.$$
(2) Soit $y \in G$ vérifiant $x \star y = y \star x = e_G$. Alors
$$y = e_G \star y = \left(x^{-1} \star x\right) \star y = x^{-1} \star (x \star y) = x^{-1} \star e_G = x^{-1}.$$

□

Définition 1.4 (Abélien)**.** Soit $(G, \star)$ un groupe. On dit qu'il est *commutatif* ou *abélien* s'il vérifie
$$\forall x, y \in G, x \star y = y \star x.$$

Exemple 1.5. Le groupe $(\mathbb{Z}, +)$ est commutatif.

Définition 1.6 (Monoïde)**.** On appelle *monoïde* un ensemble non vide G avec une opération $* : GxG \to G$ qui satisfait seulement l'associativité et l'existence d'un élément neutre. (sans inverse).

Définition 1.7 (Ordre)**.** Soit $(G, \star)$ un groupe. On appelle *ordre* de G le cardinal de G, si G est un ensemble fini on dit que G est d'*ordre fini*, sinon on dit que G est d'*ordre infini*.

Remarque 1.8. Soit $(G, \star)$ un groupe d'ordre fini. On note $G = \{e_G, g_1, ..., g_n\}$, alors on peut donner sa table de multiplication

$\star$	e_G	g_1	$\cdots$	g_j	$\cdots$	g_n
e_G	e_G	g_1	$\cdots$	g_j	$\cdots$	g_n
g_1	g_1	$g_1 \star g_1$	$\cdots$	$g_1 \star g_j$	$\cdots$	$g_1 \star g_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\iddots$	$\vdots$
g_i	g_i	$g_i \star g_1$	$\cdots$	$g_i \star g_j$	$\cdots$	$g_i \star g_n$
$\vdots$	$\vdots$	$\vdots$	$\iddots$	$\vdots$	$\ddots$	$\vdots$
g_n	g_n	$g_n \star g_1$	$\cdots$	$g_n \star g_j$	$\cdots$	$g_n \star g_n$

où chaque ligne et chaque colonne contient tous les éléments de G.

Définition 1.9 (Groupe produit)**.** Soit $(G, *)$, $(H, \cdot)$ deux groupes. Le *groupe produit* $(GxH, \star)$ est définit par: $\star : (GxH)x(GxH) \to (GxH)$; $(g_1,h_1,g_2,h_2) \mapsto (g_1,h_1) \star (g_2,h_2) \coloneqq (g_1 * g_2, h_1 \cdot h_2)$.

Proposition 1.10. Soit $(G, *)$, $(H, \cdot)$ deux groupes. Le *groupe produit* $(GxH, \star)$ est un groupe.

Démonstration.
(1) L'associativité s'ensuit de l'associativité de $*$ et $\cdot$.
(2) L'élement neutre est (e_G, e_H): $(g, h) \star (e_G, e_H) = (g * e_G, h \cdot e_H) = (g, h) = (e_G, e_H) \star (g, h)$.
(3) L'inverse de $(g, h) \in GxH$ est $\left(g^{-1}, h^{-1}\right)$.

□

Notation 1.11. Soit $(G, \star)$ un groupe. Lorsqu'il ne peut pas y avoir de confusions, on notera
- $e \coloneqq e_G$ pour le neutre,
- $\forall x, y \in G, xy \coloneqq x \star y$ pour la loi $\star$,
- $\forall x \in G, \forall n \in \mathbb{Z}, \text{si } n > 0, x^n \coloneqq \underbrace{x \star \ldots \star x}_{\text{n fois}}, \text{si } n = 0, x^0 \coloneqq e, \text{si } n < 0, x^n \coloneqq x^{-1} \star \ldots \star x^{-1}$.

2. Sous-groupes.

2.1. Définitions.

Définition 2.1 (Sous-groupes)**.** Soit $(G, \star)$ un groupe et H un sous-ensemble de G. On dit que H est un *sous-groupe* de G, noté $H < G$, s'il vérifie les propriétés suivantes :
(1) le neutre appartient à H, $e \in H$,
(2) H est stable par $\star$, $\forall x, y \in H, x \star y \in H$,
(3) H est stable par inverse, $\forall x \in H, x^{-1} \in H$.

Notation 2.2. Soit H un groupe, G un sous-groupe de H. On note $H < G$.

Définition 2.3 (Distingué)**.** Soit $(G, \star)$ un groupe et H un sous-groupe de G. On dit que H est *distingué* ou *normal*, noté $H \lhd G$, s'il vérifie

$$\forall g \in G, \forall h \in H, g \star h \star g^{-1} \in H.$$

Proposition 2.4. Soit $(G, \star)$ un groupe et H un sous-ensemble de G. Alors H est un sous-groupe de G si et seulement s'il vérifie les propriétés suivantes:
(1) le neutre appartient à H, $e \in H$,
(2) H est stable par $\star$ et par inverse, $\forall x, y \in H, x \star y^{-1} \in H$.

Démonstration.
$\Rightarrow$: Supposons que H est un sous-groupe de G. Alors
(1) le neutre appartient à H,
(2) soit $x, y \in H$, alors $y^{-1} \in H$ et $x \star y^{-1} \in H$.

$\Leftarrow$: Supposons que H vérifie les deux propriétés. Alors
(1) le neutre appartient à H,
(3) soit $x \in H$, alors $x^{-1} = e \star x^{-1} \in H$,
(2) soit $x, y \in H$, alors $y^{-1} \in H$ et $x \star y = x \star \left(y^{-1}\right)^{-1} \in H$.

□

Proposition 2.5. Soit $(G, \star)$ un groupe et H un sous-ensemble de G. Alors H est un sous-groupe de G si et seulement s'il vérifie les propriétés suivantes
(1) H est stable par $\star$, $\forall x, y \in H, x \star y \in H$,
(2) le couple $(H, \star)$ forme un groupe.

Démonstration.
$\Rightarrow$: Supposons que H est un sous-groupe de G. Alors
(1) H est stable par $\star$, $\forall x, y \in H, x \star y \in H$,
(2) On considère le couple $(H, \star)$,
   (a) soit $x, y, z \in H$, alors $x, y, z \in G$ donc $(x \star y) \star z = x \star (y \star z)$,
   (b) on pose $e_H = e_G$, alors $e_H \in H$,
   (c) soit $x \in H$, alors $x^{-1} \in H$.
   Donc $(H, \star)$ forme un groupe.

