Théorie des groupes

Table des matières

1. Groupes

Définition 1.1. Soit G un ensemble et $\star : G \times G \longrightarrow G$ une loi de composition interne. On dit que le couple $(G, \star)$ forme un *groupe* s'il vérifie les propriétés 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
$$y = e_G \star y = (x^{-1} \star x) \star y = x^{-1} \star (x \star y) = x^{-1} \star e_G = x^{-1}.$$

□

Définition 1.4. 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. 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 1.7. 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.

Notation 1.8. Soit $(G, \star)$ un groupe. Lorsqu'il ne peut pas y avoir de confusions, on notera
- $e := e_G$ pour le neutre,
- $\forall x, y \in G, xy := x \star y$ pour la loi $\star$,
- $\forall x \in G, \forall n \in \mathbb{Z}$, si $n > 0, x^n := \underbrace{x \star ... \star x}_{\text{n fois}}$, si $n = 0, x^0 := e$, si $n < 0, x^n := x^{-1} \star ... \star x^{-1}$.

2. Sous-groupes

2.1. Définitions

Définition 2.1. 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, $\forall x \in H, x^{-1} \in H$.

Définition 2.2. 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 2.3. 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 $x \star y = x \star \left(y^{-1}\right)^{-1} \in H$.

$\square$

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. 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 $(H, \star)$,
   1. soit $x, y, z \in H$, alors $x, y, z \in G$ donc $(x \star y) \star z = x \star (y \star z)$,
   2. on pose $e_H = e_G$, alors $e_H \in H$,
   3. 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 $x^{-1} \in H$.

$\square$

Proposition 2.5. 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 2.3, $H_1 \cap H_2$ est un sous-groupe de G. □

2.2. Générateurs

Définition 2.6. 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 2.7. Si $S = \{x_1, ..., x_n\}$, on note $\langle x_1, \, ..., \, x_n \rangle := \langle S \rangle$.

Proposition 2.8. 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 $F := \{H < G \mid S \subset H\}$ et $H_S := \bigcap_{H \in F} H$. Puisque $G \in F$, l'intersection est non-vide, et d'après la Proposition 2.5, 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 $H_0 \subset H_S$. Donc H_S est bien le plus petit sous-groupe de G contenant S.

Notons $K_S := \left\{ x_1 \star ... \star x_n \mid n \in \mathbb{N} \setminus \{0\}, \forall i \in \{1, ..., n\}, x_i \in S \text{ ou } x_i^{-1} \in S \right\}$. On remarque que K_S est stable par multiplication, par inverse et contient le neutre de G, donc d'après la Proposition 2.3, 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 2.9. 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.
- Si S est fini, on dit que G est *finiment engendré*.
- Si S ne contient qu'un élément, on dit que G est *monogène*, si de plus G est fini, on dit que G est *cyclique*.

Exemple 2.10.
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 2.11. On considère le groupe $(\mathbb{Z}, +)$, alors
1. $\forall n \in \mathbb{Z}, \langle n \rangle = n\mathbb{Z}$,
2. soit H est 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. *TODO* : Voir TD.

□

2.3. Ordre d'un élément

Définition 2.12. Soit $(G, \star)$ un groupe et $x \in G$. On appelle *ordre de x*, noté $\mathrm{ord}(x)$, le cardinal du sous-groupe engendré par $\{x\}$.

Proposition 2.13. Soit $(G, \star)$ un groupe et $x \in G$. Alors

$$\mathrm{ord}(x) = \inf\big(\{d \in \mathbb{N} \setminus \{0\} \mid x^d = e\}\big)$$

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

Démonstration.

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

□

3. Morphismes de groupes

3.1. Définitions

Définition 3.1. Soit $(G, \star)$ et $(H, \cdot)$ deux groupes. Une application $\varphi : G \longrightarrow H$ 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 $\varphi : G \longrightarrow H$ 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, $\forall x \in G, \varphi(x^{-1}) = \varphi(x)^{-1}$.

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

□

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

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

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

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 $\varphi : G \longrightarrow H$ et $\psi : H \longrightarrow K$ 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. $\forall \varphi : G \longrightarrow H$ isomorphisme, $\forall x \in G, \mathrm{ord}(x) = \mathrm{ord}(\varphi(x))$.

Démonstration. Soit $\varphi : G \longrightarrow H$ 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 $\mathrm{ord}(x) = \mathrm{ord}(\varphi(x))$.

