Mathieu Kieffer

Algèbre et géométrie : 38 leçons pour l'agrégation

ellipses

Chapitre 1

Groupes monogènes. Groupes cycliques. Exemples

Pré-requis

1. Généralités sur les groupes.
2. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
3. Théorème de Lagrange pour les groupes.
4. Définition d'un nombre premier.
5. P.G.C.D. de deux entiers naturels.
6. Lemme de Gauss en arithmétique.
7. Notion de corps.

1.1 Groupes monogènes

Définition 1. Soit $(G, .)$ un groupe. $(G, .)$ est dit monogène s'il existe un élément x tel que pour tout élément y de $(G, .)$, il existe un entier relatif k tel que $y = x^k$. On note alors $G = \langle x \rangle$ et l'on dit que $(G, .)$ est engendré par x ou encore que x est un générateur de $(G, .)$. Si de plus, $(G, .)$ est d'ordre fini, on dit que $(G, .)$ est cyclique.

Exemples. 1. $(\mathbb{Z}, +)$ est monogène infini engendré par 1 ou -1.

2. Pour tout entier naturel non nul n, $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique d'ordre n.

3. Pour tout entier naturel non nul n, $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ est un groupe cyclique d'ordre $n-1$.

4. Pour tout entier naturel non nul n, $\left(\mathbb{U}_n = \left\{e^{\frac{2ik\pi}{n}},\ k \in [\![0; n-1]\!]\right\}, \times\right)$ est un groupe cyclique d'ordre n.

Remarque. Tout groupe monogène est abélien. Attention, la réciproque est fausse : le groupe de Klein est abélien mais non cyclique.

Définition 2. Soit $(G,.)$ un groupe fini. Soit a un élément de G. On appelle ordre de a l'ordre du sous-groupe $\langle a\rangle = \{a^k,\ k \in \mathbb{Z}\}$ engendré par a.

Théorème 3. *Soit $(G,.)$ un groupe fini. Soit a un élément de G. Soit m l'ordre de a. Alors :*

1. *m divise l'ordre de G.*
2. *m est le plus petit entier naturel non nul tel que $a^m = 1$.*
3. *Les éléments $1,\ a,\ a^2, \ldots, a^{m-1}$ sont tous distincts dans G. De plus, $\langle a\rangle = \{1, a, a^2, \ldots, a^{m-1}\}$.*

Démonstration. 1. C'est le théorème de Lagrange.

2. Si $m = 1$, c'est évident. Si $m \geqslant 2$. On démontre que $A = \{a, a^2, a^3, \ldots, a^{m+1}\}$ possède au moins deux éléments égaux. Ainsi, il existe un entier l compris entre 1 et m tel que $a^l = 1$. Soit $s = \min\{k \in \mathbb{N}^*,\ a^k = 1\}$. On a $s \leqslant m$. Soit $k \in \mathbb{Z}$. On a $k = sq + r$ avec $0 \leqslant r \leqslant s-1$ donc $a^k = a^r$ et par conséquent $a^k \in \{1, a, a^2, \ldots, a^{s-1}\}$. Ainsi, $\langle a\rangle \subset \{1; a, \ldots, a^{s-1}\}$ et $m \leqslant s$. D'où $m = s$.

3. $\{1, a, \ldots, a^{m-1}\} \subset \langle a\rangle$ est évident. De plus, $|\langle a\rangle| = m$, d'où l'égalité. □

Corollaire 4. *Soit $n \in \mathbb{N}$. Soit $(G,.)$ un groupe fini d'ordre n. Alors, pour tout $x \in G$, $x^n = 1$.*

Démonstration. Soit m l'ordre de x. D'après le théorème 3, m divise n. Donc il existe un entier relatif k tel que $n = mk$. D'où $x^n = x^{mk} = (x^m)^k = 1^k = 1$. □

Corollaire 5. *Tout groupe $(G,.)$ d'ordre p premier est cyclique et engendré par l'un quelconque de ses éléments distincts de 1.*

Démonstration. Soit a un élément de G distinct de 1. Alors 1 et a appartiennent à $\langle a\rangle$. Donc $|\langle a\rangle| \geqslant 2$. De plus, $|\langle a\rangle|$ divise p d'après 1. du théorème 3. p étant premier, nécessairement $|\langle a\rangle| = p$ et par conséquent $G = \langle a\rangle$. □

Corollaire 6. *Soit $(G,.)$ un groupe fini. Soit $a \in G$. Soit m l'ordre de a. Alors pour tout entier naturel k, $\big(a^k = 1\big) \Leftrightarrow (m|k)$.*

Démonstration. $\Leftarrow$: il existe un entier relatif k' tel que $k = mk'$. Ainsi, d'après le théorème 3 :

$$a^k = a^{mk'} = (a^m)^{k'} = 1^{k'} = 1$$

$\Rightarrow$: division euclidienne de k par m : $k = mq + r$ avec $0 \leqslant r < m$. D'où :

$$a^k = a^{mq+r} = a^{mq}a^r = a^r = 1$$

Ce qui entraîne $r = 0$ d'après le théorème 3. Ainsi, $m|k$. □

Remarque. Attention, $a^k = 1$ n'implique pas que k est l'ordre de a mais simplement que l'ordre de a divise k.

Théorème 7. *1. Tout groupe monogène infini est isomorphe au groupe $(\mathbb{Z}, +)$.*
2. Tout groupe cyclique d'ordre $n \in \mathbb{N}^*$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Démonstration. 1. Soit $(G, .)$ est un groupe monogène infini engendré par un élément g. Considérons l'application $f : (\mathbb{Z}, +) \to (G, .)$ définie par $f(k) \coloneqq g^k$. Il est clair que f est un morphisme. De plus $(G, .)$ étant monogène engendré par g, par définition, pour tout élément x de G, il existe un entier relatif k tel que $x = g^k$. Ainsi f est donc un épimorphisme. Enfin, si $g^r = g^s$, alors $g^{r-s} = 1$ et par conséquent $r = s$, ce qui prouve que f est un monomorphisme. f est donc un isomorphisme.

2. Soit $(G, .)$ un groupe cyclique d'ordre n engendré par g.

Considérons $f : (\mathbb{Z}/n\mathbb{Z}, +) \to (G, .)$ définie par $f(\overline{k}) \coloneqq g^k$. Alors f est clairement un isomorphisme. □

1.2 Sous-groupes d'un groupe monogène

1.2.1 D'un groupe monogène infini

Proposition 8. *Soit $(G, .)$ un groupe monogène infini. Si $(H, .)$ est un sous-groupe de $(G, .)$, alors il existe un entier naturel n tel que $(H, .)$ est isomorphe à $(n\mathbb{Z}, +)$.*

Démonstration. Soit $(G, .)$ un groupe monogène infini. Alors, d'après le théorème 7, il est isomorphe à $(\mathbb{Z}, +)$. Soit $(H, +)$ un sous-groupe de $(\mathbb{Z}, +)$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Sinon, il existe un élément strictement positif dans H. Soit m le plus petit des éléments strictement positifs de H. Comme $m \in H$, naturellement, $m\mathbb{Z} \subset H$. Soit $h \in H$. Effectuons la division euclidienne de h par m. Il existe un entier relatif q et un entier naturel r tels que :

$$\begin{cases} h = mq + r \\ 0 \leqslant r < m \end{cases}$$

Or, $r = h - mq \in H$. Comme $r < m$, alors nécessairement, $r = 0$. D'où $h = mq \in m\mathbb{Z}$. Ainsi, $H \subset m\mathbb{Z}$. □

1.2.2 D'un groupe cyclique

Définition 9. On appelle fonction indicatrice d'Euler la fonction définie sur $\mathbb{N}^*$ à valeurs dans $\mathbb{N}$ qui, à chaque entier naturel non nul n, associe le nombre d'entiers compris entre 1 et n premiers avec n.

Exemples. *On a* $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$ *et* $\varphi(8) = 4$.

Remarque. La fonction indicatrice d'Euler n'est pas croissante sur $\mathbb{N}^*$ car $\varphi(9) = 6$ et $\varphi(10) = 4$.

Théorème 10. *(Description des groupes cycliques) Soit* $n \in \mathbb{N}^*$. *Soit* G *un groupe cyclique d'ordre* n. *Soit* a *un générateur de* G.

1. *Tout sous-groupe de* $\langle a \rangle$ *est cyclique.*
2. *Pour tout entier naturel* k, $\left|\langle a^k \rangle\right| = \frac{n}{n \wedge k}$.
3. *Si* d *divise* n, *alors* $\langle a \rangle$ *contient* $\varphi(d)$ *éléments d'ordre* d.
4. $\langle a \rangle$ *contient* $\varphi(n)$ *générateurs. Ce sont les* a^k *tels que* $n \wedge k = 1$.
5. *Si* d *divise* n, *alors l'ensemble* $E_d := \{x \in \langle a \rangle, x^d = 1\}$ *est l'unique sous-groupe de* $\langle a \rangle$ *d'ordre* d, *de plus il est cyclique.*

Démonstration. 1. Soit H un sous-groupe de $\langle a \rangle$. Si $H = \{1\}$, il est évidemment cyclique. Si $H \neq \{1\}$, alors il existe un entier naturel non nul l tel que $a^l \in H$. Ainsi, $\{k \in \mathbb{N}^*, a^k = 1\}$ est non vide et minoré par 0 donc admet un minimum. Soit $d := \min\{k \in \mathbb{N}^*, a^k = 1\}$. $(H, .)$ étant un groupe, $\langle a^d \rangle \subset H$. Soit $a^k \in H$. Effectuons la division euclidienne de k par d : $k = dq + r$ avec $0 \leqslant r < d$. Ainsi, $(a)^k(a^{-dq}) = a^r \in H$ car H est un groupe. Ceci contredit la minimalité de d sauf si $r = 0$. D'où $a^k = (a^d)^q \in \langle a^d \rangle$. Ainsi, $H = \langle a^d \rangle$.

2. D'après le théorème 3, on a :

$$\begin{aligned} \left|\langle a^k \rangle\right| &= \min\{m \in \mathbb{N}^*, (a^k)^m = 1\} \\ &= \min\{m \in \mathbb{N}^*, a^{km} = 1\} \\ &= \min\{m \in \mathbb{N}^*, n | km\} \end{aligned}$$

Soit $d := n \wedge k$. Il existe alors deux entiers naturels n' et k' tels que $n = dn'$ et $k = dk'$ et $n' \wedge k' = 1$. Ainsi, $n|km$ est équivalent à $dn'|dk'm$ et à $n'|m$ car $n' \wedge k' = 1$. Or, le plus petit entier $m \in \mathbb{N}^*$ tel que $n'|m$ est n', c'est-à-dire $\frac{n}{n \wedge k}$. D'où :

$$\left|\langle a^k \rangle\right| = \frac{n}{n \wedge k}$$

3. d divise n donc il existe un entier naturel q tel que $n = dq$.

Soit a^k un élément de $\langle a\rangle$, on a :

$$\begin{aligned} \left|\langle a^k\rangle\right| = d &\Leftrightarrow \frac{n}{n\wedge k} = d \\ &\Leftrightarrow \frac{dq}{n\wedge k} = d \\ &\Leftrightarrow \frac{q}{n\wedge k} = 1 \\ &\Leftrightarrow n\wedge k = q \end{aligned}$$

Or il existe un entier naturel k' tel que $k = qk'$. Ainsi :

$$\left(\left|\langle a^k\rangle\right| = d\right) \Leftrightarrow \left(dq \wedge qk' = q\right) \Leftrightarrow \left(d \wedge k' = 1\right)$$

Or, des entiers k' premiers avec d, il y en a $\varphi(d)$.

4. a^k engendre $\langle a\rangle$ si, et seulement si, a^k est d'ordre n. Or a^k est d'ordre $\frac{n}{n\wedge k}$. Donc a^k engendre $\langle a\rangle$ si, et seulement si, $n\wedge k = 1$. Il y en a bien $\varphi(n)$ d'après la définition de la fonction indicatrice d'Euler.

5. $E_d = \{x \in \langle a\rangle,\, x^d = 1\}$ est clairement un sous-groupe de $\langle a\rangle$, ce dernier étant abélien. De plus, d'après 1., il est cyclique. D'après le corollaire 4, il contient tout sous-groupe de $\langle a\rangle$ d'ordre d. Soit g un générateur de E_d. Pour tout entier naturel non nul r, on a $(g^r)^d = 1$ qui est équivalent à n divise rd. Or d divise n, donc il existe un entier relatif k tel que $n = dk$. Mais alors, $(g^r)^d = 1$ est équivalent à k divise r. Ainsi, les éléments de E_d sont : $g^k, g^{2k}, \ldots, g^{dk} = g^n = 1$. Ils sont clairement tous distincts et il y en a donc d. E_d est donc engendré par g^k. Comme tout groupe cyclique d'ordre d, il possède $\varphi(d)$ générateurs. D'après 4., ce sont les g^{kr} avec $r\wedge d = 1$. □

Remarque. On peut synthétiser ce théorème ainsi :

Soit G un groupe cyclique d'ordre n. Alors, pour chaque diviseur d de n, l'ensemble $E_d = \{x \in G,\, x^d = 1\}$ est l'unique sous-groupe d'ordre d de G. Il est cyclique et possède exactement $\varphi(d)$ éléments d'ordre d. Ces éléments sont les générateurs de E_d et s'écrivent sous la forme $x^{\frac{n}{d}r}$, avec $1 \leqslant r \leqslant d$ et $r\wedge d = 1$.