$\Leftarrow$: Supposons que H vérifie les deux propriétés. Alors
(1) soit $x \in H$, alors $x \in G$ et $x \star e_G = x = x \star e_H$, en multipliant à gauche par $x^{-1} \in G$, on obtient donc $e_G = e_H \in H$.
(2) H est stable par $\star$,
(3) soit $x \in H$, alors $x^{-1} \in H$. □

Proposition 2.6. Soit $(G, \star)$ un groupe et H_1, H_2 deux sous-groupes de G. Alors $H_1 \cap H_2$ est un sous-groupe de G.

Démonstration.
(1) $e \in H_1$ et $e \in H_2$, donc $e \in H_1 \cap H_2$,
(2) soit $x, y \in H_1 \cap H_2$, alors $x, y \in H_1$, puisque H_1 est un sous-groupe de G on a $x \star y^{-1} \in H_1$, de la même manière on a $x \star y^{-1} \in H_2$, donc $x \star y^{-1} \in H_1 \cap H_2$.

Donc d'après la Proposition 2.4, $H_1 \cap H_2$ est un sous-groupe de G. □

2.2. Générateurs

Définition 2.7 (Engendré par)**.** Soit $(G, \star)$ un groupe et S un sous-ensemble non-vide de G. On appelle *sous-groupe engendré par S*, noté $\langle S \rangle$, le plus petit sous-groupe de G contenant S.

Notation 2.8. Si $S = \{x_1, ..., x_n\}$, on note $\langle x_1, ..., x_n \rangle \coloneqq \langle S \rangle$.

Proposition 2.9. Soit $(G, \star)$ un groupe et S un sous-ensemble non-vide de G. Alors

$$\langle S \rangle = \bigcap_{\substack{H < G \\ S \subset H}} H$$

ou encore $\langle S \rangle = \left\{ x_1 \star ... \star x_n \mid n \in \mathbb{N} \setminus \{0\}, \forall i \in \{1, ..., n\}, x_i \in S \text{ ou } x_i^{-1} \in S \right\}$.

Démonstration. Notons $F \coloneqq \{H < G \mid S \subset H\}$ et $H_S \coloneqq \bigcap_{H \in F} H$. Puisque $G \in F$, l'intersection est non-vide, et d'après la Proposition 2.6, H_S est un sous-groupe de G. De plus H_S contient évidemment S. Enfin si H_0 est un sous-groupe de G contenant S, on a $H_0 \in F$, donc $H_S \subset H_0$. Donc H_S est bien le plus petit sous-groupe de G contenant S.

Notons $K_S \coloneqq \left\{ x_1 \star ... \star x_n \mid n \in \mathbb{N} \setminus \{0\}, \forall i \in \{1, ..., n\}, x_i \in S \text{ ou } x_i^{-1} \in S \right\}$. On remarque que K_S est stable par multiplication, par inverse et contient le neutre de G, donc d'après la Proposition 2.4, K_S est un sous-groupe de G. De plus G_S contient S, donc $\langle S \rangle \subset G_S$. Réciproquement, puisque $\langle S \rangle$ est un groupe, on en déduit que $\forall x \in K_S, x \in \langle S \rangle$, donc $K_S \subset \langle S \rangle$. Par double inclusion $\langle S \rangle = K_S$. □

Définition 2.10 (Système de générateurs)**.** Soit $(G, \star)$ un groupe et S un sous-ensemble de G.
Si $G = \langle S \rangle$, on dit que G est *engendré* par S et on appelle S un *système de générateurs* pour G.

Définition 2.11 (Finiment engendré)**.** Soit $(G, \star)$ un groupe et S un sous-ensemble fini de G. Si $G = \langle S \rangle$, on dit que G est *finiment engendré*.

Définition 2.12 (Monogène)**.** Soit $(G, \star)$ un groupe et S un sous-ensemble de G.
Si $G = \langle S \rangle$ et que S ne contient qu'un élément, on dit que G est *monogène*, si de plus G est fini, on dit que G est *cyclique*.

Exemples 2.13.
1. Soit $(G, \star)$ un groupe, G a au moins un système de générateur $S := G$.
2. On considère le groupe $(\mathbb{Z}, +)$, il est engendré par $\mathbb{N}$, et par $\{1\}$, donc il est monogène.
3. On considère le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, il est engendré par $\left\{\overline{1}\right\}$ et est fini, donc il est cyclique.

Proposition 2.14. On considère le groupe $(\mathbb{Z}, +)$, alors :
(1) $\forall n \in \mathbb{Z}, \langle n \rangle = n\mathbb{Z}$,
(2) soit H un sous-groupe de $(\mathbb{Z}, +)$, alors il existe $n \in \mathbb{Z}$ tel que $H = n\mathbb{Z}$,
(3) soit $a, b \in \mathbb{Z}$ avec $b \neq 0$, alors b divise a si et seulement si $\langle a \rangle \subset \langle b \rangle$,
(4) soit $a, b \in \mathbb{Z} \setminus \{0\}$, alors $\langle a, b \rangle = \text{pgcd}(a, b)\mathbb{Z}$ et $\langle a \rangle \cap \langle b \rangle = \text{ppcm}(a, b)\mathbb{Z}$.

Démonstration.
(1) Soit $n \in \mathbb{Z}$, alors $\langle n \rangle = \{k \cdot n \mid k \in \mathbb{Z}\} = n\mathbb{Z}$.
(2)
- Si $H = \{0\}$, alors $H = 0\mathbb{Z}$.
- Sinon, $H \setminus \{0\}$ est non-vide, on prend n le plus petit entier strictement positif de H.
  Puisque $n \in H$, on a $n\mathbb{Z} \subset H$. Réciproquement, soit $m \in H$, par division euclidienne il existe $q, r \in \mathbb{Z}$ tels que $m = nq + r$ et $0 \leq r < n$, puisque $r = m - nq \in H$, on a nécessairement $r = 0$, d'où $m \in n\mathbb{Z}$, donc $H \subset n\mathbb{Z}$. Donc $H = n\mathbb{Z}$.