□

3.2. Image et noyau

Définition 3.6. Soit $(G, \star)$ et $(H, \cdot)$ deux groupes, et $\varphi : G \longrightarrow H$ un morphisme de groupes.
- On appelle *image* de φ l'ensemble $\mathrm{im}(\varphi) := \varphi(G)$.
- On appelle *noyau* de φ l'ensemble $\ker(\varphi) := \varphi^{-1}(e_H)$.

Proposition 3.7. Soit $(G, \star)$ et $(H, \cdot)$ deux groupes, et $\varphi : G \longrightarrow H$ un morphisme de groupes. Alors $\mathrm{im}(\varphi)$ 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

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

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 2.3, $\varphi(G')$ 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

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

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 2.3, $\varphi^{-1}(H')$ est un sous-groupe de G. □

Proposition 3.8. Soit $(G, \star)$ et $(H, \cdot)$ deux groupes, et $\varphi : G \longrightarrow H$ un morphisme de groupes.
- φ est surjectif si et seulement si $\mathrm{im}(\varphi) = H$.
- 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 $f(x \star y^{-1}) = e_H$, et $\ker(\varphi) = e_G$ d'où $x \star y^{-1} = e_G$, donc $x = y$ et φ est injectif.

□

4. Groupes symétriques

4.1. Définitions

Définition 4.1. 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

$$\sigma := \begin{pmatrix} 1 & ... & n \\ \sigma(1) & ... & \sigma(n) \end{pmatrix}.$$

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

$$\operatorname{supp}(\sigma) := \{i \in \{1, ..., n\} \mid \sigma(i) \neq i\}.$$

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 $i \notin \operatorname{supp}(\sigma_1) \cup \operatorname{supp}(\sigma_2)$, on a $(\sigma_1 \circ \sigma_2)(i) = (\sigma_2 \circ \sigma_1)(i) = i$,
- si $i \in \operatorname{supp}(\sigma_1)$, alors $i \notin \operatorname{supp}(\sigma_2)$ et $\sigma_1(i) \notin \operatorname{supp}(\sigma_2)$, et on a $(\sigma_1 \circ \sigma_2)(i) = (\sigma_2 \circ \sigma_1)(i) = i$,
- si $i \in \operatorname{supp}(\sigma_2)$, 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. 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

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

- 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. 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

$$\sigma((a_1, ..., a_k)(\sigma^{-1}(i))) = \sigma((a_1, ..., a_k)(a_j)) = \sigma(a_{j+1}),$$

- si $i = \sigma(a_k)$, alors $\sigma^{-1}(i) = a_k$ et on a

$$\sigma((a_1, ..., a_k)(\sigma^{-1}(i))) = \sigma((a_1, ..., a_k)(a_k)) = \sigma(a_1),$$

- sinon on a

$$\sigma((a_1, ..., a_k)(\sigma^{-1}(i))) = \sigma(\sigma^{-1}(i)) = i.$$

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 $\tau_1 = (i, \sigma(i), ..., \sigma^{p-1}(i))$. Alors τ_1 agit comme σ sur l'ensemble $\{i, \sigma(i), ..., \sigma^{p-1}(i)\}$, donc on a $|\mathrm{supp}(\tau_1^{-1} \circ \sigma)| < |\mathrm{supp}(\sigma)|$. 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. 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 $\sigma_1 = (\tau_1 \circ \tau_2^{-1}) \circ \sigma_2 \circ (\tau_2 \circ \tau_1^{-1})$, 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. □

4.4. Signature d'une permutation

Définition 4.14. Soit $\sigma \in S_n$ une permutation. On appelle *signature* de σ le nombre rationnel

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

Exemple 4.15. On calcule la signature de la transposition $(1,2)$

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

Théorème 4.16. L'application $\operatorname{sign} : (S_n, \circ) \longrightarrow (\{-1,1\}, \cdot)$ est un morphisme de groupes.

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

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

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

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

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

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

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

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

donc sign est un morphisme de groupes. □

Corollaire 4.17.
- Soit $(a,b) \in S_n$ une transposition. Alors $\operatorname{sign}((a,b)) = -1$.
- Soit $(a_1, ..., a_k) \in S_n$ un k-cycle. Alors $\operatorname{sign}((a_1,...,a_k)) = (-1)^{k-1}$.
- Soit $\sigma \in S_n$ une permutation de type $(k_1,...,k_m)$. Alors $\operatorname{sign}(\sigma) = \prod_{l=1}^{m} (-1)^{k_l-1}$.

