JEAN-ÉTIENNE ROMBALDI

Mathématiques pour l'agrégation

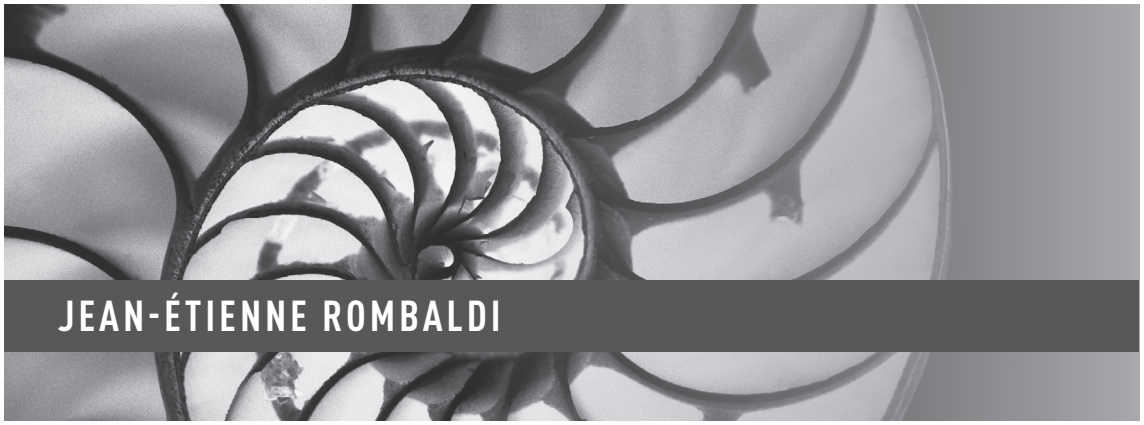
Algèbre et géométrie

2e édition

AGRÉGATION INTERNE ET EXTERNE MATHÉMATIQUES

- Éléments de cours
- Applications transversales
- Près de 300 exercices corrigés

deboeck SUPÉRIEUR



JEAN-ÉTIENNE ROMBALDI

Mathématiques pour l'agrégation

Algèbre et géométrie

2e édition

deboeck SUPÉRIEUR

Chez le même éditeur (extrait du catalogue)

Agrégation de mathématiques :

DANTZER J.-F., *Mathématiques pour l'agrégation. Analyse et probabilités* – 2e édition

ROMBALDI J.-É., *Exercices et problèmes corrigés pour l'agrégation de mathématiques*

ROMBALDI J.-É., *Leçons d'oral pour l'agrégation de mathématiques. Première épreuve : les exposés*

ROMBALDI J.-É., *Leçons d'oral pour l'agrégation de mathématiques. Seconde épreuve : les exercices*

Capes de mathématiques :

DARRACQ M.-C. & ROMBALDI J.-É., *Mathématiques pour le Capes. Analyse*

DARRACQ M.-C. & ROMBALDI J.-É., *Mathématiques pour le Capes. Algèbre et géométrie* (nouveauté 2021)

DARRACQ M.-C. & ROMBALDI J.-É., *Mathématiques pour le Capes. Probabilités* (nouveauté 2021)

En couverture : Coupe d'un nautile © AdrianHancu/Istockphoto
Maquette intérieure : Hervé Soulard/Nexeme
Mise en pages de l'auteur
Maquette de couverture : Primo&Primo
Couverture : SCM, Toulouse

Dépôt légal :
Bibliothèque royale de Belgique : 2021/13647/062
Bibliothèque nationale, Paris : avril 2021
ISBN : 978-2-8073-3220-1

Sommaire

Table des matières

Avant-propos

Cet ouvrage est dédié à un très cher ami, Richard André-Jeannin, décédé en 2011

Ce livre destiné aux candidats à l'agrégation interne et externe de Mathématiques complète le cours d'analyse et probabilités pour l'agrégation interne de Jean-François Dantzer dans la même collection. On trouvera des compléments à ces deux ouvrages, sous formes d'exercices et de problèmes, dans [32], les problèmes proposés pouvant être utilisés comme entraînements aux épreuves écrites, certains énoncés de problèmes de ce livre étant inspirés de problèmes d'agrégation interne ou externe.

Le niveau de connaissance suffisant pour la lecture de ce cours est celui du premier cycle universitaire.

Le but est de couvrir une grande partie des thèmes d'algèbre et géométrie proposés pour les épreuves orales et j'ai pris soin de faire suivre chaque théorème important d'une série d'applications.

Ce cours est aussi l'occasion de réviser des notions de base pour l'écrit et les nombreux exercices proposés, tous corrigés en détail, outre le fait qu'ils peuvent constituer un bon entraînement, peuvent être utilisés pour des développements dans les leçons d'oral de l'agrégation externe et interne ainsi que pour des leçons d'oral 2 de l'agrégation interne.

Les premiers chapitres sont consacrés à l'étude des groupes et leur utilisation en géométrie, en traitant en particulier l'étude des actions de groupe et du groupe symétrique. Le lien entre groupes et géométrie fait l'objet d'un chapitre particulier. On s'intéresse également à l'utilisation des nombres complexes en géométrie et au groupe linéaire.

L'arithmétique est étudiée dans un cadre général avec l'étude des anneaux principaux et euclidiens. L'arithmétique sur l'anneau $\mathbb{Z}$ des entiers relatifs, l'étude des nombres premiers et des anneaux $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est l'objet de chapitres particuliers, de même que l'étude des polynômes à coefficients dans un corps commutatif ou un anneau commutatif unitaire. Ces notions d'arithmétique sont approfondies avec l'étude des corps finis.

Pour ce qui est de l'algèbre linéaire et bilinéaire, on s'intéresse à la dualité, aux déterminants avec une attention particulière pour le résultant, aux formes quadratiques, aux coniques et à la réduction des endomorphismes. On s'intéresse aussi aux séries matricielles et à l'exponentielle de matrice.

La plupart des chapitres de ce livre correspondent à des leçons d'oral de l'agrégation interne et externe, mais il ne s'agit pas de modèles de leçons.

Pour cette deuxième édition, les modifications essentielles sont les suivantes :

— corrections de coquilles et erreurs diverses de la première édition ;
— modification du chapitre 4 sur les nombres complexes et la géométrie ;
— ajout du chapitre 6 sur les actions de groupes sur des espaces de matrices ;
— suppression du chapitre sur les représentations de groupes finis (pour ne pas aboutir à un livre trop volumineux) ;
— modification du chapitre 16 sur les coniques ;
— ajout du paragraphe 21.9 sur la réduction de Frobenius dans le chapitre 21 sur la réduction des endomorphismes.

Je tiens encore à remercier mes bons amis Marie-Cécile Darracq et Gérard Vinel qui ont accepté la tâche ingrate de relire quelques chapitres de ce livre. Leurs conseils me furent très utiles. Je remercie également les éditions De Boeck, et en particulier Alain Luguet, pour la confiance qu'ils m'accordent.

Chapitre 1

Quelques rappels sur les groupes

Sauf précision contraire, les groupes sont notés multiplicativement et l'élément neutre d'un groupe G est noté 1 (ou 1_G si nécessaire). Les notions de base : définition d'un groupe, d'un sous-groupe, d'un morphisme de groupes, de noyau et d'image avec leurs propriétés élémentaires sont supposées acquises.

Si G est un groupe ayant un nombre fini d'éléments son cardinal, noté $\text{card}(G)$, est aussi appelé l'ordre de G.

Pour ce qui suit, on se donne un groupe multiplicatif $(G, \cdot)$.

1.1 Sous-groupes distingués. Groupes quotients

Si H est une partie non vide G, on note alors, pour tout $g \in G$:

$$gH = \{gh \mid h \in H\} \text{ et } Hg = \{hg \mid h \in H\}$$

Dans le cas où G est commutatif, on a $gH = Hg$.

Théorème 1.1.

Pour tout sous-groupe H de G, la relation $\mathcal{R}_g$ (ou de manière plus précise $(\mathcal{R}_H)_g$) définie sur G par $g_1 \mathcal{R}_g g_2$ si, et seulement si, $g_1^{-1} g_2 \in H$ est une relation d'équivalence.

Preuve. Pour tout $g \in G$, on a $g^{-1}g = 1 \in H$, donc $\mathcal{R}_g$ est réflexive. Si g_1, g_2 dans G sont tels que $g_1^{-1}g_2 \in H$, on a alors $\left(g_1^{-1}g_2\right)^{-1} = g_2^{-1}g_1 \in H$, ce qui signifie que $g_2 \mathcal{R}_g g_1$. Cette relation est donc symétrique. Si g_1, g_2, g_3 dans G sont tels que $g_1^{-1}g_2 \in H$ et $g_2^{-1}g_3 \in H$, on a alors $g_1^{-1}g_3 = \left(g_1^{-1}g_2\right)\left(g_2^{-1}g_3\right) \in H$, ce qui signifie que $g_1 \mathcal{R}_g g_3$. Cette relation est donc transitive. □

On note, pour $g \in G$, $\overline{g}$ la classe d'équivalence de g modulo $\mathcal{R}_g$ et on dit que $\overline{g}$ est la classe à gauche modulo H de g. On a donc :

$$(h \in \overline{g}) \Leftrightarrow (g \mathcal{R}_g h) \Leftrightarrow \left(g^{-1}h \in H\right) \Leftrightarrow (\exists k \in H \mid h = gk) \Leftrightarrow (h \in gH)$$

c'est-à-dire que $\overline{g} = gH$. En particulier, $\overline{1} = H$ et $\overline{g} = H$ si, et seulement si, $g \in H$.

L'ensemble de ces classes d'équivalence est noté G/H et on l'appelle l'ensemble des classes à gauche modulo H. On a donc $G/H = \{\overline{g} \mid g \in G\} = \{gH \mid g \in G\}$.

On peut définir, de manière analogue l'ensemble $H\backslash G = \{Hg \mid g \in G\}$ des classes à droites modulo H à partir de la relation d'équivalence :

$$(g_1 \mathcal{R}_d g_2) \Leftrightarrow \left(g_1 g_2^{-1} \in H\right)$$

Théorème 1.2.

Si H est un sous-groupe de G, l'ensemble des classes à gauche [resp. à droite] modulo H deux à deux distinctes forme alors une partition de G.

Preuve. Soit $(\overline{g_i})_{i\in I}$ la famille de toutes les classes à gauche modulo H deux à deux distinctes. Pour tout $g \in g$, il existe un unique indice $i \in I$ tel que $\overline{g} = \overline{g_i}$, donc $G = \bigcup_{i\in I} \overline{g_i}$. Dire que g est dans $\overline{g_j} \cap \overline{g_k}$ signifie que g est équivalent à gauche modulo H à g_j et g_k, donc par transitivité g_j et g_k sont équivalents, ce qui revient à dire que $\overline{g_j} = \overline{g_k}$. Ces classes à gauche forment donc bien une partition de G. On peut aussi tout simplement dire que dès qu'on a une relation d'équivalence, sur G les classes d'équivalence partitionnent G. □

Définition 1.1. *Si H est un sous-groupe de G, le cardinal de l'ensemble G/H est noté $[G : H]$ et on l'appelle l'indice de H dans G.*

En remarquant que l'application $g \mapsto g^{-1}$ réalise une permutation de G, on vérifie facilement que, pour tout sous-groupe H de G, on a $\operatorname{card}(G/H) = \operatorname{card}(G\backslash H)$.

L'application $\pi_H : g \in G \mapsto \overline{g} = gH \in G/H$ est surjective. C'est la surjection canonique de G sur G/H.

Dans le cas des groupes finis, la partition en classes à gauche modulo H nous donne le résultat de démonstration élémentaire suivant qui a de nombreuses applications.

Théorème 1.3. Lagrange

Soient G un groupe fini d'ordre $n \geq 2$ et H un sous-groupe de G. Pour tout $g \in G$ on a $\operatorname{card}(gH) = \operatorname{card}(H)$ et $\operatorname{card}(G) = [G : H] \operatorname{card}(H)$, donc l'ordre de H divise celui de G.

Preuve. Pour g fixé dans le groupe G, la « translation à gauche » $h \mapsto gh$ réalise une permutation de G et sa restriction à H réalise une bijection de H sur gH. Il en résulte que gH et H ont même cardinal. Comme l'ensemble des classes à gauche suivant H réalise une partition de G, ces classes étant en nombre fini toutes de cardinal égal à celui de H, on en déduit que $\operatorname{card}(G) = [G : H] \operatorname{card}(H)$. □

Le théorème de Lagrange se traduit aussi par :

$$[G : H] = \operatorname{card}(G/H) = \frac{\operatorname{card}(G)}{\operatorname{card}(H)}$$

Définition 1.2. *On dit qu'une relation d'équivalence $\mathcal{R}$ sur G est compatible avec la loi de G si, pour tous g, g', h dans G, on a :*

$$(g\mathcal{R}g') \Rightarrow (ghRg'h \text{ et } hg\mathcal{R}hg')$$

Théorème 1.4.

Si H est un sous-groupe de G, la relation d'équivalence $\mathcal{R}_g$ associée à H est alors compatible avec la loi de G si, et seulement si, on a $gH = Hg$ pour tout $g \in G$.

Preuve. Supposons $\mathcal{R}_g$ compatible avec la loi de G. Pour tout $k \in gH$, on a $g^{-1}k\mathcal{R}_g 1$ et avec la compatibilité à gauche et à droite, on déduit que $g\left(g^{-1}k\right)\mathcal{R}_g g$ et $g\left(g^{-1}k\right)g^{-1}\mathcal{R}_g gg^{-1}$, soit $kg^{-1}\mathcal{R}_g 1$, ce qui revient à dire que $k \in Hg$. On a donc $gH \subset Hg$. De manière analogue, on voit que $Hg \subset gH$ et donc $gH = Hg$ (si $k \in Hg$, alors $kg^{-1}\mathcal{R}_g 1$, donc $\left(kg^{-1}\right)g\mathcal{R}_g g$ et $g^{-1}\left(kg^{-1}\right)g\mathcal{R}_g g^{-1}g$, soit $g^{-1}k\mathcal{R}_g 1$ et $k \in gH$). Réciproquement, supposons que $gH = Hg$ pour tout $g \in G$. Si $g\mathcal{R}_g g'$ et $h \in G$, on a alors $(gh)^{-1}g'h = h^{-1}g^{-1}g'h$ avec $g^{-1}g' \in H$, donc $g^{-1}g'h$ est dans $Hh = hH$ et $(gh)^{-1}g'h = h^{-1}hk = k \in H$, c'est-à-dire que $ghR_g g'h$. Puis avec $(hg)^{-1}hg' = g^{-1}h^{-1}hg' = g^{-1}g' \in H$, on déduit que $hg\mathcal{R}_g hg'$. Donc $\mathcal{R}_g$ est compatible avec la loi de G. □

Définition 1.3. *On dit qu'un sous-groupe H de G est distingué (ou normal), si on a $gH = Hg$ pour tout $g \in G$.*

Exemples 1.1

1. *Les sous-groupes $\{1\}$ et G sont toujours distingués dans G.*
2. *L'intersection de deux sous-groupes distingués de G est distingué.*
3. *Si le groupe G est commutatif, tous ses sous-groupes sont alors distingués.*

Un sous-groupe H de G est distingué si, et seulement si, on a $gHg^{-1} = H$ (ou $H = g^{-1}Hg$) ce qui équivaut à dire que $ghg^{-1} \in H$ (ou $g^{-1}hg \in H$) pour tout $(h, g) \in H \times G$, qui est encore équivalent à dire que H est stable par tout automorphisme intérieur $h \mapsto ghg^{-1}$.

Le résultat qui suit est souvent utilisé pour montrer qu'un sous-groupe est distingué.

Théorème 1.5.

Si G, G' sont deux groupes et φ un morphisme de groupes de G dans G', alors $\ker(\varphi)$ est un sous-groupe distingué de G.

Preuve. Pour $(g, h) \in G \times \ker(\varphi)$, on a :

$$\varphi\left(g^{-1}hg\right) = \varphi\left(g^{-1}\right)\varphi(h)\varphi(g) = \varphi(g)^{-1} \cdot 1_{G'} \cdot \varphi(g) = 1_{G'}$$

c'est-à-dire que $g^{-1}hg \in \ker(\varphi)$. Le sous-groupe $\ker(\varphi)$ de G est donc distingué. □

Définition 1.4. *Le centre (ou commutateur) $Z(G)$ d'un groupe G est la partie de G formée des éléments de G qui commutent à tous les autres éléments de G, soit $Z(G) = \{h \in G \mid \forall g \in G,\ gh = hg\}$.*

Ce centre étant le noyau du morphisme de groupes :

$$\begin{array}{ccccc} \text{Int} & G & \to & & \text{Aut}(G) \\ & g & \mapsto & \text{Int}(g) : h \mapsto ghg^{-1} & \end{array}$$

(automorphismes intérieurs), c'est un sous-groupe distingué de G. De plus ce sous-groupe est commutatif.

Il est facile de vérifier que si deux groupes sont isomorphes, il en est alors de même de leurs centres. En effet, si G, G' sont deux groupes et $\varphi : G \to G'$ un isomorphisme de groupes, on a alors :

$$\begin{aligned}(g \in Z(G)) &\Leftrightarrow (\forall h \in G,\ gh = hg) \Leftrightarrow (\forall h \in G,\ \varphi(g)\varphi(h) = \varphi(h)\varphi(g)) \\ &\Leftrightarrow (\forall h' \in G',\ \varphi(g)h' = h'\varphi(g)) \Leftrightarrow (\varphi(g) \in Z(G'))\end{aligned}$$

Il en résulte que φ induit un isomorphisme de groupes de $Z(G)$ sur $Z(G')$.

Théorème 1.6.

Un sous-groupe H de G est distingué si, et seulement si, il existe une unique structure de groupe sur l'ensemble quotient G/H des classes à gauche modulo H telle que la surjection canonique $\pi_H : G \to G/H$ soit un morphisme de groupes.

Preuve. Si G/H est muni d'une structure de groupe telle que π_H soit un morphisme de groupes, on a alors nécessairement pour tous g, g' dans G :

$$\overline{g}\overline{g'} = \pi_H(g)\pi_H(g') = \pi_H(gg') = \overline{gg'}$$

Pour (g, h) dans $G \times H$, on a alors $\overline{g^{-1}hg} = \overline{g^{-1}}\overline{h}\overline{g} = \overline{g^{-1}}\overline{g} = \overline{g^{-1}g} = \overline{1} = H$, ce qui signifie que $g^{-1}hg \in H$ (on a $\overline{g} = gH = \overline{1} = H$ si, et seulement si, $g \in H$).