Exemples. 1. Considérons le groupe cyclique $(\mathbb{Z}/12\mathbb{Z}, +)$. 4 divise 12, donc $E_4 = \{\overline{k} \in \mathbb{Z}/12\mathbb{Z},\, 4\overline{k} = \overline{0}\}$ est l'unique sous-groupe d'ordre 4 de $(\mathbb{Z}/12\mathbb{Z}, +)$. Il est cyclique et possède $\varphi(4) = 2$ éléments d'ordre 4. Ces éléments sont $\overline{3}$ et $\overline{9}$. E_4 contient aussi $\overline{0}$ et $\overline{6}$.

2. Considérons le groupe cyclique $\left(\mathbb{U}_{15} = \left\{e^{\frac{2ik\pi}{15}},\, k \in [\![0;14]\!]\right\}, \times\right)$. 3 divise 5, donc $E_3 = \left\{e^{\frac{2ik\pi}{15}} \in \mathbb{U}_{15},\, (e^{\frac{2ik\pi}{15}})^3 = 1\right\}$ est l'unique sous-groupe d'ordre 3 de $\left(\mathbb{U}_{15} = \left\{e^{\frac{2ik\pi}{15}},\, k \in [\![0;14]\!]\right\}, \times\right)$. Il est cyclique et possède $\varphi(3) = 2$ éléments d'ordre 3. Ces éléments sont $e^{\frac{2i\pi}{3}}$ et $e^{\frac{4i\pi}{3}}$. E_3 contient aussi 1.

Théorème 11. *(Formule de Möbius) Pour tout entier naturel non nul n, on a :*

$$n = \sum_{d|n} \varphi(d)$$

Démonstration. Soit $\langle a \rangle$ un groupe cyclique d'ordre n. D'après 3. du théorème 10, pour tout diviseur d de n, $\langle a \rangle$ contient $\varphi(d)$ éléments d'ordre d. Or tout élément de a a un ordre qui divise n d'après le théorème 3. D'où le résultat. □

Théorème 12. *(Caractérisation des groupes cycliques) Soit $(G, .)$ un groupe d'ordre $n \in \mathbb{N}^*$. Soit d un diviseur de n. Notons $E_d = \{x \in G,\ x^d = 1\}$ et $\alpha_G(d)$ le nombre d'éléments d'ordre d de G. Les assertions suivantes sont équivalentes :*

1. *Pour tout diviseur d de n, $|E_d| \leqslant d$.*
2. *Pour tout diviseur d de n, $\alpha_G(d) \leqslant \varphi(d)$.*
3. *Pour tout diviseur d de n, $\alpha_G(d) = \varphi(d)$.*
4. *Le groupe G est cyclique.*
5. *Pour tout diviseur d de n, $|E_d| = d$.*

Démonstration. $1 \Rightarrow 2$: si $\alpha_G(d) = 0$, c'est évident. Si $\alpha_G(d) \geqslant 1$, alors il existe un élément a de G d'ordre d. Donc $a \in E_d$ et $\langle a \rangle \subset E_d$. Par conséquent, $|\langle a \rangle| = d \leqslant |E_d|$. Ainsi, d'après 1., $d = |E_d|$ et, par suite, $E_d = \langle a \rangle$. Or $\langle a \rangle$ contient $\varphi(d)$ générateurs. Donc ce sont les seuls éléments d'ordre d de G. Par conséquent, $\alpha_G(d) \leqslant \varphi(d)$.

$2 \Rightarrow 3$: il est clair que $n = \sum_{d|n} \alpha_G(d)$. De plus, $n = \sum_{d|n} \varphi(d)$. Donc, d'après 2., nécessairement, pour tout diviseur d de n, $\alpha_G(d) = \varphi(d)$.

$3 \Rightarrow 4$: il suffit de prendre $d = n$ dans 3. Ainsi, G possède au moins un élément d'ordre n et est donc cyclique.

$4 \Rightarrow 5$: découle de 5. du théorème 10.

$5 \Rightarrow 1$: évident. □

1.3 Exemples

1.3.1 Produit de groupes cycliques

Théorème 13. *Soient G_1 et G_2 deux groupes cycliques d'ordres respectifs m et n.*

$$(m \wedge n = 1) \Leftrightarrow (G_1 \times G_2 \text{ cyclique})$$

Démonstration. $\Rightarrow$: G_1 étant cyclique d'ordre m est isomorphe à $(\mathbb{Z}/m\mathbb{Z}, +)$ et G_2 étant cyclique d'ordre n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$. Considérons l'application

$f : (\mathbb{Z}/mn\mathbb{Z}, +) \to (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, +)$ qui à $\ddot{k}$ associe $(\overline{k}, \tilde{k})$. f est clairement un morphisme de groupes. Déterminons $\ker(f)$. Supposons que $(\overline{k}, \tilde{k}) = (\overline{0}, \tilde{0})$. Alors m divise k et n divise k. Or m et n sont premiers entre eux, donc mn divise k et par conséquent $\ddot{k} = \ddot{0}$. Ainsi $\ker(f) = \{\ddot{0}\}$ et f est donc un monomorphisme. Le groupe de départ et le groupe d'arrivée ayant le même ordre, f est un isomorphisme.

$\Leftarrow$: supposons que $G_1 \times G_2$ est cyclique d'ordre mn. Raisonnons par l'absurde en supposant que $d \coloneqq m \wedge n \geqslant 2$. Alors il existe deux entiers naturels m' et n' tels que $m = dm'$ et $n = dn'$ avec $m' \wedge n' = 1$. Or :

$$(m \vee n) \times (m \wedge n) = mn$$

D'où : $m \vee n = dm'n' = m'n = mn' < mn$. Soit $(x, y) \in G_1 \times G_2$, on a :

$$(x, y)^{m \vee n} = (x^{m \vee n}, y^{m \vee n}) = (1; 1)$$

Ainsi, tout élément de $G_1 \times G_2$ a un ordre strictement inférieur à mn. Ce qui est en contradiction avec le fait que $G_1 \times G_2$ est cyclique d'ordre mn. Par conséquent, $m \wedge n = 1$. □

Exemples. Le groupe $((\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/15\mathbb{Z}), +)$ est cyclique car $8 \wedge 15 = 1$. Le groupe de Klein, $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ n'est pas cyclique car $2 \wedge 2 = 2$.

Remarque. Ce théorème permet de décomposer tout groupe cyclique en produit direct de groupes cycliques plus « petits ».

1.3.2 Sur un corps fini

Théorème 14. *Soit $(\mathbb{K}, +, \times)$ un corps fini. Alors $(\mathbb{K}^*, \times)$ est un groupe cyclique.*

Démonstration. Soit $(\mathbb{K}, +, \times)$ un corps fini. Nécessairement, $(\mathbb{K}^*, \times)$ est un groupe. Il s'agit donc de démontrer qu'il est cyclique. Soit d un diviseur de l'ordre de $(\mathbb{K}^*, \times)$. $E_d \neq \varnothing$ car $1 \in E_d$. Puisque $(\mathbb{K}, +, \times)$ est un corps, le polynôme $X^d - 1$ a au plus d racines sur $\mathbb{K}$. Donc $|E_d| \leqslant d$. Ainsi, d'après le théorème 12, $(\mathbb{K}^*, \times)$ est cyclique. □

Corollaire 15. *Soit p un nombre premier. Alors $\left((\mathbb{Z}/p\mathbb{Z})^*, \times\right)$ est un groupe cyclique. Il est isomorphe à $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$.*

Démonstration. Soit p un nombre premier. Alors $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps fini. Donc, d'après le théorème 14, $\left((\mathbb{Z}/p\mathbb{Z})^*, \times\right)$ est un groupe cyclique. Son ordre étant $p - 1$, d'après le théorème 7, il est isomorphe à $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$. □

Chapitre 2

Permutations d'un ensemble fini, groupe symétrique. Applications

Pré-requis

1. Composition de deux applications.
2. Définition d'une bijection.
3. Notions sur les groupes.
4. Relation d'équivalence sur un ensemble.
5. Division euclidienne.
6. Isométries du plan.

2.1 Permutations d'un ensemble fini

Définition 16. Soit $n \in \mathbb{N}^*$. On appelle permutation de $[\![1;n]\!]$ toute bijection de $[\![1;n]\!]$ dans $[\![1;n]\!]$. L'ensemble des permutations de $[\![1;n]\!]$ est noté $\mathfrak{S}_n$.

Remarque. Notation matricielle d'une permutation σ :

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & k & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(k) & \dots & \sigma(n) \end{pmatrix}$$

Proposition 17. *Soit $n \in \mathbb{N}^*$.*

1. *$(\mathfrak{S}_n, \circ)$ est un groupe d'ordre $n!$.*
2. *$(\mathfrak{S}_n, \circ)$ est abélien si, et seulement si, $n \leqslant 2$.*

Démonstration. 1. $(\mathfrak{S}_n, \circ)$ est clairement un groupe. Soit $\sigma \in (\mathfrak{S}_n, \circ)$. Définir σ revient à définir $\sigma(i)$ pour tout $i \in [\![1; n]\!]$. Pour $\sigma(1)$ nous avons n choix possibles, pour $\sigma(2)$, nous avons alors $n-1$ choix possibles, pour $\sigma(3)$, nous avons alors $n-2$ choix possibles, etc. D'où $n!$ manières différentes de définir σ. Ainsi $|\mathfrak{S}_n| = n!$.

2. $(\mathfrak{S}_1 = \{\mathrm{id}\}, \circ)$ est clairement abélien. On vérifie aisément que $(\mathfrak{S}_2, \circ)$ est abélien. En revanche, on a d'une part $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ et d'autre part $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.
Donc $(\mathfrak{S}_3, \circ)$ n'est pas abélien. Pour démontrer que, pour tout $n \geqslant 3$, $(\mathfrak{S}_n, \circ)$ n'est pas abélien il suffit de considérer les deux permutations σ et σ' telles que $\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 2$, $\sigma'(1) = 3$, $\sigma'(2) = 1$, $\sigma'(3) = 2$ et pour tout $i \in [\![4; n]\!]$, $\sigma(i) = \sigma'(i) = i$, lorsque $n \geqslant 4$. □

Définition 18. Soit $n \in \mathbb{N}^*$. Soit $\sigma \in (\mathfrak{S}_n, \circ)$.

1. On appelle support de σ l'ensemble des entiers $k \in [\![1; n]\!]$ tels que $\sigma(k) \neq k$. On note $\mathrm{supp}(\sigma) \coloneqq \{k \in [\![1; n]\!],\ \sigma(k) \neq k\}$.
2. On appelle point fixe de σ tout élément $k \in [\![1; n]\!]$ tel que $\sigma(k) = k$. On note $\mathrm{fix}(\sigma) \coloneqq \{k \in [\![1; n]\!],\ \sigma(k) = k\}$.

Remarque. $\forall\, \sigma \in (\mathfrak{S}_n, \circ)$, $[\![1; n]\!] = \mathrm{fix}(\sigma) \bigsqcup \mathrm{supp}(\sigma)$.

Proposition 19. *Soit $n \in \mathbb{N}^*$. Soit $\sigma \in (\mathfrak{S}_n, \circ)$. La relation binaire $\Re$ définie sur $[\![1; n]\!]$ par :*

$$(x \Re y) \iff \big(\exists\, k \in \mathbb{Z},\ y = \sigma^k(x)\big)$$

est une relation d'équivalence. La classe d'équivalence de x est appelée la σ-orbite de x. Elle est notée $orb_{\langle\sigma\rangle}(x)$. On a donc $orb_{\langle\sigma\rangle}(x) = \{\sigma^k(x),\ k \in \mathbb{Z}\}$.

Démonstration. - *Réflexivité :* $x \Re x$ car $x = \sigma^0(x) = \mathrm{id}(x)$.

- *Symétrie :* $x \Re y$. Donc il existe $k \in \mathbb{Z}$, tel que $y = \sigma^k(x)$.

D'où : $x = (\sigma^k)^{-1}(y) = \sigma^{-k}(y)$Ainsi, $y \Re x$.

