21 – Compléments sur les groupes finis

Jeremy Daniel

1 Théorème de Lagrange

1.1 Ordre d'un élément

Proposition 1.1
Soit G une groupe fini, soit $x \in G$. Il existe $n \in \mathbb{N}^*$ tel que $x^n = e_G$.

Démonstration. Comme G est fini, on peut trouver deux entiers $i < j$ tels que $x^i = x^j$. Alors, $x^{j-i} = e_G$ et $j - i \in \mathbb{N}^*$. □

Définition 1.2
Le plus petit entier n dans la proposition précédente est l'ordre de x. On le note $\omega_G(x)$.

Proposition 1.3
Pour tout $n \in \mathbb{Z}$, $x^n = e_G \iff \omega_G(x) \mid n$.

Démonstration. Soit $n \in \mathbb{Z}$. Par division euclidienne, on trouve $q \in \mathbb{Z}$ et $r \in [\![0, \omega_G(x) - 1]\!]$ tels que $n = q\omega_G(x) + r$. Alors,

$$x^n = (x^{\omega_G(x)})^q \times x^r = x^r.$$

Par définition de $\omega_G(x)$, $x^r = e_G$ ssi $r = 0$ (car $r < \omega_G(x)$) ssi $\omega_G(x)$ divise n. □

Théorème 1.4 (Lagrange – cas abélien)
Si G est abélien, $\omega_G(x)$ divise $|G|$.

Démonstration. D'après la proposition précédente, il s'agit de montrer que $x^{|G|} = e_G$. Considérons $P = \prod_{y \in G} y$; ce produit étant bien défini par abélianité de G. L'application $\tau_x : y \mapsto xy$ de G dans G est une bijection, de bijection réciproque $y \mapsto x^{-1}y$. Ainsi,

$$P = \prod_{y \in G} y = \prod_{z \in G} (xz) = x^{|G|} \prod_{z \in G} x = x^{|G|} \times P.$$

En multipliant par l'inverse de P, on obtient $x^{|G|} = e_G$. □

Remarque 1.5
Le théorème est encore vrai si G n'est pas abélien. Cependant, la démonstration est hors programme de MP.

Exemples 1.6
- Soit p un nombre premier. Soit $x \in \mathbb{Z}$ premier avec p. Alors $x^{p-1} \equiv 1\,[p]$ (petit théorème de Fermat).
  Notons en effet u la classe de x modulo p. C'est un élément de $\left(\mathbb{Z}/p\mathbb{Z}\right) \setminus \{0\}$, groupe abélien (multiplicatif) de cardinal $p-1$. Donc, u^{p-1} est la classe de 1 modulo p, ce qui revient à dire que $x^{p-1} \equiv 1\,[p]$.
- Si le cardinal d'un groupe G est un nombre premier p, alors G est cyclique. En effet, si $x \neq \{e_G\}$ est un élément de G, son ordre doit diviser p. Comme il est différent de 1, il est égal à p. Ceci montre que x est un générateur de G, donc que G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ (cf. section suivante).

1.2 Théorème de Lagrange – cas général

Lemme 1.7
Soit G un groupe fini, soit H un sous-groupe de G. On définit une relation d'équivalence $\mathcal{R}_H$ par

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

Toutes les classse d'équivalence ont même cardinal $|H|$.

Démonstration.
- Si $x \in G$, $xx^{-1} = e_G \in H$. Donc la relation est réflexive.
- Si $x, y \in G$ sont tels que $xy^{-1} \in H$, alors comme H est stable par inverse, $yx^{-1} = (xy^{-1})^{-1} \in H$ et donc la relation est symétrique.
- Si $x, y, z \in G$ sont tels que xy^{-1} et yz^{-1} sont dans H, alors leurs produit xz^{-1} est aussi dans H. Et donc la relation est transitive.

Ainsi, $\mathcal{R}_H$ est une relation d'équivalence. Soit $x \in G$. Un élément y de G est dans la classe d'équivalence de x ssi xy^{-1} est dans H ssi $\exists h \in H : xy^{-1} = h$ ssi $\exists h \in H : x = hy$. Ainsi, la classe d'équivalence de x est l'ensemble $Hx = \{hx, h \in H\}$. C'est donc l'image de H par l'application $\tau_x : G \to G, g \mapsto g$. Comme τ_x est une bijection, $|Hx| = |H|$. □

Corollaire 1.8
Si G est un groupe fini et H un sous-groupe, alors $|H|$ divise $|G|$.