Supposons H distingué. L'analyse que l'on vient de faire nous montre que la seule loi possible sur G/H est définie par $\overline{g}\overline{g'} = \overline{gg'}$. Pour montrer qu'une telle définition est permise, il s'agit de montrer qu'elle ne dépend pas des choix des représentants de $\overline{g}$ et $\overline{g'}$, ce qui résulte du fait que $\mathcal{R}_g$ est compatible avec la loi de G. En effet, si $g\mathcal{R}_g g_1$ et $g'\mathcal{R}_g g_1'$, on a alors $gg'\mathcal{R}_g g_1 g'$ et $g_1 g'\mathcal{R}_g g_1 g_1'$, donc $gg'\mathcal{R}_g g_1 g_1'$ et $\overline{gg'} = \overline{g_1 g_1'}$. Il reste à vérifier que G/H muni de cette loi de composition interne est bien un groupe. Avec :

$$\overline{g_1}\,(\overline{g_2}\ \overline{g_3}) = \overline{g_1 g_2 g_3} = \overline{g_1\,(g_2 g_3)} = \overline{(g_1 g_2)\,g_3} = \overline{g_1 g_2 g_3} = (\overline{g_1}\ \overline{g_2})\,\overline{g_3}$$

on déduit que cette loi est associative. Avec $\overline{g}\overline{1} = \overline{g \cdot 1} = \overline{g}$, on déduit que $\overline{1}$ est le neutre. Avec $\overline{g}\overline{g^{-1}} = \overline{g \cdot g^{-1}} = \overline{1}$, on déduit que tout élément de G/H est inversible avec $(\overline{g})^{-1} = \overline{g^{-1}}$. Par définition de cette loi, l'application π est surjective. □

Pour H distingué dans G, le noyau de la surjection canonique est :

$$\ker(\pi_H) = \left\{g \in G \mid \overline{g} = \overline{1}\right\} = \overline{1} = H$$

Comme on a vu que le noyau d'un morphisme de groupes est distingué, on déduit qu'un sous-groupe distingué de G est le noyau d'un morphisme de groupes.

Dans le cas où G est commutatif, pour tout sous-groupe H de G, G/H est un groupe puisque tous les sous-groupes de G sont distingués. On le note alors $\dfrac{G}{H}$ (il est aussi égal à $G\backslash H$).

Théorème 1.7.

Si G, G' sont deux groupes et $\varphi : G \to G'$ un morphisme de groupes, il existe alors un unique isomorphisme de groupes $\overline{\varphi} : G/\ker(\varphi) \to \mathrm{Im}(\varphi)$ tel que $\varphi = i \circ \overline{\varphi} \circ \pi$, en notant $i : \mathrm{Im}(\varphi) \to G'$ est l'injection canonique et $\pi : G \to G/\ker(\varphi)$ la surjection canonique.

Preuve. Comme $\ker(\varphi)$ est distingué dans G, $G/\ker(\varphi)$ est un groupe. Si un tel isomorphisme $\overline{\varphi}$ existe, on a alors $\varphi(g) = i \circ \overline{\varphi} \circ \pi(g) = i \circ \overline{\varphi}(\overline{g}) = \overline{\varphi}(\overline{g})$ pour tout $g \in G$, ce qui prouve l'unicité de $\overline{\varphi}$.

En exploitant l'analyse du problème, on montre d'abord que l'on peut définir $\overline{\varphi}$ par $\overline{\varphi}(\overline{g}) = \varphi(g)$ pour tout $\overline{g} \in G/\ker(\varphi)$. Pour justifier cette définition, on doit vérifier qu'elle ne dépend pas du choix d'un représentant de $\overline{g}$. Si $\overline{g} = \overline{h}$, on a alors $g^{-1}h \in \ker(\varphi)$, donc $(\varphi(g))^{-1}\varphi(h) = \varphi\left(g^{-1}h\right) = 1$ et $\varphi(g) = \varphi(h)$. L'application $\overline{\varphi}$ est donc bien définie et par construction, on a $\varphi = i \circ \overline{\varphi} \circ \pi$. Avec $\overline{\varphi}\left(\overline{g}\overline{h}\right) = \overline{\varphi}\left(\overline{gh}\right) = \varphi(gh) = \varphi(g)\varphi(h) = \overline{\varphi}(\overline{g})\overline{\varphi}\left(\overline{h}\right)$, on voit que c'est un morphisme de groupes.

L'égalité $\overline{\varphi}(\overline{g}) = 1$ équivaut à $\varphi(g) = 1$, soit à $g \in \ker(\varphi)$ ou encore à $\overline{g} = \overline{1}$. Ce morphisme est donc injectif et étant à valeurs dans $\mathrm{Im}(\varphi) = \mathrm{Im}(\overline{\varphi})$, il est surjectif. □

Corollaire 1.1. *Soient G, G' deux groupes et $\varphi : G \to G'$ un morphisme de groupes. Si G est fini, on a alors* $\mathrm{card}(G) = \mathrm{card}(\ker(\varphi))\,\mathrm{card}(\mathrm{Im}(\varphi))$.

Preuve. Comme $G/\ker(\varphi)$ et $\mathrm{Im}(\varphi)$ sont isomorphes, dans le cas où G est fini, on a $\mathrm{card}(\mathrm{Im}(\varphi)) = \mathrm{card}(G/\ker(\varphi)) = \dfrac{\mathrm{card}(G)}{\mathrm{card}(\ker(\varphi))}$. □

Pour H sous-groupe de G, la compatibilité de $\mathcal{R}_g$ avec la loi de G est une condition nécessaire et suffisante pour définir naturellement une structure de groupe sur l'ensemble quotient G/H par $\overline{g}\ \overline{g'} = \overline{gg'}$. Précisément, on a le théorème qui suit, où $G/\mathcal{R}$ est l'ensemble des classes d'équivalence modulo une relation d'équivalence $\mathcal{R}$ et $\pi : g \mapsto \overline{g} = \{h \in G \mid g\mathcal{R}h\}$ est la surjection canonique de G sur $G/\mathcal{R}$.

Théorème 1.8.

Soit $\mathcal{R}$ une relation d'équivalence sur G. Cette relation est compatible avec la loi de G si, et seulement si, il existe une unique structure de groupe sur l'ensemble quotient $G/\mathcal{R}$ telle que la surjection canonique $\pi : G \to G/\mathcal{R}$ soit un morphisme de groupes.

Preuve. Si $G/\mathcal{R}$ est muni d'une structure de groupe telle que π soit un morphisme de groupe, on a alors nécessairement $\overline{g}\overline{g'} = \pi(g)\pi(g') = \pi(gg') = \overline{gg'}$ pour tous

g, g' dans G. On en déduit que pour g, g', h, h' dans G tels que $g\mathcal{R}h$ et $g'\mathcal{R}h'$, on a $\overline{gg'} = \overline{g}\ \overline{g'} = \overline{h}\ \overline{h'} = \overline{hh'}$, ce qui signifie que $gg'\mathcal{R}hh'$. La relation $\mathcal{R}$ est donc compatible avec la loi de G.

Réciproquement, supposons que $\mathcal{R}$ soit compatible avec la loi de G. L'analyse que l'on vient de faire nous montre que la seule loi possible sur $G/\mathcal{R}$ est définie par $\overline{g}\overline{g'} = \overline{gg'}$. Pour montrer qu'une telle définition est permise, il s'agit de montrer qu'elle ne dépend pas des choix des représentants de $\overline{g}$ et $\overline{g'}$. Si $\overline{g} = \overline{h}$ et $\overline{g'} = \overline{h'}$, on a alors $g\mathcal{R}h$ et $g'\mathcal{R}h'$, ce qui entraîne $gg'\mathcal{R}hh'$, soit $\overline{gg'} = \overline{hh'}$. □

L'exercice 1.8 nous dit que les relations d'équivalence sur un groupe compatibles avec sa loi sont celles suivant un groupe distingué (à gauche ou à droite).

1.2 Ordre d'un élément dans un groupe

Définition 1.5. *L'ordre de $g \in G$ est $\theta(g) = \operatorname{card}(\langle g\rangle) \in \mathbb{N}^* \cup \{+\infty\}$, où $\langle g\rangle$ est le sous-groupe de G engendré par g (voir le paragraphe 1.4).*

Si $\theta(g)$ est dans $\mathbb{N}^*$, on dit alors que g est d'ordre fini, sinon on dit qu'il est d'ordre infini.

Seul l'élément neutre 1_G est d'ordre 1 dans G. En effet, si $g = 1$, alors $\langle g\rangle = \{1\}$ et si $g \neq 1$, alors $g^0 \neq g^1$ et $\langle g\rangle$ a au moins deux éléments.

Pour tout $g \in G$, on a $\theta(g) = \theta\left(g^{-1}\right)$ puisque :

$$\left\langle g^{-1}\right\rangle = \left\{\left(g^{-1}\right)^n \mid n \in \mathbb{Z}\right\} = \left\{g^{-n} \mid n \in \mathbb{Z}\right\} = \{g^n \mid n \in \mathbb{Z}\} = \langle g\rangle$$

Théorème 1.9.

Si φ est un isomorphisme de groupes de G sur un groupe G', on a alors $\theta(\varphi(g)) = \theta(g)$ pour tout $g \in G$.

Preuve. On a $\langle\varphi(g)\rangle = \{(\varphi(g))^n \mid n \in \mathbb{Z}\} = \{\varphi(g^n) \mid n \in \mathbb{Z}\} = \varphi(\langle g\rangle)$ pour tout $g \in G$ avec φ bijective, donc $\operatorname{card}(\langle\varphi(g)\rangle) = \operatorname{card}(\langle g\rangle)$. □

Pour tout $g \in G$, le sous-groupe de G engendré par g peut être vu comme l'image du morphisme de groupes $\varphi_g : k \in \mathbb{Z} \mapsto g^k \in G$ (pour j, k dans $\mathbb{Z}$, on a $\varphi_g(j+k) = g^{j+k} = g^j g^k = \varphi_g(j)\,\varphi_g(k)$ et φ_g est bien un morphisme de groupes).

Connaissant les sous-groupes additifs de $\mathbb{Z}$ (voir le paragraphe 10.1), on a le résultat suivant.

Théorème 1.10.

Pour $g \in G$, on a $\theta(g) = +\infty$ si, et seulement si, φ_g est injectif et pour g d'ordre fini, on a $\ker(\varphi_g) = \theta(g)\,\mathbb{Z}$.

Preuve. Le noyau de φ_g étant un sous-groupe additif de $\mathbb{Z}$, il existe un unique entier $n \geq 0$ tel que $\ker(\varphi_g) = n\mathbb{Z}$. On aura $n = 0$ si, et seulement si, φ_g est injectif, ce qui revient à dire que $\varphi_g(k) = a^k \neq 1$ pour tout $k \in \mathbb{Z}^*$ ou encore que $\varphi_g(k) = g^k \neq \varphi_g(j) = g^j$ pour tous $j \neq k$ dans $\mathbb{Z}$ et le sous-groupe $\langle g\rangle = \operatorname{Im}(\varphi_g)$

est infini. Si $n \geq 1$, en effectuant, pour $k \in \mathbb{Z}$, la division euclidienne de k par n, on a $k = qn + r$ avec $0 \leq r \leq n-1$ et $g^k = (g^n)^q g^r = g^r$, ce qui nous donne :

$$\langle g \rangle = \mathrm{Im}\,(\varphi_g) = \{g^r \mid 0 \leq r \leq n-1\}$$

De plus pour $1 \leq r \leq n-1$, on a $g^r \neq 1$ puisque $n = \inf(\ker(\varphi_g) \cap \mathbb{N}^*)$, ce qui entraîne $g^r \neq g^s$ pour $0 \leq r \neq s \leq n-1$ (pour $s \geq r$, l'égalité $g^r = g^s$ équivaut à $g^{s-r} = 1$ avec $s-r$ compris entre 0 et $n-1$, ce qui équivaut à $r = s$). Le groupe $\langle g \rangle$ a donc exactement n éléments. □

Dans le cas, où le groupe G est fini d'ordre $n \geq 1$, le théorème de Lagrange nous dit que l'ordre de tout élément de G divise l'ordre de G et en conséquence, on a $g^n = 1$ pour tout $g \in G$.

Le théorème précédent nous permet de donner d'autres définitions de l'ordre d'un élément d'un groupe.

Corollaire 1.2. *Pour $g \in G$ et $n \in \mathbb{N}^*$, les assertions suivantes sont équivalentes :*

1. *g est d'ordre n ;*
2. *$g^n = 1$ et $g^k \neq 1$ pour tout k est compris entre 1 et $n-1$ ($\theta(g)$ est le plus petit entier naturel non nul tel que $g^n = 1$) ;*
3. *pour $k \in \mathbb{Z}$, on a $g^k = 1$ si, et seulement si, k est multiple de n.*

Preuve. Si g est d'ordre $n \geq 1$, on a vu avec la démonstration du théorème précédent que $g^n = 1$ et $g^k \neq 1$ pour tout k est compris entre 1 et $n-1$.

Réciproquement s'il existe un entier $n \geq 1$ tel que $g^n = 1$ et $g^k \neq 1$ pour k est compris entre 1 et $n-1$, le morphisme de groupes φ_g est non injectif, donc g est d'ordre fini et $\ker(\varphi_g) = \theta(g)\,\mathbb{Z}$ avec $\theta(g) = \inf(\ker(\varphi_g) \cap \mathbb{N}^*) = n$.

Si g est d'ordre n, on a alors $g^n = 1$ et pour $k = qn + r \in \mathbb{Z}$ avec $q \in \mathbb{Z}$ et $0 \leq r \leq n-1$ (division euclidienne), on a $g^k = g^r = 1$ si, et seulement si, $r = 0$.

Réciproquement supposons que $g^k = 1$ si, et seulement si, k est multiple de n. On a alors $g^n = 1$ et $g^k \neq 1$ si k est compris entre 1 et $n-1$, ce qui signifie que g est d'ordre n. □

En résumé, on retiendra que :

— $(\theta(g) = +\infty) \Leftrightarrow (\varphi_g \text{ injectif}) \Leftrightarrow (\ker(\varphi_g) = \{0\}) \Leftrightarrow$
$\big(\forall k \in \mathbb{Z}^*,\ g^k \neq 1\big) \Leftrightarrow (\langle g \rangle \text{ est infini isomorphe à } \mathbb{Z})$;

— $(\theta(g) = n \in \mathbb{N}^*) \Leftrightarrow (\ker(\varphi_g) = n\mathbb{Z}) \Leftrightarrow (\langle g \rangle = \{g^r \mid 0 \leq r \leq n-1\})$
$\Leftrightarrow \big(k \in \mathbb{Z} \text{ et } g^k = 1 \text{ équivaut à } k \equiv 0 \mod(n)\big) \Leftrightarrow$
(n est le plus petit entier naturel non nul tel que $g^n = 1$).

Pour g d'ordre fini, le groupe $\langle g \rangle$ est dit cyclique, ce qui est justifié par l'égalité $g^{qn+r} = g^r$ pour $q \in \mathbb{Z}$ et $0 \leq r \leq n-1$.

Dans le cas où le groupe G est additif, l'ordre de $g \in G$ est défini comme le plus petit entier $n \geq 1$ tel que $ng = 0$, quand cet ordre est fini. L'égalité $mg = 0$ équivaut alors à dire que m est multiple de n. Le groupe engendré par g est alors :

$$\langle g \rangle = \{kg \mid k \in \mathbb{Z}\} = \{rg \mid 0 \leq r \leq n-1\}$$

Théorème 1.11.

Soient g, h dans G d'ordre fini et $k \in \mathbb{Z}^*$.

1. *On a $\theta\left(g^k\right) = \dfrac{\theta(g)}{\operatorname{pgcd}(\theta(g), k)}$ (en particulier $\theta\left(g^{-1}\right) = \theta(g)$).*
2. *Si k divise $\theta(g)$, on a alors $\theta\left(g^k\right) = \dfrac{\theta(g)}{|k|}$.*
3. *Si k est premier avec $\theta(g)$, on a alors $\theta\left(g^k\right) = \theta(g)$.*
4. *Si $gh = hg$, alors hg est d'ordre fini divisant $\theta(g) \vee \theta(h)$. Dans le cas où $\langle g\rangle \cap \langle h\rangle = \{1\}$, on a $\theta(gh) = \operatorname{ppcm}(\theta(g), \theta(h))$. Si $\theta(g)$ et $\theta(h)$ sont premiers entre eux, on a alors $\langle g\rangle \cap \langle h\rangle = \{1\}$ et $\theta(gh) = \operatorname{ppcm}(\theta(g), \theta(h)) = \theta(g)\theta(h)$.*

Preuve.

1. Soit $\delta = \operatorname{pgcd}(\theta(g), k)$ et n', k' premiers entre eux tels que $\theta(g) = \delta n'$, $k = \delta k'$. Pour tout entier relatif j, on a :

$$\left(\left(g^k\right)^j = g^{kj} = 1\right) \Leftrightarrow (\exists q \in \mathbb{Z} \mid kj = q\theta(g)) \Leftrightarrow (\exists q \in \mathbb{Z} \mid k'j = qn')$$
$$\Leftrightarrow (n' \text{ divise } j) \text{ (théorème de Gauss)}$$

   et en conséquence, on a $\theta\left(g^k\right) = n' = \dfrac{\theta(g)}{\operatorname{pgcd}(\theta(g), k)}$.