(3) On sait que b divise a si et seulement il existe $q \in \mathbb{Z}$ tel que $a = bq$ si et seulement $a \in \langle b \rangle$ si et seulement si $\langle a \rangle \subset \langle b \rangle$.
(4)
- D'après le point (2), il existe $d \in \mathbb{Z}$ tel que $\langle a, b \rangle = d\mathbb{Z}$. On a $a \in a\mathbb{Z} \subset \langle a, b \rangle = d\mathbb{Z}$ et de la même manière $b \in d\mathbb{Z}$, donc $d \mid a$ et $d \mid b$. Soit $d' \in \mathbb{Z}$ tel que $d' \mid a$ et $d' \mid b$. Alors $a, b \in d'\mathbb{Z}$, on en déduit $d\mathbb{Z} = \langle a, b \rangle \subset d'\mathbb{Z}$, donc $d' \mid d$. Donc $\langle a, b \rangle = \text{pgcd}(a, b)\mathbb{Z}$.
- D'après le point (2), il existe $m \in \mathbb{Z}$ tel que $\langle a \rangle \cap \langle b \rangle = m\mathbb{Z}$. On a $m \in m\mathbb{Z} \subset \langle a \rangle$ et de la même manière $m \in \langle b \rangle$, donc $a \mid m$ et $b \mid m$. Soit $m' \in \mathbb{Z}$ tel que $a \mid m'$ et $b \mid m'$. Alors $m' \in \langle a \rangle$ et $m' \in \langle b \rangle$, on en déduit $m' \in \langle a \rangle \cap \langle b \rangle = m\mathbb{Z}$, donc $m \mid m'$. Donc $\langle a \rangle \cap \langle b \rangle = \text{ppcm}(a, b)\mathbb{Z}$. □

2.3. Ordre d'un élément

Définition 2.15 (Ordre)**.** Soit $(G, \star)$ un groupe et $x \in G$. On appelle *ordre de* x, noté $\text{ord}(x)$, le cardinal du sous-groupe engendré par $\{x\}$.

Proposition 2.16. Soit $(G, \star)$ un groupe et $x \in G$. Alors

$$\text{ord}(x) = \inf\left(\left\{d \in \mathbb{N} \setminus \{0\} \mid x^d = e\right\}\right)$$

de plus si $n \in \mathbb{Z}$ vérifie $x^n = e$, alors $\text{ord}(x)$ divise n.

Démonstration.
- Si $\text{ord}(x) = +\infty$, supposons par l'absurde qu'il existe $d \in \mathbb{N} \setminus \{0\}$ tel que $x^d = e$.
  Alors $\langle x \rangle = \left\{e, x, \ldots, x^{d-1}\right\}$ est fini, d'où une contradiction.
- Sinon $\text{ord}(x) \in \mathbb{N} \setminus \{0\}$.
  Puisque $\langle x \rangle$ est fini, il existe $m, n \in \mathbb{N} \setminus \{0\}$ tels que $n < m$ et $x^m = x^n$, alors $x^{m-n} = e$, donc l'ensemble $\left\{d \in \mathbb{N} \setminus \{0\} \mid x^d = e\right\}$ est non-vide. Posons $d := \inf\left(\left\{d \in \mathbb{N} \setminus \{0\} \mid x^d = e\right\}\right)$, puisque $x^d = e$, on obtient $\langle x \rangle = \left\{e, x, \ldots, x^{d-1}\right\}$, donc $\text{ord}(x) = \left|\left\{e, x, \ldots, x^{d-1}\right\}\right| = d$.
- Soit $n \in \mathbb{Z}$ tel que $x^n = e$. Par division euclidienne il existe $q, r \in \mathbb{Z}$ tels que $n = \text{ord}(x)q + r$ et $0 \leq r < d$, alors $x^r = x^{n - \text{ord}(x)q} = x^n \star x^{\text{ord}(x)^{-q}} = e$, par définition de $\text{ord}(x)$ on a nécessairement $r = 0$, donc $\text{ord}(x)$ divise n. □

3. Morphismes de groupes

3.1. Définitions

Définition 3.1 (Morphisme)**.** Soit $(G, \star)$ et $(H, \cdot)$ deux groupes. Une application $\varphi : G \to H$ est un *morphisme de groupes* si elle vérifie

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

- Si $H = G$, on dit que φ est un *endomorphisme*.
- Si φ est une bijection, on dit que φ est un *isomorphisme*, et G et H sont *isomorphes*, noté $G \simeq H$.

Proposition 3.2. Soit $(G, \star)$ et $(H, \cdot)$ deux groupes, et $\varphi : G \to H$ un morphisme de groupes.
(1) le neutre est envoyé sur le neutre, $\varphi(e_G) = e_H$,
(2) l'inverse est envoyé sur l'inverse, $\forall x \in G, \varphi\left(x^{-1}\right) = \varphi(x)^{-1}$.

Démonstration.
(1) On a $\varphi(e_G) = \varphi(e_G \star e_G) = \varphi(e_G) \cdot \varphi(e_G)$, donc $(\varphi(e_G))^{-1} \cdot \varphi(e_G) = \left(\varphi\left(e_g\right)\right)^{-1} \cdot \varphi(e_G) \cdot \varphi(e_G)$ $\Rightarrow e_H = \varphi(e_G)$,
(2) soit $x \in G$, alors $e_H = \varphi(e_G) = \varphi\left(x \star x^{-1}\right) = \varphi(x) \cdot \varphi\left(x^{-1}\right)$, donc $\varphi\left(x^{-1}\right) = \varphi(x)^{-1}$.

□

Proposition 3.3. Soit $(G, \star)$ et $(H, \cdot)$ deux groupes, et $\varphi : G \to H$ un isomorphisme. Alors sa réciproque, noté φ^{-1}, est un isomorphisme.

Démonstration. Soit $x, y \in H$. Puisque φ est un morphisme de groupes on a

$$\varphi\left(\varphi^{-1}(x \cdot y)\right) = x \cdot y = \varphi\left(\varphi^{-1}(x)\right) \cdot \varphi\left(\varphi^{-1}(y)\right) = \varphi\left(\varphi^{-1}(x) \star \varphi^{-1}(y)\right)$$

et par injectivité de φ, on obtient $\varphi^{-1}(x \cdot y) = \varphi^{-1}(x) \star \varphi^{-1}(y)$, donc φ^{-1} est un morphisme. □

Proposition 3.4. Soit $(G, \star)$, $(H, \cdot)$ et $(K, \blacksquare)$ trois groupes, et $\varphi : G \to H$ et $\psi : H \to K$ deux morphismes de groupes. Alors $\psi \circ \varphi$ est un morphisme de groupes.