- *Transitivité :* $x \Re y$ et $y \Re z$. Donc il existe k, $k' \in \mathbb{Z}$, tels que $y = \sigma^k(x)$ et $z = \sigma^{k'}(y)$. Ainsi, $z = (\sigma^{k'} \circ \sigma^k)(x) = \sigma^{k+k'}(x)$ et $x \Re z$. □

Exemple. Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix} \in \mathfrak{S}_5$, on a :

$$\begin{cases} \mathrm{orb}_{\langle\sigma\rangle}(4) = \{4\} \\ \mathrm{orb}_{\langle\sigma\rangle}(3) = \{3\} \\ \mathrm{orb}_{\langle\sigma\rangle}(1) = \mathrm{orb}_{\langle\sigma\rangle}(2) = \mathrm{orb}_{\langle\sigma\rangle}(5) = \{1;2;5\} \end{cases}$$

Définition 20. Soit n un entier naturel tel que $n \geqslant 2$. On dit qu'une permutation $\sigma \in (\mathfrak{S}_n, \circ)$ est un cycle lorsqu'il existe une unique σ-orbite non réduite à un point. Autrement dit, $\sigma \in (\mathfrak{S}_n, \circ)$ est un cycle lorsqu'il existe un entier naturel p tel que $p \geqslant 2$, $a_1, \ldots, a_p \in [\![1; n]\!]$ deux à deux distincts tels que :

$$\begin{cases} \forall\, k \in \{1, \ldots, p-1\},\ \sigma(a_k) = a_{k+1} \\ \sigma(a_p) = a_1 \\ \forall\, x \notin \{a_1, \ldots, a_p\},\ \sigma(x) = x \end{cases}$$

L'entier p est alors appelé la longueur du cycle σ. On la note $l(\sigma)$.
σ est alors appelé un p-cycle et est noté $\sigma := (a_1,\, a_2, \ldots,\, a_p)$. Un cycle de longueur 2 est appelé une transposition.

Exemples. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix} \in \mathfrak{S}_5$ est un 5-cycle car elle n'admet qu'une seule σ-orbite non réduite à un point. On écrit $\sigma = (1,\, 4,\, 5,\, 2,\, 3)$.

$\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix} \in \mathfrak{S}_5$ n'est pas un cycle car elle admet deux orbites non réduites à un point. En effet, $\mathrm{orb}_{\langle\sigma\rangle}(1) = \{1;4;5\}$ et $\mathrm{orb}_{\langle\sigma\rangle}(2) = \{2;3\}$.

Remarque. On a :
$\mathrm{supp}(a_1,\, a_2, \ldots,\, a_p) = \{a_1, a_2, \ldots, a_p\}$.
$\mathrm{fix}(a_1,\, a_2, \ldots,\, a_p) = [\![1; n]\!] \backslash \{a_1, a_2, \ldots, a_p\}$.

Proposition 21. *Soient n, $p \in \mathbb{N}$ tels que $2 \leqslant p \leqslant n$. Soit $c := (a_1,\, a_2, \ldots,\, a_p)$ un p-cycle de $(\mathfrak{S}_n, \circ)$.*

1. $\forall\, \sigma \in \mathfrak{S}_n,\ \sigma \circ c \circ \sigma^{-1} = (\sigma(a_1),\, \sigma(a_2), \ldots,\, \sigma(a_p))$.
2. $\forall\, x \in \mathrm{supp}(c),\ \mathrm{supp}(c) = \{c^k(x),\, k \in \mathbb{Z}\}$.
3. *L'ordre de c dans $(\mathfrak{S}_n, \circ)$ vaut $l(c)$.*
4. $\forall\, x \in \mathrm{supp}\ (c),\ c = \big(x,\, c(x),\, c^2(x), \ldots,\, c^{l(c)-1}(x)\big)$.

Démonstration. 1. On a :

$$\begin{aligned} & x \in \text{fix}(\sigma \circ c \circ \sigma^{-1}) \\ \Leftrightarrow \quad & (\sigma \circ c \circ \sigma^{-1})(x) = x \\ \Leftrightarrow \quad & (c \circ \sigma^{-1})(x) = \sigma^{-1}(x) \\ \Leftrightarrow \quad & \sigma^{-1}(x) = \text{fix}(c) \\ \Leftrightarrow \quad & x \in (\sigma \text{fix}(c)) \\ \Leftrightarrow \quad & x \in \text{fix}\left((\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_p))\right) \end{aligned}$$

et :

$$\begin{aligned} & x \in \text{supp}(\sigma \circ c \circ \sigma^{-1}) \\ \Leftrightarrow \quad & (\sigma \circ c \circ \sigma^{-1})(x) \neq x \\ \Leftrightarrow \quad & (c \circ \sigma^{-1})(x) \neq \sigma^{-1}(x) \\ \Leftrightarrow \quad & \sigma^{-1}(x) \in \text{supp}(c) \\ \Leftrightarrow \quad & x \in \sigma\left(\text{supp}(c)\right) \\ \Leftrightarrow \quad & x \in \text{supp}\left((\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_p))\right) \end{aligned}$$

2. Soit $x \in \text{supp}(c)$. Alors il existe $i \in [\![1; p-1]\!]$ tel que $x = c^i(a_1)$. Démontrons que $\text{supp}(c) = \{c^k(x),\, k \in \mathbb{Z}\}$.

$\subset$: Soit $y \in \text{supp}(c)$. Alors il existe $j \in [\![0; p-1]\!]$ tel que $y = c^j(a_1)$.

D'où $y = c^j\left(c^{-i}(x)\right) = c^{j-i}(x)$. Or $j - i \in \mathbb{Z}$. D'où $y \in \{c^k(x),\, k \in \mathbb{Z}\}$.

$\supset$: Soit $y \in \{c^k(x),\, k \in \mathbb{Z}\}$. Alors il existe $k \in \mathbb{Z}$ tel que $y = c^k(x)$.

D'où $y = c^k\left(c^j(a_1)\right) = c^{k+j}(a_1)$ et par conséquent $y \in \text{supp}(c)$.

3. $\forall\, i \in [\![1; p]\!]$, $c^{l(c)}(a_i) = a_i$. Donc $c^{l(c)} = \text{id}$. Donc l'ordre de c divise $l(c)$ et lui est donc inférieur. Soit $k \in [\![1; p-1]\!]$, $c^k(a_1) = a_{k+1} \neq a_1$ donc $c^k \neq \text{id}$. Donc $l(c)$ est inférieur ou égal à l'ordre de c. D'où l'égalité.

4. C'est une conséquence immédiate de 2. et 3. □

Proposition 22. *Soit n un entier naturel tel que $n \geqslant 2$. Deux cycles de $(\mathfrak{S}_n, \circ)$ dont les supports sont disjoints commutent.*

Démonstration. Soient c et c' deux cycles de $\mathfrak{S}_n$ dont les supports sont disjoints. Soit $x \in [\![1; n]\!]$.

Si $x \notin \text{supp}(c) \cup \text{supp}(c')$, alors on a :

$$(c \circ c')(x) = c\left(c'(x)\right) = c(x) = x = c'(x) = c'\left(c(x)\right) = (c' \circ c)(x)$$

Si $x \in \text{supp}(c)$ et $x \notin \text{supp}(c')$, alors d'après la proposition 21, $c(x) \notin \text{supp}(c')$. D'où :

$$(c' \circ c)(x) = c'\left(c(x)\right) = c(x) = c\left(c'(x)\right) = (c \circ c')(x)$$

De même si $x \notin \text{supp}(c)$ et $x \in \text{supp}(c')$. □

2.2 Décomposition d'une permutation

Théorème 23. *(Décomposition d'une permutation) Soit n un entier naturel tel que $n \geqslant 2$. Toute permutation de $(\mathfrak{S}_n, \circ)$ se décompose de manière unique (à l'ordre des facteurs près) en un produit de cycles à supports deux à deux disjoints.*

Démonstration. 1. *Existence :* Soit $\sigma \in \mathfrak{S}_n$. L'ensemble $[\![1; n]\!]$ étant fini, il existe un nombre fini r, avec $r \in [\![1; n]\!]$, de σ-orbite(s). Soient $O_1, \ldots, O_r$ ces orbites. On a : $[\![1; n]\!] = \bigsqcup_{i=1}^{i=r} O_i$. Pour tout $i \in [\![1; r]\!]$, définissons c_i par $c_i(x) := \begin{cases} \sigma(x) & \text{si } x \in O_i \\ x & \text{si } x \notin O_i \end{cases}$.

Si $x \notin O_i$, $\text{orb}_{\langle c_i \rangle}(x) = \{x\}$.

Si $x \in O_i$, alors $c_i(x) = \sigma(x)$ et donc $\text{orb}_{\langle c_i \rangle}(x) = \text{orb}_{\langle \sigma \rangle}(x) = O_i$. Ainsi, il y a au plus une c_i-orbite non réduite à un point et par conséquent, c_i est un cycle ou l'identité. Posons alors $s := c_1 \circ c_2 \circ \ldots \circ c_r$ et démontrons que $s = \sigma$:

Soit $x \in [\![1; n]\!]$. Alors il existe un unique $i \in [\![1; r]\!]$ tel que $x \in O_i$. On a donc :

$$\begin{cases} \forall\, j \in [\![1; n]\!] \text{ tel que } j \neq i,\ c_j(x) = x \\ c_i(x) = \sigma(x). \\ \forall\, j \in [\![1; n]\!] \text{ tel que } j \neq i,\ c_j\left(\sigma(x)\right) = \sigma(x) \text{ car } \sigma(x) \in O_i \end{cases}$$

D'où $s(x) = \sigma(x)$.

2. *Unicité :* Soient $d_1, \ldots, d_q$ des cycles à supports deux à deux disjoints tels que $\sigma = d_1 \circ d_2 \circ \ldots \circ d_q$. Soit $x \in [\![1; n]\!]$. Il existe un unique $j \in [\![1; q]\!]$ tel que $x \in \text{supp}(d_j)$. Comme les supports de $d_1, \ldots, d_q$ sont deux à deux disjoints, seul d_j a un effet sur x. D'où $\sigma(x) = d_j(x)$ et, par récurrence, pour tout $k \in \mathbb{Z}$, $\sigma^k(x) = d_j^k(x)$. Ainsi, $\text{orb}_{\langle \sigma \rangle}(x) = \text{orb}_{\langle d_j \rangle}(x) = \text{supp}(d_j)$. Par conséquent, $\text{supp}(d_1), \ldots, \text{supp}(d_q)$ sont les σ-orbites. On en déduit que $r = q$ et que, pour tout $i \in [\![1; q]\!]$, $\text{supp}(d_i) = O_i$. Donc pour tout $i \in [\![1; q]\!]$, $d_i = c_i$. D'où l'unicité. □

Exemple. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 1 & 7 & 6 & 5 & 2 \end{pmatrix} \in \mathfrak{S}_7$. Décomposons σ en produit de cycles à supports disjoints. On a : $\text{orb}_{\langle \sigma \rangle}(1) = \{1; 4; 7; 2; 3\}$ et $\text{orb}_{\langle \sigma \rangle}(5) = \{5; 6\}$ d'où : $\sigma = (1,\, 4,\, 7,\, 2,\, 3) \circ (5,\, 6)$.

Remarque. Cette décomposition permet de calculer σ^{2024}.

En effet, $\sigma^{2024} = (1,\, 4,\, 7,\, 2,\, 3)^{2024} \circ (5\,6)^{2024} = (1,\, 3,\, 2,\, 7,\, 4)$ d'après les propositions 21 et 22.

Corollaire 24. *Soit n un entier naturel tel que $n \geqslant 2$. $(\mathfrak{S}_n, \circ)$ est engendré par les transpositions.*

Démonstration. D'après le théorème 23, il suffit de démontrer que tout cycle se décompose en un produit de transposition(s). Soit $c := (a_1, a_2, \ldots, a_p)$ un p-cycle de $\mathfrak{S}_n$. On a alors :

$$c = (a_1, a_2, \ldots, a_p) = (a_1, a_2) \circ (a_2, a_3) \circ \ldots \circ (a_{p-1}, a_p)$$

En effet, on vérifie aisément que :

$$\begin{cases} \forall\, i \in [\![1; p-1]\!],\ (a_1, a_2) \circ (a_2, a_3) \circ \ldots \circ (a_{p-1}, a_p)(a_i) = a_{i+1} = c(a_i) \\ (a_1, a_2) \circ (a_2, a_3) \circ \ldots \circ (a_{p-1}, a_p)(a_p) = a_1 = c(a_p) \\ \forall\, x \notin \mathrm{supp}(c),\ (a_1, a_2) \circ (a_2, a_3) \circ \ldots \circ (a_{p-1}, a_p)(x) = x = c(x) \end{cases}$$

□

Remarque. Il n'y a plus unicité ici. En effet :

$$(1, 2, 3) = (1, 2) \circ (2, 3) = (1, 2) \circ (1, 2) \circ (1, 2) \circ (2, 3) = (1, 3) \circ (1, 2)$$

Exemple. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 1 & 7 & 6 & 5 & 2 \end{pmatrix} \in \mathfrak{S}_7$. Nous avons vu que : $\sigma = (1, 4, 7, 2, 3) \circ (5, 6)$. D'où $\sigma = (1, 4) \circ (4, 7) \circ (7, 2) \circ (2, 3) \circ (5, 6)$.

Corollaire 25. *(Systèmes de générateurs de $\mathfrak{S}_n$) Soit n un entier naturel tel que $n \geqslant 2$. $(\mathfrak{S}_n, \circ)$ est engendré par :*

1. $\{(i, j),\ 1 \leqslant i < j \leqslant n\}$.
2. $\{(i, i+1),\ 1 \leqslant i \leqslant n-1\}$.
3. $\{(1, i),\ 2 \leqslant i \leqslant n\}$.

Démonstration. 1. Découle directement du corollaire 24 et en remarquant que $(i, j) = (j, i)$.

2. Soient $i, j \in [\![1; n]\!]$ tels que $1 \leqslant i < j \leqslant n$. On vérifie aisément que $(i, j) = (i, i+1) \circ (i+1, i+2) \circ \ldots \circ (j-2, j-1) \circ (j-1, j) \circ (j-2, j-1) \circ \ldots \circ (i, i+1)$. Le point 1. permet alors de conclure.