2. Si k divise $\theta(g)$, on a alors $\operatorname{pgcd}(\theta(g), k) = |k|$ et $\theta\left(g^k\right) = \dfrac{\theta(g)}{|k|}$.
3. Si k est premier avec $\theta(g)$, on a alors $\operatorname{pgcd}(\theta(g), k) = 1$ et $\theta\left(g^k\right) = \theta(g)$.
4. Soit $\mu = \operatorname{ppcm}(\theta(g), \theta(h))$. Si g et h commutent, on a alors $(gh)^\mu = g^\mu h^\mu = 1$ avec $\mu \geq 1$, donc gh est d'ordre fini et cet ordre divise μ. En désignant par $n = \theta(gh)$ l'ordre de gh, on a $g^n h^n = (gh)^n = 1$ et $g^n = h^{-n} \in \langle g\rangle \cap \langle h\rangle$. Si $\langle g\rangle \cap \langle h\rangle = \{1\}$, on a alors $g^n = h^n = 1$ et n est multiple de $\theta(g)$ et $\theta(h)$, donc de $\operatorname{ppcm}(\theta(g), \theta(h))$ et $n = \operatorname{ppcm}(\theta(g), \theta(h))$. Si $\operatorname{pgcd}(\theta(g), \theta(h)) = 1$, on a alors $\operatorname{ppcm}(\theta(g), \theta(h)) = \theta(g)\theta(h)$. De plus avec $\langle g\rangle \cap \langle h\rangle \subset \langle g\rangle$ et $\langle g\rangle \cap \langle h\rangle \subset \langle h\rangle$, on déduit que $\operatorname{card}(\langle g\rangle \cap \langle h\rangle)$ divise $\theta(g) = \operatorname{card}(\langle g\rangle)$ et $\theta(h) = \operatorname{card}(\langle h\rangle)$, donc $\operatorname{card}(\langle g\rangle \cap \langle h\rangle) = 1$ et $\langle g\rangle \cap \langle h\rangle = \{1\}$, ce qui implique que $\theta(gh) = \operatorname{ppcm}(\theta(g), \theta(h)) = \theta(g)\theta(h)$.

□

On retiendra de ce théorème que si g, h sont deux éléments de G qui commutent avec des ordres premiers entre eux, le produit gh est alors d'ordre $\theta(g)\theta(h)$.

Si g et h ne commutent pas ce résultat est faux. Par exemple dans le groupe symétrique $\mathcal{S}_3$ d'ordre 6, $g = (1,2)$ est d'ordre 2, $h = (1,2,3)$ est d'ordre 3 et gh ne peut être d'ordre 6, sans quoi $\mathcal{S}_3$ serait cyclique, ce qui n'est pas (il n'est pas commutatif).

Pour g et h ne commutant pas, le produit gh peut être d'ordre infini, même si g et h sont d'ordre fini. Considérer, par exemple, le produit de deux matrices de réflexion dans $GL_2(\mathbb{R})$.

Si $\theta(g)$ et $\theta(h)$ ne sont pas premiers entre eux, avec g, h commutant et d'ordre fini, l'ordre de gh n'est pas nécessairement le ppcm de $\theta(g)$ et $\theta(h)$. En prenant par exemple g d'ordre $n \geq 2$ dans G et $h = g^{-1}$ qui est également d'ordre n, on $gh = hg = 1$ d'ordre $1 \neq \text{ppcm}(n, n) = n$.

Théorème 1.12.

Si $(G, \cdot)$ est un groupe commutatif, $r \geq 2$ un entier et $g_1, \cdots, g_r$ des éléments deux à deux distincts de G d'ordres respectifs $m_1, \cdots, m_r$, il existe dans G un élément g_0 d'ordre égal au ppcm *de ces ordres.*

Preuve. On procède par récurrence sur $r \geq 2$. Pour $r = 2$, on procède comme suit. Pour $\theta(g_1), \theta(g_2)$ premiers entre eux, $g_0 = g_1 g_2$ est d'ordre $m_1 m_2 = \text{ppcm}(m_1, m_2)$. Pour le cas général, l'idée est de se ramener à ce cas de figure. On écrit les décompositions en facteurs premiers de m_1 et m_2 sous la forme :

$$m_1 = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=k+1}^{r} p_i^{\alpha_i},\ m_2 = \prod_{i=1}^{k} p_i^{\beta_i} \prod_{i=k+1}^{r} p_i^{\beta_i}$$

où les facteurs premiers p_i ont été regroupés de sorte que $\alpha_i > \beta_i$ pour $1 \leq i \leq k$ et $\alpha_i \leq \beta_i$ pour $k+1 \leq i \leq r$, les exposants α_i, β_i étant positifs ou nuls (si l'une des conditions $\alpha_i > \beta_i$ ou $\alpha_i \leq \beta_i$ n'est jamais vérifiée, alors le produit correspondant vaut 1). Avec ces écritures, on a $\text{ppcm}(m_1, m_2) = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=k+1}^{r} p_i^{\beta_i} = q_1 q_2$, où $q_1 = \prod_{i=1}^{k} p_i^{\alpha_i}$ et $q_2 = \prod_{i=k+1}^{r} p_i^{\beta_i}$ sont premiers entre eux et $m_1 = q_1 n_1$, $m_2 = q_2 n_2$. Les éléments $g_1' = g_1^{n_1}$ et $g_2' = g_2^{n_2}$ sont alors d'ordres respectifs q_1 et q_2 et $g_0 = g_1' g_2'$ est d'ordre $q_1 q_2 = \text{ppcm}(m_1, m_2)$.

Supposons le résultat acquis pour $r \geq 2$ et soient $g_1, \cdots, g_{r+1}$ deux à deux distincts dans G d'ordres respectifs $m_1, \cdots, m_{r+1}$. L'hypothèse de récurrence nous dit qu'il existe un élément g_0' de G d'ordre $m_0' = \text{ppcm}(m_1, \cdots, m_r)$ et le cas $r = 2$ qu'il existe g_0 d'ordre :

$$\text{ppcm}(m_0', m_{r+1}) = \text{ppcm}(\text{ppcm}(m_1, \cdots, m_r), m_{r+1}) = \text{ppcm}(m_1, \cdots, m_{r+1})$$

(associativité du ppcm). □

Théorème 1.13.

Si $(G, \cdot)$ est un groupe commutatif fini, on a alors :

$$\max_{g \in G} \theta(g) = \text{ppcm}\{\theta(g) \mid g \in G\}$$

Preuve. Comme G est commutatif fini, il existe $g_0 \in G$ tel que :

$$\theta(g_0) = \text{ppcm}\{\theta(g) \mid g \in G\}$$

En désignant par g_1 un élément de G tel que $\theta(g_1) = \max_{g\in G} \theta(g)$, on a $\theta(g_0) \leq \theta(g_1)$ ($\theta(g_1)$ est le plus grand) et $\theta(g_1)$ divise $\theta(g_0)$ ($\theta(g_0)$ est multiple de tous les ordres) donc $\theta(g_1) \leq \theta(g_0)$ et $\theta(g_0) = \theta(g_1)$. □

Pour un groupe fini G, l'entier $\max_{g\in G} \theta(g)$ est l'exposant du groupe.

Théorème 1.14.

Si $(G,\cdot)$ un groupe commutatif fini d'ordre $n \geq 2$, alors n et l'exposant $m = \max_{g\in G} \theta(g)$ ont les mêmes facteurs premiers.

Preuve. Soit $G = \{g_1, \cdots, g_n\}$ un groupe commutatif fini d'ordre $n \geq 2$. Comme il existe $i \in \{1, \cdots, n\}$ tel que $m = \theta(g_i)$, cet entier m divise l'ordre n de G et l'ensemble des facteurs premiers de m est contenu dans l'ensemble des facteurs premiers de n. En utilisant l'application φ du groupe produit $H = \prod_{k=1}^{n} \langle g_k \rangle$ dans G définie par $\varphi(h) = \prod_{i=1}^{n} h_i$ pour tout $h = (h_i)_{1\leq i\leq n} \in H$, on vérifie d'abord que n divise le produit des ordres $\prod_{k=1}^{n} \theta(g_k)$. L'application φ est surjective et comme G est commutatif, c'est un morphisme de groupes. Ce morphisme φ induit alors un isomorphisme du groupe quotient $H/\ker(\varphi)$ sur G, ce qui entraîne que $\operatorname{card}(H) = \operatorname{card}(\ker(\psi))\operatorname{card}(G)$ et en conséquence, $n = \operatorname{card}(G)$ divise $\operatorname{card}(H) = \prod_{k=1}^{n} \theta(g_k)$. Sachant que m est aussi le ppcm des ordres des éléments de G, il est multiple de chaque $\theta(g_k)$ et m^n est multiple de $\prod_{k=1}^{n} \theta(g_k)$ donc de n. Donc l'ensemble des facteurs premiers de n est contenu dans l'ensemble des facteurs premiers de m. En définitive m et n ont les mêmes facteurs premiers. □

Du théorème précédent, on déduit que si $(G,\cdot)$ est un groupe commutatif fini d'ordre $n \geq 2$ tel que tous les éléments de $G\setminus\{1\}$ soient d'ordre un nombre premier $p \geq 2$, on a alors $n = p^r$ avec $r \geq 1$. En effet, dans ce cas $\operatorname{ppcm}\{\theta(g) \mid g \in G\} = p$ et c'est le seul facteur premier de n (voir aussi l'exercice 1.11).

1.3 Sous-groupe engendré par une partie

Théorème 1.15.

L'intersection d'une famille quelconque $(H_i)_{i\in I}$ de sous-groupes de G est un sous-groupe de G.

Preuve. Soient $(H_i)_{i\in I}$ une famille de sous-groupes de G et $H = \bigcap_{i\in I} H_i$. Comme l'élément neutre 1 est dans tous les H_i, il est aussi dans H et $H \neq \emptyset$. Si g_1, g_2 sont dans H, ils sont alors dans tous les H_i, donc $g_1 g_2^{-1} \in H_i$ pour tout $i \in I$, ce qui signifie que $g_1 g_2^{-1} \in H$. En conclusion, H est un sous-groupe de G. □

Corollaire 1.3. *Si X est une partie de $(G,\cdot)$, l'intersection de tous les sous-groupes de G qui contiennent X est un sous-groupe de G.*

Preuve. L'ensemble des sous-groupes de G qui contiennent X est non vide puisque G en fait partie et le théorème précédent nous dit que l'intersection de tous ces sous-groupes est un sous-groupe de G. □

Définition 1.6. *Si X est une partie de $(G,\cdot)$, le sous-groupe de G engendré par X est l'intersection de tous les sous-groupes de G qui contiennent X.*

On note $\langle X\rangle$ le sous-groupe de G engendré par X et ce sous-groupe $\langle X\rangle$ est le plus petit (pour l'ordre de l'inclusion) des sous-groupes de G qui contiennent X. Dans le cas où X est l'ensemble vide, on a $\langle X\rangle = \{1\}$. Pour X non vide formée d'un nombre fini d'éléments $(x_i)_{1\leq i\leq n}$, on note $\langle X\rangle = \langle x_1,\cdots,x_n\rangle$ le groupe engendré par X.

Définition 1.7. *Si X est une partie de $(G,\cdot)$, on dit que X engendre G (ou que X est une partie génératrice de G), si $G = \langle X\rangle$. On dit que G est de type fini s'il admet une partie génératrice finie.*

Théorème 1.16.

Soient X, Y deux parties de G.

1. *On a $X \subset \langle X\rangle$ et l'égalité est réalisée si, et seulement si, X est un sous-groupe de G.*
2. *Si $X \subset Y$, on a alors $\langle X\rangle \subset \langle Y\rangle$.*
3. *En notant, pour X non vide, $X^{-1} = \left\{x^{-1} \mid x \in X\right\}$, les éléments de $\langle X\rangle$ sont de la forme $x_1 \cdot \cdots \cdot x_r$ où $r \in \mathbb{N}^*$ et les x_k sont dans $X \cup X^{-1}$ pour tout k compris entre 1 et r.*

Preuve. Les points **1.** et **2.** se déduisent immédiatement des définitions. Pour le point **3.** on montre tout d'abord que l'ensemble :

$$H = \left\{ \prod_{k=1}^{r} x_k \mid r \in \mathbb{N}^* \text{ et } x_k \in X \cup X^{-1} \text{ pour } 1 \leq k \leq r \right\}$$

est un sous-groupe de G. Pour $x_1 \in X$, on a $1 = x_1 \cdot x_1^{-1} \in H$ et pour $x = \prod_{k=1}^{r} x_k$, $y = \prod_{k=1}^{s} y_k$ dans H, on a $x \cdot y^{-1} = \prod_{k=1}^{r} x_k \prod_{k=s}^{1} y_k^{-1} \in H$. Donc H est bien un sous-groupe de G. Comme H est un sous-groupe de G qui contient X, on a $\langle X\rangle \subset H$.

Réciproquement, tout élément $h = \prod_{k=1}^{r} x_k$ de H est un produit d'éléments de $X \cup X^{-1} \subset \langle X\rangle$, donc dans $\langle X\rangle$ et on a bien $\langle X\rangle = H$. □

Le point **3.** de ce théorème nous dit aussi que $\langle X\rangle = \left\langle X^{-1}\right\rangle = \left\langle X \cup X^{-1}\right\rangle$.
On a aussi :

$$\langle X\rangle = \left\{ \prod_{k=1}^{r} x_k^{\varepsilon_k} \mid r \in \mathbb{N}^*,\ x_k \in X \text{ et } \varepsilon_k \in \{-1,1\} \text{ pour } 1 \leq k \leq r \right\}$$

Dans le cas où les éléments de X sont en nombre fini et commutent, on a le résultat suivant.

Théorème 1.17.

Pour tout $p \in \mathbb{N}^*$ et tout p-uplet $(g_1, \cdots, g_p)$ d'éléments de G qui commutent deux à deux, on a $\langle g_1, \cdots, g_p\rangle = \left\{ \prod_{k=1}^{p} g_k^{\alpha_k} \mid (\alpha_1, \cdots, \alpha_p) \in \mathbb{Z}^p \right\}$ et ce groupe est commutatif.

Preuve. En notant $X = \{g_1, \cdots, g_p\}$, on a $X^{-1} = \left\{g_1^{-1}, \cdots, g_p^{-1}\right\}$ et comme les g_k commutent, on déduit que :

$$\begin{aligned}\langle g_1, \cdots, g_p\rangle &= \left\{ \prod_{k=1}^{m} h_k \mid m \in \mathbb{N}^* \text{ et } h_k \in X \cup X^{-1} \text{ pour } 1 \leq k \leq m \right\} \\ &= \left\{ \prod_{k=1}^{p} g_k^{\alpha_k} \mid (\alpha_1, \cdots, \alpha_p) \in \mathbb{Z}^p \right\}\end{aligned}$$

($g_k g_j = g_j g_k$ entraîne $g_j^{-1} g_k = g_j^{-1} g_k g_j g_j^{-1} = g_j^{-1} g_j g_k g_j^{-1} = g_k g_j^{-1}$ et les éléments de $X \cup X^{-1}$ commutent) et comme les g_k commutent, ce groupe est commutatif. □

Pour une loi de groupe notée additivement, on a dans le cas où G est commutatif $\langle g_1, \cdots, g_p\rangle = \left\{ \sum_{k=1}^{p} \alpha_k g_k \mid (\alpha_1, \cdots, \alpha_p) \in \mathbb{Z}^p \right\}$. Par exemple pour le groupe additif $G = \mathbb{Z}$, on a $\langle g_1, \cdots, g_p\rangle = \sum_{k=1}^{p} g_k \mathbb{Z} = \delta\mathbb{Z}$, où $\delta \in \mathbb{N}$ est le pgcd de $g_1, \cdots, g_p$.

Définition 1.8. *Le groupe dérivé d'un groupe $(G, \cdot)$ est le sous-groupe $D(G)$ de G engendré par les commutateurs, c'est-à-dire l'ensemble des éléments de G de la forme $[a,b] = aba^{-1}b^{-1}$, où a, b sont dans G.*

Deux éléments a, b de G commutent si, et seulement, on a $[a,b] = 1$ (d'où l'appellation commutateur).

Pour un groupe commutatif, on a $D(G) = \{1\}$.

L'inverse d'un commutateur est un commutateur. En effet, pour a, b dans G, on a $[a,b]^{-1} = \left(aba^{-1}b^{-1}\right)^{-1} = bab^{-1}a^{-1} = [b,a]$. Il en résulte que $D(G)$ est l'ensemble de tous les produits finis de commutateurs.

Théorème 1.18.

Le groupe dérivé $D(G)$ d'un groupe G est le plus petit sous-groupe distingué H de G tel que le groupe $\dfrac{G}{H}$ soit commutatif.

Preuve. Le sous-groupe dérivé $D(G)$ est distingué dans G. En effet, pour a, b, c dans G, on a :

$$\begin{aligned} c[a,b]c^{-1} &= c\left(aba^{-1}b^{-1}\right)c^{-1} = \left(cac^{-1}\right)\left(cbc^{-1}\right)\left(ca^{-1}c^{-1}\right)\left(cb^{-1}c^{-1}\right) \\ &= \left[cac^{-1}, cbc^{-1}\right] \end{aligned}$$

Le groupe quotient $\dfrac{G}{D(G)}$ est commutatif. En effet, pour a, b dans G, on a :

$$\begin{aligned} \overline{a}\overline{b} = \overline{ab} &= (ab)D(G) = (ba)\left(a^{-1}b^{1}ab\right)D(G) \\ &= (ba)\left[a^{-1}, b^{-1}\right]D(G) = (ba)D(G) = \overline{b}\overline{a} \end{aligned}$$

Soit H un sous-groupe distingué de G tel que le groupe $\dfrac{G}{H}$ soit commutatif. Pour tous a, b dans G, on a $\overline{[a,b]} = \left[\overline{a}, \overline{b}\right] = \overline{1}$ dans le quotient $\dfrac{G}{H}$, ce qui revient à dire que $[a,b] \in H$. Le groupe H contient donc tous les commutateurs et en conséquence il contient le groupe dérivé $D(G)$. □

1.4 Groupes monogènes, groupes cycliques

Définition 1.9. *On dit que G est monogène s'il existe un élément g de G tel que $G = \langle g \rangle$. Si de plus G est fini, on dit alors qu'il est cyclique.*

Un groupe cyclique est nécessairement commutatif et s'il est engendré par un élément $g \neq 1$, il a alors au moins deux élément. Le théorème 1.17, nous dit en particulier que $\langle g \rangle = \left\{ \prod_{k=1}^{r} g^{\varepsilon_k} \mid r \in \mathbb{N}^*,\ \varepsilon_k = \pm 1 \text{ pour } 1 \leq k \leq r \right\} = \{g^n \mid n \in \mathbb{Z}\}$. Pour un groupe additif, on a $\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}$.