Démonstration. Soit $x, y \in G$. Alors

$$\begin{aligned}(\psi \circ \varphi)(x \star y) &= \psi(\varphi(x \star y)) \\ &= \psi(\varphi(x) \cdot \varphi(y)) \\ &= \psi(\varphi(x)) \blacksquare \psi(\varphi(y)) \\ &= (\psi \circ \varphi)(x) \blacksquare (\psi \circ \varphi)(y)\end{aligned}$$

donc $\psi \circ \varphi$ est un morphisme de groupes. □

Proposition 3.5. Soit $(G, \star)$ et $(H, \cdot)$ deux groupes isomorphes. Alors
(1) G et H ont le même ordre,
(2) G est abélien si et seulement si H est abélien,
(3) G est monogène si et seulement si H est monogène,
(4) $\forall \varphi : G \to H$ isomorphisme, $\forall x \in G, \operatorname{ord}(x) = \operatorname{ord}(\varphi(x))$.

Démonstration. Soit $\varphi : G \to H$ un isomorphisme.
(1) G et H sont en bijection, donc $|G| = |H|$.
(2) $\Rightarrow$: Supposons que G est abélien. Soit $x, y \in H$, puisque φ est un isomorphisme

$$\varphi^{-1}(x) \star \varphi^{-1}(y) = \varphi^{-1}(y) \star \varphi^{-1}(x) \Rightarrow x \cdot y = y \cdot x$$

donc H est abélien.

$\Leftarrow$: On montre la réciproque de la même manière.

(3) $\Rightarrow$: Supposons que G est monogène. Alors il existe $x \in G$ tel que $G = \langle x \rangle$, ainsi

$$H = \varphi(G) = \varphi(\langle x \rangle) = \langle \varphi(x) \rangle$$

donc H est monogène.

$\Rightarrow$: On montre la réciproque de la même manière.

(4) Soit $x \in G$, alors $\forall d \in \mathbb{N} \setminus \{0\}, x^d = e_G \Leftrightarrow \varphi(x)^d = e_H$, donc $\text{ord}(x) = \text{ord}(\varphi(x))$.

□

3.2. Image et noyau

Définition 3.6. Soit $(G, \star)$ et $(H, \cdot)$ deux groupes, et $\varphi : G \to H$ un morphisme de groupes.

- On appelle *image* de φ l'ensemble $\text{im}(\varphi) \coloneqq \varphi(G)$.
- On appelle *noyau* de φ l'ensemble $\ker(\varphi) \coloneqq \varphi^{-1}(e_H)$.

Proposition 3.7. Soit $(G, \star)$ et $(H, \cdot)$ deux groupes, et $\varphi : G \to H$ un morphisme de groupes. Alors $\text{im}(\varphi)$ est un sous-groupe de H et $\ker(\varphi)$ est un sous-groupe de G. Plus généralement si G' est un sous groupe de G et H' un sous-groupe de H, alors $\varphi(G')$ est un sous-groupe de H et $\varphi^{-1}(H')$ est un sous-groupe de G.

Démonstration. On considère $\varphi(G')$,

(1) $e_H = \varphi(e_G)$, donc $e_H \in \varphi(G')$,

(2) soit $x, y \in \varphi(G')$, il existe $u, v \in G'$ tels que $x = \varphi(u)$ et $y = \varphi(v)$, alors

$$x \cdot y^{-1} = \varphi(u) \cdot \varphi(y)^{-1} = \varphi\left(u \star v^{-1}\right)$$

puisque G' est un sous-groupe de G, on a $u \star v^{-1} \in G'$, donc $x \cdot y^{-1} \in \varphi(G')$.

D'après la Proposition 2.4, $\varphi(G')$ est un sous-groupe de H.

On considère $\varphi^{-1}(H')$,

(1) $e_G = \varphi(e_H)$, donc $e_G \in \varphi^{-1}(H')$.

(2) soit $x, y \in \varphi^{-1}(H')$, alors $\varphi(x), \varphi(y) \in H'$ et

$$x \star y^{-1} \in \varphi^{-1}(H') \Leftrightarrow \varphi\left(x \star y^{-1}\right) \in H' \Leftrightarrow \varphi(x) \cdot \varphi(y)^{-1} \in H'$$

puisque H' est un sous-groupe de H, on a $\varphi(x) \cdot \varphi(y)^{-1} \in H'$, donc $x \star y^{-1} \in \varphi^{-1}(H')$.

D'après la Proposition 2.4, $\varphi^{-1}(H')$ est un sous-groupe de G. □

Proposition 3.8. Soit $(G, \star)$ et $(H, \cdot)$ deux groupes, et $\varphi : G \to H$ un morphisme de groupes.

- φ est surjectif si et seulement si $\text{im}(\varphi) = H$.
- φ est injectif si et seulement si $\ker(\varphi) = \{e_G\}$.

Démonstration.

- Par définition.
- $\Rightarrow$: Supposons que φ est injectif. Soit $x \in \ker(\varphi)$, alors $\varphi(x) = e_H$, donc $x = e_G$.
  $\Leftarrow$: Supposons que $\ker(\varphi) = \{e_G\}$. Soit $x, y \in G$ tels que $f(x) = f(y)$, puisque φ est un morphisme on a $f\left(x \star y^{-1}\right) = e_H$, et $\ker(\varphi) = e_G$ d'où $x \star y^{-1} = e_G$, donc $x = y$ et φ est injectif.

□

Exemples 3.9.