3. Soient $i, j \in [\![1; n]\!]$ tels que $1 \leqslant i < j \leqslant n$. On vérifie aisément que $(i, j) = (1, i) \circ (1, j) \circ (1, i)$. Le point 1. permet alors de conclure. □

2.3 Signature

Définition 26. Soit n un entier supérieur ou égal à 2. Soit $\sigma \in (\mathfrak{S}_n, \circ)$. On appelle inversion de σ tout couple $(i, j) \in [\![1; n]\!]^2$ tel que $i < j$ et $\sigma(i) > \sigma(j)$. On note $I(\sigma)$ le nombre d'inversions de σ. On appelle signature de σ le nombre noté $\varepsilon(\sigma)$ tel que $\varepsilon(\sigma) = (-1)^{I(\sigma)}$.

Exemple. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix} \in \mathfrak{S}_5$. $\sigma(1) > \sigma(2)$, $\sigma(1) > \sigma(3)$, $\sigma(1) > \sigma(4)$, $\sigma(1) > \sigma(5)$, $\sigma(2) > \sigma(3)$. σ compte 5 inversions. Sa signature est donc $\varepsilon(\sigma) = (-1)^5 = -1$.

Théorème 27. *Soit n un entier supérieur ou égal à 2. Alors :*

1. $\forall \sigma \in \mathfrak{S}_n$, $\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i)-\sigma(j)}{i-j}$.
2. *L'application $\varepsilon : (\mathfrak{S}_n, \circ) \to (\{-1; 1\}, \times)$ définie par $\varepsilon(\sigma) = (-1)^{I(\sigma)}$ est un morphisme de groupes. Il est le seul non trivial.*

Démonstration. 1. σ étant une permutation de $[\![1; n]\!]$, on a naturellement, pour tous $i, j \in [\![1; n]\!]$ tels que $1 \leqslant i < j \leqslant n$, $\prod_{1 \leqslant i < j \leqslant n} |\sigma(i) - \sigma(j)| = \prod_{1 \leqslant i < j \leqslant n} |i - j|$. D'où $\left| \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i)-\sigma(j)}{i-j} \right| = 1$. De plus, le nombre de paires $\{i; j\}$ telles que $1 \leqslant i < j \leqslant n$ et $\frac{\sigma(i)-\sigma(j)}{i-j} < 0$ est égal à $I(\sigma)$. Donc $\prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i)-\sigma(j)}{i-j}$ est du même signe que $\varepsilon(\sigma)$. D'où le résultat.

2. Soient $\sigma, \sigma' \in \mathfrak{S}_n$. On a :

$$\begin{aligned}
\varepsilon(\sigma \circ \sigma') &= \prod_{1 \leqslant i < j \leqslant n} \frac{(\sigma \circ \sigma')(j) - (\sigma \circ \sigma')(i)}{j - i} \\
&= \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(\sigma')(j) - \sigma(\sigma')(i)}{\sigma'(j) - \sigma'(i)} \times \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma'(j) - \sigma'(i)}{j - i} \\
&= \prod_{1 \leqslant i' < j' \leqslant n} \frac{\sigma(j') - \sigma(i')}{j' - i'} \times \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma'(j) - \sigma'(i)}{j - i} \\
&= \varepsilon(\sigma) \times \varepsilon(\sigma')
\end{aligned}$$

Soit $\varphi : (\mathfrak{S}_n, \circ) \to (\{-1; +1\}, \times)$ un morphisme de groupes. Soient $i, j \in [\![1; n]\!]$ tels que $1 \leqslant i < j \leqslant n$. D'après le corollaire 25, $(i, j) = (1, i) \circ (1, j) \circ (1, i)$. Donc $\varphi((i, j)) = \varphi((1, j)) \times \varphi((1, i))^2 = \varphi((1, j))$. De même, on démontre que $\varphi((i, j)) = \varphi((1, i))$. D'où $\varphi((i, j)) = \varphi((1, i)) = \varphi((1, j))$.
Si $\varphi((1, i)) = \varphi((1, j)) = 1$, alors $\varphi((i, j)) = 1$ et φ est le morphisme trivial. Sinon, $\varphi((i, j)) = \varphi((1, i)) = \varphi((1, j)) = -1$ et alors φ et ε coïncident sur les transpositions de $\mathfrak{S}_n$ et par conséquent sur $\mathfrak{S}_n$ tout entier d'après le corollaire 24. □

Remarque. Si σ est une transposition, alors $\varepsilon(\sigma) = -1$. Si σ est un cycle, alors $\varepsilon(\sigma) = (-1)^{l(\sigma)-1}$.

Exemple. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 1 & 6 & 3 \end{pmatrix} \in \mathfrak{S}_6$. On a $\sigma = (1, 5, 6, 3, 2, 4)$. D'où $\varepsilon(\sigma) = (-1)^5 = -1$.

Définition 28. Soit n un entier supérieur ou égal à 2. On appelle groupe alterné d'ordre n le sous-ensemble de $\mathfrak{S}_n$ noté $\mathfrak{A}_n$ des permutations de signature 1.

Théorème 29. *Soit n un entier supérieur ou égal à 2.*

1. *$(\mathfrak{A}_n, \circ)$ est un sous-groupe de $(\mathfrak{S}_n, \circ)$ d'ordre $\frac{n!}{2}$.*
2. *$(\mathfrak{A}_n, \circ)$ est engendré par les 3-cycles.*

Démonstration. 1. $\mathfrak{A}_n = \ker(\varepsilon)$ donc $(\mathfrak{A}_n, \circ)$ est un sous-groupe de $(\mathfrak{S}_n, \circ)$. Soit τ une transposition quelconque de $\mathfrak{S}_n$. L'application $\Psi : \mathfrak{A}_n \to \mathfrak{S}_n \backslash \mathfrak{A}_n$ définie par $\Psi(\sigma) = \tau \circ \sigma$ est une bijection. Donc $|\mathfrak{A}_n| = |\mathfrak{S}_n \backslash \mathfrak{A}_n|$. D'où :

$$|\mathfrak{A}_n| = \frac{|\mathfrak{S}_n|}{2} = \frac{n!}{2}$$

2. Soit $\sigma \in \mathfrak{A}_n$. Par définition de $(\mathfrak{A}_n, \circ)$, σ se décompose en un nombre pair de transpositions. Or tout produit de deux transpositions est égal à un 3-cycle :

$$\begin{aligned}(a,\, b) \circ (b,\, c) &= (a,\, b,\, c)\\ (a,\, b) \circ (a,\, c) &= (a,\, c,\, b)\\ (a,\, b) \circ (c,\, d) &= (a,\, b,\, c) \circ (b,\, c,\, d)\end{aligned}$$

D'où le résultat. □

2.4 Applications

2.4.1 Théorème de Cayley

Lemme 30. *Soit $n \in \mathbb{N}^*$. Soit E un ensemble de cardinal n. Le groupe $(\mathfrak{S}(E), \circ)$ des bijections de E dans E est isomorphe à $(\mathfrak{S}_n, \circ)$.*

Démonstration. E et $[\![1; n]\!]$ étant équipotents, il existe une bijection $f : E \to [\![1; n]\!]$. Soit $\Psi : (\mathfrak{S}(E), \circ) \to (\mathfrak{S}_n, \circ)$ l'application définie par $\Psi(\sigma) = f \circ \sigma \circ f^{-1}$. Ψ est évidemment bien définie. Ψ est bijective en tant que composée de bijections. Prouvons que Ψ est un morphisme de groupes. Soient σ_1, $\sigma_2 \in \mathfrak{S}(E)$, on a :

$$\begin{aligned}\Psi(\sigma_1 \circ \sigma_2) &= f \circ (\sigma_1 \circ \sigma_2) \circ f^{-1}\\ &= f \circ (\sigma_1 \circ (f^{-1} \circ f) \circ \sigma_2) \circ f^{-1}\\ &= (f \circ \sigma_1 \circ f^{-1}) \circ (f \circ \sigma_2 \circ f^{-1})\\ &= \Psi(\sigma_1) \circ \Psi(\sigma_2)\end{aligned}$$

□

Théorème 31. *(Théorème de Cayley) Soit $n \in \mathbb{N}^*$. Soit $(G, .)$ un groupe d'ordre n. Il existe un sous-groupe G' de $(\mathfrak{S}_n, \circ)$ isomorphe à G.*

Démonstration. On a : $|G| = |[\![1; n]\!]|$. Donc, d'après le lemme 30, il existe un isomorphisme $\Psi : (\mathfrak{S}(G), \circ) \to (\mathfrak{S}_n, \circ)$. Soit alors $\Phi : (G, .) \to (\mathfrak{S}_n, \circ)$ l'application définie par $\Phi(g) = \Psi(L_g)$, où $L_g : G \to G$ est définie par $L_g(x) = g.x$.
Φ est bien définie car L_g est une permutation de G. Prouvons que Φ est un morphisme de groupes. Soient g_1 et g_2 deux éléments de G, on a :

$$\Phi(g_1.g_2) = \Psi(L_{g_1.g_2}) = \Psi(L_{g_1} \circ L_{g_2}) = \Psi(L_{g_1}) \circ \Psi(L_{g_2}) = \Phi(g_1) \circ \Phi(g_2)$$

Prouvons que Φ est injectif. $g \in \ker(\Phi)$ si, et seulement si, $\Phi(g) = \Psi(L_g) = \mathrm{id}$. C'est-à-dire si, et seulement si, $L_g \in \ker(\Psi)$. Or Ψ est un isomorphisme. Donc $\ker(\Psi) = \{\mathrm{id}\}$ et $L_g = \mathrm{id}$. D'où $L_g(e) = \mathrm{id}(e) = e$ et donc $g.e = g = e$. Ainsi, $\ker(\Phi) = \{e\}$ et Φ est injectif. Par conséquent, G est isomorphe à $\mathrm{im}(\Phi)$ qui est un sous-groupe de $(\mathfrak{S}_n, \circ)$. □

Remarque. Tout groupe fini peut donc être vu comme un sous-groupe d'un groupe de permutations.

2.4.2 Le jeu du taquin

Le jeu du taquin est un carré constitué de seize cases. Sur chacune d'elle sauf une repose un pavé. Ces pavés sont numérotés de un à quinze. La case vide permet le mouvement des pavés, un pavé pouvant glisser vers la case vide. En 1870, le problémiste américain Sam Loyd offrit une récompense de 1 000 dollars à la personne qui proposerait une solution pour passer de la position initiale :

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

à la position finale :

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Théorème 32. *Le jeu du taquin n'est pas résoluble.*

Démonstration. Ne comptons pas la case vide et suivons le sens de lecture suivant :

→	→	→	↘
↙	←	←	↙
↘	→	→	↘
←	←	←	↙

On peut alors associer à la position initiale la permutation :

$$\begin{aligned}\sigma_i &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 2 & 3 & 4 & 8 & 7 & 6 & 5 & 9 & 10 & 11 & 12 & 15 & 14 & 13 \end{pmatrix} \\ &= (5,\,8) \circ (6,\,7) \circ (13,\,15)\end{aligned}$$

Ainsi, à la position initiale est associée la permutation σ_i telle que $\varepsilon(\sigma_i) = -1$. De la même façon, à la position finale est associée la permutation :

$$\begin{aligned}\sigma_f &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 2 & 3 & 4 & 8 & 7 & 6 & 5 & 9 & 10 & 11 & 12 & 14 & 15 & 13 \end{pmatrix} \\ &= (5,\,8) \circ (6,\,7) \circ (13,\,14,\,15) \\ &= (5,\,8) \circ (6,\,7) \circ (13,\,14) \circ (14,\,15)\end{aligned}$$

Ainsi, à la position finale est associée la permutation σ_f telle que $\varepsilon(\sigma_f) = 1$. Démontrons que chaque déplacement autorisé correspond à une permutation de signature 1.

1	2	3	4
7		6	5
8	9	10	11
12	13	14	15

La « descente » du 2 correspond au 5-cycle : (2, 3, 4, 5, 6).

La « montée » du 9 correspond au 3-cycle : (7, 8, 9).

La translation vers la gauche de 6 et 5 accompagnée de la « descente » de 4 correspondent au 7-cycle : (4, 5, 6, 7, 1, 2, 3).

Donc, tout déplacement correspond à un cycle de longueur 3, 5 ou 7.

Or, d'après le théorème 27, la signature d'un cycle de longueur impaire vaut 1. On ne pourra donc passer de σ_i à σ_f. □

Chapitre 3

Anneau $\mathbb{Z}/n\mathbb{Z}$. Applications

Pré-requis

1. Notions de groupe, anneau et corps.
2. Théorème de Lagrange.
3. L'anneau $(\mathbb{Z}, +, \times)$.
4. Théorème de Bézout.
5. Notion de polynôme.

3.1 L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Définition 33. Soit $n \in \mathbb{N}$. Soient x, $y \in \mathbb{Z}$. On dit que x est congru à y modulo n et l'on écrit $x \equiv y[n]$ lorsque $x - y \in n\mathbb{Z}$.

Exemple. $17 \equiv 2[5]$.