Exemples 1.2

1. *Le groupe additif $(\mathbb{Z}, +)$ est monogène engendré par 1 et ses sous-groupes qui sont tous de la forme $n\mathbb{Z}$ avec $n \geq 0$ sont monogènes. Comme $(\mathbb{Z}, +)$ est commutatif, chaque ensemble quotient $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est naturellement muni d'une structure de groupe. D'autre part, le théorème de division euclidienne nous permet d'écrire tout entier relatif k sous la forme $k = qn + r$ avec $0 \leq r \leq n-1$, ce qui entraîne $k - r \in n\mathbb{Z}$ et $\overline{k} = \overline{r}$. Et comme $\overline{r} \neq \overline{s}$ pour $0 \leq r \neq s \leq n-1$ (on a $0 < |r-s| < n$ et $r - s$ ne peut être multiple de n), on en déduit que le*

groupe $\dfrac{\mathbb{Z}}{n\mathbb{Z}} = \left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\}$ *a* n *éléments. Ce groupe est cyclique d'ordre* n *engendré par* $\overline{1}$ *(les anneaux* $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ *sont étudiés au chapitre 10).*

2. *Le groupe multiplicatif* $\mathbb{U}_n$ *des racines* n*-ièmes de l'unité, qui est cyclique d'ordre* n*, est isomorphe à* $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ *par l'application* $\overline{k} \mapsto e^{\frac{2ik\pi}{n}}$.

Théorème 1.19.

Soit G *un groupe monogène. S'il est infini, il est alors isomorphe à* $(\mathbb{Z}, +)$*, s'il est cyclique d'ordre* n*, il est alors isomorphe à* $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$.

Preuve. Si $G = \langle g \rangle$ est un groupe monogène, l'application $\varphi : k \mapsto g^k$ est alors un morphisme de groupes surjectif de $(\mathbb{Z}, +)$ sur G et son noyau est un sous-groupe additif de $\mathbb{Z}$, donc de la forme $\ker(\varphi) = n\mathbb{Z}$ avec $n \in \mathbb{N}$. Pour $n = 0$, φ est injectif et G est infini isomorphe à $\mathbb{Z}$. Pour $n \geq 1$, le théorème d'isomorphisme nous dit que $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est isomorphe à G et G est cyclique d'ordre n. □

Dire que G est cyclique d'ordre n, signifie que G est de cardinal égal à n et qu'il existe dans G au moins un élément g d'ordre n. Dans ce cas, on a :

$$G = \langle g \rangle = \left\{1, g, \cdots, g^{n-1}\right\}$$

Théorème 1.20.

Si $G = \langle g \rangle$ *est un groupe cyclique d'ordre* n*, ses générateurs sont alors les* g^k*, où* k *est un entier compris entre* 1 *et* $n-1$ *premier avec* n.

Preuve. Si $k \in \{1, \cdots, n-1\}$ est premier avec n, le théorème de Bézout nous dit alors qu'il existe deux entiers relatifs u, v tels que $uk + vn = 1$, ce qui entraîne $g = \left(g^k\right)^u \in \left\langle g^k \right\rangle$ et $G = \left\langle g^k \right\rangle$. Réciproquement si $k \in \{1, \cdots, n-1\}$ est tel que $G = \left\langle g^k \right\rangle$, il existe alors $u \in \mathbb{Z}$ tel que $g = \left(g^k\right)^u = g^{ku}$, ce qui s'écrit aussi $g^{1-ku} = 1$ et n divise $1 - ku$ (puisque n est l'ordre de g), ce qui signifie qu'il existe un entier relatif v tel que $1 - ku = vn$, donc $uk + vn = 1$ et k est premier avec n. □

Le nombre de générateurs d'un groupe cyclique G d'ordre n est égal à $\varphi(n)$ (φ est la fonction indicatrice d'Euler). On pourra consulter le paragraphe 10.2 pour une étude plus détaillée de cette fonction d'Euler.

Le théorème qui suit nous dit qu'à isomorphisme près, il y a un seul groupe d'ordre p premier, à savoir $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$.

Théorème 1.21.

Un groupe de cardinal premier est cyclique.

Preuve. Soit $(G, \cdot)$ un groupe de cardinal premier $p \geq 2$. Si $g \in G \setminus \{1\}$, il est alors d'ordre différent de 1 qui divise p, donc cet ordre est p et G est cyclique

engendré par g. L'application $[k] = k + p\mathbb{Z} \in \mathbb{Z}_p \mapsto g^k$ réalise un isomorphisme du groupe $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}, +\right)$ sur $(G, \cdot)$. □

Si p et q sont deux nombres premiers, un groupe d'ordre pq n'est pas nécessairement cyclique comme le montre l'exemple du groupe symétrique $\mathcal{S}_3$ qui est d'ordre 6 non commutatif et donc non cyclique. Mais pour G commutatif d'ordre pq avec $p \neq q$, on a le résultat suivant.

Théorème 1.22.

Un groupe commutatif d'ordre pq, où p et q sont deux nombres premiers distincts, est cyclique.

Preuve. Soit G commutatif d'ordre pq avec $2 \leq p < q$ premiers.

On peut montrer que G est cyclique en utilisant le théorème de Cauchy qui nous dit qu'il existe dans G un groupe d'ordre p et un d'ordre q (théorème 1.33), ces groupes sont cycliques et on a ainsi un élément g d'ordre p et un élément h d'ordre q. L'élément gh est alors d'ordre pq (G est commutatif) et G est cyclique.

On peut se passer du théorème de Cauchy en procédant comme suit. S'il existe dans G un élément g d'ordre p et un élément h d'ordre q, alors gh est d'ordre pq et G est cyclique. Sinon les éléments de $G \setminus \{1\}$ sont tous d'ordre p ou tous d'ordre q. Supposons les tous d'ordre p. Si $g \in G$ est d'ordre p, alors le groupe quotient $G/\langle g \rangle$ est d'ordre q premier, donc cyclique engendré par $\overline{g_0}$ d'ordre q dans $G/\langle g \rangle$, ce qui entraîne que $\theta(g_0) = p$ divise q (puisque $\overline{g_0}^p = \overline{g_0^p} = \overline{1}$), ce qui est impossible pour $p \neq q$ premiers. □

Pour $p = q$ premier, le théorème précédent est faux comme le montre l'exemple de $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$ qui est d'ordre p^2 non cyclique puisque tous ses éléments distincts du neutre sont d'ordre p.

En utilisant le théorème 1.21 et les actions de groupe (paragraphe 1.6), on peut montrer qu'un groupe d'ordre p^2 avec p premier est commutatif isomorphe au groupe cyclique $\dfrac{\mathbb{Z}}{p^2\mathbb{Z}}$ ou au groupe non cyclique $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$ (théorème 1.32).

Théorème 1.23.

Si $n \geq 2$ est un entier premier avec $\varphi(n)$, alors tout groupe commutatif d'ordre n est cyclique.

Preuve. Comme $m = \text{ppcm}\{\theta(g) \mid g \in G\} = \theta(g_0)$ et n ont les mêmes facteurs premiers (théorème 1.14), on a les décompositions en facteurs premiers $n = \prod_{k=1}^{r} p_k^{\alpha_k}$ et $m = \prod_{k=1}^{r} p_k^{\beta_k}$, où les p_k sont premiers deux à deux distincts et $1 \leq \beta_k \leq \alpha_k$ pour tout k compris entre 1 et n. Sachant que $\varphi(n) = \prod_{k=1}^{r} p_k^{\alpha_k - 1}(p_k - 1)$, on déduit que si $\varphi(n)$ est premier avec n, alors tous les α_k valent 1 (sinon p_k divise $\varphi(n)$ et n) et

les β_k valent aussi 1, ce qui donne $n = m$ et G est cyclique puisque g_0 est d'ordre $n = \text{card}(G)$.

On peut aussi utiliser le théorème de Cauchy (théorème 1.33). Si n est premier avec $\varphi(n)$, on a alors $n = \prod_{k=1}^{r} p_k$, où les p_k sont premiers deux à deux distincts. Le théorème de Cauchy nous assure l'existence, pour tout entier k compris entre 1 et n, d'un élément g_k d'ordre p_k dans G. Comme G est commutatif, le produit $g = \prod_{k=1}^{r} g_k$ est d'ordre n. □

Plus généralement, on peut montrer qu'un entier $n \geq 2$ est premier avec $\varphi(n)$ si, et seulement si, tout groupe d'ordre n est cyclique (voir [15], volume 1).

1.5 Sous-groupes d'un groupe cyclique

Soient $n \geq 2$ un entier et $G = \langle a \rangle$ un groupe cyclique d'ordre n.

Théorème 1.24.

1. *Les sous-groupes de $G = \langle a \rangle$ sont tous cycliques d'ordre divisant n.*
2. *Pour tout diviseur positif d de n, il existe un unique sous-groupe d'ordre d de G. Ce sous-groupe est le groupe cyclique $H = \left\langle a^{\frac{n}{d}} \right\rangle$. C'est également l'ensemble de tous les éléments de G d'ordre divisant d et les générateurs de H sont tous les éléments d'ordre d de G.*

Preuve.

1. Soit H un sous-groupe de G d'ordre d. Le théorème de Lagrange nous dit que d divise n, donc $n = qd$ avec $q \in \mathbb{N}^*$. Pour tout élément $h = a^k$ de H, on a $h^d = a^{kd} = 1$, donc l'ordre n de a divise kd et il existe un entier $j \in \mathbb{N}^*$ tel que $kd = jn = jqd$ et $k = jq$, ce qui nous dit que $h = a^k = (a^q)^j \in \langle a^q \rangle$. On a donc $H \subset \langle a^q \rangle$ et d divise $\text{card}(\langle a^q \rangle)$. Mais $(a^q)^d = a^n = 1$, donc l'ordre de a^q divise d, soit $\text{card}(\langle a^q \rangle)$ divise d et $\text{card}(\langle a^q \rangle) = d$, ce qui nous dit que $H = \langle a^q \rangle$. Un sous-groupe d'ordre d de G, s'il en existe, est donc unique.
2. Réciproquement, soient d un diviseur de n, $q = \dfrac{n}{d}$ et $H = \langle a^q \rangle$ le sous-groupe de G engendré par a^q. Si δ est l'ordre de H, on a $(a^q)^\delta = a^{q\delta} = 1$ et n divise $q\delta$, soit $\delta q = kn = kqd$ et d divise δ. Mais on a aussi $(a^q)^d = a^n = 1$, donc δ divise d et $\delta = d$. En conclusion $\langle a^q \rangle$ est l'unique sous-groupe d'ordre d de G. Le théorème de Lagrange nous dit que tous les éléments de H ont un ordre qui divise d. Réciproquement si $h = a^k \in G$ est d'ordre divisant d, on a alors $h^d = a^{kd} = 1$ et $n = qd$ divise kd, donc q divise k et $h = (a^q)^j \in H$. Le groupe H est donc l'ensemble de tous les éléments de G d'ordre divisant d. Les générateurs de H sont tous d'ordre d et réciproquement tout élément de G d'ordre d est dans H et l'engendre.

□

Le résultat précédent est en fait caractéristique des groupes cycliques.

Théorème 1.25.

Un groupe commutatif fini d'ordre $n \geq 1$ est cyclique si, et seulement si, pour tout diviseur d de n, il existe un unique sous-groupe d'ordre d de G.

Preuve. Le théorème précédent nous dit que la condition est nécessaire.

Pour la réciproque, on utilise le théorème de structure des groupes abéliens finis (théorème 1.36). Si G est groupe commutatif fini d'ordre $n \geq 2$ non cyclique, il est alors isomorphe à un groupe $\Gamma = \prod_{k=1}^{r} \frac{\mathbb{Z}}{n_k\mathbb{Z}}$ produit de $r \geq 2$ groupes cycliques, où $(n_k)_{1\leq k\leq r}$ est une suite d'entiers telle que $n_1 \geq 2$ et n_k est multiple de n_{k-1} pour tout k compris entre 2 et r. Dans Γ, il y a au moins deux sous-groupes cycliques d'ordre n_1 (diviseur de n), à savoir $H_1 = \left\{(x_1, \pi_2(1), \cdots, \pi_r(1)) \mid x_1 \in \frac{\mathbb{Z}}{n_1\mathbb{Z}}\right\}$ et $H_2 = \{(\pi_1(1), x_2, \cdots, \pi_r(1)) \mid x_2 \in K_2\}$, où on a noté π_k la projection canonique de $\mathbb{Z}$ sur $\frac{\mathbb{Z}}{n_k\mathbb{Z}}$ et K_2 est l'unique sous-groupe de $\frac{\mathbb{Z}}{n_2\mathbb{Z}}$ d'ordre n_1 (qui divise n_2). □

Si $G = \langle a\rangle$ est un groupe cyclique d'ordre $n \geq 1$, il y a autant de sous-groupes de G que de diviseurs de n puisque l'application $d \in \mathcal{D}_n \mapsto \langle a^{\frac{n}{d}}\rangle$ réalise une bijection de l'ensemble $\mathcal{D}_n$ des diviseurs positifs de n sur l'ensemble des sous-groupes de G.

Du théorème de structure des groupes abéliens finis (théorème 1.36), on déduit que si G est un groupe commutatif fini d'ordre $n \geq 1$, il existe alors, pour tout diviseur d de n, un sous-groupe d'ordre d (non unique pour G non cyclique).

Pour un groupe fini non commutatif d'ordre $n \geq 4$ et pour d divisant n, il n'existe pas nécessairement de sous-groupe d'ordre d. Par exemple dans $\mathcal{A}_4$ qui est d'ordre 12, il n'y a pas de sous-groupes d'ordre 6 (exercice 2.17). Mais pour tout diviseur premier p de n, il existe un sous-groupe de G d'ordre p (théorème 1.27).

Pour $G = \frac{\mathbb{Z}}{n\mathbb{Z}}$, d diviseur de n, l'unique sous-groupe d'ordre d du groupe G est $H = \langle q\overline{1}\rangle = \frac{q\mathbb{Z}}{n\mathbb{Z}}$, où $q = \frac{n}{d}$ et ce sous-groupe est isomorphe à $\frac{\mathbb{Z}}{d\mathbb{Z}}$. Ce résultat est en fait un cas particulier du suivant.

Théorème 1.26.

Soient G un groupe et H un sous-groupe distingué de G. Les sous-groupes du groupe quotient G/H sont de la forme K/H où K est un sous-groupe de G qui contient H.

Preuve. Soit K un sous-groupe de G qui contient H. Comme H est distingué dans G, il l'est aussi dans K et $K/H = \{gH \mid g \in K\} \subset G/H = \{gH \mid g \in G\}$ est un sous-groupe de G/H.

Réciproquement soit L un sous-groupe de G/H et $K = \{g \in G \mid gH \in L\}$. On a $H \subset L$ (pour $g \in H$, on a $gH = H = \overline{1} \in L$ puisque L est un groupe) et K est un sous-groupe de G (si $g \in K$, on a $gH = \overline{g} \in L$, donc $g^{-1}H = \overline{g^{-1}} = \overline{g}^{-1} \in L$ et pour g_1, g_2 dans K, on a $g_1g_2H = \overline{g_1g_2} \in L$). Comme H est distingué dans G, il l'est dans K et $K/H = \{gH \mid g \in K\} = L$ par construction. □

Le théorème précédent nous dit que si H est un sous-groupe distingué de G, on a alors une bijection entre les sous-groupes de G/H et les sous-groupes de G qui contiennent H.

Exemple 1.1 *Les sous-groupes de* $\mathbb{U}_n = \{z \in C \mid z^n = 1\} = \left\langle e^{\frac{2i\pi}{n}} \right\rangle$ *sont les* $\left\langle \left(e^{\frac{2i\pi}{n}}\right)^{\frac{n}{d}} \right\rangle = \left\langle e^{\frac{2i\pi}{d}} \right\rangle = \mathbb{U}_d$ *où* d *est un diviseur de* n *et il y en a autant que de diviseurs de* n.

Corollaire 1.4. *Pour tout entier* $n \geq 2$, *on a* $n = \sum_{d \in \mathcal{D}_n} \varphi(d)$, *où* $\mathcal{D}_n$ *est l'ensemble des diviseurs strictement positifs de* n.

Preuve. Pour tout $d \in \mathcal{D}_n$, $H = \left\langle \overline{\frac{n}{d}} \right\rangle \backsimeq \frac{\mathbb{Z}}{d\mathbb{Z}}$ est l'unique sous-groupe d'ordre d de $\frac{\mathbb{Z}}{n\mathbb{Z}}$, donc $\varphi(d) = \text{card}\{\text{générateurs de } H\} = \text{card}\left\{x \in \frac{\mathbb{Z}}{n\mathbb{Z}} \mid \theta(x) = d\right\}$ ($\theta(x)$ est l'ordre de x dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$). Le théorème de Lagrange nous dit que les ensembles $\left\{x \in \frac{\mathbb{Z}}{n\mathbb{Z}} \mid \theta(x) = d\right\}$, pour d décrivant $\mathcal{D}_n$, forment une partition de $\{1, \cdots, n\}$, ce qui nous donne le résultat annoncé. □

Au paragraphe 10.2 nous donnons une autre démonstration du corollaire précédent.

Le théorème 1.25 nous permet de montrer le théorème de Cauchy dans le cas commutatif.

Théorème 1.27. Cauchy

Soit G *un groupe commutatif fini d'ordre* $n \geq 2$. *Pour tout diviseur premier* p *de* n *il existe dans* G *un élément d'ordre* p.

Preuve. On procède par récurrence sur l'ordre $n \geq 2$ de G. Pour $n = 2$, c'est clair puisque $G = \{1, g\}$ est le seul sous-groupe d'ordre 2. Supposons le acquis pour les groupes commutatifs d'ordre $m < n$, où $n \geq 3$. On se donne un groupe commutatif G d'ordre n, un diviseur premier p de n et un élément $a \in G \setminus \{1\}$. Si $G = \langle a \rangle$, alors G est cyclique et a est d'ordre n. Pour tout diviseur premier p de n, on a vu que $a^{\frac{n}{p}}$ est d'ordre p dans G. Si $G \neq \langle a \rangle$ et p divise $m = \text{card}(\langle a \rangle) < n$, alors l'hypothèse de récurrence nous assure de l'existence d'un élément h dans $\langle a \rangle$ qui est d'ordre p. Supposons enfin que $G \neq \langle a \rangle$ et p ne divise pas $m = \text{card}(\langle a \rangle)$. Comme p est premier ne divisant pas m, il est premier avec m et le groupe quotient $G/\langle a \rangle$ est commutatif d'ordre $r = \frac{n}{m} < n$ divisible par p (p divise $n = rm$ et p est premier avec m, le théorème de Gauss nous dit alors que p divise r). L'hypothèse de récurrence nous assure alors de l'existence d'un élément $\overline{h}$ d'ordre p dans $G/\langle a \rangle$. Comme l'ordre s de h est multiple de $\theta\left(\overline{h}\right) = p$ (exercice 1.9), $k = h^{\frac{s}{p}}$ est d'ordre p dans G. □

Pour G commutatif non cyclique et d diviseur quelconque de n, il n'existe pas nécessairement d'élément d'ordre d dans G. Par exemple, pour G non cyclique et $d = n$, il n'existe pas d'élément d'ordre n.