1. $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)\ ;\ n \mapsto 2n$. φ est un morphisme: $\varphi(n+m) = 2(n+m) = \varphi(n) + \varphi(m)$. $\ker(\varphi) = \{0\}$, et $\mathrm{Im}(\varphi) = 2\mathbb{Z} =< 2 >\neq \mathbb{Z}$ donc φ est injective. mais pas surjective.
2. Soit $n \in \mathbb{N} \setminus \{0\}, \varphi : (\mathbb{Z}, +) \to (\mathbb{Z}/_{n\mathbb{Z}}, +)$.
   φ est un morphisme car $\varphi(x+y) = \overline{x+y} = \overline{x} + \overline{y} = \varphi(x) + \varphi(y)$. $\mathrm{im}(\varphi) = \mathbb{Z}/_{n\mathbb{Z}}$,et $\ker(\varphi) = n\mathbb{Z}$ donc φ est surjective mais pas injective.
3. $\det : \left(\mathrm{GL}_{n(\mathbb{C})}, .\right) \to (\mathbb{C} \setminus \{0\}, \cdot) x : A$. det est un morphisme car $\det(AB) = \det A \det B$ $\mathrm{im}(\varphi) = \mathbb{C} \setminus \{0\}$, pas injectif car $\det \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \det \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = 1$. donc det n'est pas injective.
4. $\mathrm{Tr} : (M_n(\mathbb{C}), +) \to (\mathbb{C}, +)\ ;\ A \mapsto \mathrm{Tr}\, A$. Tr est un mophisme de groupes : $\mathrm{Tr}(A+B) = \mathrm{Tr}\, A + \mathrm{Tr}\, B$. $\mathrm{im}(\mathrm{Tr}) = \mathbb{C}, \ker(\mathrm{Tr}) = \{M \in M_n(\mathbb{C}) \mid \mathrm{Tr}(M) = 0\} \neq \left\{O_{M_n}\right\}$ donc Tr est surjective mais pas injective.
5. $\exp : (\mathbb{R}, +) \to (\mathbb{R} \setminus \{0\}, \cdot)\ ;\ x \mapsto \exp(x)$
6. $\exp : (\mathbb{C}, +) \to (\mathbb{C} \setminus \{0\}, \cdot)\ ;\ z = a + ib \mapsto \exp(z)$. $\mathrm{im}(\exp) = \mathbb{C}^+$, $\ker(\exp) = 2\pi i\mathbb{Z}$

4. Groupes symétriques

4.1. Définitions

Définition 4.1 (Groupe symétrique)**.** Soit $n \in \mathbb{N}$. On appelle *groupe symétrique*, noté S_n, l'ensemble de toutes les bijections de $\{1, ..., n\}$ dans lui-même muni de la composition.

- On appelle *permutations* les éléments de S_n.
- Soit σ une permutation, on la note

$$\sigma \coloneqq \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}.$$

Définition 4.2 (Support)**.** Soit $\sigma \in S_n$ une permutation. On appelle *support* de σ l'ensemble

$$\mathrm{supp}(\sigma) \coloneqq \{i \in \{1, ..., n\} \mid \sigma(i) \neq i\}.$$

Lemme 4.3. Soit $\sigma_1, \sigma_2 \in S_n$ deux permutations. Si σ_1 et σ_2 sont de supports disjoints, alors elles commutent.

Démonstration. Soit $i \in \{1, ..., n\}$. Alors

- si $i \notin \mathrm{supp}(\sigma_1) \cup \mathrm{supp}(\sigma_2)$, on a $(\sigma_1 \circ \sigma_2)(i) = (\sigma_2 \circ \sigma_1)(i) = i$,
- si $i \in \mathrm{supp}(\sigma_1)$, alors $i \notin \mathrm{supp}(\sigma_2)$ et $\sigma_1(i) \notin \mathrm{supp}(\sigma_2)$, et on a $(\sigma_1 \circ \sigma_2)(i) = (\sigma_2 \circ \sigma_1)(i) = i$,
- si $i \in \mathrm{supp}(\sigma_2)$, de la même manière $(\sigma_1 \circ \sigma_2)(i) = (\sigma_2 \circ \sigma_1)(i) = i$.

Donc σ_1 et σ_2 commutent. □

4.2. k-cycles.

Définition 4.4 (k-cycle / Transposition)**.** Soit $a_1, ..., a_k \in \{1, ..., n\}$ deux à deux distincts. On appelle *k-cycle*, noté $(a_1, ..., a_k)$, la permutation définie par

$$\forall i \in \{1, ..., n\}, (a_1, ..., a_k)(i) \coloneqq \begin{cases} a_{j+1} & \text{si } j \in \{1, ..., k-1\} \text{ avec } i = a_j \\ a_1 & \text{si } i = a_k \\ i & \text{sinon} \end{cases}$$

- On dit que k est sa *longueur*.
- On appelle *transposition* un 2-cycle.

Proposition 4.5. Soit $(a_1, ..., a_k) \in S_n$ un k-cycle. Alors l'inverse de $(a_1, ..., a_k)$ est $(a_k, ..., a_1)$.

Démonstration. Soit $i \in \{1, ..., n\}$. Alors
- s'il existe $j \in \{1, ..., k-1\}$ tel que $i = a_j$, on a
$$(a_k, ..., a_1)\big((a_1, ..., a_k)(a_j)\big) = (a_k, ..., a_1)(a_{j+1}) = a_j = i,$$
- si $i = a_k$, on a
$$(a_k, ..., a_1)((a_1, ..., a_k)(a_k)) = (a_k, ..., a_1)(a_1) = a_k = i,$$
- sinon on a
$$(a_k, ..., a_1)((a_1, ..., a_k)(i)) = (a_k, ..., a_1)(i) = i.$$

Donc $(a_k, ..., a_1)$ est l'inverse de $(a_1, ..., a_k)$. □

Proposition 4.6. Soit $(a_1, ..., a_k) \in S_n$ un k-cycle. Alors on peut l'écrire comme une composition de $k-1$ transpositions.

Démonstration. On écrit $(a_1, ..., a_k) = (a_1, a_2) \circ ... \circ (a_{k-1}, a_k)$. □

4.3. Permutations conjuguées

Définition 4.7 (Conjuguée)**.** Soit $\sigma_1, \sigma_2 \in S_n$ deux permutations. On dit que σ_1 et σ_2 sont conjuguées s'il existe $\tau \in S_n$ telle que $\sigma_1 = \tau \circ \sigma_2 \circ \tau^{-1}$.