Démonstration. En effet, d'après le lemme, on a $|G| = k \times |H|$, si k est le nombre de classes d'équivalence de $\mathcal{R}_H$. □

Corollaire 1.9 (Lagrange – cas général)
Si G est un groupe fini et si $x \in G$, $\omega_G(x)$ divise $|G|$.

Démonstration. Notons $\langle x \rangle$ le sous-groupe engendré par x. C'est l'ensemble $\{x^n, n \in \mathbb{Z}\} = \{x^n, 0 \leq n \leq \omega_G(x) - 1\}$. En effet, l'inclusion droite-gauche est évidente et si $n \in \mathbb{Z}$, n s'écrit $n = q\omega_G(x) + r$ avec $0 \leq r \leq \omega_G(x) - 1$ et $x^n = x^r$.
De plus, les éléments x^n pour $0 \leq n \leq \omega_G(x) - 1$ sont deux à deux distincts. Sinon, en considérant deux indices $i < j \in [\![0, \omega_G(x) - 1]\!]$, on aurait $x^{j-i} = e_G$ avec $0 < j - i < \omega_G(x)$, en contradiction avec la définition de $\omega_G(x)$.
Ainsi, $\omega_G(x)$ est le cardinal du sous-groupe $\langle x \rangle$. Par le corollaire précédente, $\omega_G(x)$ divise $|G|$. □

Remarque 1.10
On peut réciproquement se demander si, dans un groupe G de cardinal n, on peut trouver un élément d'ordre un diviseur d de n fixé.
C'est faux en général puisque l'existence d'un élément d'ordre n lui-même est équivalente au caractère cyclique de G. Cependant, si p est un nombre premier divisant n, alors il existe un élément d'ordre p (lemme de Cauchy) ; on peut même raffiner : si p^α divise n, alors il existe un sous-groupe de G d'ordre p^α.

2 Groupes cycliques

2.1 Description des groupes cycliques

Définition 2.1
Un groupe cyclique est un groupe fini engendré par un élément.

Théorème 2.2
Si G est un groupe cyclique de cardinal n, alors G est isomorphe au groupe additif $\mathbb{Z}/n\mathbb{Z}$.

Démonstration. Notons x un générateur de G. Comme $G = \{x^k, 0 \leq k \leq \omega_G(x) - 1\}$, on a $n = |G| = \omega_G(x)$. On définit un morphisme de groupes $f : \mathbb{Z} \to G$, par $f(k) = x^k$.
Si k, ℓ sont deux entiers congrus modulo n, alors $\ell - k$ est divisible par n, donc $x^{\ell-k} = e_G$, donc $x^k = x^\ell$. Ceci montre que f induit une application $\bar{f} : \mathbb{Z}/n\mathbb{Z} \to G, \bar{k} \mapsto x^k$. Et $\bar{f}$ est aussi un morphisme de groupes : si $\bar{k}, \bar{\ell} \in \mathbb{Z}/n\mathbb{Z}$, on a

$$\bar{f}(\bar{k} + \bar{\ell}) = \bar{f}(\overline{k + \ell}) = x^{k+\ell} = x^k \times x^\ell = \bar{f}(\bar{k}) \times \bar{f}(\bar{\ell}).$$

Enfin, comme $\mathbb{Z}/n\mathbb{Z}$ et G ont même cardinal, $\bar{f}$ est bijective. On a donc construit un isomorphisme de groupes de $\mathbb{Z}/n\mathbb{Z}$ vers G. □

Exemple 2.3
Le groupe multiplicatif $\mathbb{U}_n$ des racines n-èmes de l'unité est engendré par $e^{2i\pi/n}$. Il est donc isomorphe au groupe additif $\mathbb{Z}/n\mathbb{Z}$.
En pratique, $\mathbb{U}_n$ peut servir de *modèle* aux groupes cycliques autant que $\mathbb{Z}/n\mathbb{Z}$: ou bien les calculs sont écrits multiplicativement avec un exponentielle complexe ; ou bien les calculs sont écrits additivement avec des classes d'entiers modulo n.

Proposition 2.4
Si G est un groupe cyclique de cardinal n, tous les sous-groupes de G sont cycliques et, si d est un diviseur de n, il existe exactement un sous-groupe de G de cardinal d.