1.6 Actions de groupes

Pour ce paragraphe, E est un ensemble non vide et $\mathcal{S}(E)$ est le groupe des permutations de E (ce groupe est étudié au chapitre 2).

Définition 1.10. *On dit que le groupe G opère à gauche sur l'ensemble E si on a une application $(g,x) \in G \times E \mapsto g \cdot x \in E$ telle que :*

$$\begin{cases} \forall x \in E,\ 1 \cdot x = x \\ \forall (g,g',x) \in G^2 \times E,\ g \cdot (g' \cdot x) = (gg') \cdot x \end{cases}$$

Une telle application est aussi appelée action à gauche de G sur E.

On peut définir de manière analogue la notion d'action à droite d'un groupe sur un ensemble non vide comme une application $(g,x) \in G \times E \mapsto x \cdot g \in E$ telle que :

$$\begin{cases} \forall x \in E,\ x \cdot 1 = x \\ \forall (g,g',x) \in G^2 \times E,\ (x \cdot g) \cdot g' = x \cdot (gg') \end{cases}$$

Pour tout $g \in G$, l'application $\varphi(g) : x \in E \mapsto g \cdot x \in E$ est une bijection de E sur E, c'est-à-dire que $\varphi(g) \in \mathcal{S}(E)$. En effet, de $1 \cdot x = x$ pour tout $x \in E$, on déduit que $\varphi(1) = Id_E$ et de $g \cdot \left(g^{-1} \cdot x\right) = \left(gg^{-1}\right) \cdot x = 1 \cdot x = x$ et $g^{-1} \cdot (g \cdot x) = x$ on déduit que $\varphi(g) \circ \varphi\left(g^{-1}\right) = \varphi\left(g^{-1}\right) \circ \varphi(g) = Id_E$, ce qui signifie que $\varphi(g)$ est bijective d'inverse $\varphi\left(g^{-1}\right)$. De plus avec $g \cdot (g' \cdot x) = (gg') \cdot x$, pour tous g, g', x, on déduit que $\varphi(gg') = \varphi(g) \circ \varphi(g')$, c'est-à-dire que l'application φ est un morphisme de groupes de $(G,\cdot)$ dans $(\mathcal{S}(E), \circ)$. Le noyau de ce morphisme φ est le noyau de l'action à gauche de G sur E. Réciproquement un tel morphisme φ définit une action à gauche de G sur E avec $g \cdot x = \varphi(g)(x)$.

Exemples 1.3 *G est un groupe multiplicatif.*

1. *G agit sur lui même par translations à gauche $(g,h) \in G \times G \mapsto g \cdot h = gh$.*
2. *G agit sur lui même par conjugaison $(g,h) \in G \times G \mapsto g \cdot h = ghg^{-1}$, le morphisme de groupes correspondant de $(G,\cdot)$ dans $(\mathcal{S}(G), \circ)$ est alors noté $\mathrm{Int}(g) : h \in G \mapsto ghg^{-1} \in G$. L'image de ce morphisme est le groupe $\mathrm{Int}(G)$ des automorphismes intérieurs de G.*
3. *G agit sur tout sous-groupe distingué H par conjugaison :*

$$(g,h) \in G \times H \mapsto g \cdot h = ghg^{-1} \in H$$

4. *Le groupe $\mathcal{S}(E)$ agit naturellement sur E par :*

$$(\sigma, x) \in \mathcal{S}(E) \times E \mapsto \sigma \cdot x = \sigma(x) \in E$$

Définition 1.11. *Soit G un groupe opérant sur un ensemble non vide E. Pour tout $x \in E$, le sous-ensemble $G \cdot x = \{g \cdot x \mid g \in G\}$ de E, est appelé orbite de x sous l'action de G.*

Remarque 1.1 *On vérifie facilement que la relation $x \sim y$ si, et seulement si, il existe $g \in G$ tel que $y = g \cdot x$ est une relation d'équivalence sur E ($x = 1 \cdot x$ donne la réflexivité, $y = g \cdot x$ équivalent à $x = g^{-1} \cdot y$ donne la symétrie et $y = g \cdot x$, $z = h \cdot y$ qui entraîne $z = (hg) \cdot x$ donne la transitivité) et la classe de $x \in E$ pour cette relation est l'orbite de x. Il en résulte que les orbites forment une partition de E.*

Exemples 1.4

1. *Pour l'action de $\mathcal{S}(E)$ sur E il y a une seule orbite. En effet, pour tout x dans E, on a $\mathcal{S}(E) \cdot x = \{\sigma(x) \mid \sigma \in \mathcal{S}(E)\} = E$ (tout $y \in E$ s'écrit $y = \tau(x)$, où τ est la transposition $\tau = (x, y)$ si $y \neq x$, $\tau = Id$ si $y = x$).*
2. *Pour l'action de G sur lui même par conjugaison, les orbites sont appelées classes de conjugaison :*

$$\forall h \in G,\ G \cdot h = \left\{ghg^{-1} \mid g \in G\right\}$$

Le groupe G est commutatif si, et seulement si, $G \cdot h = \{h\}$ pour tout $h \in G$.

3. *Si H est un sous-groupe de G, il agit par translation à droite sur G :*

$$(h, g) \in H \times G \mapsto h \cdot g = gh^{-1}$$

($1 \cdot g = g1 = g$ et $h_1 \cdot (h_2 \cdot g) = \left(gh_2^{-1}\right) h_1^{-1} = g\left(h_1 h_2\right)^{-1} = (h_1 h_2) \cdot g$) et pour tout $g \in G$ l'orbite de g est la classe à gauche modulo H :

$$H \cdot g = \{h \cdot g \mid h \in H\} = \left\{gh^{-1} \mid h \in H\right\} = \{gk \mid k \in H\} = gH$$

L'ensemble de ces orbites est l'ensemble quotient G/H des classes à gauche modulo H. En utilisant les translation à gauche $(h, g) \in H \times G \mapsto h \cdot g = hg$, les orbites sont les classes à droite modulo H, $H \cdot g = \{hg \mid h \in H\} = Hg$.

Définition 1.12. *On dit que l'action de G sur E est transitive [resp. simplement transitive] si :*

$$\forall (x, y) \in E^2,\ \exists g \in G \mid y = g \cdot x \text{ [resp. } \exists! g \in G \mid y = g \cdot x\text{]}$$

Dans le cas d'une action transitive ou simplement transitive, il y a une seule orbite.

Définition 1.13. *On dit que l'action de G sur E est fidèle si le morphisme de groupes $\varphi : g \in G \mapsto (\varphi(g) : x \mapsto g \cdot x) \in \mathcal{S}(E)$ est injectif, ce qui signifie que :*

$$(g \in G \text{ et } \forall x \in E,\ g \cdot x = x) \Leftrightarrow (g = 1)$$

Une action fidèle permet d'identifier G à un sous-groupe de $\mathcal{S}(E)$.

Théorème 1.28. Cayley

L'action de G sur lui même par translation à gauche est fidèle et G est isomorphe à un sous-groupe de $\mathcal{S}(G)$.

Preuve. Pour $g \in G$, on a $g \cdot h = gh = h$ pour tout $h \in G$ si, et seulement si, $g = 1$, donc φ est injectif. □

Définition 1.14. *Soit G un groupe opérant sur un ensemble non vide E. Pour tout $x \in E$, le sous-ensemble $G_x = \{g \in G \mid g \cdot x = x\}$ de G est le stabilisateur de x sous l'action de G.*

On vérifie facilement que ces stabilisateurs G_x sont des sous-groupes de G (en général non distingués).

Exemple 1.2 *En faisant agir $G = \mathcal{S}(E)$ sur un ensemble E non réduit à un point par $\sigma \cdot x = \sigma(x)$, le stabilisateur de $x \in E$ est isomorphe à $\mathcal{S}(E \setminus \{x\})$. À $\sigma \in G_x$, on associe la restriction σ' de σ à $E \setminus \{x\}$, ce qui définit un isomorphisme de G_x sur $\mathcal{S}(E \setminus \{x\})$.*

Théorème 1.29.

Soit $(G, \cdot)$ un groupe opérant sur un ensemble E. Pour tout $x \in E$ l'application $\varphi_x : \overline{g} = gG_x \in G/G_x \mapsto g \cdot x \in G \cdot x$ est bien définie et bijective. Dans le cas où G fini, on a $\operatorname{card}(G \cdot x) = [G : G_x] = \dfrac{\operatorname{card}(G)}{\operatorname{card}(G_x)}$ (en particulier, $\operatorname{card}(G \cdot x)$ divise $\operatorname{card}(G)$).

Preuve. En remarquant que pour g, h dans G et $x \in E$, l'égalité $g \cdot x = h \cdot x$ équivaut à $\left(h^{-1}g\right) \cdot x = x$, soit à $h^{-1}g \in G_x$ ou encore à $\overline{g} = \overline{h}$ dans G/G_x, on déduit que l'application φ_x est bien définie et injective. Cette application étant clairement surjective, elle définie une bijection de G/G_x sur $G \cdot x$. Dans le cas où G fini, on a $\operatorname{card}(G \cdot x) = \operatorname{card}(G/G_x) = \dfrac{\operatorname{card}(G)}{\operatorname{card}(G_x)}$. □

Théorème 1.30. Équation des classes

Soit $(G, \cdot)$ un groupe fini opérant sur un ensemble fini E. En notant $G \cdot x_1, \cdots, G \cdot x_r$ toutes les orbites deux à deux distinctes, on a :

$$\operatorname{card}(E) = \sum_{i=1}^{r} \operatorname{card}(G \cdot x_i) = \sum_{i=1}^{r} \frac{\operatorname{card}(G)}{\operatorname{card}(G_{x_i})}$$

Preuve. Pour E fini, on a un nombre fini d'orbites $G \cdot x_1, \cdots, G \cdot x_r$ qui forment une partition de E et $\operatorname{card}(E) = \displaystyle\sum_{i=1}^{r} \operatorname{card}(G \cdot x_i)$. En utilisant la bijection de G/G_x

sur $G \cdot x_i$, on déduit que si G est aussi fini, on a alors $\operatorname{card}(E) = \sum_{i=1}^{r} \frac{\operatorname{card}(G)}{\operatorname{card}(G_{x_i})}$.

□

Pour $(G, \cdot)$ opérant sur un ensemble E, on note $E^G = \{x \in E \mid G \cdot x = \{x\}\}$. C'est l'ensemble des éléments de E dont l'orbite est réduite à un point. En séparant dans la formule des classes les orbites réduites à un point des autres, elle s'écrit $\operatorname{card}(E) = \operatorname{card}\left(E^G\right) + \sum_{\substack{i=1 \\ \operatorname{card}(G\cdot x_i)\geq 2}}^{r} \operatorname{card}(G \cdot x_i)$ (la somme étant nulle si toutes les orbites sont réduites à un point).

Définition 1.15. *Si $p \geq 2$ est un nombre premier, on appelle p-groupe tout groupe de cardinal p^α où α est un entier naturel non nul.*

Corollaire 1.5. *Si $p \geq 2$ est un nombre premier et $(G, \cdot)$ est un p-groupe opérant sur un ensemble fini E, on a alors* $\operatorname{card}\left(E^G\right) \equiv \operatorname{card}(E) \pmod{p}$.

Preuve. Dans le cas d'un p-groupe de cardinal p^α avec $\alpha \geq 1$, pour toute orbite $G \cdot x_i$ non réduite à un point (s'il en existe), on a :

$$\operatorname{card}(G \cdot x_i) = \operatorname{card}\left(\frac{G}{G_{x_i}}\right) = \frac{\operatorname{card}(G)}{\operatorname{card}(G_{x_i})} \geq 2$$

donc $\operatorname{card}(G_{x_i}) = p^{\beta_i}$ avec $0 \leq \beta_i < \alpha$ et $\operatorname{card}(G \cdot x_i) = p^{\alpha-\beta_i}$ avec $1 \leq \alpha - \beta_i \leq \alpha$. Il en résulte que :

$$\operatorname{card}(E) = \operatorname{card}\left(E^G\right) + \sum_{\substack{i=1 \\ \operatorname{card}(G\cdot x_i)\geq 2}}^{r} \operatorname{card}(G \cdot x_i) \equiv \operatorname{card}\left(E^G\right) \pmod{p}$$

□

Corollaire 1.6. *Soit G un groupe fini que l'on fait opérer sur lui même par conjugaison ($g \cdot h = ghg^{-1}$, pour $(g, h) \in G \times G$). En notant $G \cdot h_1, \cdots, G \cdot h_r$ toutes les orbites deux à deux distinctes, on a :*

$$\begin{aligned} \operatorname{card}(G) &= \operatorname{card}(Z(G)) + \sum_{\substack{i=1 \\ \operatorname{card}(G\cdot h_i)\geq 2}}^{r} \operatorname{card}(G \cdot h_i) \\ &= \operatorname{card}(Z(G)) + \sum_{\substack{i=1 \\ \operatorname{card}(G\cdot h_i)\geq 2}}^{r} \frac{\operatorname{card}(G)}{\operatorname{card}(G_{h_i})} \end{aligned}$$

Preuve. Une orbite $G \cdot h$ est réduite à $\{h\}$ si, et seulement si, $ghg^{-1} = h$ pour tout $g \in G$, ce qui revient à dire que $gh = hg$, ou encore que $h \in Z(G)$. On a donc $Z(G) = G^G$ et le résultat annoncé. □

Théorème 1.31.

Pour tout nombre premier p, le centre d'un p-groupe n'est pas réduit à $\{1\}$.

Preuve. Soit G un p-groupe à p^α éléments. On a, avec les notations des corollaires qui précèdent, $\text{card}\,(Z(G)) = \text{card}\left(G^G\right) \equiv \text{card}\,(G) \pmod p$ et comme $\text{card}\,(Z(G)) \geq 1$, il en résulte que $\text{card}\,(Z(G)) \geq p$ et $Z(G)$ est non trivial. □

Théorème 1.32.

Tout groupe d'ordre p^2 avec p premier est commutatif.

Preuve. Soit G d'ordre p^2. On sait que $Z(G)$ est non trivial, il est donc de cardinal p ou p^2 et il s'agit de montrer qu'il est de cardinal p^2. Si $Z(G)$ est de cardinal p, il est alors cyclique, soit $Z(G) = \langle g\rangle$. Un élément h de $G \setminus Z(G)$ ne pouvant être d'ordre p^2 (sinon $G = \langle h\rangle$ et G serait commutatif ce qui contredit l'hypothèse $G \neq Z(G)$), il est d'ordre p et $Z(G) \cap \langle h\rangle = \{1\}$. En effet, $Z(G) \cap \langle h\rangle$ est un sous-groupe de $Z(G)$, donc d'ordre 1 ou p. S'il est d'ordre p, il est alors égal à $Z(G)$ et $h \in Z(G)$, ce qui n'est pas. Il est donc d'ordre 1 et $Z(G) \cap \langle h\rangle = \{1\}$. En utilisant l'application $\varphi : (i,j) \in \{0,1,\cdots,p-1\}^2 \mapsto g^i h^j \in G$, on déduit que tout élément de G s'écrit de manière unique $g^i h^j$. Pour ce faire il suffit de montrer que φ est injective. Si (i,j) et (i',j') sont tels que $g^i h^j = g^{i'} h^{j'}$, on a alors $g^{i-i'} = h^{j'-j} \in Z(G) \cap \langle h\rangle = \{1\}$ et $g^{i-i'} = h^{j'-j} = 1$ ce qui entraîne que p divise $i - i'$ et $j - j'$ et comme $|i - i'| < p$, $|j - j'| < p$, on a nécessairement $i = i'$, $j = j'$. Avec les cardinaux il en résulte que φ est une bijection. Si k, k' sont dans G, il s'écrivent $k = g^i h^j$ et $k' = g^{i'} h^{j'}$ et comme g commute à tout G, on en déduit que k et k' commutent. Le groupe G serait alors commutatif ce qui est contraire à l'hypothèse $G \neq Z(G)$. En définitive $Z(G)$ ne peut être de cardinal p, il est donc de cardinal p^2 et G est commutatif. □

Si G d'ordre p^2 a un élément d'ordre p^2, il est alors cyclique isomorphe à $\dfrac{\mathbb{Z}}{p^2\mathbb{Z}}$. Dans le cas où tous ses éléments sont d'ordre p, il est isomorphe à $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$.

1.7 Le théorème de Cauchy

Soient G un groupe fini de cardinal $n \geq 2$, $p \geq 2$ un nombre premier et :

$$E = \{(g_1,\cdots,g_p) \in G^p \mid g_1 \cdots g_p = 1\}$$

Lemme 1.1 *Avec les notations qui précèdent, on a* $\text{card}\,(E) = n^{p-1}$.

Preuve. L'application $(g_1,\cdots,g_{p-1}) \mapsto \left(g_1,\cdots,g_{p-1},(g_1\cdots g_{p-1})^{-1}\right)$ est bijective de G^{p-1} sur E (de l'égalité $g_1 \cdots g_p = 1$, on déduit que la connaissance des g_k pour $1 \leq k \leq p-1$ détermine g_p de manière unique). On a donc $\text{card}\,(E) = n^{p-1}$. □

On désigne par $H = \langle\sigma\rangle$ le sous-groupe du groupe symétrique $\mathcal{S}_p$ engendré par le p-cycle $\sigma = (1, 2, \cdots, p)$ et on fait agir le groupe H sur l'ensemble E par $\left(\sigma^k, (g_1, \cdots, g_p)\right) \mapsto \left(g_{\sigma^k(1)}, \cdots, g_{\sigma^k(p)}\right)$.