Démonstration. Puisque sign est un morphisme de groupes.
- Comme (a, b) est conjuguée à $(1, 2)$, $\mathrm{sign}((a, b)) = \mathrm{sign}((1, 2)) = -1$.
- Comme $(a_1, ..., a_k) = (a_1, a_2) \circ ... \circ (a_{k-1}, a_k)$, on a

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

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

□

4.5. Groupes alternés

Définition 4.18. Soit $\sigma \in S_n$ une permutation. On dit que σ est *paire* si $\mathrm{sign}(\sigma) = 1$, ou *impaire* si $\mathrm{sign}(\sigma) = -1$. On appelle *groupe alterné* l'ensemble

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

Proposition 4.19. 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.
$\Rightarrow$: 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 $(a, b) \circ (c, d) = \mathrm{id}$,
- si $\{a, b\} \cap \{c, d\} = \{b\} = \{c\}$, alors $(a, b) \circ (c, d) = (a, b, d)$,
- si $\{a, b\} \cap \{c, d\} = \emptyset$, 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 $\mathrm{sign}(\sigma) = 1$, donc σ est paire. □

5. Groupes quotients

5.1. Relations d'équivalence

Définition 5.1. 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. Soit R une relation sur un ensemble E. On dit que R est une *relation d'équivalence* si elle vérifie les propriétés suivantes
1. R est réflexive, $\forall x \in E, xRx$,
2. R est symétrique, $\forall x, y \in E, xRy \Rightarrow yRx$,
3. R est transitive, $\forall x, yz \in E, xRy$ et $yRz \Rightarrow xRz$.

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

Exemple 5.3. Soit $n \in N \setminus \{0\}$, 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 $x, y, z \in \mathbb{Z}$, si xR_ny et yR_nz, alors $n|x - y$ 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. 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 $\overline{x}$.
- On appelle *espace quotient* de E modulo $\sim$ l'ensemble $E/\sim := \{\overline{x} \mid x \in E\}$.
- On appelle *projection canonique* de E sur $E/\sim$ l'application $\pi : E \to E/\sim, x \mapsto \overline{x}$.

Exemple 5.5. 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 5.6. 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 5.7. 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 $y \in \overline{y}$, 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 $x, y \in E$. 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. 1. Soit $x \in E$, alors il existe $i \in I$ tel que $x \in E_i$, donc xRx.
   2. Soit $x, y \in E$, alors si xRy, il existe $i \in I$ tel que $x, y \in E_i$, donc yRx.
   3. Soit $x, y \in E$, alors si xRy et yRz, il existe $i, j \in I$ tels que $x, y \in E_i$ et $y, z \in E_j$, mais puisque $(E_i)_{i \in I}$, alors $y \in E_i \cap E_j$, puisqu'il s'agit d'une partition on a $i = j$, donc xRz.

   Donc R est une relation d'équivalence.

□

Définition 5.8. 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 5.9. 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 5.10. 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. □

5.2. Classes modulo un sous-groupe

Définition 5.11. Soit $(G, \star)$ un groupe et H un sous-groupe de G. On appelle *relation modulo H à gauche*, la relation $\sim_H$ sur G définie par

$$\forall x, y \in G, x \sim_H y \Leftrightarrow y \in xH \Leftrightarrow x^{-1} \star y \in H$$

où $xH = \{x \star y \mid y \in H\}$.

Remarque 5.12. On peut définir la *relation modulo H à droite* ${}_H\!\sim$ d'une manière similaire.

Proposition 5.13. Soit $(G, \star)$ un groupe et H un sous-groupe de G. Alors $\sim_H$ est une relation d'équivalence sur G, dont les classes d'équivalences sont $\forall x \in G, \overline{x} = xH$.

Démonstration.
1. Soit $x \in G$, alors $x \star e \in xH$, donc $x \sim_H x$.
2. Soit $x, y \in G$, alors si $x \sim_H y$, on a $x^{-1} \star y \in H$, d'où $y^{-1} \star x = (x^{-1} \star y)^{-1} \in H$, donc $y \sim_H x$.
3. Soit $x, y, z \in G$, alors si $x \sim_H y$ et $y \sim_H z$, on a $y \in xH$ et $z \in yH$, d'où $z \in xH$, donc $x \sim_H z$.