Démonstration. Cette propriété est stable par isomorphisme (si on la montre pour un groupe, on la montre immédiatement pour un groupe isomorphe). On peut donc se placer dans $G = \mathbb{U}_n$.
Soit H un sous-groupe de $\mathbb{U}_n$ de cardinal d. Alors, par le théorème de Lagrange, tout élément x de H vérifie $x^d = 1$, donc $x \in \mathbb{U}_d$. On a donc $H \subset \mathbb{U}_d$ et par égalité des cardinaux, $H = \mathbb{U}_d$.
Réciproquement, $\mathbb{U}_d$ est pour tout d diviseur de n un sous-groupe de $\mathbb{U}_n$ et il est cyclique. □

Remarque 2.5
Un produit de groupes cycliques n'est pas cyclique en général. En fait, le théorème de structure des groupes abéliens finis affirme que tout groupe abélien fini est isomorphe à un produit de groupes cycliques.

Proposition 2.6
Si G et H sont deux groupes cycliques de cardinal n et m premiers entre eux, alors $G \times H$ est cyclique.

Démonstration. Notons x et y des générateurs de G et H. Soit $(u, v) \in G \times H$. On peut trouver $k, \ell \in \mathbb{Z}$ tels que $u = x^k$ et $v = y^\ell$. Par théorème des restes chinois, il existe un entier p tel que $p \equiv k\,[n]$ et $p \equiv \ell\,[m]$. Alors, $u = x^p$ et $v = y^p$, donc $(u, v) = (x, y)^p$. Ceci montre que (x, y) est un générateur de $G \times H$, donc que $G \times H$ est cyclique. □

Remarque 2.7
Une version plus précise du théorème dit qu'on a un isomorphisme d'anneaux

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

si n et m sont premiers entre eux.

2.2 Indicatrice d'Euler

Définition 2.8
Soit $n \in \mathbb{N}^*$. L'indicatrice d'Euler $\phi(n)$ est le nombre d'entiers $k \in [\![1, n]\!]$ premiers avec n.

Proposition 2.9
On a les propriétés suivantes :
- *$\phi(n)$ est le cardinal du groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.*
- *$\phi(n)$ est le nombre de générateurs du groupe additif $\mathbb{Z}/n\mathbb{Z}$.*
- *Pour tout $a \in \mathbb{Z}$ premier avec n, $a^{\phi(n)} \equiv 1\,[n]$.*

– $\sum_{d|n} \phi(d) = n$.

Démonstration.
– Si $k \in [\![0, n-1]\!]$, la classe $\bar{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ssi k est premier avec n.
– Soit $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$. On a (attention, convention additive !),

$$\forall a \in \mathbb{Z}, a\overline{k} = \overline{0} \iff n \mid ak \iff \frac{n}{n \wedge k} \mid a\frac{k}{n \wedge k} \iff \frac{n}{n \wedge k} \mid a$$

car $\dfrac{n}{n \wedge k}$ et $\dfrac{k}{n \wedge k}$ sont premiers entre eux. Ceci montre que l'ordre de $\bar{k}$ dans $\mathbb{Z}/n\mathbb{Z}$ est $\dfrac{n}{n \wedge k}$. En particulier, cet ordre vaut n ssi $n \wedge k = 1$.
– Si a est premier avec $\mathbb{Z}$, sa classe modulo n est un inversible de $\mathbb{Z}/n\mathbb{Z}$. Par le théorème de Lagrange appliqué au groupe $(\mathbb{Z}/n\mathbb{Z})^*$, $\bar{a}^{\phi(n)} = \bar{1}$, ce qui signifie que $a^{\phi(n)} \equiv 1\,[n]$.
– Pour chaque diviseur d de n, on sait qu'il existe un unique sous-groupe H_d de $\mathbb{Z}/n\mathbb{Z}$ de cardinal d et que celui-ci est cyclique. Par le deuxième point, ce sous-groupe a $\phi(d)$ générateurs. Il y a donc exactement $\phi(d)$ éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$ (puisqu'un élément d'ordre d est générateur d'un groupe de cardinal d, qui doit être H_d). En distinguant selon l'ordre des éléments de $\mathbb{Z}/n\mathbb{Z}$, on a donc $n = \sum_{d|n} \phi(d)$.