Pour tout $g = (g_1, \cdots, g_p)$ dans E, on a $\left(\prod_{k=2}^{p} g_k\right) g_1 = g_1^{-1} g_1 = 1$, donc $\left(g_{\sigma(k)}\right)_{1\leq k\leq p} = (g_2, \cdots, g_p, g_1) \in E$. Il en résulte que pour tout entier k compris entre 0 et $p-1$, $\left(g_{\sigma^k(1)}, \cdots, g_{\sigma^k(p)}\right) \in E$ et l'application :

$$\left(\sigma^k, (g_1, \cdots, g_p)\right) \mapsto \sigma^k \cdot (g_1, \cdots, g_p) = \left(g_{\sigma^k(1)}, \cdots, g_{\sigma^k(p)}\right)$$

est bien à valeurs dans E. Cette application définit bien une action puisque :

$$\begin{aligned}\sigma^j \cdot \left(\sigma^k \cdot (g_1, \cdots, g_p)\right) &= \sigma^j \cdot \left(g_{\sigma^k(1)}, \cdots, g_{\sigma^k(p)}\right) = \left(g_{\sigma^{j+k}(1)}, \cdots, g_{\sigma^{k+j}(p)}\right) \\ &= \sigma^{j+k} \cdot (g_1, \cdots, g_p) = \left(\sigma^j \circ \sigma^k\right) \cdot (g_1, \cdots, g_p)\end{aligned}$$

et $Id \cdot (g_1, \cdots, g_p) = (g_1, \cdots, g_p)$.

Lemme 1.2 *Avec ces notations,* $E^H = \{x \in E \mid H \cdot x = \{x\}\}$ *est non vide et* $\operatorname{card}\left(E^H\right)$ *est divisible par* p *si* p *est un diviseur premier de* n.

Preuve. En remarquant que $x = (1, \cdots, 1)$ est dans E^H, on déduit que E^H est non vide. Comme H est de cardinal p (un p-cycle est d'ordre p dans $\mathcal{S}_p$), on a :

$$\operatorname{card}\left(E^H\right) \equiv \operatorname{card}(E) \pmod{p}$$

(corollaire 1.5) avec $\operatorname{card}(E) = n^{p-1}$ divisible par p comme n, ce qui entraîne que $\operatorname{card}\left(E^H\right)$ est également divisible par p. □

Théorème 1.33. Cauchy

Soit G un groupe fini d'ordre $n \geq 2$. Pour tout diviseur premier p de n, il existe dans G un élément d'ordre p (donc un sous-groupe d'ordre p).

Preuve. On utilise les notations précédentes. De $\operatorname{card}\left(E^H\right) \geq 1$ divisible par p, on déduit que $\operatorname{card}\left(E^H\right) \geq p \geq 2$ et remarquant que $(g_k)_{1\leq k\leq p} \in E^H$ équivaut à dire que $g_1 = \cdots = g_p = g$ avec $g \in G$ tel que $g^p = 1$, on déduit qu'il existe $g \neq 1$ tel que $g^p = 1$, ce qui signifie que g est d'ordre p. □

1.8 Sous-groupes multiplicatifs d'un corps commutatif

Dans ce paragraphe, on s'intéresse aux sous-groupes finis du groupe multiplicatif $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ d'un corps commutatif $\mathbb{K}$.

Théorème 1.34.

Tout sous-groupe fini du groupe multiplicatif $\mathbb{K}^*$ d'un corps commutatif $\mathbb{K}$ est cyclique.

Preuve. Soit $(G,\cdot)$ un sous-groupe d'ordre n de $\mathbb{K}^*$. Il existe dans le groupe fini commutatif G un élément g_0 d'ordre $m \leq n$ égal au ppcm des ordres des éléments de G (théorème 1.12). L'ordre de tout élément de G divisant m, on déduit que tout $g \in G$ est racine du polynôme $P(X) = X^m - 1$, ce qui donne n racines distinctes de P dans $\mathbb{K}$, mais sur un corps commutatif un polynôme de degré m a au plus m racines [1], on a donc $n \leq m$ et $m = n$. Le groupe G d'ordre n ayant un élément d'ordre n est cyclique.

On peut aussi montrer ce résultat en utilisant la formule $n = \sum_{d\in\mathcal{D}_n} \varphi(d)$, où $\mathcal{D}_n$ est l'ensemble des diviseurs de n (corollaire 1.4). Pour $n = 1$, le résultat est clair. On suppose donc que G est d'ordre $n \geq 2$ et pour tout diviseur d de n, on note $\psi(d) = \operatorname{card}\{g \in G \mid \theta(g) = d\}$. Le théorème de Lagrange nous dit que les ensembles $\{g \in G \mid \theta(g) = d\}$, pour d décrivant $\mathcal{D}_n$, forment une partition de $\{1,\cdots,n\}$, donc $n = \sum_{d\in\mathcal{D}_n} \psi(d)$. Pour $d \in \mathcal{D}_n$ tel que $\psi(d) \geq 1$ (les $\psi(d)$ ne peuvent pas être tous nuls), il existe dans G au moins un élément g d'ordre d et le groupe $H = \langle g\rangle$ est formé de d solutions distinctes de l'équation $X^d - 1 = \overline{0}$, or cette équation a au plus d solutions dans le corps commutatif $\mathbb{K}$, donc H est exactement l'ensemble de toutes les solutions de cette équation. Les éléments d'ordre d dans G sont donc les générateurs du groupe cyclique H et il y a $\varphi(d)$ tels générateurs, donc $\psi(d) = \varphi(d)$ si $\psi(d) \geq 1$. On en déduit que $\sum_{d\in\mathcal{D}_n} \psi(d) = n = \sum_{d\in\mathcal{D}_n} \varphi(d)$ avec $\psi(d) = 0$ ou $\psi(d) = \varphi(d)$, ce qui entraîne que $\psi(d) = \varphi(d)$ pour tout $d \in \mathcal{D}_n$. En particulier, on a $\psi(n) \geq 1$, ce qui signifie qu'il existe dans G au moins un élément d'ordre n et en conséquence, G est cyclique. □

On note $\mu_n(\mathbb{K}) = \{\lambda \in \mathbb{K} \mid \lambda^n = 1\}$ l'ensemble des racines n-ièmes de l'unité dans le groupe multiplicatif $\mathbb{K}^*$.

Corollaire 1.7. *$\mu_n(\mathbb{K})$ est un sous-groupe cyclique de $\mathbb{K}^*$.*

Preuve. $\mu_n(\mathbb{K})$ est le noyau du morphisme de groupes $\varphi_n \in \lambda \in \mathbb{K}^* \mapsto \lambda^n$, c'est donc un sous-groupe fini du groupe multiplicatif $\mathbb{K}^*$ de cardinal au plus égal à n (racines dans $\mathbb{K}$ du polynôme de degré n, $X^n - 1$) et en conséquence il est cyclique. □

Pour $\mathbb{K} = \mathbb{C}$, $\mu_n(\mathbb{C}) = \left\{e^{\frac{2ik\pi}{n}},\ 0 \leq k \leq n-1\right\}$, est cyclique d'ordre n.

Pour $\mathbb{K} = \mathbb{R}$:

$$\mu_n(\mathbb{R}) = \begin{cases} \{1\} \text{ si } n \text{ est impair} \\ \{-1,1\} \text{ si } n \text{ est pair} \end{cases}$$

est cyclique d'ordre 1 ou 2.

1. Ce résultat est faux sur un corps non commutatif, voir par exemple le corps des quaternions.

1.9 Théorème de structure des groupes abéliens finis

On note $\theta(g)$ l'ordre d'un élément g d'un groupe G. Pour un groupe abélien fini G, l'entier $e(G) = \max_{g\in G} \theta(g)$ est l'exposant du groupe. On rappelle qu'on a aussi $e(G) = \text{ppcm}\{\theta(g) \mid g \in G\}$ (théorème 1.13).

Un caractère d'un groupe G est un morphisme de groupes de G dans $\mathbb{C}^*$.

Pour tout entier $m \geq 2$, on note $\mathbb{U}_m$ le groupe cyclique des racines m-ièmes de l'unité dans $\mathbb{C}^*$.

Dans ce qui suit, on se donne un groupe commutatif G d'ordre $n \geq 2$ et en utilisant les caractères nous allons montrer que G est isomorphe à un produit $\prod_{k=1}^{r} \mathbb{U}_{n_k}$ où la suite d'entiers $(n_k)_{1\leq k\leq r}$ telle que $n_1 \geq 2$, n_2 est multiple de n_1, ..., n_k est multiple de n_{k-1} est uniquement déterminée.

Lemme 1.3 *Soit H un sous-groupe de G. Tout caractère $\varphi : H \to \mathbb{C}^*$ peut se prolonger en un caractère sur G.*

Preuve. Pour $H = G$, le résultat est évident. On suppose donc que $H \neq G$ et on se donne un élément g de $G \setminus H$ et on vérifie que le caractère $\varphi : H \to \mathbb{C}^*$ peut se prolonger en un caractère sur le groupe $\langle g, H\rangle$ engendré par g et H. Comme $g^{\theta(g)} = 1 \in H$ (ou $g^n = 1 \in H$), on peut définir l'entier $r = \min\left\{k \in \mathbb{N}^* \mid g^k \in H\right\}$ et comme $\mathbb{C}$ est algébriquement clos, il existe $\alpha \in \mathbb{C}^*$ tel que $\varphi(g^r) = \alpha^r$. On note $K = \left\{g^k h \mid k \in \mathbb{Z},\ h \in H\right\}$ le sous-groupe de G engendré par g et H et on vérifie que l'application :

$$\begin{array}{rccc} \varphi_K : & K & \to & \mathbb{C}^* \\ & g^k h & \mapsto & \alpha^k \varphi(h) \end{array}$$

est bien définie, puis que c'est un morphisme de groupes. Si $g^k h = g^{k'} h'$ avec $k \geq k'$ dans $\mathbb{Z}$ et h, h' dans H, on a alors $g^{k-k'} = h' h^{-1} \in H$ et $k - k' = qr$ (la division euclidienne par r donne $k - k' = qr + s$ avec $0 \leq s \leq r - 1$, donc $h' h^{-1} = g^{k-k'} = (g^r)^q g^s$ et $g^s = \left((g^r)^q\right)^{-1} h' h^{-1} \in H$, ce qui impose $s = 0$ par caractère minimal de r), donc $\varphi\left(h' h^{-1}\right) = \varphi\left(g^{k-k'}\right) = \varphi(g^r)^q = (\alpha^r)^q = \alpha^{k-k'}$ et $\alpha^k \varphi(h) = \alpha^{k'} \varphi(h')$. Donc l'application φ_K est bien définie. On vérifie facilement que c'est un morphisme de groupes. En effet, pour $g^k h$ et $g^{k'} h'$ dans K, on a :

$$\begin{aligned} \varphi_K\left(\left(g^k h\right)\left(g^{k'} h'\right)\right) &= \varphi_K\left(g^{k+k'} h h'\right) = \alpha^{k+k'} \varphi(h h') \\ &= \alpha^k \varphi(h)\, \alpha^{k'} \varphi(h') = \varphi_K\left(g^k h\right) \varphi_K\left(g^{k'} h'\right) \end{aligned}$$

Avec la construction précédente, si $K = G$, on a bien prolongé φ à G. Sinon on reprend cette construction à partir de K. Comme le groupe G est fini, on aura prolongé φ à G par ces itérations. □

Lemme 1.4 *On se donne un élément g_0 de G d'ordre égal à l'exposant de G, soit :*

$$m = \theta(g_0) = \max_{g\in G} \theta(g) = \text{ppcm}\{\theta(g) \mid g \in G\}$$

et en supposant que $m \leq n-1$, on note $K = \langle g_0 \rangle$ le sous-groupe cyclique de G engendré par g_0.

1. *Il existe un unique caractère $\varphi_0 : K \to \mathbb{C}^*$ tel que $\varphi_0(g_0) = \omega = e^{\frac{2i\pi}{m}}$.*
2. *En prolongeant le caractère φ_0 en un caractère φ de G, l'application :*

$$\begin{array}{rccc} \theta : & \langle g_0 \rangle \times \ker(\varphi) & \to & G \\ & \left(g_0^k, h\right) & \mapsto & g_0^k h \end{array}$$

est un isomorphisme de groupes.

Preuve. Comme G n'est pas réduit à $\{1\}$, on a $2 \leq m \leq n-1$ en supposant que $m \neq n$.

1. Si un tel caractère existe, on a alors pour tout entier relatif k, $\varphi_0\left(g_0^k\right) = \omega^k$, ce qui prouve son unicité. Définissant l'application φ_0 de la sorte, on vérifie que c'est un caractère de K. D'une part cette application est bien définie puisque l'égalité $g_0^k = g_0^{k'}$ dans G équivaut à $k \equiv k' \pmod{m}$, ce qui donne $\omega^k = \omega^{k'}$ et d'autre part, on vérifie facilement que c'est un morphisme de groupes.
2. Comme le groupe G est commutatif, l'application θ est bien un morphisme de groupes. Si $\left(g_0^k, h\right) \in \ker(\theta)$, on a alors $g_0^k h = 1$ et $\varphi\left(g_0^k h\right) = \omega^k = 1$, donc $k \equiv 0 \pmod{m}$, ce qui nous donne $g_0^k = 1$ et $h = 1$. Donc θ est injective. Pour tout $g \in G$, on a $g^m = 1$, donc $\varphi(g^m) = (\varphi(g))^m = 1$ et $\varphi(g) \in \mathbb{U}_m$, soit $\varphi(g) = \omega^k = \varphi\left(g_0^k\right)$ pour un entier k et $h = g\left(g_0^k\right)^{-1} \in \ker(\varphi)$, ce qui nous donne $g = g_0^k h = \theta\left(g_0^k, h\right)$. Donc θ est surjective et θ est un isomorphisme.

□

De ces deux lemmes, on déduit l'existence d'une décomposition de G en produit direct de groupes cycliques.

Théorème 1.35.

Il existe une suite d'entiers $(n_k)_{1 \leq k \leq r}$ telle que $n_1 \geq 2$, n_2 est multiple de $n_1, \cdots, n_k$ est multiple de n_{k-1} et G est isomorphe au groupe produit $\Gamma = \prod_{k=1}^{r} \mathbb{U}_{n_k}$.

Preuve. On prouve l'existence d'une telle suite d'entiers par récurrence sur l'ordre $n \geq 2$ du groupe commutatif G. Pour $n = 2$, le groupe G est cyclique isomorphe à $\mathbb{U}_2 = \{-1, 1\}$. Supposons le résultat acquis pour les groupes commutatifs d'ordre au plus égal à $n-1 \geq 2$ et soit G un groupe commutatif d'ordre $n \geq 3$. Si, avec les notations introduites avec les lemmes précédents, on a $m = n$, le groupe G est alors cyclique d'ordre n isomorphe à $\mathbb{U}_n$. Supposons que $2 \leq m \leq n-1$. Dans ce cas $\operatorname{card}(\ker(\varphi)) = \dfrac{\operatorname{card}(G)}{\operatorname{card}(\langle g_0 \rangle)} = \dfrac{n}{m}$ est compris entre 2 et $n-1$ et par hypothèse de récurrence, $\ker(\varphi)$ est isomorphe à un groupe produit $\Gamma = \prod_{k=1}^{r} \mathbb{U}_{n_k}$ avec $n_1 \geq 2$ qui divise $n_2, \cdots, n_{k-1}$ qui divise n_k. Le groupe cyclique $\langle g_0 \rangle$ étant isomorphe à

$\mathbb{U}_m = \mathbb{U}_{n_{r+1}}$, on en déduit un isomorphisme de $\prod_{k=1}^{r+1} \mathbb{U}_{n_k}$ sur G. Comme m est le ppcm des ordres des éléments de G, c'est aussi le ppcm des ordres des éléments du groupe produit $\Gamma = \prod_{k=1}^{r+1} \mathbb{U}_{n_k}$ et en particulier, il est multiple de n_k qui est l'ordre de $\left(1, \cdots, e^{\frac{2i\pi}{n_k}}, 1\right)$. □

Pour prouver l'unicité d'une telle décomposition, nous utilisons le résultat suivant.

Lemme 1.5 *Soient $(n_k)_{1\leq k\leq r}$ et $(m_j)_{1\leq j\leq s}$ deux suites d'entiers telles que $r \geq 2$, $s \geq 2$, $n_1 \geq 2$, $m_1 \geq 2$, n_{k-1} divise n_k et m_{j-1} divise m_j pour k compris entre 2 et r et j compris entre 2 et s. Ces suites sont identiques si, et seulement si, on a :*

$$\forall m \in \mathbb{N}^*,\ \prod_{k=1}^{r} \operatorname{pgcd}(m, n_k) = \prod_{j=1}^{s} \operatorname{pgcd}(m, m_j)$$

Preuve. La condition nécessaire est évidente.

Supposons que $\prod_{k=1}^{r} \operatorname{pgcd}(m, n_k) = \prod_{j=1}^{s} \operatorname{pgcd}(m, m_j)$ pour tout $m \in \mathbb{N}^*$. Prenant $m = \prod_{k=1}^{r} n_k \prod_{j=1}^{j} m_j$, on a $\operatorname{pgcd}(m, n_k) = n_k$ pour $1 \leq k \leq r$ et $\operatorname{pgcd}(m, m_j) = m_j$ pour $1 \leq j \leq s$, donc $\prod_{k=1}^{r} n_k = \prod_{j=1}^{s} m_j$. Prenant $m = n_r$ qui est multiple de tous les n_k, on a $\operatorname{pgcd}(m, n_k) = n_k$ pour $1 \leq k \leq r$ et $\prod_{k=1}^{r} n_k = \prod_{j=1}^{s} \operatorname{pgcd}(n_r, m_j)$, donc $\prod_{j=1}^{j} m_j = \prod_{j=1}^{j} \operatorname{pgcd}(n_r, m_j)$, ou encore $\prod_{j=1}^{s} \frac{m_j}{\operatorname{pgcd}(n_r, m_j)} = 1$ dans $\mathbb{N}^*$, ce qui équivaut à dire que l'on a $\operatorname{pgcd}(n_r, m_j) = m_j$ pour $1 \leq j \leq s$. En particulier, on a $m_s = \operatorname{pgcd}(n_r, m_s)$ divise n_r. Comme les suites $(n_k)_{1\leq k\leq r}$ et $(m_j)_{1\leq j\leq s}$ jouent des rôles symétriques, on a aussi n_r qui divise m_s et l'égalité $n_r = m_s$. Par récurrence, on en déduit que $r = s$ et $n_k = m_k$ pour tout k compris entre 1 et r. □

Théorème 1.36. Kronecker

Il existe une unique suite d'entiers $(n_k)_{1\leq k\leq r}$ telle que $n_1 \geq 2$, n_2 est multiple de $n_1, \cdots, n_k$ est multiple de n_{k-1} et G est isomorphe au groupe produit $\Gamma = \prod_{k=1}^{r} \mathbb{U}_{n_k}$.