□

Notation 5.14. Soit $(G, \star)$ un groupe et H un sous-groupe de G. Alors on note les espaces quotients $G/H \coloneqq G/\sim_H$ et $H \setminus G \coloneqq G/\ {}_H\!\sim$.

Proposition 5.15. Soit $(G, \star)$ un groupe et H un sous-groupe de G. Alors les ensembles G/H et $H \setminus G$ sont isomorphes. En particulier si G est fini, on a $|G/H| = |H \setminus G|$.

Démonstration. On considère le morphisme $\varphi : G/H \to H \setminus G, xH \mapsto Hx^{-1}$, il est bien définie et admet pour inverse $\psi : H \setminus G \to G/H, Hx \mapsto x^{-1}H$, donc c'est un isomorphisme. □

5.3. Théorème du nombre de classes et théorème de Lagrange

Définition 5.16. Soit $(G, \star)$ un groupe et H un sous-groupe de G. On appelle *indice* de H dans G

$$[G : H] \coloneqq |G/H|.$$

Théorème 5.17. (Théorème du nombre de classes) Soit $(G, \star)$ un groupe et H un sous-groupe de G. Alors si G est fini

$$|G| = [G : H]|H|$$

Démonstration. On pose $n \coloneqq [G : H]$ et on considère $\{x_1, ..., x_n\}$ un système de représentants pour $\sim_H$. On sait que la famille $(x_i H)_{i \in \{1,...,n\}}$ forme une partition de G, d'où

$$|G| = \sum_{i=1}^{n} |x_i H| = \sum_{i=1}^{n} |H| = n|H|$$

c'est-à-dire $|G| = [G : H]|H|$. □

Corollaire 5.18. (Théorème de Lagrange) Soit $(G, \star)$ un groupe et H un sous-groupe de G. Alors si G est fini, $|H|$ divise $|G|$, en particulier si $x \in G$, $\operatorname{ord}(x)$ divise $|G|$.

Corollaire 5.19.

1. Soit $(G, \star)$ un groupe fini d'ordre n et $x \in G$. Alors $x^n = e$.
2. Soit $(G, \star)$ un groupe fini, H un sous-groupe de G et K un sous-groupe de H. Alors K est un sous-groupe de G et

$$[G : K] = [G : H][H : K].$$

Démonstration.

1. D'après le Corollaire 5.18, $\operatorname{ord}(x)$ divise n, donc $x^n = e$.
2. D'après le Théorème 5.17,

$$[G : K] = \frac{|G|}{|K|} = \frac{[G : H]|H|}{|K|} = \frac{[G : H][H : K]|K|}{|K|} = [G : H][H : K].$$

□

5.4. Sous-groupes distingués et groupes quotients

Théorème 5.20. Soit $(G, \star)$ un groupe et H un sous-groupe de G. Alors les énoncés suivants sont équivalents

1. H est distingué.
2. Il existe un morphisme $\varphi : G \to G$ tel que $H = \ker(\varphi)$.
3. G/H a une structure de groupes.

Démonstration.

1. ⇒ 3. : Supposons que H est distingué.

On considère l'application $\cdot : G/H \times G/H \to G/H, (xH, yH) \mapsto xyH$, alors elle est bien définie et $(G/H, \cdot)$ forme un groupe.

3. $\Rightarrow$ 2. : Supposons que G/H a une structure de groupe.
Alors la projection canonique $\pi : G \to G/H$ est un morphisme de groupes et $\ker(\pi) = H$.

2. $\Rightarrow$ 1. : Supposons qu'il existe un tel morphisme φ.
Soit $h \in H$ et $g \in G$, alors

$$\varphi(g \star h \star g^{-1}) = \varphi(g) \star \varphi(h) \star \varphi(g)^{-1} = \varphi(x) \star \varphi(x)^{-1} = e$$

puisque $H = \ker(\varphi)$, on a $g \star h \star g^{-1} \in H$. $\square$

Corollaire 5.21. Soit $(G, \star)$ un groupe et H un sous-groupe de G. Si G est abélien, alors G/H a une structure de groupes.