□

Théorème 2.10
Si K est un corps fini, le groupe multiplicatif K^* est cyclique.

Démonstration. Notons n le cardinal de K^*. Soit d un diviseur de n et x un élément de K^* d'ordre d. Alors, le groupe $\langle x \rangle$ est de cardinal d et tous ses éléments y vérifient $y^d = 1$. Comme K est un corps, le polynôme $X^d - 1$ a au plus d racines ; donc toutes ces racines sont contenues dans $\langle x \rangle$. En particulier, les éléments d'ordre d sont les générateurs de $\langle x \rangle$: il y en a donc $\phi(d)$.
Ainsi, pour tout diviseur d de n, on a l'alternative suivante : ou bien il n'y a pas d'élément d'ordre d dans K^*, ou bien il y en a exactement $\phi(d)$.
Pour tout d divisant n, on note m_d le nombre d'éléments d'ordre d. Comme l'ordre de chaque élément divise n, on a $n = \sum_{d|n} m_d$. Donc,

$$n = \sum_{d|n} m_d \leq \sum_{d|n} \phi(d) = n.$$

Ainsi, toutes les inégalités sont des inégalités : pour tout d divisant n, on a $m_d = \phi(d)$. En particulier, m_n est non nul : il existe un générateur de K^*. □

Remarque 2.11
Même pour les corps finis $\mathbb{F}_p$, il n'y a pas de formule générale pour déterminer un générateur

du groupe des inversibles. Il y en a $\phi(p-1)$ et donc la probabilité qu'une classe modulo p (non nulle) prise au hasard soit un générateur est $\dfrac{\phi(p-1)}{p-1}$.
Par exemple, $\phi(12) = 4$ et il y a donc 4 générateurs pour les inversibles de $\mathbb{F}_{13}$. On constate que $2^6 = 64 \equiv -1\,[13]$, donc la classe de 2 est d'ordre 12 dans les inversibles de $\mathbb{F}_{13}$: c'en est un générateur.
Le lecteur pourra écrire un programme Python calculant un (les) générateur(s) de $\mathbb{F}_p$.

3 Groupe symétrique

3.1 Décomposition en produit de cycles à supports disjoints

Définition 3.1 (Groupe symétrique)
Soit $n \in \mathbb{N}^*$. On note $\mathcal{S}_n$ le groupe des permutations de $[\![1, n]\!]$.

Notation 3.2 (Écriture d'une permutation)
Pour écrire une permutation $\sigma \in \mathcal{S}_n$, on utilise une notation matricielle. Sur la première ligne, on énumère les entiers de 1 à n ; sur la deuxième ligne, on écrit leur image par σ.

Exemple 3.3
Pour $n = 4$, la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ est la permutation telle que $\sigma(1) = 4$, $\sigma(2) = 2$, $\sigma(3) = 1$ et $\sigma(4) = 1$.

Définition 3.4 (Orbite d'un point)
Soit $\sigma \in S_n$, soit $k \in [\![1, n]\!]$. L'orbite de k sous σ est l'ensemble $\left\{\sigma^\ell(k), \ell \in \mathbb{Z}\right\}$.

Remarque 3.5
Si ω est l'ordre de σ, on a $\sigma^{\omega-1} = \sigma^{-1}$. Plus généralement, $\sigma^{-\ell} = \sigma^{\ell(\omega-1)}$, pour tout $\ell \in \mathbb{N}$. Donc, dans la définition précédente, on peut se limiter aux puissances positives de σ.

Exemples 3.6
- Pour la permutation σ définie plus haut, l'orbite de 1 est l'ensemble $\{1, 4, 3\}$. L'orbite de 2 est l'ensemble $\{2\}$.
- Si σ est l'identité de $[\![1, n]\!]$, l'orbite de k sous σ est réduite au singleton $\{k\}$.

Proposition 3.7 (Les orbites forment une partition de $[\![1, n]\!]$)
Soit $\sigma \in \mathcal{S}_n$. L'ensemble des orbites sous σ définit une partition de $[\![1, n]\!]$.