Lemme 4.8. Soit $(a_1, ..., a_k) \in S_n$ un k-cycle. Alors
$$\forall \sigma \in S_n, \sigma \circ (a_1, ..., a_k) \circ \sigma^{-1} = (\sigma(a_1), ..., \sigma(a_k))$$

Démonstration. Soit $\sigma \in S_n$. Soit $i \in \{1, ..., n\}$, alors
- s'il existe $j \in \{1, ..., k-1\}$ tel que $i = \sigma(a_j)$, alors $\sigma^{-1}(i) = a_j$ et on a
$$\sigma\big((a_1, ..., a_k)(\sigma^{-1}(i))\big) = \sigma\big((a_1, ..., a_k)(a_j)\big) = \sigma(a_{j+1}),$$
- si $i = \sigma(a_k)$, alors $\sigma^{-1}(i) = a_k$ et on a
$$\sigma\big((a_1, ..., a_k)(\sigma^{-1}(i))\big) = \sigma((a_1, ..., a_k)(a_k)) = \sigma(a_1),$$
- sinon on a
$$\sigma\big((a_1, ..., a_k)(\sigma^{-1}(i))\big) = \sigma(\sigma^{-1}(i)) = i.$$

Donc $\sigma \circ (a_1, ..., a_k) \circ \sigma^{-1} = (\sigma(a_1), ..., \sigma(a_k))$. □

Corollaire 4.9. Soit $(a_1, ..., a_k) \in S_n$ un k-cycle. Alors il est conjugué à $(1, ..., k)$.

Démonstration. On prend $\sigma \in S_n$ telle que $\forall i \in \{1, ..., k\}, \sigma(a_i) = i$. □

Théorème 4.10. Soit $\sigma \in S_n$ une permutation. On peut écrire σ comme une composition de cycles à supports disjoints $\tau_1, ..., \tau_m \in S_n$. De plus cette écriture est unique à l'ordre des cycles près, et leurs longueurs $k_1, ..., k_m$ vérifient $\sum_{l=1}^{m} k_l = n$.

Démonstration. On raisonne par récurrence sur le cardinal de $\mathrm{supp}(\sigma)$.
- Pour $|\mathrm{supp}(\sigma)| = 0$, on a $\sigma = \mathrm{id}$.
- Pour $|\mathrm{supp}(\sigma)| > 0$, supposons que la propriété soit vérifiée pour toute permutation dont le cardinal du support est inférieur.
  Soit $i \in \mathrm{supp}(\sigma)$, puisque $\sigma \in S_n$, il existe $p \in \{1, ..., n\}$ minimal tel que $\sigma^p(i) = i$, alors on pose $\tau_1 = \big(i, \sigma(i), ..., \sigma^{p-1}(i)\big)$. Alors τ_1 agit comme σ sur l'ensemble $\big\{i, \sigma(i), ..., \sigma^{p-1}(i)\big\}$, donc on

a $|\text{supp}(\tau_1^{-1} \circ \sigma)| < |\text{supp}(\sigma)|$. Par hypothèse de récurrence, on peut écrire $\tau_1^{-1} \circ \sigma$ comme une composition de cycles à supports disjoints $\tau_2, ..., \tau_m \in S_n$, et $\sigma = \tau_1 \circ \tau_2 \circ ... \circ \tau_m$.

Soit $i \in \{1, ..., n\}$, puisques les supports sont disjoints, i se trouve dans le support d'un seul des cycles, d'où l'unicité de l'écriture et $\sum_{l=1}^{m} k_l = n$. □

Définition 4.11 (Type)**.** Soit $\sigma \in S_n$ et $\tau_1, ..., \tau_m \in S_n$ la décomposition de σ en cycles à supports disjoints, ordonnés par longueur $k_1 \leq ... \leq k_m$. On appelle $(k_1, ..., k_m)$ le *type* de σ.

Théorème 4.12. Soit $\sigma_1, \sigma_2 \in S_n$ deux permutations. Alors σ_1 et σ_2 sont conjuguées si et seulement si elles ont le même type.

Démonstration.
$\Rightarrow$: Supposons que σ_1 et σ_2 sont conjuguées. D'après le Lemme 4.8, σ_1 et σ_2 ont le même type.
$\Leftarrow$: Supposons que σ_1 et σ_2 ont le même type $(k_1, ..., k_m)$.
D'après le Corollaire 4.9, σ_1 et σ_2 sont conjuguées à

$$\sigma_3 := (1, ..., k_1) \circ (k_1 + 1, ..., k_1 + k_2) \circ ... \circ (k_1 + ... + k_{m-1} + 1, ..., k_m)$$

donc il existe $\tau_1, \tau_2 \in S_n$ telles que $\sigma_1 = \tau_1 \circ \sigma_3 \circ \tau_1^{-1}$ et $\sigma_2 = \tau_2 \circ \sigma_3 \circ \tau_2^{-1}$.
Alors $\sigma_1 = \left(\tau_1 \circ \tau_2^{-1}\right) \circ \sigma_2 \circ \left(\tau_2 \circ \tau_1^{-1}\right)$, donc σ_1 et σ_2 sont conjuguées. □

Corollaire 4.13. Soit $\sigma \in S_n$ une permutation. On peut écrire σ comme une composition de transpositions.

Démonstration. On peut écrire σ comme une composition de cycles à supports disjoints, et chaque cycle comme une composition de transpositions. □

Corollaire 4.14.
(1) Les k-cycles pour $k \in \{2, ..., n\}$ engendrent S_n.
(2) $S_n = \langle (i, j) \mid 1 \leq i \leq j \leq n \rangle$.
(3) $S_n = \langle (i, i+1) \mid 1 \leq i \leq n-1 \rangle$.

Démonstration.
(1)
(2) On a montré que $(a_1, ..., a_n) = (a_1, a_2)(a_2, a_3)...(a_{n-1}a_n)$. □

4.4. Signature d'une permutation.

Définition 4.15 (Signature)**.** Soit $\sigma \in S_n$ une permutation. On appelle *signature* de σ le nombre rationnel

$$\text{sign}(\sigma) := \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Exemple 4.16. On calcule la signature de la transposition $(1, 2)$

$$\begin{aligned}
\text{sign}((1,2)) &= \frac{\sigma(2) - \sigma(1)}{2 - i} \cdot \prod_{2 < j \leq n} \frac{\sigma(j) - \sigma(1)}{j - 1} \cdot \prod_{2 < j \leq n} \frac{\sigma(j) - \sigma(2)}{j - 2} \cdot \prod_{3 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} \\
&= \frac{2-1}{1-2} \cdot \prod_{2 < j \leq n} \frac{j-2}{j-1} \frac{j-1}{j-2} \cdot 1 \\
&= -1
\end{aligned}$$

Théorème 4.17. L'application sign : $(S_n, \circ) \to (\{-1, 1\}, \cdot)$ est un morphisme de groupes.