Preuve. On remarque que l'exposant du groupe $\Gamma = \prod_{k=1}^{r} \mathbb{U}_{n_k}$ est n_r. En effet, comme n_r est multiple de tous les n_k, on a :

$$(z_1, \cdots, z_r)^{n_r} = (z_1^{n_r}, \cdots, z_r^{n_r}) = (1, \cdots, 1)$$

donc les éléments de $\mathbb{U}$ sont d'ordre au plus égal à n_r et comme $(1, \cdots 1, , \omega_{n_r})$ est d'ordre n_r, cet entier n_r est bien l'exposant de Γ. Supposons qu'il existe deux suites d'entiers $(n_k)_{1\leq k\leq r}$ et $(m_j)_{1\leq j\leq s}$ avec les propriétés voulues. Si $r = 1$, on a alors $n = n_1 = e(G) = m_s$ et nécessairement $s = 1$ (sinon $n = \operatorname{card}(\Gamma) = m_1 \cdots m_s \geq 2m_s = 2n$, ce qui n'est pas). Si $r \geq 2$, on a alors $s \geq 2$. Pour tout entier $m \geq 1$ l'image du groupe $\prod_{k=1}^{r} \mathbb{U}_{n_k} \backsimeq \prod_{j=1}^{s} \mathbb{U}_{m_j}$ par le morphisme de groupe $\varphi_m : x \mapsto x^m$ est le groupe $\prod_{k=1}^{r} \langle \omega_{n_k}^m \rangle \backsimeq \prod_{j=1}^{s} \left\langle \omega_{m_j}^m \right\rangle$.

On utilise alors le fait que si dans un groupe un élément ω est d'ordre p, l'élément ω^m est d'ordre $p' = \dfrac{p}{\operatorname{pgcd}(m,p)}$ (en notant $\delta = \operatorname{pgcd}(m,p)$, on a $p = \delta p'$, $m = \delta m'$, avec $\operatorname{pgcd}(m', p') = 1$ et pour tout entier k, l'égalité $(\omega^m)^k = 1$ équivaut à $km = \alpha p$, soit à $km' = \alpha p'$ ce qui revient à dire que p' divise k puisque $\operatorname{pgcd}(m', p') = 1$, donc $p' = \theta(\omega^m)$). On a donc l'égalité des cardinaux :

$$\prod_{k=1}^{r} \frac{n_k}{\operatorname{pgcd}(m, n_k)} = \prod_{j=1}^{s} \frac{m_j}{\operatorname{pgcd}(m, m_j)}$$

pour tout entier $m \geq 1$. De l'égalité $\prod_{k=1}^{r} n_k = \prod_{j=1}^{s} m_j$, on déduit que pour tout $m \geq 1$, on a les égalités $\prod_{k=1}^{r} \operatorname{pgcd}(m, n_k) = \prod_{j=1}^{s} \operatorname{pgcd}(m, m_j)$, ce qui équivaut à l'unicité de la suite $(n_k)_{1\leq k\leq r}$. □

1.10 Exercices

Exercice 1.1. *Soient H un sous-groupe de G et K un sous-groupe de H. Montrer que si l'indice de K dans G est fini, alors l'indice de H dans G et celui de K dans H sont aussi finis et on a $[G : K] = [G : H][H : K]$.*

Solution. On note respectivement $(g_i H)_{i\in I}$ et $(h_j K)_{j\in J}$ les classes à gauche modulo H dans G et modulo K dans H deux à deux distinctes. Nous allons alors montrer que la famille des classes à gauches modulo K dans G deux à deux distinctes est $(g_i h_j K)_{(i,j)\in I\times J}$. Dans le cas où $[G : K]$ est fini, il n'y a qu'un nombre fini de telles classes, ce qui impose que I et J sont finis et on a :

$$[G : K] = \operatorname{card}(I \times J) = \operatorname{card}(I) \operatorname{card}(J) = [G : H][H : K]$$

Si $g \in G$, il existe un unique indice $i \in I$ tel que $gH = g_i H$ et il existe $h \in H$ tel que $g = g_i h$. De même il existe un unique indice $j \in J$ tel que $hK = h_j K$ et h s'écrit $h = h_j k$ avec $k \in K$, ce qui donne $g = g_i h_j k \in g_i h_j K$, soit $g \sim_K g_i h_j$ et $gK = g_i h_j K$. Les classes à gauche dans G modulo K sont donc les $g_i h_j K$ pour

$(i,j) \in I \times J$. Il reste à montrer que ces classes sont deux à deux distinctes. Si (i,j) et (i',j') dans $I \times J$ sont tels que $g_i h_j K = g_{i'} h_{j'} K$, il existe $k \in K$ tel que $g_i h_j = g_{i'} h_{j'} k$ et $g_i = g_{i'} \left(h_{j'} k h_j^{-1}\right)$ avec $h_{j'} k h_j^{-1} \in H$, donc $g_i \sim_H g_{i'}$, soit $g_i H = g_{i'} H$ et $i = i'$. Il en résulte que $h_j = h_{j'} k$ avec $k \in K$ et $h_j K = h_{j'} K$, qui équivaut à $j = j'$.

Exercice 1.2. *Soit H un sous-groupe de G. Montrer que :*

$$(H \text{ distingué}) \Leftrightarrow (\forall g \in G,\ gH \subset Hg) \Leftrightarrow \left(\forall g \in G,\ gHg^{-1} \subset H\right)$$

Solution. Il est clair que :

$$(H \text{ distingué}) \Rightarrow (\forall g \in G,\ gH \subset Hg) \Rightarrow \left(\forall g \in G,\ gHg^{-1} \subset H\right)$$

Si $gHg^{-1} \subset H$ pour tout $g \in H$, on a alors $gH \subset Hg$ et $g^{-1}Hg \subset H$ (l'hypothèse pour g^{-1}) et $Hg \subset gH$, ce qui donne $gH = Hg$.

Exercice 1.3. *Soient G, G' deux groupes et φ un morphisme de groupes de G dans G'.*

1. *Montrer que si H est un sous-groupe distingué de G et φ est surjectif, alors $\varphi(H)$ est un sous-groupe distingué de G'.*
2. *Montrer que si H' est un sous-groupe distingué de G', alors $\varphi^{-1}(H')$ est un sous-groupe distingué de G.*

Solution. On sait déjà que $\varphi(H)$ est un sous-groupe de G' (que φ soit surjectif ou non) et que $\varphi^{-1}(H')$ est un sous-groupe de G.

1. Si φ est surjectif, tout $g' \in G'$ s'écrit $g' = \varphi(g)$ avec $g \in G$ et pour tout $h' = \varphi(h) \in \varphi(H)$ (avec $h \in H$), on a :
$$g' h' (g')^{-1} = \varphi(g)\varphi(h)(\varphi(g))^{-1} = \varphi(g)\varphi(h)\varphi\left(g^{-1}\right) = \varphi\left(ghg^{-1}\right) \in \varphi(H)$$
ce qui signifie que $\varphi(H)$ est distingué dans G'.
2. Pour $g \in G$ et $h \in \varphi^{-1}(H')$, on a :
$$\varphi\left(ghg^{-1}\right) = \varphi(g)\varphi(h)(\varphi(g))^{-1} \in \varphi(g) H' (\varphi(g))^{-1} = H'$$
et $ghg^{-1} \in \varphi^{-1}(H')$. Donc $\varphi^{-1}(H')$ est distingué dans G.

Exercice 1.4. *Soient $(G,\cdot)$ un groupe fini d'ordre $n \geq 2$ et H un sous-groupe de G d'indice 2. Montrer que H distingué.*

Solution. Si H est d'indice 2, on a alors $G/H = \{H, g_1 H\}$ avec $g_1 \notin H$ et la partition $G = H \cup g_1 H$. Il s'agit alors de montrer que pour tous $g \in G$ et $h \in H$, on a forcément $ghg^{-1} \in H$. Si $g \in H$ c'est clair, sinon $g = g_1 k$ avec $k \in H$ et $ghg^{-1} = g_1 khk^{-1} g_1^{-1} = g_1 \ell g_1^{-1}$ avec $\ell \in H$ et $g_1 \ell g_1^{-1} \in g_1 H$ donne $g_1 \ell g_1^{-1} = g_1 m$ avec $m \in H$, ce qui entraîne $g_1 = \ell m^{-1} \in H$ qui est faux, on a donc $ghg^{-1} = g_1 \ell g_1^{-1} \in H$ et H est distingué dans G.

Exercice 1.5. *Soient G, H deux groupes, $\varphi : G \to H$ un morphisme de groupes, G' un sous-groupe distingué de G et H' un sous-groupe distingué de H tel que $\varphi(G') \subset H'$. Montrer qu'il existe un unique morphisme de groupes $\overline{\varphi} : G/G' \to H/H'$ tel que $\pi_H \circ \varphi = \overline{\varphi} \circ \pi_G$, où $\pi_G : G \to G/G'$ et $\pi_H : H \to H/H'$ sont les surjections canoniques.*

Solution. En supposant que $\overline{\varphi}$ existe, on a nécessairement $\pi_H \circ \varphi(g) = \overline{\varphi} \circ \pi_G(g)$ pour tout $g \in G$, ce qui assure l'unicité de $\overline{\varphi}$. On définit donc $\overline{\varphi}$ par :

$$\forall \overline{g} \in G/G',\ \overline{\varphi}(\overline{g}) = \widetilde{\varphi(g)}$$

en notant $\overline{g} = gG'$ la classe de $g \in G$ modulo G' et $\widetilde{h}$ la classe de $h \in H$ modulo H'. Pour justifier cette définition, on doit vérifier qu'elle ne dépend pas du choix d'un représentant de $\overline{g}$. Si $\overline{g_1} = \overline{g_2}$, on a alors $g_2 g_1^{-1} \in G'$, ce qui nous donne $\varphi(g_2)(\varphi(g_1))^{-1} = \varphi\left(g_2 g_1^{-1}\right) \in \varphi(G') \subset H'$ et $\widetilde{\varphi(g_1)} = \widetilde{\varphi(g_2)}$. L'application $\overline{\varphi}$ est donc bien définie et par construction, on a $\pi_H \circ \varphi = \overline{\varphi} \circ \pi_G$. Avec :

$$\overline{\varphi}(\overline{g_1}\ \overline{g_2}) = \overline{\varphi}(\overline{g_1 g_2}) = \widetilde{\varphi(g_1 g_2)} = \varphi(\widetilde{g_1)\varphi}(g_2) = \widetilde{\varphi(g_1)}\widetilde{\varphi(g_2)} = \overline{\varphi}(\overline{g_1})\,\overline{\varphi}(\overline{g_2})$$

on voit que c'est un morphisme de groupes.

Exercice 1.6. *Soit E un espace euclidien de dimension $n \geq 2$. Montrer que le sous-groupe $\mathcal{O}^+(E)$ est distingué d'indice 2 dans $\mathcal{O}(E)$.*

Solution. $\mathcal{O}^+(E)$ est un sous-groupe distingué de $\mathcal{O}(E)$ comme noyau du morphisme de groupes $\det : \mathcal{O}(E) \to \{-1, 1\}$. Comme cette application est surjective ($Id \in \mathcal{O}^+(E)$ et en désignant par $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base orthonormée de E, l'application u définie par $u(e_1) = -e_1$ et $u(e_i) = e_i$ pour i compris entre 2 et n est dans $\mathcal{O}^-(E)$), $\mathcal{O}(E)/\mathcal{O}^+(E)$ est isomorphe à $\{-1, 1\}$ et $[\mathcal{O}(E) : \mathcal{O}^+(E)] = 2$.

Exercice 1.7. *Montrer que pour g, h dans G, on a $\theta(gh) = \theta(hg)$.*

Solution. L'application $\varphi : k \mapsto g^{-1}kg$ est isomorphisme de G sur lui même, donc $\theta(gh) = \theta(\varphi(gh)) = \theta(hg)$.

Exercice 1.8. *Soit $\mathcal{R}$ une relation d'équivalence sur G compatible avec la loi de G. Montrer que :*

1. *pour tous g, h dans G, on a $g\overline{h} = \overline{gh}$ et $\overline{h}g = \overline{hg}$;*
2. *$H = \overline{1}$ est un sous-groupe distingué de G ;*
3. *pour tout $g \in G$, $\overline{g} = gH = Hg$ et $G/\mathcal{R} = G/H$.*

Solution.

1. On a :

$$\left(k \in g\overline{h}\right) \Leftrightarrow (\exists h' \in G \mid h'\mathcal{R}h \text{ et } k = gh') \Rightarrow (k = gh'\mathcal{R}gh) \Rightarrow \left(k \in \overline{gh}\right)$$

donc $g\overline{h} \subset \overline{gh}$. Et réciproquement :

$$\left(k \in \overline{gh}\right) \Leftrightarrow (k\mathcal{R}gh) \Rightarrow \left(g^{-1}k\mathcal{R}h\right) \Rightarrow \left(g^{-1}k \in \overline{h}\right) \Rightarrow \left(k \in g\overline{h}\right)$$

soit $\overline{gh} \subset g\overline{h}$ et $g\overline{h} = \overline{gh}$. On procède de manière analogue pour l'égalité $\overline{h}g = \overline{hg}$.

2. On a $1 \in H = \overline{1}$, si g, h sont dans H, on a $g\mathcal{R}1$ et $h\mathcal{R}1$, donc $gh\mathcal{R}1$ et pour $g \in H$, $1\mathcal{R}g$ et $g^{-1}\mathcal{R}g^{-1}$ entraîne $g^{-1}\mathcal{R}1$, soit $g^{-1} \in H$. Donc H est bien un sous-groupe de G. Pour $g \in G$, on a $gH = g\overline{1} = \overline{g}$ et $Hg = \overline{1}g = \overline{g} = gH$, ce qui signifie que H est distingué dans G.
3. On a aussi montré en **2.** que $G/\mathcal{R} = G/H$.

Exercice 1.9. *Soient $(G, \cdot)$ un groupe fini d'ordre $n \geq 2$ et H un sous-groupe distingué de G. Comparer l'ordre de $\overline{g}$ dans G/H avec l'ordre de g dans G.*

Solution. Soit $g \in G$ d'ordre p et q l'ordre de $\overline{g}$ dans le groupe quotient G/H (H est distingué dans G). Avec $\overline{g}^p = \overline{g^p} = \overline{1}$, on déduit que $q = \theta(\overline{g})$ divise $p = \theta(g)$. Pour $G = \{1, -1, i, -i\} \subset \mathbb{C}^*$, $H = \{1, -1\}$, $g = i$ est d'ordre 4 et $\overline{g} = gH = \{i, -i\}$ est d'ordre 2 ($\overline{g} \neq \overline{1} = H$ et $\overline{g}^2 = \overline{i^2} = \overline{-1} = H = \overline{1}$).

Exercice 1.10. *Montrer qu'un groupe G est fini si, et seulement si, l'ensemble de ses sous-groupes est fini. En conséquence, un groupe infini a une infinité de sous-groupes.*

Solution. Si G est un groupe fini alors l'ensemble $\mathcal{P}(G)$ des parties de G est fini (de cardinal $2^{\mathrm{card}(G)}$) et il en est de même de l'ensemble des sous-groupes de G. Réciproquement soit $(G, \cdot)$ un groupe tel que l'ensemble de ses sous-groupes soit fini. On peut écrire $G = \bigcup_{g \in G} \langle g \rangle$ et cette réunion est finie, soit $G = \bigcup_{k=1}^{r} \langle g_k \rangle$. Si l'un de ces sous-groupes $\langle g_k \rangle$ est infini, alors les $\langle g_k^n \rangle$ où n décrit $\mathbb{N}$ forment une famille infinie de sous-groupes de G : en effet l'égalité $\langle g_k^n \rangle = \langle g_k^m \rangle$ entraîne $g_k^n = g_k^{jm}$, soit $g_k^{n-jm} = 1$ et $n - jm = 0$ (g_k est d'ordre infini), c'est-à-dire que m divise n. Comme n et m jouent des rôles symétriques, on a aussi n qui divise m et en définitive $n = m$ (on peut aussi dire plus rapidement que $\langle g_k \rangle$ est isomorphe à $\mathbb{Z}$ et de ce fait a une infinité de sous-groupes). On a donc une contradiction si l'un des $\langle g_k \rangle$ est infini. Donc tous les $\langle g_k \rangle$ sont finis et aussi G.

Exercice 1.11. *Soit $(G, \cdot)$ un groupe tel que tout élément de G soit d'ordre au plus égal à 2. Montrer que G est commutatif et, pour G fini, qu'il existe un entier $n \geq 0$ tel que* $\mathrm{card}(G) = 2^n$.

Solution. Dire que tous les éléments de G sont d'ordre au plus égal à 2, revient à dire que l'on a $g^2 = 1$, ou encore $g = g^{-1}$, pour tout $g \in G$.

1. Pour g_1, g_2 dans G, on a $g_1 g_2 = (g_1 g_2)^{-1} = g_2^{-1} g_1^{-1} = g_2 g_1$.

2. On peut montrer ce résultat de diverses manières.

   (a) On peut raisonner par récurrence sur l'ordre de G. Si G est réduit à $\{1\}$, on a alors $\text{card}\,(G) = 1 = 2^0$. Si G est d'ordre $n \geq 2$, pour tout $g \in G \setminus \{1\}$, on a $\langle g \rangle = \{1, g\}$ et le groupe quotient $\dfrac{G}{\langle g \rangle}$ (c'est un groupe car G est commutatif) est de cardinal $\dfrac{n}{2} < n$ avec tous ses éléments d'ordre au plus égal à 2. En supposant le résultat acquis pour les groupes d'ordre strictement inférieur à n, on a $\text{card}\left(\dfrac{G}{\langle g \rangle}\right) = 2^p$ et $\text{card}\,(G) = 2^{p+1}$.

   (b) On peut procéder de façon plus astucieuse comme suit. En notant la loi de G sous forme additive, on a $2 \cdot g = 0$ pour tout $g \in G$ et on peut munir G d'une structure de $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$-espace vectoriel en définissant la loi externe par $\overline{0}g = 0$ et $\overline{1}g = g$ pour tout $g \in G$, la loi interne étant l'addition de G (qui est bien commutative). Si G est fini, il est nécessairement de dimension finie sur $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$ et notant p sa dimension, on a $\text{card}\,(G) = \text{card}\left(\left(\dfrac{\mathbb{Z}}{2\mathbb{Z}}\right)^p\right) = 2^p$.