Démonstration. On vérifie rapidement que la relation $\mathcal{R}$ définie par

$$\forall k, \ell \in [\![1, n]\!], k \,\mathcal{R}\, \ell \iff \exists i \in \mathbb{Z} : \sigma^i(k) = \ell$$

est une relation d'équivalence sur $[\![1, n]\!]$, dont les orbites sous σ sont les classes d'équivalence. □

Définition 3.8 (Cycle, support)
Soit $p \geq 2$ un entier. Un p-cycle de $\mathcal{S}_n$ est une permutation σ de $\mathcal{S}_n$ pour laquelle il existe p éléments $a_1, \ldots, a_p$ dans $[\![1, n]\!]$, deux à deux distincts, tels que
- $\forall x \notin \{a_1, \ldots, a_p\}, \sigma(x) = x$
- $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, …, $\sigma(a_{p-1}) = a_p$ et $\sigma(a_p) = a_1$.

Le support du p-cycle est l'ensemble $\{a_1, \ldots, a_p\}$, c'est-à-dire l'ensemble des x dans $[\![1, n]\!]$ tels que $\sigma(x) \neq x$.

Définition 3.9 (Transposition)
On appelle transposition un 2-cycle.

Notation 3.10 (Écriture des cycles)
Avec les notations de la définition ci-dessus, le cycle se note $\begin{pmatrix} a_1 & a_2 & \ldots & a_p \end{pmatrix}$.

Exemple 3.11
On reprend l'exemple de la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$. C'est un 3-cycle, qui s'écrit simplement $\begin{pmatrix} 1 & 4 & 3 \end{pmatrix}$. On notera que l'écriture allégée d'un p-cycle n'est pas unique. Ici,

$$\begin{pmatrix} 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 4 \end{pmatrix}.$$

Attention !
Une permutation n'est pas caractérisée par sa partition en orbites. Pour $n = 4$, les 3-cycles $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ et $\begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$ ont toutes les deux comme orbites $\{1, 2, 3\}$ et $\{4\}$.

Théorème 3.12 (Décomposition en produit de cycles à supports disjoints)
Soit $\sigma \in \mathcal{S}_n$. Il existe un entier $k \geq 0$, des entiers $p_1, \ldots, p_k \geq 2$, des permutations $\sigma_1, \ldots, \sigma_k$ telles que :
- *Pour tout $i \in [\![1, k]\!]$, σ_i est un p_i-cycle.*
- *Les supports des σ_i sont deux à deux disjoints.*
- *$\sigma = \sigma_1 \circ \cdots \circ \sigma_k$.*

Une telle décomposition de σ est unique à l'ordre près*, au sens où l'ensemble $\{\sigma_1, \ldots, \sigma_k\}$ est entièrement déterminé par σ et par les conditions ci-dessus.*

Démonstration. On note k le nombre d'orbites sous σ non réduites à un singleton et $O_1, \ldots, O_k$ ces orbites. Par définition, $\sigma(O_i) \subset O_i$ pour tout $i \in [\![1, k]\!]$. On note σ_i l'unique permutation de $[\![1, n]\!]$ qui coïncide avec σ sur O_i et qui envoie tout élément de $[\![1, n]\!] \setminus O_i$ sur lui-même. Alors, chaque σ_i est un cycle de longueur $p_i = |O_i|$.
Soit x un élément de $[\![1, n]\!]$.

– Si x est un point fixe de σ, il n'est dans aucun O_i. Donc, $\sigma_i(x) = x$ pour tout i et $\sigma(x) = x = \sigma_1 \circ \cdots \circ \sigma_k(x)$.

– Si x n'est pas un point fixe de σ, il est dans un unique O_i. Pour ce i, on a $\sigma_i(x) = \sigma(x)$ et pour les $j \neq i$, on a $\sigma_j(x) = x$ ainsi que $\sigma_j(\sigma_i(x)) = \sigma_i(x)$ (car $\sigma_i(x) \in O_i$). On en déduit immédiatement que $\sigma_1 \circ \cdots \circ \sigma_k(x) = \sigma(x)$.

Donc, $\sigma = \sigma_1 \circ \cdots \circ \sigma_k$.

L'unicité se montre de façon analogue (*arnaque ?*).

□

Remarque 3.13
Comme les supports des cycles σ_i sont disjoints, ces cycles commutent deux à deux.