Proposition 34. *Soit $n \in \mathbb{N}$. La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.*

Démonstration. - *Réflexivité* : $x - x = 0 \in n\mathbb{Z}$, donc $x \equiv x[n]$.
- *Symétrie* : Si $x \equiv y[n]$ alors $x - y \in n\mathbb{Z}$. Par conséquent, $y - x \in n\mathbb{Z}$ et donc $y \equiv x[n]$.
- *Transitivité* : Si $x \equiv y[n]$ et $y \equiv z[n]$, alors $x - y \in n\mathbb{Z}$ et $y - z \in n\mathbb{Z}$. $(n\mathbb{Z}, +)$ étant un groupe, $x - y + y - z \in n\mathbb{Z}$ soit $x - z \in n\mathbb{Z}$, c'est-à-dire $x \equiv z[n]$. □

Proposition 35. *Soit $n \in \mathbb{N}^*$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences de $\mathbb{Z}$ pour la relation de congruence et $\overline{x}$ la classe d'équivalence de $x \in \mathbb{Z}$. Alors :*

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$$

Démonstration. $\supset$: Évident.

$\subset$: Soit $x \in \mathbb{Z}$. Division euclidienne de x par n : $x = nq + r$ avec $q \in \mathbb{Z}$ et $r \in \{0, \dots, n-1\}$. D'où $x \equiv r[n]$ et donc $\overline{x} = \overline{r}$. Ainsi, $\mathbb{Z}/n\mathbb{Z} \subset \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$. □

Remarque. Si $n = 0$, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}$ que l'on connaît bien.

Proposition 36. *Soit $n \in \mathbb{N}^*$. La relation de congruence est compatible avec l'addition et la multiplication de $\mathbb{Z}$:*

1. $\forall\, x, x', y, y' \in \mathbb{Z}$, $(x \equiv x'[n]\ et\ y \equiv y'[n]) \Rightarrow (x + y \equiv x' + y'[n])$
2. $\forall\, x, x', y, y' \in \mathbb{Z}$, $(x \equiv x'[n]\ et\ y \equiv y'[n]) \Rightarrow (x \times y \equiv x' \times y'[n])$

Démonstration. 1. Soient x, x', y, $y' \in \mathbb{Z}$ tels que $x \equiv x'[n]$ et $y \equiv y'[n]$. Alors n divise $x - x'$ et n divise $y - y'$. Ainsi, il existe deux entiers q_1, $q_2 \in \mathbb{Z}$ tels que $x - x' = nq_1$ et $y - y' = nq_2$. D'où $x - x' + y - y' = n(q_1 + q_2)$. Ainsi, n divise $x + y - (x' + y')$. C'est-à-dire, $x + y \equiv x' + y'[n]$.

2. Soient x, x', y, $y' \in \mathbb{Z}$, tels que $x \equiv x'[n]$ et $y \equiv y'[n]$. Alors n divise $x - x'$ et n divise $y - y'$. Ainsi, il existe deux entiers q_1, $q_2 \in \mathbb{Z}$ tels que $x - x' = nq_1$ et $y - y' = nq_2$. D'où $x \times y = x' \times y' + n(x' \times q_2 + y' \times q_1)$. Ainsi, n divise $x \times y - x' \times y'$. C'est-à-dire, $x \times y \equiv x' \times y'[n]$. □

Théorème 37. *Soit $n \in \mathbb{N}^*$. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.*

Démonstration. 1. Définissons la somme de deux classes α et β de $\mathbb{Z}/n\mathbb{Z}$. Soit x un représentant de α. Soit y un représentant de β. On peut alors former l'entier $x + y$ et sa classe associée $\overline{x + y}$. Soient x' un autre représentant de α et y' un autre représentant de β. On peut alors former l'entier $x' + y'$ et sa classe associée $\overline{x' + y'}$. Or, $x \equiv x'[n]$ et $y \equiv y'[n]$. Donc, d'après la proposition 36, $x + y \equiv x' + y'[n]$, c'est-à-dire, $\overline{x + y} \equiv \overline{x' + y'}$. Ainsi, la classe $\overline{x + y}$ est indépendante des représentants choisis. On dit que c'est la somme des classes $\overline{x}$ et $\overline{y}$. On pose donc $\overline{x} + \overline{y} := \overline{x + y}$.

2. On définit de la même manière $\overline{x} \times \overline{y} := \overline{x \times y}$.

3. On vérifie aisément que l'addition et la multiplication sur $\mathbb{Z}/n\mathbb{Z}$ remplissent les propriétés caractéristiques d'un anneau commutatif avec $\overline{0}$ l'élément neutre pour l'addition et $\overline{1}$ l'élément neutre pour la multiplication. □

Proposition 38. *(Caractérisation des générateurs de $\mathbb{Z}/n\mathbb{Z}$)*
Soit $x \in \mathbb{Z}$. Soit $n \in \mathbb{N}^*$. Les assertions suivantes sont équivalentes :

1. *$\overline{x}$ est inversible dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.*
2. *x et n sont premiers entre eux.*
3. *$\overline{x}$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.*

Démonstration. $1 \Rightarrow 2$: $\overline{x}$ est inversible dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$. Donc il existe $\overline{u} \in \mathbb{Z}/n\mathbb{Z}$, tel que $\overline{x}.\overline{u} = \overline{1}$. Ainsi, il existe un entier relatif q tel que $xu + nq = 1$. Par conséquent, d'après le théorème de Bézout, x et n sont premiers entre eux.

$2 \Rightarrow 3$: x et n sont premiers entre eux. Donc, d'après le théorème de Bézout, il existe deux entiers relatifs u et v tels que $xu + nv = 1$. Alors, $\overline{x}.\overline{u} = \overline{1}$. Soit $\overline{k} \in (\mathbb{Z}/n\mathbb{Z}, +)$, $\overline{k} = k\overline{1} = k\overline{x}\overline{u} = ku\overline{x} = w\overline{x}$ avec $w \in \mathbb{Z}$. Donc $\overline{x}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$.

$3 \Rightarrow 1$: $\overline{x}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$. En particulier, il existe un entier relatif k tel que $k\overline{x} = \overline{1}$. D'où $\overline{k}\overline{x} = \overline{1}$. Ainsi, $\overline{x}$ est inversible dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$. □

Remarque. L'ensemble des éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est noté $(\mathbb{Z}/n\mathbb{Z})^\times$. Alors $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ est un groupe.

Théorème 39. *Soit $n \in \mathbb{N}^*$. Les assertions suivantes sont équivalentes :*

1. *n est premier.*
2. *L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps.*
3. *L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est intègre.*

Démonstration. $1 \Rightarrow 2$: n est premier donc $n \geqslant 2$ et $\mathbb{Z}/n\mathbb{Z} \neq \{\overline{0}\}$. Ainsi, il existe $\overline{r} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{r} \neq \overline{0}$. Nécessairement r est premier avec n, donc, d'après la proposition 38, $\overline{r} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Par conséquent, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps.

$2 \Rightarrow 3$: Évident.

$3 \Rightarrow 1$: Supposons n non premier. Si $n = 1$, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}\}$ et n'est pas intègre. Si $n \geqslant 2$, alors il existe deux entiers r et s dans $\{2, \ldots, n-1\}$ tels que $n = rs$. Alors, $\overline{r} \neq \overline{0}$ et $\overline{s} \neq \overline{0}$ mais $\overline{r}.\overline{s} = \overline{0}$. Donc $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ n'est pas intègre. □

3.2 Applications

3.2.1 Théorème des restes chinois

Théorème 40. *(Théorème des restes chinois)*
Soient m et n deux entiers premiers entre eux.

- *Pour tout couple $(a; b) \in \mathbb{Z}^2$, il existe $c \in \mathbb{Z}$ tel que l'on ait l'équivalence :*

$$\left(\begin{cases} x \equiv a[m] \\ x \equiv b[n] \end{cases} \right) \Leftrightarrow (x \equiv c[mn])$$

- *Ce système admet une infinité de solutions dans $\mathbb{Z}$, ce sont les entiers de la forme $x = c + kmn$, où $k \in \mathbb{Z}$. Deux solutions distinctes sont congrues modulo mn.*
- *L'application $\Psi : (\mathbb{Z}/mn\mathbb{Z}, +, \times) \to (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, +, \times)$ qui, à $\overline{x}$ associe $(\tilde{x}; \ddot{x})$, est un isomorphisme d'anneaux.*

Démonstration. m et n étant premiers entre eux, il existe, d'après le théorème de Bézout, deux entiers relatifs u et v tels que $mu + nv = 1$. Soit $c := bmu + anv$.

Démontrons alors que : $\left(\begin{cases} x \equiv a[m] \\ x \equiv b[m] \end{cases} \right) \Leftrightarrow (x \equiv c[mn])$.

$\Rightarrow$: Soit x un entier relatif tel que $\begin{cases} x \equiv a[m] \\ x \equiv b[mn] \end{cases}$. Alors, il existe deux entiers relatifs q et q' tels que $x = a + mq$ et $x = b + nq'$. En outre :

$$\begin{aligned} x &= x.1 = x(mu + nv) = xmu + xnv = (b + nq')mu + (a + mq)nv \\ &= bmu + mnq'u + anv + mnqv = c + mn(q'u + qv) \equiv c[mn] \end{aligned}$$

$\Leftarrow$: Soit x un entier relatif tel que $x \equiv c[mn]$. Alors, il existe un entier relatif k tel que $x = c + mnk$. D'où $x = bmu + anv + mnk$. On en déduit que $x = m(bu+nk)+anv = m(bu+nk)+a(1-mu) = m(bu+nk-au)+a \equiv a[m]$ et que $w = bmu + n(av + mk) = b(1 - nv) + n(av + mk) = b + n(av + mk - bv) \equiv b[n]$.

Ψ est clairement un morphisme d'anneaux. D'après le point précédent, Ψ est surjective. Or les anneaux $(\mathbb{Z}/mn\mathbb{Z}, +, \times)$ et $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, +, \times)$ ont tous les deux mn éléments. Ψ est donc un isomorphisme. □

Exemple. Résolvons le système de congruences $\begin{cases} x \equiv 4[5] \\ x \equiv 2[7] \end{cases}$. Il existe deux entiers relatifs k et k' tels que $x = 4 + 5k$ et $x = 2 + 7k'$. Travaillons dans $(\mathbb{Z}/5\mathbb{Z}, +, \times)$. On a $\overline{x} = \overline{4}$ et $\overline{x} = \overline{2} + \overline{7k'}$. D'où $\overline{7k'} = \overline{2}$. Or, 7 est premier avec 5, donc $\overline{7}$ est inversible dans $(\mathbb{Z}/5\mathbb{Z}, +, \times)$ d'après la proposition 38. Son inverse est $\overline{3}$ car $\overline{3} \times \overline{7} = \overline{21} = \overline{1}$. Ainsi, on a $\overline{7} \times \overline{3} = \overline{1}$ et $\overline{7}\overline{k'} = \overline{2}$, donc nécessairement, $\overline{k'} = \overline{2 \times 3} = \overline{6} = \overline{1}$. Et par conséquent, il existe un entier relatif l tel que $k' = 1 + 5l$. D'où $x = 2 + 7(1 + 5l) = 9 + 35l$. Ainsi, $\mathscr{S} = \{9 + 35l,\ l \in \mathbb{Z}\}$.

3.2.2 Théorèmes d'Euler et de Fermat

Définition 41. On appelle fonction indicatrice d'Euler la fonction définie sur $\mathbb{N}^*$ à valeurs dans $\mathbb{N}$ qui, à chaque entier naturel non nul n, associe le nombre d'entiers compris entre 1 et n premiers avec n.

Exemples. *On a* $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$ *et* $\varphi(8) = 4$.

Remarque. 1. La fonction indicatrice d'Euler n'est pas croissante sur $\mathbb{N}^*$ car $\varphi(9) = 6$ et $\varphi(10) = 4$.

2. D'après la proposition 38, $\varphi(n)$ est aussi le nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ et le nombre d'éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, c'est-à-dire l'ordre du groupe $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$.

Théorème 42. *(Théorème d'Euler) Soit* $n \in \mathbb{N}^*$. $\forall\, \overline{x} \in (\mathbb{Z}/n\mathbb{Z})^\times$, $\overline{x}^{\varphi(n)} = \overline{1}$.

Démonstration. $((\mathbb{Z}/n\mathbb{Z})^\times, +)$ est le groupe des éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$. D'après la proposition 38, ce groupe est d'ordre $\varphi(n)$. Donc, d'après le théorème de Lagrange, $\forall\, \overline{x} \in (\mathbb{Z}/n\mathbb{Z})^\times$, $\overline{x}^{\varphi(n)} = \overline{1}$. □

Corollaire 43. *(Petit théorème de Fermat) Soit p un nombre premier. On a :*

1. $\forall\, \overline{x} \in (\mathbb{Z}/p\mathbb{Z})^*$, $\overline{x}^{p-1} = \overline{1}$.
2. $\forall\, \overline{x} \in (\mathbb{Z}/p\mathbb{Z})$, $\overline{x}^p = \overline{x}$.