Démonstration. Soit $\sigma \in S_n$. Alors on calcule

$$|\text{sign}(\sigma)| = \prod_{1\leq i<j\leq n} \frac{|\sigma(j)-\sigma(i)|}{|j-i|}$$

puisque σ est une bijection, on a $\{\{\sigma(i),\sigma(j)\} \mid 1 \leq i < j \leq n\} = \{\{i,j\} \mid 1 \leq i < j \leq n\}$, alors

$$|\text{sign}(\sigma)| = \prod_{1\leq i<j\leq n} \frac{|j-i|}{|j-i|} = 1$$

donc $\text{sign}(\sigma) \in \{-1, 1\}$.
Soit $\tau \in S_n$. Alors

$$\begin{aligned}\text{sign}(\sigma\circ\tau) &= \prod_{1\leq i<j\leq n} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{j-i} \\ &= \prod_{1\leq i<j\leq n} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)} \cdot \prod_{1\leq i<j\leq n} \frac{\tau(j)-\tau(i)}{j-i}\end{aligned}$$

puisque τ est une bijection, de la même manière on a

$$\begin{aligned}\text{sign}(\sigma\circ\tau) &= \prod_{1\leq i<j\leq n} \frac{\sigma(j)-\sigma(i)}{j-i} \cdot \prod_{1\leq i<j\leq n} \frac{\tau(j)-\tau(i)}{j-i} \\ &= \text{sign}(\sigma)\cdot\text{sign}(\tau)\end{aligned}$$

donc sign est un morphisme de groupes. □

Corollaire 4.18.

- Soit $(a,b) \in S_n$ une transposition. Alors $\text{sign}((a,b)) = -1$.
- Soit $(a_1,\ldots,a_k) \in S_n$ un k-cycle. Alors $\text{sign}((a_1,\ldots,a_k)) = (-1)^{k-1}$.
- Soit $\sigma \in S_n$ une permutation de type $(k_1,\ldots,k_m)$. Alors $\text{sign}(\sigma) = \prod_{l=1}^{m} (-1)^{k_l-1}$.

Démonstration. Puisque sign est un morphisme de groupes.

- Comme (a,b) est conjuguée à $(1,2)$, $\text{sign}((a,b)) = \text{sign}((1,2)) = -1$.
- Comme $(a_1,\ldots,a_k) = (a_1,a_2)\circ\ldots\circ(a_{k-1},a_k)$, on a

$$\text{sign}((a_1,\ldots,a_k)) = \text{sign}((a_1,a_2))\ldots\text{sign}((a_{k-1},a_k)) = (-1)^{k-1}.$$

- De la même manière, σ se décompose en cycles à supports disjoints, $\text{sign}(\sigma) = \prod_{l=1}^{m} (-1)^{k_l-1}$.

□

4.5. Groupes alternés.

Définition 4.19 (Parité)**.** Soit $\sigma \in S_n$ une permutation. On dit que σ est *paire* si $\text{sign}(\sigma) = 1$, ou *impaire* si $\text{sign}(\sigma) = -1$. On appelle *groupe alterné* l'ensemble

$$A_n \coloneqq \{\sigma \in S_n \mid \sigma \text{ est paire}\} = \ker(\text{sign}).$$

Proposition 4.20. Soit $\sigma \in S_n$ une permutation. Alors σ est paire si et seulement si elle peut s'écrire comme une composition de 3-cycles.

Démonstration.

⇒ : Supposons que σ est paire. Alors σ est la composition d'un nombre pair de transpositions. On considère la permutation $(a,b)\circ(c,d) \in S_n$,

- si $\{a,b\} = \{c,d\}$, alors $(a,b)\circ(c,d) = \text{id}$,
- si $\{a,b\}\cap\{c,d\} = \{b\} = \{c\}$, alors $(a,b)\circ(c,d) = (a,b,d)$,
- si $\{a,b\}\cap\{c,d\} = \varnothing$, alors $(a,b)\circ(c,d) = (a,b,c)\circ(b,c,d)$,

donc $(a,b)\circ(b,c)$ est un produit de 3-cycles.
$\Leftarrow$: Supposons que σ est une composition de 3-cycles. Alors $\text{sign}(\sigma)=1$, donc σ est paire. □

5. Groupes quotients

5.1. Relations d'équivalence

Définition 5.1 (Relation)**.** Soit E un ensemble. On appelle *relation* sur E un sous-ensemble R de $E\times E$. Si $(x,y)\in R$, on écrit xRy.

Définition 5.2 (Equivalence)**.** Soit R une relation sur un ensemble E. On dit que R est une *relation d'équivalence* si elle vérifie les propriétés suivantes
- R est réflexive, $\forall x\in E, xRx$,
- R est symétrique, $\forall x,y\in E, xRy\Rightarrow yRx$,
- R est transitive, $\forall x,yz\in E, xRy$ et $yRz\Rightarrow xRz$.

Dans ce cas, on notera $\sim$ pour R.

Exemples 5.3. Soit $n\in\mathbb{N}\setminus\{0\}$, on pose $R_n := \{(a,b)\in\mathbb{Z}^2 \mid n|a-b\}$.
1. Soit $x\in\mathbb{Z}$, alors $n|0=x-x$, donc xR_nx,
2. Soit $x,y\in\mathbb{Z}$, si xR_ny, alors $n|x-y$, d'où $n|y-x$, donc yR_nx,
3. Soit $x,y,z\in\mathbb{Z}$, xR_ny et $yR_nz,\Rightarrow n|x-y$ et $n|y-z$, d'où $n|(x-y)+(y-z)=x-z$, donc xR_nz.

Donc R_n est une relation d'équivalence, si $(a,b)\in\mathbb{Z}^2$ on notera $a\equiv b \bmod n$ pour aR_nb.

Définition 5.4 (Classe et représentant)**.** Soit $\sim$ une relation d'équivalence sur un ensemble E.
- Soit $x\in E$. On appelle *classe d'équivalence* de x, notée $\overline{x}$, l'ensemble $\overline{x} := \{y\in E \mid x\sim y\}$.
- Soit $x\in E$. On appelle *représentant* de x tout élément de $\overline{x}$.

Définition 5.5 (Espace quotient)**.** Soit $\sim$ une relation d'équivalence sur un ensemble E. On appelle *espace quotient* de E modulo $\sim$ l'ensemble $E/\sim := \{\overline{x} \mid x\in E\}$.