Méthode 3.14 (Écriture en produit de cycles)
Pour écrire une permutation sous cette forme, on suit l'algorithme suivant :
– On commence par l'élément 1 et on écrit les éléments $\sigma^k(1)$ dans l'ordre d'apparition ($k \geq 1$) jusqu'à boucler sur 1 (si 1 est envoyé sur lui-même, il n'apparait pas dans la décomposition).
– On a alors traité l'orbite de 1. On prend le premier entier qui n'est pas dans l'orbite de 1 et on recommence.
– On procède ainsi jusqu'à avoir épuisé tous les éléments de $[\![1, n]\!]$.

Par exemple, pour $n = 8$, on considère $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 7 & 1 & 3 & 5 & 8 & 6 \end{pmatrix}$. On calcule

$$\sigma = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 3 & 7 & 8 & 6 & 5 \end{pmatrix}.$$

Remarque 3.15
Le *produit* des permutations étant en réalité une composition, le calcul d'un produit de cycles se fait de droite à gauche.

Exemple 3.16
On souhaite écrire comme produit de cycles à supports disjoints la permutation

$$\sigma = \begin{pmatrix} 1 & 3 & 7 \end{pmatrix} \begin{pmatrix} 3 & 2 & 5 & 6 \end{pmatrix} \begin{pmatrix} 5 & 4 & 1 \end{pmatrix}.$$

– 1 est envoyé sur 6, 6 sur 7, 7 sur 1.
– 2 est envoyé sur 5, 5 sur 4, 4 sur 3, 3 sur 2.

Donc, $\sigma = \begin{pmatrix} 1 & 6 & 7 \end{pmatrix} \begin{pmatrix} 2 & 5 & 4 & 3 \end{pmatrix}$.

Théorème 3.17 (Les transpositions engendrent $\mathcal{S}_n$)
Toute permutation σ de $\mathcal{S}_n$ s'écrit comme un produit de transpositions.

Démonstration. Comme toute permutation est un produit de cycles, il suffit de montrer que tout cycle est un produit de transposition. Or, si $a_1, \ldots, a_p$ sont des entiers deux à

deux distincts de $[\![1, n]\!]$, on constate que

$$\begin{pmatrix} a_1 & \dots & a_p \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \begin{pmatrix} a_2 & a_3 \end{pmatrix} \dots \begin{pmatrix} a_{p-1} & a_p \end{pmatrix}.$$

□

Remarque 3.18
Il n'y a pas unicité. Par exemple, le 3-cycle $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ est égal à $\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix}$, mais aussi à $\begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}$.

3.2 Inversions et signature

Définition 3.19 (Inversion d'une permutation)
Soit σ un élément de $\mathcal{S}_n$. Une *inversion* de σ est un couple (k, ℓ) d'entiers de $[\![1, n]\!]$, tels que $k < \ell$ et $\sigma(k) > \sigma(\ell)$.

Notation 3.20 (Nombre d'inversions)
On note $I(\sigma)$ le nombre d'inversions de σ.

Définition 3.21 (Signature d'une permutation)
La signature de σ – notée $\varepsilon(\sigma)$ – est le nombre $(-1)^{I(\sigma)}$.

Exercice 3.22
Montrer que la signature d'une transposition est égale à -1.

Démonstration. Considérons $\tau = \begin{pmatrix} k & \ell \end{pmatrix}$, avec $k < \ell$. Un couple (i, j) avec $i < j$ est une inversion de σ ssi on a l'un des cas suivants :
- $(i, j) = (k, \ell)$: une inversion
- $i = k$ et $k < j < \ell$: $\ell - k - 1$ inversions
- $k < i < \ell$ et $j = \ell$: $\ell - k - 1$ inversions

Ainsi, $I(\sigma) = 1 + 2(\ell - k - 1)$, donc $\varepsilon(\sigma) = -1$. □

Lemme 3.23
Pour tout $\sigma \in \mathcal{S}_n$, $\varepsilon(\sigma) = \displaystyle\prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$.