Démonstration. 1. Cela découle directement du théorème d'Euler après avoir remarqué que $\varphi(p) = p - 1$ et que $(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z})^*$ lorsque p est premier.
2. Évidente si $\overline{x} = \overline{0}$ et découle de 1. par une multiplication par $\overline{x}$ sinon. □

Remarque. La réciproque du petit théorème de Fermat est fausse. 561 n'est pas premier puisque $561 = 3 \times 11 \times 17$. Soit x un entier naturel non premier avec p. D'après le petit théorème de Fermat, nous savons que $x^2 \equiv 1[3]$. En élevant cette égalité à la puissance 280, on obtient $x^{560} \equiv 1[3]$. De même $x^{10} \equiv 1[3]$ et, en élevant à la puissance 56, on obtient $x^{560} \equiv 1[11]$. Enfin, en élevant la congruence $x^{16} \equiv 1[17]$ à la puissance 35, il vient : $x^{560} \equiv 1[17]$. Comme 3, 11 et 17 sont des nombres premiers et qu'ils divisent tous trois $x^{560} - 1$, leur produit 561 divise $x^{560} - 1$.

3.2.3 Théorème de Wilson

Proposition 44. *Soit p un nombre premier.*
Dans $((\mathbb{Z}/p\mathbb{Z})[X], +, \times)$, on a $X^{p-1} - \overline{1} = \prod_{r=1}^{r=p-1} (X - \overline{r})$.

Démonstration. D'après le petit théorème de Fermat, les $p - 1$ éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ sont racines du polynôme $X^{p-1} - 1$ de degré $p - 1$. La factorisation en découle. □

Théorème 45. *(Théorème de Wilson) Soit $p \in \mathbb{N}\backslash\{0; 1\}$. p est premier si, et seulement si, $(p-1)! \equiv -1[p]$.*

Démonstration. 2 est premier et $(2-1)! \equiv -1[2]$.

$\Rightarrow$: Soit p un nombre premier strictement supérieur à 2.
Alors $\overline{1.2 \dots (p-1)} = \overline{1}.\overline{2} \dots \overline{p-1}$. Or $\overline{1}.\overline{2} \dots \overline{p-1}$ est le produit des $p - 1$ racines du polynôme $X^{p-1} - \overline{1}$. D'où $\overline{1}.\overline{2} \dots \overline{p-1} = \overline{-1}$ soit $(p-1)! \equiv -1[p]$.

$\Leftarrow$: Supposons que $(p-1)! \equiv -1[p]$. Soit d un diviseur positif de p strictement inférieur à p. Alors naturellement, d divise $(p-1)!$. Or, par hypothèse, d divise $(p-1)! + 1$. Donc d divise 1. Ainsi, tout diviseur positif de p strictement inférieur à p est égal à 1. p est donc premier. □

Remarque. Le théorème de Wilson est un joli résultat théorique mais n'est pas très utile en pratique du fait du nombre de calculs engendrés par la factorielle dans l'éventualité d'un test de primalité.

3.2.4 Critère d'Eisenstein

Théorème 46. *(Critère d'Eisenstein) Soit $n \in \mathbb{N}$.*
Soit $P(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ un polynôme à coefficients dans $\mathbb{Z}$. S'il existe un nombre premier p tel que :

1. *$\forall\, i \in \{0, 1, 2, \ldots, n-1\}$, p divise a_i.*
2. *p ne divise pas a_n.*
3. *p^2 ne divise pas a_0.*

Alors $P(X)$ est irréductible sur $\mathbb{Z}$.

Démonstration. Soit $P(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ un polynôme à coefficients dans $\mathbb{Z}$. Soit p un nombre premier vérifiant 1., 2. et 3. Supposons que $P(X)$ ne soit pas irréductible sur $(\mathbb{Z}[X], +, \times)$. Alors il existe deux polynômes non constants $B(X)$ et $C(X)$ de $(\mathbb{Z}[X], +, \times)$ tels que $P(X) = B(X) \times C(X)$. Par conséquent, il existe $k \in \{1, 2, \ldots, n-1\}$ et il existe $b_0, \ldots, b_k$, $c_0, \ldots, c_{n-k} \in \mathbb{Z}$ tels que :

$$\sum_{i=0}^{i=n} a_iX^i = \left(\sum_{i=0}^{i=k} b_iX^i\right)\left(\sum_{i=0}^{i=n-k} c_iX^i\right)$$

Égalité qui, dans $((\mathbb{Z}/p\mathbb{Z})[X], +, \times)$ devient :

$$\sum_{i=0}^{i=n} \overline{a_i}X^i = \left(\sum_{i=0}^{i=k} \overline{b_i}X^i\right)\left(\sum_{i=0}^{i=n-k} \overline{c_i}X^i\right)$$

Et donc, d'après 1. et 2. :

$$\overline{a_n}X^n = \left(\sum_{i=0}^{i=k} \overline{b_i}X^i\right)\left(\sum_{i=0}^{i=n-k} \overline{c_i}X^i\right)$$

Soit :

$$\overline{a_n}X^n = \overline{b_k}X^k \times \overline{c_{n-k}}X^{n-k}$$

Par conséquent, $\overline{b_0} = \overline{c_0} = \overline{0}$. Donc, p^2 divise b_0c_0. Or $b_0c_0 = a_0$. Donc p^2 divise a_0. Ce qui est en contradiction avec 3. □

Exemples. 1. Considérons le polynôme $P(X) = 3X^4 + 15X^2 + 10$. $p = 5$ divise le coefficient constant, divise le coefficient en X, divise le coefficient en X^2, divise le coefficient en X^3 et ne divise pas le coefficient en X^4. De plus, $p^2 = 25$ ne divise pas le coefficient constant. Donc, d'après le critère d'Eisenstein, $P(X)$ est irréductible sur $\mathbb{Z}$.

2. Considérons le polynôme $\Phi_5(X) = \frac{X^5-1}{X-1} = X^4 + X^3 + X^2 + X + 1$. $\Phi_5(X)$ est irréductible si, et seulement si, $\Phi_5(X+1)$ l'est.
Or, $\Phi_5(X+1) = \frac{(X+1)^5-1}{X} = X^4 + 5X^3 + 10X^2 + 10X + 5$. L'entier $p = 5$ permet de conclure, en utilisant le critère d'Eisenstein, que $\Phi_5(X)$ est irréductible.

Remarque. Il existe des polynômes irréductibles de tout degré. En effet, pour tout entier $n \in \mathbb{N}^*$, le polynôme $X^n - p$, où p est premier, est irréductible sur $\mathbb{Z}[X]$.

Chapitre 4

Structures quotients, exemples et applications

Pré-requis

1. Relation d'équivalence.
2. Partition d'un ensemble.
3. Division euclidienne dans $\mathbb{R}[X]$.
4. Groupe, sous-groupe et morphisme.
5. Norme sur un $\mathbb{K}$-espace vectoriel.

4.1 Quotient d'un ensemble par une relation

4.1.1 Généralités

Définition 47. Soit E un ensemble. Soit $\Re$ une relation d'équivalence sur E. L'ensemble des classes d'équivalence de E pour la relation $\Re$, noté $E/\Re$, est appelé l'ensemble quotient de E par la relation d'équivalence $\Re$. Plus formellement, $E/\Re := \{\overline{x},\, x \in E\}$, où $\overline{x} := \{y \in E,\, y\Re x\}$.

Exemple. Si $\mathbb{Z}$ est muni de la relation d'équivalence « avoir même parité », alors l'ensemble quotient est réduit à deux éléments : 0 et 1 (pair et impair).

Proposition 48. *Soit E un ensemble non vide. Soit $\Re$ une relation d'équivalence sur E. Alors :*

1. $\forall\, x, y \in E,\ (x\Re y) \Leftrightarrow (\overline{x} = \overline{y})$.
2. *Deux classes d'équivalence sont soit disjointes, soit égales.*
3. *Les classes d'équivalence forment une partition de E.*

Démonstration. 1. $\Leftarrow$: soient x, $y \in E$. Si $\overline{x} = \overline{y}$, alors $x \in \overline{x} = \overline{y}$ et donc $x\Re y$.

$\Rightarrow$: soient x, $y \in E$ tels que $x\Re y$. Soit $z \in \overline{x}$. Alors $z\Re x$. Or $x\Re y$. Donc, par transitivité de la relation $\Re$, $z\Re y$. Ainsi $z \in \overline{y}$. Donc $\overline{x} \subset \overline{y}$. Mais, puisque $x\Re y$, on a également $y\Re x$ et un raisonnement identique montre que $\overline{y} \subset \overline{x}$. D'où $\overline{x} = \overline{y}$.

2. Soient $\overline{x}$ et $\overline{y}$ deux classes d'équivalence. Supposons-les non disjointes. Alors il existe $z \in E$ tel que $z \in \overline{x}$ et $z \in \overline{y}$. Par définition, on a alors $x\Re z$ et $y\Re z$ et donc $x\Re z$ et $z\Re y$. Par transitivité de la relation $\Re$, on en déduit $x\Re y$. Ainsi, d'après 1., $\overline{x} = \overline{y}$.

3. D'après 2., les classes d'équivalence sont deux à deux disjointes. De plus, les classes d'équivalence de E sont non vides puisque, pour tout $x \in E$, $x \in \overline{x}$ et leur réunion est évidemment égale à E. Par conséquent, elles forment bien une partition de E. □

Définition 49. Soit E un ensemble non vide muni d'une relation d'équivalence $\Re$. L'application surjective $\pi : E \longrightarrow E/\Re$ définie par $\pi(x) = \overline{x}$ est appelée la projection canonique.

Remarque. Si $\varphi : E/\Re \longrightarrow F$ est une application, alors l'application $\varphi \circ \pi : E \longrightarrow F$ est constante sur les classes d'équivalence. En effet, si $x\Re y$, alors $\overline{x} = \overline{y}$ d'après la proposition 48, et donc $(\varphi \circ \pi)(x) = \varphi(\pi(x)) = \varphi(\overline{x}) = \varphi(\overline{y}) = \varphi((\pi(y)) = (\varphi \circ \pi)(y)$. Réciproquement, on a la proposition suivante :

Proposition 50. *Soient E et F deux ensembles non vides. Soit $\Re$ une relation d'équivalence sur E. Soit $f : E \longrightarrow F$ une application. Si f est constante sur ses classes d'équivalence (i.e. si, pour tous x, $y \in E$, $(x\Re y) \Rightarrow (f(x) = f(y))$), alors il existe une unique application $\overline{f} : E/\Re \longrightarrow F$ telle que $f = \overline{f} \circ \pi$. Elle est définie par : $\forall\, \omega \in E/\Re$, $\overline{f}(\omega) = f(x)$, où x est un représentant arbitraire de ω. En particulier, pour tout $x \in E$, $\overline{f}(\overline{x}) = f(x)$. En outre, il existe une correspondance bijective entre l'ensemble des applications $\varphi : E/\Re \longrightarrow F$ et l'ensemble des applications $f : E \longrightarrow F$ constantes sur les classes d'équivalence. Cette bijection est donnée par $\varphi \longmapsto \varphi \circ \pi$ et $\overline{f} \longleftarrow\!\shortmid f$.*

Démonstration. Analyse : supposons qu'une telle application $\overline{f}$ existe. Soit $\omega \in E/\Re$. Si x est un représentant de la classe ω, alors $\omega = \overline{x} = \pi(x)$ et par conséquent $\overline{f}(\omega) = \overline{f}(\pi(x)) = (\overline{f} \circ \pi)(x) = f(x)$. Cela prouve que si $\overline{f}$ existe, alors est définie par : $\forall\, \omega \in E/\Re$, $\overline{f}(\omega) = f(x)$, où x est un représentant arbitraire de ω. En particulier, une telle application est alors unique.

Synthèse : vérifions que cette formule définit bien une application. Il s'agit de vérifier que $\overline{f}(\omega)$ ne dépend pas du représentant de la classe d'équivalence choisi. Soient x, $y \in E$ deux représentants de ω. On a donc x, $y \in \omega$. Montrons que $f(x) = f(y)$. C'est exactement l'hypothèse faite sur f. Par conséquent, l'application $\overline{f}$ existe. De plus, pour tout $x \in E$, x est un représentant de $\overline{x}$, donc $\overline{f}(\overline{x}) = f(x)$.