Théorème 5.22. (Propriété d'universalité du groupe quotient) Soit $(G, \star)$ un groupe et H un sous-groupe distingué de G. Soit $(K, \cdot)$ un groupe, $\pi : G \to G/H$ la projection canonique et $\varphi : G \to K$ un morphisme de groupes. Alors il existe un morphisme $\overline{\varphi} : G/H \to K$ tel que $\overline{\varphi} \circ \pi = \varphi$, si et seulement si $H \subset \ker(\varphi)$. Dans ce cas $\operatorname{im}(\overline{\varphi}) = \operatorname{im}(\varphi)$ et $\ker(\overline{\varphi}) = \ker(\pi(\varphi))$.

Démonstration.
$\Rightarrow$: Supposons qu'il existe un tel morphisme $\overline{\varphi}$.
Soit $x \in H$, alors $\varphi(x) = \overline{\varphi}(\pi(x)) = \overline{\varphi}(\{e\}) = H$, donc $H \subset \ker(\varphi)$.

$\Leftarrow$: Supposons que $H \subset \ker(\varphi)$.
Soit $x \in H$, on définit $\overline{\varphi}(xH) = \varphi(x)$, alors $\overline{\varphi}$ est bien définie. Puisque $\overline{\varphi} \circ \pi = \varphi$ et π est surjectif, on a $\operatorname{im}(\overline{\varphi}) = \operatorname{im}(\varphi)$on a $\ker(\overline{\varphi}) = \pi(\ker(\varphi))$. $\square$

Corollaire 5.23. (Théorème d'isomorphisme) Soit $(G, \star)$ et $(K, \cdot)$ deux groupes, et $\varphi : G \to K$ un morphisme de groupes. Alors il existe un isomorphisme $\overline{\varphi} : G/\ker(\varphi) \to \operatorname{im}(\varphi)$.

Démonstration. On pose $H := \ker(\varphi)$, alors par le Théorème 5.22, il existe $\overline{\varphi} : G/\ker(\varphi) \to \operatorname{im}(\varphi)$ telle que $\overline{\varphi} \circ \pi = \varphi$. Puisque $\ker(\overline{\varphi}) = \pi(\ker(\varphi)) = \pi(H) = \{e\}$, $\overline{\varphi}$ est injectif, et par définition $\overline{\varphi}$ est surjectif. Donc $\overline{\varphi}$ est un isomorphisme. $\square$

Proposition 5.24. Soit $(G, \star)$ un groupe. Alors si $(G, \star)$ est monogène, il existe $n \in \mathbb{N}$ tel qu'il est isomorphe à $(\mathbb{Z}, +)$ ou à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Démonstration. Soit $x \in G$ un générateur et $\varphi : \mathbb{Z} \to G, m \mapsto x^m$.
Alors φ est un morphisme de groupes et $\operatorname{im}(\varphi) = \langle x \rangle = G$, donc φ est surjectif. Soit $d := \operatorname{ord}(x)$
- si $d = +\infty$, alors φ est injectif, et par le Corollaire 5.23, $\mathbb{Z}/\ker(\varphi) \simeq \operatorname{im}(\varphi)$, c'est-à-dire $\mathbb{Z} \simeq G$,
- sinon $\ker(\varphi) = d\mathbb{Z}$, et par le Corollaire 5.23, $\mathbb{Z}/\ker(\varphi) \simeq \operatorname{im}(\varphi)$, c'est-à-dire $\mathbb{Z}/d\mathbb{Z} \simeq G$.

$\square$

Proposition 5.25. Soit $(G, \star)$ un groupe et $x, y \in G$ tels que $x \star y = y \star x$. Notons $a := \operatorname{ord}(x)$ et $b := \operatorname{ord}(y)$, alors $\operatorname{ord}(x \star y)$ divise $\operatorname{ppcm}(a, b)$. De plus si $\langle x \rangle \cap \langle y \rangle = \{e\}$, on a $\operatorname{ord}(x \star y) = \operatorname{ppcm}(a, b)$

Démonstration. Posons $m := \operatorname{ppcm}(a, b)$ et $d := \operatorname{pgcd}(a, b)$.
Alors il existe $a', b' \in \mathbb{Z}$ tels que $a = da'$ et $b = db'$, d'où $m = da'b'$. Alors

$$(x \star y)^m = x^m \star y^m = \left(x^{da'}\right)^{b'} \star \left(y^{db'}\right)^{a'} = e$$

donc $\operatorname{ord}(x \star y)$ divise $\operatorname{ppcm}(a, b)$. $\square$

Proposition 5.26. Soit $n, m \in \mathbb{Z}$. Alors $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est isomorphe à $\mathbb{Z}/nm\mathbb{Z}$ si et seulement si $\mathrm{pgcd}(n, m) = 1$.