Définition 5.6 (Projection canonique)**.** Soit $\sim$ une relation d'équivalence sur un ensemble E. On appelle *projection canonique* de E sur $E/\sim$ l'application $\pi : E\to E/\sim; x\mapsto\overline{x}$.

Exemple 5.7. Soit $n\in\mathbb{N}$, on considère de nouveau la relation d'équivalence R_n. Alors

$$\forall x\in\mathbb{Z}, \overline{x}=\{y\in\mathbb{Z} \mid x\equiv y \bmod n\}=\{x+nk \mid k\in\mathbb{Z}\}$$

on notera $\mathbb{Z}/n\mathbb{Z}$ pour $\mathbb{Z}/R_n$.

Définition 5.8 (Partition)**.** Soit E un ensemble. On appelle *partition* de E une famille $(E_i)_{i\in I}$ de sous-ensembles de E qui vérifie les propriétés suivantes
(1) les sous-ensembles sont deux à deux disjoints, $\forall i,j\in I, i\neq j\Rightarrow E_i\cap E_j=\emptyset$,
(2) l'union des sous-ensembles forme E, $\bigsqcup_{i\in I}E_i := \bigcup_{i\in I}E_i = E$.

Proposition 5.9. Soit E un ensemble et $\sim$ une relation d'équivalence sur E.
(1) Soit $x,y\in E$, alors les énoncés suivants sont équivalents
   (a) $\overline{x}=\overline{y}$,
   (b) $x\in\overline{y}$,
   (c) $x\sim y$.
(2) L'espace quotient de E modulo $\sim$ forme une partition de E.
(3) Soit $(E_i)_{i\in I}$ une partition de E. Alors $R := \{(x,y)\in E \mid \exists i\in I, x,y\in E_i\}$ est une relation d'équivalence.

Démonstration.

(1) $(a) \Rightarrow (b)$: Supposons que $\overline{x} = \overline{y}$, alors $x \in \overline{x}$, donc $x \in \overline{y}$.
$(b) \Rightarrow (c)$: Supposons que $x \in \overline{y}$, alors $y \in \overline{y}$ par (a), donc $x \sim y$.
$(c) \Rightarrow (a)$: Supposons que $x \sim y$. Soit $z \in \overline{x}$, alors $z \sim x$, et par transitivité $z \sim y$, donc $z \in \overline{y}$.
Réciproquement si $z \in \overline{y}$, alors $z \in \overline{x}$, donc $\overline{x} = \overline{y}$.

(2) • Soit $x \neq y \in E$. Si $\overline{x} \cap \overline{y} \neq \emptyset$, il existe $z \in \overline{x} \cap \overline{y}$ tel que $z \sim x$ et $z \sim y$, donc $x \sim y$ et $\overline{x} = \overline{y}$.
• Soit $x \in E$, alors $x \in \overline{x} \subset \bigsqcup_{x \in E} \overline{x}$, donc $E = \bigsqcup_{x \in E} \overline{x}$.

(3) (a) Soit $x \in E$, alors il existe $i \in I$ tel que $x \in E_i$, donc xRx.
(b) Soit $x, y \in E$, alors si xRy, il existe $i \in I$ tel que $x, y \in E_i$, donc yRx.
(c) Soit $x, y \in E$, alors si xRy et yRz, il existe $i, j \in I$ tels que $x, y \in E_i$ et $y, z \in E_j$, alors $y \in E_i \cap E_j$, mais puisque $(E_i)_{i \in I}$ forme une partition on a $i = j$, donc xRz.
Donc R est une relation d'équivalence.

□

Définition 5.10 (Système de représentants)**.** Soit E un ensemble et $\sim$ une relation d'équivalence sur E. On appelle *système de représentants* pour $\sim$ un sous-ensemble F de E tel que

$$\forall \alpha \in E/\sim, \exists! x \in F, x \in \alpha$$

c'est-à-dire $\pi_{|F} : F \to E/\sim$ est bijective.

Définition 5.11 (Bien définie)**.** Soit E et F deux ensembles, et $f : E \to F$ une fonction. On dit que f est *bien définie* si

$$\forall x, y \in E, x = y \Rightarrow f(x) = f(y).$$

Proposition 5.12. Soit E et F deux ensembles, et $\sim$ une relation d'équivalence. Soit $f : E \to F$ une application, $\pi : E \to E/\sim$ la projection canonique. Alors il existe $\overline{f} : E/\sim \to F$ bien définie telle que $\overline{f} \circ \pi = f$ si et seulement si

$$\forall x, y \in E, x \sim y \Rightarrow f(x) = f(y).$$

Démonstration.
$\Rightarrow$: Supposons que $\overline{f}$ soit bien définie et que $\overline{f} \circ \pi = f$. Soit $x, y \in E$ tels que $x \sim y$, alors $\pi(x) = \pi(y)$, d'où $\overline{f}(\pi(x)) = \overline{f}(\pi(y))$, donc $f(x) = f(y)$.
$\Leftarrow$: Supposons que $\forall x, y \in E, x \sim y \Rightarrow f(x) = f(y)$.
Soit $\alpha \in E/\sim$, on pose $x_\alpha \in E$ un représentant de α, on définit $\overline{f}(\alpha) = f(x_\alpha)$.
Soit $\beta \in E/\sim$, si $\beta = \alpha$, alors $x_\beta \sim x_\alpha$, d'où $f(x_\beta) = f(x_\alpha)$, donc $\overline{f}(\beta) = \overline{f}(\alpha)$, c'est-à-dire $\overline{f}$ est bien définie.

□

Exemples 5.13.
1. $\overline{f} : \mathbb{Z}/_{2\mathbb{Z}} \to \mathbb{Z}$; $[n] \mapsto n$ n'est pas bien définie car $[3] = [5]$ mais $\overline{f}([3]) = 3 \neq 5 = \overline{f}([5])$.
2. $\overline{f} : \mathbb{Z}/_{4\mathbb{Z}} \to \mathbb{Z}/_{2\mathbb{Z}}$; $[n] \mapsto \overline{n}$ est bien défini car $nRm \Leftrightarrow 4 \mid n - m \Rightarrow 2 \mid n - m \Rightarrow f(n) = f(m)$ donc $\overline{f}$ existe.