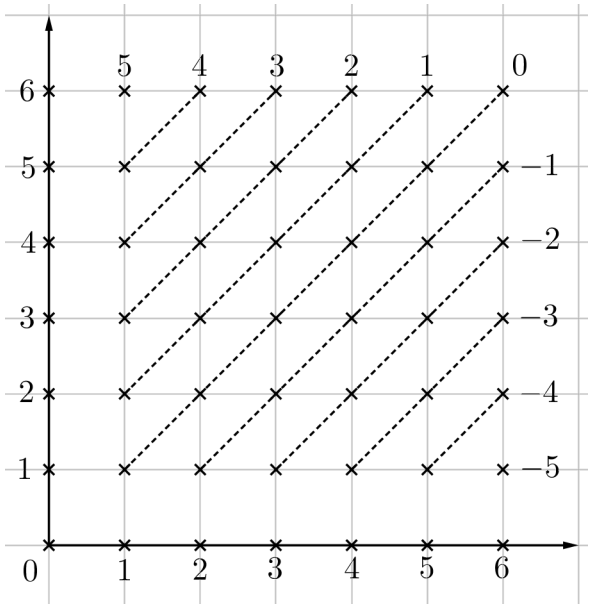
Enfin, démontrons que les deux applications $\varphi \longmapsto \varphi \circ \pi$ et $\overline{f} \longleftarrow\!\shortmid f$ sont inverses l'une de l'autre. Soit $\varphi : E/\Re \longrightarrow F$ une application. Alors, l'application $\overline{\varphi \circ \pi}$ est l'unique application $\psi : E/\Re \longrightarrow F$ telle que $\psi \circ \pi = \varphi \circ \pi$. Or, φ est une telle application. On en déduit alors que $\overline{\varphi \circ \pi} = \varphi$. Réciproquement, si $f : E \longrightarrow F$ est constante sur les classes d'équivalence, alors $\overline{f} \circ \pi = f$ par définition. □

4.1.2 Constructions de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$

Construction de $\mathbb{Z}$:

1. Sur l'ensemble $\mathbb{N} \times \mathbb{N}$, on définit la relation $\Re$ de la façon suivante : $(a;b)\Re(c;d)$ si, et seulement si, $a + d = b + c$.
2. On vérifie que $\Re$ est une relation d'équivalence sur $\mathbb{N} \times \mathbb{N}$.
3. Si $b \geqslant a$, alors on note $b - a$ la classe de $(a;b)$.
4. Si $b < a$, alors on note $-(a - b)$ la classe de $(a;b)$.
5. On obtient $\mathbb{Z} := \mathbb{N} \times \mathbb{N}/\Re$.
6. On peut alors vérifier que l'addition de $\mathbb{N} \times \mathbb{N}$ est compatible avec la relation $\Re$ et ainsi la transférer sur $\mathbb{Z}$.

Illustration :



Construction de $\mathbb{Q}$:

1. Sur l'ensemble $\mathbb{Z} \times \mathbb{N}^*$, on définit la relation $\Re$ de la façon suivante : $(a;b)\Re(c;d)$ si, et seulement si, $b \times c = d \times a$.
2. On vérifie que $\Re$ est une relation d'équivalence sur $\mathbb{Z} \times \mathbb{N}^*$.
3. On note $\frac{a}{b}$ la classe de $(a;b)$.
4. On obtient $\mathbb{Q} := \mathbb{Z} \times \mathbb{N}^*/\Re$.
5. On peut alors vérifier que l'addition de $\mathbb{Z} \times \mathbb{N}^*$ est compatible avec la relation $\Re$ et ainsi la transférer sur $\mathbb{Q}$.

Construction de $\mathbb{R}$:

1. Sur l'ensemble $\mathcal{C}$ des suites de Cauchy d'éléments de $\mathbb{Q}$, on définit la relation $\Re$ de la façon suivante : $u\Re v$ si, et seulement si, $\lim\limits_{n\to+\infty}(u_n - v_n) = 0$.
2. On vérifie que $\Re$ est une relation d'équivalence sur $\mathcal{C}$.
3. On note l la classe de u.
4. On obtient $\mathbb{R} \coloneqq \mathcal{C}/\Re$.
5. On peut alors vérifier que l'addition de $\mathcal{C}$ est compatible avec la relation $\Re$ et ainsi la transférer sur $\mathbb{R}$.

Construction de $\mathbb{C}$:

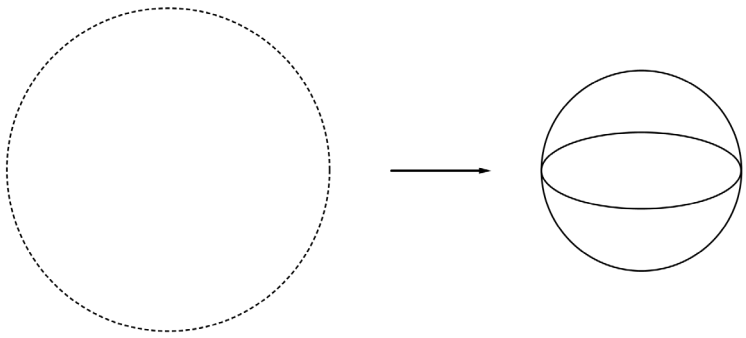
1. Sur l'ensemble $\mathbb{R}[X]$ des polynômes à coefficients dans $\mathbb{R}$, on définit la relation $\Re$ de la façon suivante : $A\Re B$ si, et seulement si, il existe $Q \in \mathbb{R}[X]$, a, $b \in \mathbb{R}$ tels que $A(X) = (X^2+1)B(X) + bX + a$.
2. On vérifie que $\Re$ est une relation d'équivalence sur $\mathbb{R}[X]$.
3. On note $a + ib$ la classe de A.
4. On obtient $\mathbb{C} \coloneqq \mathbb{R}[X]/\Re$.
5. On peut alors vérifier que l'addition de $\mathbb{R}[X]$ est compatible avec la relation $\Re$ et ainsi la transférer sur $\mathbb{C}$.

4.1.3 Constructions topologiques

Construction de la sphère :

1. Sur l'ensemble $\mathcal{D} = \{z \in \mathbb{C}, |z| \leqslant 1\}$, on définit la relation $\Re$ de la façon suivante : $\begin{cases} \forall\, z \in \mathcal{D},\ z\Re z \\ \forall\, z,\, z' \in \mathcal{D},\ (|z| = |z'| = 1) \Rightarrow (z\Re z') \end{cases}$
2. On vérifie que $\Re$ est une relation d'équivalence sur $\mathcal{D}$.
3. Le quotient $\mathcal{D}/\Re$ est une sphère.

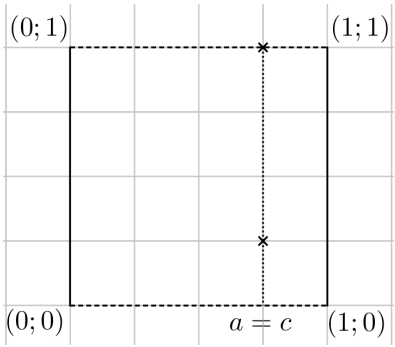
Illustration :



Construction du cylindre :

1. Sur l'ensemble $[0;1]^2$, on définit la relation $\Re$ de la façon suivante : $(a;b)\Re(c;d)$ si, et seulement si $\begin{cases} a = c \text{ et } b = d \\ \text{ou} \\ b = 0, d = 1 \text{ et } a = c \end{cases}$
2. On vérifie que $\Re$ est une relation d'équivalence sur $[0;1]^2$.
3. Le quotient $[0;1]^2/\Re$ est un cylindre.

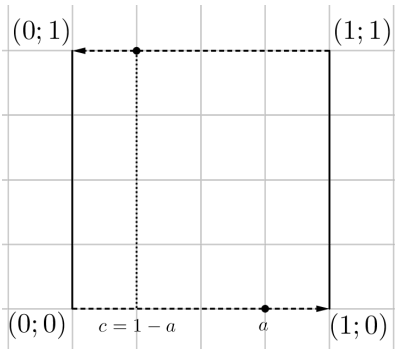
Illustration :



Construction du ruban de Möbius :

1. Sur l'ensemble $[0;1]^2$, on définit la relation $\Re$ de la façon suivante : $(a;b)\Re(c;d)$ si, et seulement si $\begin{cases} a = c \text{ et } b = d \\ \text{ou} \\ b = 0, d = 1 \text{ et } a = 1 - c \end{cases}$
2. On vérifie que $\Re$ est une relation d'équivalence sur $[0;1]^2$.
3. Le quotient $[0;1]^2/\Re$ est un ruban de Möbius.

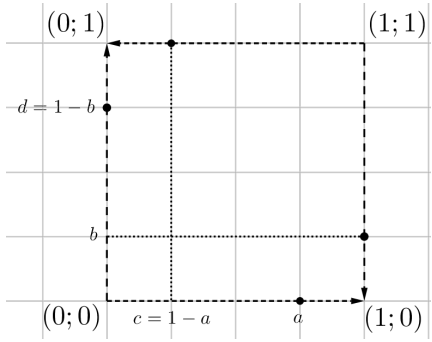
Illustration :



Construction de la bouteille de Klein :

1. Sur l'ensemble $[0;1]^2$, on définit la relation $\Re$ de la façon suivante :
$$(a;b)\Re(c;d) \text{ si, et seulement si } \begin{cases} a = c \text{ et } b = d \\ \text{ou} \\ b = 0,\ d = 1 \text{ et } a = 1 - c \\ \text{ou} \\ a = 0,\ c = 1 \text{ et } d = 1 - b \end{cases}$$
2. On vérifie que $\Re$ est une relation d'équivalence sur $[0;1]^2$.
3. Le quotient $[0;1]^2/\Re$ est une bouteille de Klein.

Illustration :



4.2 Le cas particulier des groupes

Proposition 51. *Soit G un groupe. Soit H un sous-groupe de G. La relation $\Re$ définie sur G par $x\Re y$ si $x^{-1}y \in H$ est une relation d'équivalence.*

Démonstration. Réflexivité : soit $x \in G$. $x^{-1}x = 1_G \in H$ car H est un sous-groupe de G. Donc $x\Re x$.

Symétrie : soient x, $y \in G$ tels que $x\Re y$. Alors $x^{-1}y \in H$. Or H est un groupe, donc $\left(x^{-1}y\right)^{-1} \in H$. Donc $y^{-1}x \in H$. Autrement dit, $y\Re x$.

Transitivité : soient x, y, $z \in G$ tels que $x\Re y$ et $y\Re z$. Alors $x^{-1}y \in H$ et $y^{-1}z \in H$. Or H est un groupe, donc $(x^{-1}y)(y^{-1}z) \in H$. Donc $x^{-1}z \in H$. Autrement dit, $x\Re z$. □

Définition 52. Les classes d'équivalence pour la relation $\Re$ sont appelées les classes à gauche modulo H. Plus formellement, pour tout $x \in G$, $\overline{x} := xH = \{xh,\ h \in H\}$. On note G/H l'ensemble des classes d'équivalence. Plus formellement :

$$G/H := \{xH,\ x \in G\}$$

Remarque. 1. Les éléments de l'ensemble G/H ne sont pas des éléments de G, ce sont des parties de G.

2. L'application $\pi : G \longrightarrow G/H$ définie par $\pi(x) = \overline{x}$ est clairement surjective. On voudrait alors définir une structure de groupe sur l'ensemble G/H de manière à ce que cette projection canonique π soit un morphisme de groupes. Pour cela, il nous faudrait poser, pour tous x, $y \in G$, $\overline{x}\,\overline{y} := \overline{xy}$. Cependant, rien ne garantit qu'une telle loi de composition soit bien définie. En effet, le résultat ne doit pas dépendre des éléments choisis pour représenter les classes d'équivalence de x et de y. Plus formellement, si $\overline{x_1} = \overline{x_2}$ et $\overline{y_1} = \overline{y_2}$, alors $\overline{x_1 y_1} = \overline{x_2 y_2}$. Or cette égalité n'est pas toujours vérifiée.

Exemple. Soient $G = \mathfrak{S}_3$ et $H = \langle (1\,2) \rangle$.
Soient $x_1 = (1\,3)$, $x_2 = (1\,3)(1\,2) = (1\,2\,3)$ et $y_1 = y_2 = (2\,3)$.
$x_1^{-1} x_2 = (1\,3)(1\,2\,3) = (1\,2) \in H$. Donc $x_1 \Re x_2$ et $\overline{x_1} = \overline{x_2}$.
$y_1^{-1} y_2 = y_1^{-1} y_1 = 1_G \in H$. Donc $y_1 \Re y_2$ et $\overline{y_1} = \overline{y_2}$.
$x_1 y_1 = (1\,3)(2\,3) = (1\,3\,2) \notin H$ et $x_2 y_2 = (1\,2\,3)(2\,3) = (1\,2) \in H$. Donc $\overline{x_1 y_1} \neq \overline{x_2 y_2}$.

3. Analysons la situation. Supposons bien définie la loi de composition interne qui, à tout élément $(\overline{x}, \overline{y})$ de G/H, associe l'élément $\overline{xy}$ de G/H. Alors, pour tout $g \in G$, $\overline{g} = \overline{1_G g} = \overline{1_G}\,\overline{g}$. Or, par définition de G/H, pour tout $h \in H$, $\overline{h} = \overline{1_G}$. D'où, pour tout $g \in G$, pour tout $h \in H$, $\overline{g} = \overline{h}\,\overline{g} = \overline{hg}$. Autrement dit, pour tout $g \in G$, pour tout $h \in H$, $g^{-1} h g \in H$. Le passage à l'inverse induisant une bijection de G dans lui-même, en remplaçant g par g^{-1}, on constate que cela équivaut à $ghg^{-1} \in H$, pour tout $g \in G$ et pour tout $h \in H$.

Définition 53. Soit G un groupe. Soit H un sous-groupe de G. On dit que H est distingué dans G si, pour tout $h \in H$, pour tout $g \in G$, $ghg^{-1} \in H$. On note alors $H \lhd G$.

Remarque. 1. Si G est abélien, alors tout sous-groupe de G est distingué dans G.