Démonstration. On note $\mathcal{D}$ l'ensemble des couples (i, j) avec $1 \leq i < j \leq n$. On définit une application $f : \mathcal{D} \to \mathcal{D}$ par $f\big((i, j)\big) = \big(\sigma(i), \sigma(j)\big)$ si $\sigma(i) < \sigma(j)$; $\big(\sigma(j), \sigma(i)\big)$ sinon. Si (i, j) et (i', j') dans $\mathcal{D}$ ont même image, alors $\{\sigma(i), \sigma(j)\} = \{\sigma(i'), \sigma(j')\}$, donc $\{i, j\} = \{i', j'\}$ car σ est une permutation et donc $(i, j) = (i', j')$ car $i < j$ et $i' < j'$. Ainsi, f est une injection de $\mathcal{D}$ (ensemble fini) dans lui-même, donc une bijection.
Le produit $\displaystyle\prod_{1 \leq i < j \leq n} \big(\sigma(j) - \sigma(i)\big)$ vaut $\displaystyle\prod_{1 \leq k < \ell < n} \varepsilon_{k,\ell}(\ell - k)$ après changement de variable donné

par f, où $\varepsilon_{k,\ell}$ vaut -1 si (k,ℓ) est une inversion de σ et 1 sinon. On a donc :

$$\prod_{1\leq i<j\leq n}\frac{\sigma(j)-\sigma(i)}{j-i}=(-1)^{I(\sigma)}\frac{\prod_{1\leq k<\ell\leq n}(\ell-k)}{\prod_{1\leq i<j\leq n}(j-i)}=\varepsilon(\sigma).$$

□

Théorème 3.24 (La signature est un morphisme de groupes)
Le morphisme de signature $\varepsilon:\mathcal{S}_n\to\{\pm 1\}$ est un morphisme de groupes :

$$\forall\sigma,\tau\in\mathcal{S}_n,\varepsilon(\sigma\circ\tau)=\varepsilon(\sigma)\varepsilon(\tau).$$

Démonstration. On a

$$\varepsilon(\sigma\circ\tau)=\prod_{1\leq i<j\leq n}\frac{\sigma\circ\tau(j)-\sigma\circ\tau(i)}{j-i}=\prod_{1\leq i<j\leq n}\frac{\sigma\circ\tau(j)-\sigma\circ\tau(i)}{\tau(j)-\tau(i)}\times\frac{\tau(j)-\tau(i)}{j-i}.$$

On casse le produit en deux. Le deuxième vaut $\varepsilon(\tau)$.
Le premier peut se réécrire $\displaystyle\prod_{1\leq k<\ell\leq n}\frac{\sigma(\ell)-\sigma(k)}{\ell-k}=\varepsilon(\sigma)$. On réutilise en effet la bijection $f:\mathcal{D}\to\mathcal{D}$ définie dans la démonstration précédente, avec τ au lieu de σ.
Donc, $\varepsilon(\sigma\circ\tau)=\varepsilon(\sigma)\varepsilon(\tau)$. □

Corollaire 3.25 (Signature d'un p-cycle)
La signature d'un p-cycle est $(-1)^{p-1}$.

Démonstration. On a vu précédemment qu'un p-cycle peut s'écrire comme produit de $p-1$ transpositions. On utilise alors le fait que les transpositions ont signature -1 et que la signature est un morphisme de groupes. □

Corollaire 3.26 (Signature d'une permutation écrite en produit de cycles)
On suppose que, dans la décomposition en produits de cycles à supports disjoints de σ, il y a k cycles de longueur $p_1,\ldots,p_k$. La signature de σ est $(-1)^{\sum_{i=1}^k p_i-k}$.

Démonstration. Immédiat avec le corollaire précédente, en utilisant le fait que la signature est un morphisme de groupes. □

4 Exemples de groupes finis

Proposition 4.1
Un groupe de cardinal p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Démonstration. C'est un corollaire du théorème de Lagrange. L'ordre de tout élément autre que l'élément neutre doit être p et cet élément est donc un générateur du groupe. □

Proposition 4.2
À isomorphisme près, il existe deux groupes de cardinal 4 *:* $\mathbb{Z}/4\mathbb{Z}$ *et* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Démonstration. Soit G un groupe de cardinal 4. Si G admet un élément d'ordre 4, alors G est cyclique, donc isomorphe à $\mathbb{Z}/4\mathbb{Z}$. Sinon, tous les éléments sauf e_G sont d'ordre 2 par le théorème de Lagrange. Notons x et y deux éléments distincts différents de e_G. L'élément xy ne peut pas être égal à x (sinon on aurait $y = e_G$) ni à y (sinon $x = e_G$) ni à e (car x est son propre inverse). Donc, $G = \{e, x, y, xy\}$. Comme chaque élément est son propre inverse, si $u, v \in G$, on a $uv = u^{-1}v^{-1} = (vu)^{-1} = vu$ et donc G est abélien.
On considère alors $f : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to G$ envoyant $(\bar{0}, \bar{0})$ sur e_G, $(\bar{0}, \bar{1})$ sur x, $(\bar{1}, \bar{0})$ sur y et $(\bar{1}, \bar{1})$ sur xy et on constate que f est un isomorphisme de groupes (*écrire les deux tables de multiplication*). □

Proposition 4.3
À isomorphisme près, il existe deux groupes de cardinal 6 *:* $\mathbb{Z}/6\mathbb{Z}$ *et* $\mathcal{S}_3$.