Démonstration. Soit $x \in \mathbb{Z}$. Notons $\overline{x}$ et $[x]$ les classes respectives de x modulo n et m.
$\Rightarrow$: Supposons que $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est isomorphe à $\mathbb{Z}/nm\mathbb{Z}$. Alors $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est cyclique. Soit (a, b) un générateur de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, c'est-à-dire $\mathrm{ord}((a, b)) = nm$, alors

$$\mathrm{ppcm}(\mathrm{ord}(a), \mathrm{ord}(b)) \cdot (a, b) = \left(\overline{0}, [0]\right)$$

donc $nm|\mathrm{ppcm}(\mathrm{ord}(a), \mathrm{ord}(b))$, on en déduit $nm|\mathrm{ppcm}(n, m)$, d'où $\mathrm{pcgd}(n, m) = 1$.

$\Leftarrow$: Supposons que $\mathrm{pgcd}(n, m) = 1$. Posons $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, x \mapsto (\overline{x}, [x])$.
Alors φ est bien un morphisme, et on a

$$\begin{aligned}
\ker(\varphi) &= \left\{k \in \mathbb{Z} \mid \left(\overline{k}, [k]\right) = \left(\overline{0}, [0]\right)\right\} \\
&= \{k \in \mathbb{Z} \mid n|k \text{ et } m|k\} \\
&= \{k \in \mathbb{Z} \mid nm|k\} = nm\mathbb{Z}
\end{aligned}$$

d'après le Théorème 5.22, il existe un morphisme $\overline{\varphi} : \mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ injectif. Enfin puisque $|\mathbb{Z}/nm\mathbb{Z}| = |\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}|$, on en déduit que $\overline{\varphi}$ est un isomorphisme. $\square$

6. Actions de groupes

6.1. Définitions

Définition 6.1. Soit $(G,\star)$ un groupe et X un ensemble. On appelle *action* de G sur X une application $\psi : G \times X \longrightarrow X$ qui vérifie les propriétés suivantes
1. $\forall x \in X, \psi(e,x) = x$,
2. $\forall g,h \in G, \forall x \in X, \psi(g,\psi(h,X)) = \psi(gh,x)$.

Dans ce cas, on notera $\forall g \in G, \forall x \in X, g \star x := \psi(g,x)$.

Notation 6.2. Soit $(G,\star)$ un groupe et X un ensemble. Si G agit sur X, on note $G \circlearrowleft X$.

Définition 6.3. Soit $(G,\star)$ un groupe qui agit sur un ensemble X et $x \in X$.
1. On appelle *stabilisateur* de x, l'ensemble $G_x := \{g \in G \mid g \star x = x\}$.
2. On appelle *orbite* de x, l'ensemble $O_x := \{g \star x \mid g \in G\}$.

Lemme 6.4. Soit $(G,\star)$ un groupe qui agit sur un ensemble X et $x \in X$. Alors le stabilisateur de x est un sous-groupe de G. De plus

$$\forall g \in G, G_{g \star x} = g(G_x)g^{-1}.$$

Démonstration. On vérifie facilement que G_x est un sous-groupe de G. Soit $g \in G$, alors $h \in G_{gx}$ si et seulement si $h \star (g \star x) = g \star x$, si et seulement si $(g^{-1} \star h \star g) \star x = x$, si et seulement si $g^{-1} \star h \star g \in G_x$, si et seulement si $h \in g(G_x)g^{-1}$. □

6.2. Espace des orbites

Définition 6.5. Soit $(G,\star)$ un groupe qui agit sur un ensemble X et $x,y \in X$. Alors on définit la relation $\sim$ par

$$x \sim y \Leftrightarrow y \in O_x.$$

Proposition 6.6. Soit $(G,\star)$ un groupe qui agit sur un ensemble X. Alors $\sim$ est une relation d'équivalence sur X, dont les classes d'équivalences sont $\forall x \in X, \overline{x} = O_x$.

Démonstration.
1. Soit $x \in X$, alors $x = e \star x$, d'où $x \in O_x$, donc $x \sim x$.
2. Soit $x,y \in X$, alors si $x \sim y$, il existe $g \in G$ tel que $y = g \star x$, d'où $x = g^{-1} \star y$, donc $y \sim x$.
3. Soit $x,y,z \in X$, alors si $x \sim y$ et $y \sim z$, il existe $g,h \in G$ tels que $y = \star x$ et $z = h \star y$, d'où $z = (h \star g) \star x$, donc $x \sim z$.