2. Les sous-groupes $\{1_G\}$ et G sont distingués dans G.

3. Soit $f : G \longrightarrow G'$ un morphisme de groupes. Alors $\ker(f) \lhd G$.

Démonstration. On démontre facilement que $\ker(f)$ est un sous-groupe de G. Soit $g \in G$. Soit $x \in \ker(f)$. On a :

$$f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)f(x)f(g)^{-1} = f(g)1_{G'}f(g)^{-1} = f(g)f(g)^{-1} = 1_{G'}$$

□

Proposition 54. *Soit H un sous-groupe distingué de G. Alors, la loi de composition interne qui, à tout élément $(\overline{x}, \overline{y})$ de G/H, associe l'élément $\overline{xy}$ de G/H est bien définie, d'élément neutre $\overline{1_G}$, et induit sur G/H une structure de groupe. De plus, l'application $\pi : G \longrightarrow G/H$ définie par $\pi(x) = \overline{x}$ est un morphisme de groupes.*

Démonstration. Soient x_1, x_2, y_1, $y_2 \in G$ tels que $\overline{x_1} = \overline{x_2}$ et $\overline{y_1} = \overline{y_2}$. Alors il existe h, $h' \in H$ tels que $x_2 = x_1 h$ et $y_2 = y_1 h'$. D'où $x_2 y_2 = x_1 h y_1 h' = x_1 y_1 (y_1^{-1} h y_1) h'$.

Or H est un sous-groupe distingué de G, donc $y_1^{-1}hy_1 \in H$, et par conséquent $(y_1^{-1}hy_1)h' \in H$. Ainsi, $\overline{x_1y_1} = \overline{x_2y_2}$ et la loi de composition interne qui, à tout élément $(\overline{x}, \overline{y})$ de G/H, associe l'élément $\overline{xy}$ de G/H est bien définie. Soit $\overline{x} \in G/H$. $\overline{1_G}\overline{x} = \overline{1_Gx} = \overline{x}$ et de même $\overline{x}\overline{1_G} = \overline{x}$. Donc $\overline{1_G}$ est un élément neutre dans G/H. Soient $\overline{x}$, $\overline{y}$, $\overline{z} \in G/H$. $(\overline{xy})\overline{z} = \overline{xyz} = \overline{(xy)z} = \overline{x(yz)} = \overline{xyz} = \overline{x}(\overline{yz})$. Donc la loi est associative. Soit $\overline{x} \in G/H$. $\overline{x}\overline{x^{-1}} = \overline{xx^{-1}} = \overline{1_G}$. Donc $(\overline{x})^{-1} = \overline{x^{-1}}$. Ainsi, tout élément de G/H est inversible. Par conséquent, G/H est muni d'une structure de groupe. La loi de groupe sur G/H implique alors naturellement que l'application $\pi : G \longrightarrow G/H$ définie par $\pi(x) = \overline{x}$ est un morphisme de groupes. □

Définition 55. Soit G un groupe. Soit H un sous-groupe distingué de G. Le groupe G/H est appelé groupe quotient de G par H.

Théorème 56. *(Théorème de factorisation) Soient G et G' deux groupes. Soit H un sous-groupe distingué de G. Soit $f : G \longrightarrow G'$ un morphisme de groupes tel que $H \subset \ker(f)$. Alors, il existe un unique morphisme de groupe $\overline{f} : G/H \longrightarrow G'$ tel que $f = \overline{f} \circ \pi$. Pour tout $\overline{x} \in G/H$, $\overline{f}(\overline{x}) = f(x)$. De plus, à tout élément φ de $\mathrm{Hom}(G/H, G')$ correspond un unique élément $\varphi \circ \pi$ de $\{f \in \mathrm{Hom}(G, G'),\ H \subset \ker(f)\}$ et réciproquement, à tout élément f de $\{f \in \mathrm{Hom}(G, G'),\ H \subset \ker(f)\}$ correspond un unique élément $\overline{f}$ de $\mathrm{Hom}(G/H, G')$.*

Démonstration. Démontrons tout d'abord qu'un morphisme $f : G \longrightarrow G'$ est constant sur les classes d'équivalence si, et seulement si, $H \subset \ker(f)$.
$\Leftarrow$: si $H \subset \ker(f)$, alors, $\forall\, x \in G, \forall\, h \in H$, $f(xh) = f(x)f(h) = f(x)1_{G'} = f(x)$.
$\Rightarrow$: si f est constante sur chaque classe d'équivalence, alors elle est constante sur H. Or H contient 1_G. Donc, pour tout $h \in H$, $f(h) = f(1_G) = 1_{G'}$. Ainsi, $H \subset \ker(f)$.

La proposition 50 fournit l'existence et l'unicité d'une application $\overline{f}$ vérifiant les propriétés souhaitées. De plus, pour tous x_1, $x_2 \in G$, on a :

$$\overline{f}(\overline{x_1x_2}) = \overline{f}(\overline{x_1x_2}) = f(x_1x_2) = f(x_1)f(x_2) = \overline{f}(\overline{x_1})\overline{f}(\overline{x_2})$$

De la sorte, $\overline{f}$ est un morphisme de groupes.

Toujours d'après la proposition 50, il existe une bijection entre l'ensemble des applications de G/H dans G' et l'ensemble des applications de G dans G' constantes sur les classes d'équivalence. Elle est donnée par :

$$\begin{aligned} \varphi &\longmapsto \varphi \circ \pi \\ \overline{f} &\longmapsfrom f \end{aligned}$$

Si φ est un morphisme de groupes, alors $\varphi \circ \pi$ est un morphisme de groupes dont le noyau contient H. De plus, si f est un morphisme de groupes, alors $\overline{f}$ est un morphisme de groupes. Ainsi, la correspondance se restreint pour définir une bijection entre les ensembles $\mathrm{Hom}(G/H, G')$ et $\{f \in \mathrm{Hom}(G, G'),\ H \subset \ker(f)\}$. □

Lemme 57. *Soit $f : G \longrightarrow G'$ un morphisme de groupes. Alors, le morphisme de groupes $\overline{f} : G/\ker(f) \longrightarrow G'$ est injectif.*

Démonstration. Soit $\overline{x} \in \ker(f)$. $\overline{f}(\overline{x}) = 1_{G'}$ si, et seulement si, $f(x) = 1_{G'}$, c'est-à-dire si, et seulement si, $x \in \ker(f)$, ce qui revient encore à dire que $\overline{x} = \overline{1_G} \in G/\ker(f)$. Ainsi, $\ker(\overline{f}) = \left\{\overline{1_G}\right\}$ et $\overline{f}$ est injectif. □

Théorème 58. *(Premier théorème d'isomorphisme de Noether) Soient G et G' deux groupes. Soient $f : G \longrightarrow G'$ un morphisme de groupes. Alors le morphisme $\overline{f} : G/\ker(f) \longrightarrow G'$ induit un isomorphisme de groupes $G/\ker(f) \cong \mathrm{im}(f)$.*

Démonstration. D'après le lemme 57, le morphisme $\overline{f} : G/\ker(f) \longrightarrow G'$ est injectif. Il induit donc naturellement un isomorphisme de $G/\ker(f)$ sur son image. Or $\mathrm{im}(\overline{f}) = \left\{\overline{f}(\overline{x}),\, \overline{x} \in G/\ker(f)\right\} = \{f(x),\, x \in G\} = \mathrm{im}(f)$. D'où le résultat. □

Remarque. En pratique, le premier théorème d'isomorphisme permet d'identifier un groupe quotient G/H à un groupe connu de la manière suivante : on essaye d'identifier H au noyau d'un morphisme de groupes $f : G \longrightarrow G'$ bien choisi, et l'on calcule $\mathrm{im}(f)$ (idéalement, f est surjectif).

Exemples. 1. Soit $f : \left(\mathbb{C}^*, \times\right) \longmapsto \left(\mathbb{R}_+^*, \times\right)$ le morphisme défini par $f(z) = |z|$. f est clairement surjectif de noyau $\mathbb{U} = \left\{z \in \mathbb{C}^*,\, |z| = 1\right\}$. Le premier théorème d'isomorphisme de Noether nous donne donc :

$$\mathbb{C}^*/\mathbb{U} \cong \mathbb{R}_+^*$$

2. Soit $f : (\mathbb{R}, +) \longmapsto (\mathbb{U}, \times)$ le morphisme défini par $f(\theta) = e^{i\theta}$. f est clairement surjectif de noyau $2\pi\mathbb{Z}$. Le premier théorème d'isomorphisme de Noether nous donne donc :

$$\mathbb{R}/2\pi\mathbb{Z} \cong \mathbb{U}$$

Théorème 59. *(Deuxième théorème d'isomorphisme de Noether) Soit G un groupe. Soient H et K deux sous-groupes de G. Si H est distingué dans G, alors :*

1. *$HK = \{hk,\, h \in H,\, k \in K\}$ et $KH = \{kh,\, h \in H,\, k \in K\}$ sont des sous-groupes de G et $\langle H, K\rangle = HK = KH$.*
2. *$H \lhd HK$ et $H \cap K \lhd K$.*
3. *$HK/H \cong K/(H \cap K)$.*

Démonstration. 1. Démontrons tout d'abord que HK et KH sont des sous groupes de G.
Puisque H et K sont des sous-groupes de G, par définition, $1_G \in H$ et $1_G \in K$. Donc HK contient $1_G 1_G = 1_G$.
Soient h_1k_1 et h_2k_2 deux éléments de HK. On a $(h_1k_1)(h_2k_2) = \left(h_1\left(k_1h_2k_1^{-1}\right)\right)(k_1k_2)$.

Or H est distingué dans G, donc $k_1 h_2 k_1^{-1} \in H$. H étant un sous-groupe de G, $h_1\left(k_1 h_2 k_1^{-1}\right) \in H$. De même, K étant un sous-groupe de G, $k_1 k_2 \in K$. Ainsi, $\left(h_1\left(k_1 h_2 k_1^{-1}\right)\right)(k_1 k_2) \in HK$ et donc $(h_1 k_1)(h_2 k_2) \in HK$.

Soit $hk \in HK$. On a $(hk)^{-1} = k^{-1}h^{-1} = \left(k^{-1}h^{-1}k\right)k^{-1}$. Or $k^{-1}h^{-1}k \in H$ car H est distingué dans G. D'où $(hk)^{-1} \in HK$.

Par conséquent, HK est bien un sous-groupe de G.
Démontrons à présent l'égalité $\langle H, K\rangle = HK$.

$\subset$: $H \subset \langle H, K\rangle$ et $K \subset \langle H, K\rangle$. Donc $HK \subset \langle H, K\rangle$.

$\supset$: HK est un sous-groupe de G contenant H et K. Donc $\langle H, K\rangle \subset HK$.

Terminons en démontrant que $HK = KH$.

H, K et HK sont des sous-groupes de G. Donc $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$, où $P^{-1} := \left\{p^{-1},\, p \in P\right\}$.

2. et 3. Pour tout $h' \in H$, pour tout $hk \in HK$, on a $(hk)h'(hk)^{-1} = h(kh'k^{-1})h^{-1}$. Or H est distingué dans G (donc dans K). Donc $kh'k^{-1} \in H$. De plus, H étant un sous-groupe de G, $h(kh'k^{-1})h^{-1} \in H$. Autrement dit, $(hk)h'(hk)^{-1} \in H$. Par conséquent, H est distingué dans HK.

D'après la proposition 54, on peut ainsi former le groupe quotient HK/H. Considérons alors le morphisme de groupes $f : K \longrightarrow HK/K$ défini par $f(k) = \overline{k}$. D'une part, pour tout $hk \in HK$, on a $\overline{hk} = \overline{hk} = \overline{1_G k} = \overline{k} = f(k)$. Donc f est surjectif. D'autre part, pour tout $k \in K$, on a : $\left(\overline{k} = \overline{1_G}\right) \Leftrightarrow (k \in H)$. Autrement dit, $\ker(f) = H \cap K$. Ainsi, $H \cap K$ est distingué dans K et, d'après le premier théorème d'isomorphisme, $HK/H \cong K/(H \cap K)$. □

Théorème 60. *(Troisième théorème d'isomorphisme de Noether) Soit G un groupe. Soient H et K deux sous-groupes distingués de G. Si K est un sous-groupe de H, alors :*

1. $K \lhd H$.
2. $H/K \lhd G/K$.
3. $(G/K)(H/K) \cong G/H$.

Démonstration. 1. $K \lhd G$ et $K \subset H \subset G$ donc $K \lhd H$.

2. Soit $\pi : G \longrightarrow G/H$ la projection canonique. Comme $K \subset H = \ker(\pi)$, d'après le théorème de factorisation, π induit un morphisme de groupes $\overline{\pi} : G/K \longrightarrow G/H$ défini par $\overline{\pi}(\widetilde{x}) = \overline{x}$, où $\widetilde{x}$ et $\overline{x}$ désignent respectivement les classes à gauche de x modulo K et modulo H. $\overline{\pi}$ est naturellement surjectif. De plus, pour tout $x \in G$:

$$\left(\overline{x} = \overline{1_{G/H}}\right) \Leftrightarrow (x \in H) \Leftrightarrow (\widetilde{x} \in H/K)$$

Autrement dit, $\ker(\overline{\pi}) = H/K$. Ainsi, H/K est distingué dans G/K et, d'après le premier théorème d'isomorphisme, $(G/K)(H/K) \cong G/H$. □