Démonstration. Soit G un groupe de cardinal 6. Si G a un élément d'ordre 6 donc G est cyclique, isomorphe à $\mathbb{Z}/6\mathbb{Z}$.
On suppose que G n'a pas d'élément d'ordre 6. Par le théorème de Lagrange, les éléments différents de e_G sont d'ordre 2 ou 3.

- Supposons que tous les éléments non triviaux soient d'ordre 2. Alors, comme précédemment, G serait abélien. En notant x et y deux éléments distincts et non triviaux, le groupe engendré par x et y serait $\{e_G, x, y, xy\}$ de cardinal 4. Comme 4 ne divise pas 6, c'est impossible. Donc, il existe au moins un élément d'ordre 3.
- Supposons que tous les éléments non triviaux soient d'ordre 3. Notons x un tel élément ; on a $\langle x \rangle = \{e_G, x, x^2\}$. Notons y un element distinct des précédents ; on a $\langle y \rangle = \{e_G, y, y^2\}$. De plus, les éléments e, x, x^2, y, y^2 sont deux à deux distincts (car $\langle x \rangle = \langle x^2 \rangle$ et $\langle y \rangle = \langle y^2 \rangle$). Il reste donc un autre élément z d'ordre 3. Mais par le même argument, les éléments $e_G, x, x^2, y, y^2, z, z^2$ sont deux à deux distincts, ce qui est absurde. Donc, G a un élément d'ordre 2.

Notons x un élément d'ordre 3 et y un élément d'ordre 2. Si x et y commutent, on a $(xy)^k = x^k y^k$. Donc, $(xy)^k = e_G$ ssi $x^k = y^k$ (y vaut son inverse) ssi k est divisible par 6 (comparer les ordres de x^k et y^k). Ainsi, xy serait d'ordre 6, ce qui est exclu. Donc, x et y ne commutent pas.
Les éléments de G sont e_G, x, x^2, y, xy et yx. En effet, ces 6 éléments sont deux à deux distincts (on compare les ordres et on utilise que $xy \neq yx$) et G est de cardinal 6. On peut alors écrire la table de multiplication de G ; comme tout élément dans un groupe est simplifiable, chaque élément doit apparaître sur chaque ligne et chaque colonne ce qui permet de résoudre les ambiguïtés. Par exemple, on a $x \times e_G = x$; $x \times x = x^2$;

$x \times x^2 = e_G$; $x \times y = xy$ et donc $x \times xy$ et $x \times yx$ doivent prendre les valeurs y ou yx. Nécessairement, on doit avoir $x \times xy = yx$ et $x \times yx = y$. On écrit enfin la table de multiplication de $\mathcal{S}_3$ en remarquant que les éléments de $\mathcal{S}_3$ sont id, σ, σ^2, τ, $\sigma \circ \tau$ et $\tau \circ \sigma$ où $\sigma = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 \end{pmatrix}$. On constate que les tables de multiplication se correspondent, ce qui conclut. □

Proposition 4.4
À isomorphisme près, il existe 5 *groupes de cardinal* 8 *:* $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$ *et deux groupes non abéliens : le groupe diédral* D_8 *et le groupe des quaternions* H_8.

Remarque 4.5
On se contente de décrire les deux groupes non abéliens.

- Le groupe diédral D_8 peut être défini comme le groupe des isométries du plan préservant les sommets d'un carré. Il est isomorphe au sous-groupe de $\mathcal{S}_4$ engendré par $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 3 \end{pmatrix}$.
- On peut écrire les éléments de H_8 comme ± 1, $\pm i$, $\pm j$, $\pm k$, qui vérifient entre autres relations $i^2 = j^2 = k^2 = -1$ et $ij = k$. On peut le réaliser comme le sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ engendré par les matrices I et J définies par

$$I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ et } J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$