□

Définition 6.7. Soit $(G,\star)$ un groupe qui agit sur un ensemble X. On dit que l'action est
1. *transitive*, si $\forall x,y \in X, \exists G, y = g \star x$,
2. *fidèle*, si $\forall g \in G \setminus \{e\}, \exists x \in X, g \star x \neq x$,
3. *libre*, si $\forall g \in G \setminus \{e\}, \forall x \in X, g \star x \neq x$.

Dans ce cas, on dit que G agit respectivement *transitivement*, *fidèlement* et *librement* sur X.

Proposition 6.8. Soit $(G,\star)$ un groupe qui agit transitivement sur un ensemble X et $x \in X$. Alors l'application $f_x : G/G_x \to X, gG_x \mapsto g \star x$, est bien définie et est bijective.

Démonstration. Soit $g,h \in G$ tels que $g \sim h$. Alors $gG_x = hG_x$, d'où $h^{-1} \star g \in G_x$, c'est-à-dire $g \star x = h \star x$, donc f_x est bien définie. De plus f_x est injective puisque $g \star x = h \star x$ donne $gG_x = hG_x$. Enfin f_x est surjective puisque G agit transitivement sur X. □

Théorème 6.9. (Formule des classes) Soit $(G, \star)$ un groupe fini qui agit sur un ensemble fini X et $x_1, ..., x_n \in X$ un système de représentant pour $\sim$. Alors

$$|X| = \sum_{i=0}^{n} |O_{x_i}| = \sum_{i=0}^{n} \left[G : G_{x_i}\right].$$

7. Classification des groupes abéliens finis

7.1. Décomposition en p-groupes

Définition 7.1. Soit $(G, \star)$ un groupe abélien d'ordre n et p un nombre premier qui divise n. On appelle composante *p-primaire* de G, l'ensemble

$$G_p \coloneqq \{x \in G \mid \exists q \in \mathbb{N}, \operatorname{ord}(x) = p^q\}.$$

Remarque 7.2. Soit $(G, \star)$ un groupe abélien d'ordre n et $p_1^{r_1}...p_k^{r_k}$ la décomposition de n en facteurs premiers. Alors

$$\forall i \in \{1, ..., k\}, G_{p_i} = \left\{x \in G \mid x^{p_i^{r_i}} = e\right\}.$$

Lemme 7.3. Soit $(G, \star)$ un groupe abélien d'ordre $n = ab$ tels que $\operatorname{pgcd}(a, b) = 1$. Soit $k \in \mathbb{N}$,

$$G(k) \coloneqq \{x \in G \mid x^k = e\}$$

alors $G(k)$ est un sous-groupe de G et G est isomorphe à $G(a) \times G(b)$.

Démonstration. Puisque G est abélien, l'application $\varphi_k : \mathbb{N} \to G, x \mapsto x^k$ est un morphisme de groupes, donc $G(k) = \ker(\varphi_k)$ est un sous-groupe de G.

Posons $\varphi : G(a) \times G(b) \to G, (x, y) \mapsto x \star y$, G est abélien donc c'est un morphisme de groupes. Soit $x \in G$, puisque $\operatorname{pgcd}(a, b) = 1$, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$, alors

$$x = x^{au+bv} = x^{au} \star x^{bv}$$

or $\left(x^{bv}\right)^a = (x^v)^n = e$ et $(x^{au})^b = (x^u)^n = e$, d'où $x^{bv} \in G(a)$ et $x^{au} \in G(b)$, on en déduit que φ est surjectif puisque $x = \varphi\left(x^{bv}, x^{au}\right)$.
Soit $(x, y) \in G(a) \times G(b)$ tel que $\varphi(x, y) = e$, alors $x = y^{-1} \in G(a) \cap G(b)$, on en déduit $\operatorname{ord}(x)|a$ et $\operatorname{ord}(x)|b$, d'où $\operatorname{ord}(x)|\operatorname{pgcd}(a, b) = 1$ et $x = y = e$, donc φ est injectif. Donc G est isomorphe à $G(a) \times G(b)$ □

Définition 7.4. Soit $(G, \star)$ un groupe d'ordre n et p un nombre premier. On dit que G est un *p-groupe* s'il existe $k \in \mathbb{N}$ tel $n = p^k$.

Lemme 7.5. Soit $(G, \star)$ un groupe abélien d'ordre n et p un nombre premier tel que

$$\forall x \in G, \exists l_x \in \mathbb{N}, \operatorname{ord}(x) = p^{l_x}.$$

Alors G est un p-groupe.

Démonstration. Notons $G \coloneqq \{x_1, ..., x_n\}$.
Posons $\varphi : H = \langle x_1 \rangle \times ... \times \langle x_n \rangle \to G, (y_1, ..., y_n) \mapsto y_1...y_n$, puisque G est abélien φ est un morphisme de groupes. Il est évidemment surjectif, alors d'après le Corollaire 5.23, G est isomorphe à $H/\ker(\varphi)$. De plus $|H| = \prod_{i=1}^{n} p^{l_{x_i}} = p^{\sum_{i=1}^{n} l_{x_i}}$, et $|G|$ divise $|H/\ker(\varphi)| \cdot |\ker(\varphi)| = |H|$, donc G est un p-groupe. □

Théorème 7.6. Soit $(G, \star)$ un groupe abélien d'ordre n et $p_1^{r_1}...p_k^{r_k}$ la décomposition de n en facteurs premiers. Soit $i \in \{1, ..., k\}$, alors la composante p_i-primaire de G est un groupe à $p_i^{r_i}$ éléments et G est isomorphe à $G_{p_1} \times ... \times G_{p_k}$.

Démonstration. Soit $i \in \{1, ..., k\}$, on a d'après les Lemme 7.3 et Lemme 7.5, avec $G_{p_i} = G\left(p_i^{r_i}\right)$ est bien un sous-groupe de G, et donc un p_i-groupe. Par récurrence directe sur le Lemme 7.3, G est isomorphe à $G_{p_1} \times ... \times G_{p_k}$, en comparant l'ordre des deux groupes, on en déduit que G_{p_i} est d'ordre $p_i^{r_i}$. □

Exemple 7.7. On considère $G \coloneqq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/7^3\mathbb{Z}$. Alors les composantes p-primaires de G sont

$$\begin{aligned} G_2 &= \mathbb{Z}/2\mathbb{Z} \times \{\overline{0}\} \times \{\overline{0}\} \times \{\overline{0}\} \\ G_5 &= \{\overline{0}\} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z} \times \{\overline{0}\} \\ G_7 &= \{\overline{0}\} \times \{\overline{0}\} \times \{\overline{0}\} \times \mathbb{Z}/7^3\mathbb{Z}. \end{aligned}$$

7.2. Décomposition des p-groupes en produit de groupes cycliques

Théorème 7.8. Soit p un nombre premier et $(G, \star)$ un p-groupe abélien. Alors il existe $n_1, ..., n_k \in \mathbb{N}$, uniquement déterminés par G, tels que G est isomorphe à

$$\left(\mathbb{Z}/p^k\mathbb{Z}\right)^{n_k} \times ... \times (\mathbb{Z}/p\mathbb{Z})^{n_1}.$$

Démonstration. Admis. □

Corollaire 7.9. Soit $(G, \star)$ un groupe abélien fini. Alors G est isomorphe à un produit de groupes cycliques

Corollaire 7.10. Soit $(G, \star)$ un groupe abélien fini. Alors il existe $n_1, ..., n_k \in \mathbb{N}$, uniquement déterminés par G, tels que $n_1 | ... | n_k$ et G est isomorphe à

$$\mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_k\mathbb{Z}.$$

Exemple 7.11. Considérons le groupe

$$G = \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/8\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^2$$

dans lequel 3 est le nombre maximal de facteurs dans la décomposition d'un p-groupe ($p = 2$). On fait donc un tableau avec 3 colonnes

$p = 2$	2^2	2^3	2^3
$p = 3$	1	3	3^2
$p = 5$	1	5	5
	4	120	360

et on en déduit que

$$G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z} \times \mathbb{Z}/360\mathbb{Z}.$$

7.3. Facteurs invariants d'un groupe

Définition 7.12. Soit $(G, \star)$ un groupe abélien fini. On appelle *facteurs invariants* de G, les $n_1, ..., n_k \in \mathbb{N}$ de sa décomposition en groupes cycliques

Corollaire 7.13. Soit $(G, \star)$ et $(H, \cdot)$ deux groupes abéliens finis. Alors G et H sont isomorphes si et seulement si ils ont les mêmes facteurs invariants.