   (c) Comme G est fini, on peut aussi utiliser un système générateur minimal de G, c'est-à-dire que :

$$G = \langle g_1, \cdots, g_p \rangle = \left\{ \prod_{k=1}^{p} g_k^{\alpha_k} \mid (\alpha_1, \cdots, \alpha_p) \in \mathbb{Z}^p \right\}$$

   (G est commutatif). Si $p = 1$, on a $G = \langle g_1 \rangle = \{1\}$ ou $\{1, g_1\}$ et c'est terminé. On suppose donc que $p \geq 2$. Comme tous les éléments de G sont d'ordre 1 ou 2, en effectuant des divisions euclidiennes par 2 tout élément de G s'écrit $g = \prod_{k=1}^{p} g_k^{\alpha_k}$ avec $(\alpha_1, \cdots, \alpha_p) \in \{0, 1\}^p$ et l'application :

$$\begin{array}{rccc} \varphi & (\{0,1\})^p & \to & G \\ & (\alpha_1, \cdots, \alpha_p) & \mapsto & \displaystyle\prod_{k=1}^{p} g_k^{\alpha_k} \end{array}$$

   est une bijection de $((\{0,1\})^p, \cdot)$ sur G. On vient de voir la surjectivité et pour α, β dans $(\{0,1\})^p$, l'égalité $\varphi(\alpha) = \varphi(\beta)$ équivaut à $\prod_{k=1}^{p} g_k^{\beta_k - \alpha_k} = 1$. Si $\alpha \neq \beta$, il existe alors un indice k compris entre 1 et p tel que $\beta_k \neq \alpha_k$ et $\beta_k - \alpha_k = \pm 1$, ce qui entraîne que $g_k = \prod_{\substack{j=1 \\ j \neq k}}^{p} g_k^{\gamma_j}$ est dans le groupe engendré par les g_j avec $j \neq k$ et G est égal à ce groupe, ce qui contredit le caractère minimal de p. On a donc $\alpha = \beta$ et φ est injective, donc bijective. En conséquence, on a $\text{card}\,(G) = \text{card}\,(\{0,1\})^p = 2^p$.

   (d) On peut aussi utiliser le théorème de Cauchy (voir le paragraphe 1.7). Notons $n = 2^p m$ le cardinal de G avec m impair. Si $m = 1$, c'est terminé,

sinon, il admet un diviseur premier $q \geq 3$ et le théorème de Cauchy nous dit qu'il existe dans $G \setminus \{1\}$ un élément d'ordre q, ce qui contredit le fait que tous ses éléments sont d'ordre 2.

(e) Une autre solution consiste à dire que le ppcm des ordres des éléments de G est égal à 2, et comme ce ppcm a les mêmes facteurs premiers que n (théorème 1.14), on a nécessairement $n = 2^p$.

Exercice 1.12. *En utilisant l'exercice précédent, montrer le cas particulier suivant du théorème de Cauchy : si G est un groupe fini d'ordre $2p$ avec p premier, il existe alors un élément d'ordre p dans G.*

Solution. Si G est d'ordre $2p \geq 4$ avec p premier, le théorème de Lagrange nous dit que les éléments de $G \setminus \{1\}$ sont d'ordre 2, p ou $2p$. S'il n'y a aucun élément d'ordre p, il n'y en a pas d'ordre $2p$ (si $g \in G \setminus \{1\}$ est d'ordre $2p$, on a alors $g^2 \neq 1$, $g^p \neq 1$ et $\left(g^2\right)^p = g^{2p} = 1$, donc g^2 est d'ordre p), donc tous les éléments de $G \setminus \{1\}$ sont d'ordre 2 et G est commutatif d'ordre $2^n = 2p$, donc $p = 2^{n-1}$, $n = 2$ et $p = 2$ puisque p est premier, soit une contradiction avec l'hypothèse qu'il n'y a pas d'élément d'ordre p $(= 2)$. Il existe donc dans G des éléments d'ordre p.

Exercice 1.13. *Soit $X = \{r_1, \cdots, r_n\}$ une partie finie de $\mathbb{Q}$ et $G = \langle X \rangle$ le sous-groupe de $(\mathbb{Q}, +)$ engendré par X. Montrer que G est monogène infini.*

Solution. En désignant par μ le ppcm des dénominateurs de $r_1, \cdots, r_n$, il existe des entiers relatifs $a_1, \cdots, a_n$ tels que $r_k = \dfrac{a_k}{\mu}$ pour tout k compris entre 1 et n et en désignant par δ le pgcd de $a_1, \cdots, a_n$, on a :

$$G = \left\{ \sum_{k=1}^{n} \alpha_k \frac{a_k}{\mu} \mid (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n \right\} = \left\{ \frac{\delta}{\mu} \sum_{k=1}^{n} \alpha_k b_k \mid (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n \right\}$$

où $b_1, \cdots, b_n$ sont des entiers relatifs premiers entre eux dans leur ensemble. On a donc $G = \dfrac{\delta}{\mu}\mathbb{Z}$, ce qui signifie que G est monogène engendré par $\dfrac{\delta}{\mu}$.

Exercice 1.14. *Montrer que, pour tout entier $n \geq 1$, il existe un unique sous-groupe de $(\mathbb{Q}/\mathbb{Z}, +)$ d'ordre n et que ce groupe est cyclique.*

Solution. Supposons que G soit un sous-groupe de $(\mathbb{Q}/\mathbb{Z}, +)$ d'ordre n. Tout $\overline{r} \in G$ a un ordre qui divise n (théorème de Lagrange), donc $n\overline{r} = \overline{0}$, c'est-à-dire qu'il existe $q \in \mathbb{Z}$ tel que $nr = q$ et $r = \dfrac{q}{n}$. On a donc $\overline{r} = \overline{\dfrac{q}{n}} = q\overline{\dfrac{1}{n}} \in \left\langle \overline{\dfrac{1}{n}} \right\rangle$ et $G \subset \left\langle \overline{\dfrac{1}{n}} \right\rangle$. Comme $\overline{\dfrac{1}{n}}$ est d'ordre n dans $\mathbb{Q}/\mathbb{Z}$ (on a $k\overline{\dfrac{1}{n}} = \overline{\dfrac{k}{n}} = \overline{0}$ si, et seulement si, $\dfrac{k}{n} \in \mathbb{Z}$, ce qui équivaut à dire que k est multiple de n), on a nécessairement $G = \left\langle \overline{\dfrac{1}{n}} \right\rangle$. D'où l'unicité d'un groupe d'ordre n et ce groupe existe (c'est $\left\langle \overline{\dfrac{1}{n}} \right\rangle$).

Exercice 1.15. *En utilisant l'action naturelle de $\mathcal{S}(E)$ sur E, montrer que si E est un ensemble fini à n éléments, on a alors* $\operatorname{card}(\mathcal{S}(E)) = n!$

Solution. On utilise l'action de $\mathcal{S}(E)$ sur E définie par :

$$\forall (\sigma, x) \in \mathcal{S}(E) \times E,\ \sigma \cdot x = \sigma(x)$$

Cette action est transitive (il y a une seule orbite), donc $\mathcal{S}(E) \cdot x = E$ pour tout $x \in E$. Le stabilisateur de $x \in E$ est $\mathcal{S}(E)_x = \{\sigma \in \mathcal{S}(E) \mid \sigma(x) = x\}$ et l'application qui associe à $\sigma \in \mathcal{S}(E)_x$ sa restriction à $F = E \setminus \{x\}$ réalise un isomorphisme de $\mathcal{S}(E)_x$ sur $\mathcal{S}(F)$. On a donc $\operatorname{card}(\mathcal{S}(E)_x) = \operatorname{card}(\mathcal{S}(F))$ et :

$$\begin{aligned}\operatorname{card}(\mathcal{S}(E)) &= \operatorname{card}(\mathcal{S}(E) \cdot x) \operatorname{card}(\mathcal{S}(E)_x) \\ &= \operatorname{card}(E) \operatorname{card}(\mathcal{S}(F)) = n \operatorname{card}(\mathcal{S}(F))\end{aligned}$$

On conclut alors par récurrence sur $n \geq 1$.

Exercice 1.16. (Formule de Burnside) *Soit $(G, \cdot)$ un groupe fini opérant sur un ensemble fini E. Pour tout $g \in G$, on note $\operatorname{Fix}(g) = \{x \in E \mid g \cdot x = x\}$. Montrer que le nombre d'orbites est $\dfrac{1}{\operatorname{card}(G)} \displaystyle\sum_{g \in G} \operatorname{card}(\operatorname{Fix}(g))$.*

Solution. L'idée est de calculer le cardinal de $F = \{(g, x) \in G \times E \mid g \cdot x = x\}$ de deux manières en utilisant les partitions :

$$F = \bigcup_{g \in G} \{(g, x) \mid x \in \operatorname{Fix}(g)\} = \bigcup_{x \in E} \{(g, x) \mid g \in G_x\}$$

ce qui donne $\operatorname{card}(F) = \displaystyle\sum_{g \in G} \operatorname{card}(\operatorname{Fix}(g))$ et en notant $G \cdot x_1, \cdots, G \cdot x_r$ les orbites distinctes :

$$\begin{aligned}\operatorname{card}(F) &= \sum_{x \in E} \operatorname{card}(G_x) = \sum_{x \in E} \frac{\operatorname{card}(G)}{\operatorname{card}(G \cdot x)} \\ &= \sum_{i=1}^{r} \sum_{x \in G \cdot x_i} \frac{\operatorname{card}(G)}{\operatorname{card}(G \cdot x)} = \sum_{i=1}^{r} \operatorname{card}(G) \left(\sum_{x \in G \cdot x_i} \frac{1}{\operatorname{card}(G \cdot x)} \right) \\ &= \sum_{i=1}^{r} \operatorname{card}(G) \left(\sum_{x \in G \cdot x_i} \frac{1}{\operatorname{card}(G \cdot x_i)} \right) = \sum_{i=1}^{r} \operatorname{card}(G) = r \operatorname{card}(G)\end{aligned}$$

du fait que $G \cdot x = G \cdot x_i$ pour $x \in G \cdot x_i$ (remarque 1.1). Ce qui donne le résultat annoncé.

Exercice 1.17. *Montrer que, pour tout entier $n \geq 1$, il existe un unique sous-groupe de $(\mathbb{C}^*, \cdot)$ d'ordre n et que ce groupe est cyclique.*

Solution. Si G est un sous-groupe d'ordre $n \geq 1$ de $(\mathbb{C}^*, \cdot)$, on a alors $z^n = 1$ pour tout $z \in G$ (théorème de Lagrange), donc G est contenu dans le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité et $G = \mathbb{U}_n$ puisque ces ensembles sont de même cardinal.

Exercice 1.18. *Déterminer les sous-groupes finis du groupe multiplicatif $\mathbb{R}^*$.*

Solution. Si $G \subset \mathbb{R}^*$ est un groupe d'ordre $n \geq 1$, on a alors $x^n = 1$ pour $x \in G$ et G est contenu dans l'ensemble :

$$\Delta_n = \{x \in \mathbb{R} \mid x^n = 1\} = \begin{cases} \{-1, 1\} \text{ si } n \text{ est pair} \\ \{1\} \text{ si } n \text{ est impair} \end{cases}$$

On a donc nécessairement $n = 1$ et $G = \{1\}$ ou $n = 2$ et $G = \{-1, 1\}$.

Exercice 1.19. *Montrer que tout sous-groupe d'ordre $n \geq 1$ du groupe $O_2^+(\mathbb{R})$ des matrices de rotations du plan vectoriel euclidien $\mathbb{R}^2$ est cyclique engendré par $R\left(\frac{2\pi}{n}\right)$ (rotation d'angle $\frac{2\pi}{n}$).*

Solution. Le groupe $O_2^+(\mathbb{R})$ est isomorphe au groupe multiplicatif $\mathbb{U}$ des nombres complexes de module égal à 1, un isomorphisme étant défini par l'application :

$$R(\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \mapsto e^{i\theta}$$

Un sous-groupe fini de $O_2^+(\mathbb{R})$ est donc identifié à un sous-groupe fini de $\mathbb{U}$, donc de $\mathbb{C}^*$, et en conséquence il est cyclique engendré par $R\left(\frac{2\pi}{n}\right)$.

Chapitre 2

Groupe des permutations d'un ensemble fini

E est un ensemble ayant au moins deux éléments et Id_E est l'application identité sur E. On note $\text{card}(E)$ le cardinal de E.

2.1 Permutations, cycles et transpositions

On note $\mathcal{S}(E)$ le groupe des bijections de E sur lui même.

Définition 2.1. *Le groupe $\mathcal{S}(E)$ est appelé groupe des permutations de E.*

Pour $E = \{1, 2, \cdots, n\} \subset \mathbb{N}$, on note $\mathcal{S}_n$ le groupe $\mathcal{S}(E)$ et on l'appelle groupe symétrique à n éléments.

Pour toute permutation $\sigma \in \mathcal{S}_n$, on note :

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

pour signifier que σ est la bijection $\sigma : k \in E \mapsto \sigma(k)$.

Pour toute permutation $\sigma \in \mathcal{S}(E)$ et tout entier relatif r, σ^r est la permutation de E définie par :

$$\sigma^r = \begin{cases} Id_E \text{ si } r = 0 \\ \sigma \circ \cdots \circ \sigma \ (r \text{ fois}) \text{si } r \geq 1 \\ \left(\sigma^{-r}\right)^{-1} \text{ si } r \leq -1 \end{cases}$$

Définition 2.2. *Soit r un entier compris entre 2 et $\text{card}(E)$. On appelle cycle d'ordre r (ou r-cycle), toute permutation $\sigma \in \mathcal{S}(E)$ qui permute circulairement r éléments de E et laisse fixe les autres, c'est-à-dire qu'il existe une partie $\{x_1, \cdots, x_r\}$ de E telle que :*

$$\begin{cases} \forall k \in \{1, \cdots, r-1\}, \ \sigma(x_k) = x_{k+1} \\ \sigma(x_r) = x_1 \\ \forall x \in E \setminus \{x_1, \cdots, x_r\}, \ \sigma(x) = x \end{cases}$$

On notera $\sigma = (x_1, \cdots, x_r)$ un tel cycle et on dit que $\{x_1, \cdots, x_r\}$ est le support de σ et on le note $\text{Supp}(\sigma)$.

Les r permutations circulaires :

$$(x_1, x_2, \cdots, x_r),\ (x_2, x_3, \cdots, x_r, x_1),\ , (x_r, x_1, \cdots, x_{r-1})$$

définissent le même r-cycle.

L'inverse d'un r-cycle est un r-cycle de même support. Précisément, on a :

$$(x_1, x_2, \cdots, x_r)^{-1} = (x_r, x_{r-1}, \cdots, x_1)$$

Si $\sigma = (x_1, \cdots, x_r)$ est un r-cycle, on a alors pour tout entier k compris entre 1 et r, $x_k = \sigma^{k-1}(x_1)$.

Définition 2.3. *On appelle transposition, un 2-cycle.*

On peut remarquer qu'une transposition τ est d'ordre 2 dans le groupe $\mathcal{S}(E)$ et en conséquence, on a $\tau^{-1} = \tau$. Plus généralement, on a le résultat suivant.

Lemme 2.1 *Un r-cycle est d'ordre r dans le groupe $(\mathcal{S}(E), \circ)$.*

Preuve. Soit $\sigma = (x_1, \cdots, x_r)$ un r-cycle avec $r \geq 2$. Pour tout entier k compris entre 1 et r, on a :

$$\begin{aligned}\sigma^r(x_k) &= \sigma^r\left(\sigma^{k-1}(x_1)\right) = \sigma^{k-1}(\sigma^r(x_1)) \\ &= \sigma^{k-1}\left(\sigma\left(\sigma^{r-1}(x_1)\right)\right) = \sigma^{k-1}(\sigma(x_r)) = \sigma^{k-1}(x_1) = x_k\end{aligned}$$

Comme $\sigma(x) = x$, pour $x \in E \setminus \{x_1, \cdots, x_r\}$, on en déduit que $\sigma^r = Id_E$. Enfin avec $\sigma^{k-1}(x_1) = x_k \neq x_1$, pour $2 \leq k \leq r$, on déduit que $\sigma^{k-1} \neq Id_E$ et σ est d'ordre r. □

L'inverse d'un r-cycle σ est donc le r-cycle $\sigma^{-1} = \sigma^{r-1}$.

Lemme 2.2 *Soit r un entier compris entre 2 et $\text{card}(E)$. Le conjugué dans $\mathcal{S}(E)$ d'un r-cycle est encore un r-cycle. Plus précisément, pour tout r-cycle $\sigma = (x_1, x_2, \cdots, x_r)$ et toute permutation τ, on a :*

$$\tau \circ \sigma \circ \tau^{-1} = (\tau(x_1), \tau(x_2), \cdots, \tau(x_r))$$

Réciproquement, deux cycles de même longueur sont conjugués dans $\mathcal{S}(E)$, c'est-à-dire que si σ et σ' sont deux cycles de même longueur r, il existe alors une permutation τ telle que $\sigma' = \tau \circ \sigma \circ \tau^{-1}$.

Preuve. En notant $\sigma'' = (\tau(x_1), \tau(x_2), \cdots, \tau(x_r))$, il s'agit de montrer que $\tau \circ \sigma = \sigma'' \circ \tau$.

Pour $x \in E \setminus \{x_1, \cdots, x_r\}$, on a $\sigma(x) = x$ et $\tau(x) \in E \setminus \{\tau(x_1), \cdots, \tau(x_r)\}$, donc $\tau \circ \sigma(x) = \tau(x) = \sigma''(\tau(x)) = \sigma'' \circ \tau(x)$. Si x est l'un des x_k, on a alors $\tau \circ \sigma(x) = \tau(\sigma(x_k)) = \tau(x_{k+1})$ avec $x_{r+1} = x_1$ et $\sigma'' \circ \tau(x) = \sigma''(\tau(x_k)) = \tau(x_{k+1})$. On a donc bien $\tau \circ \sigma = \sigma'' \circ \tau$, soit $\tau \circ \sigma \circ \tau^{-1} = \sigma''$.

Soient $\sigma = (x_1, \cdots, x_r)$ et $\sigma' = (x'_1, \cdots, x'_r)$ deux r-cycles. En se donnant une bijection φ de $E \setminus \{x_1, \cdots, x_r\}$ sur $E \setminus \{x'_1, \cdots, x'_r\}$, on définit une permutation

τ de E en posant $\tau(x_k) = x'_k$ pour $k = 1, \cdots, r$ et $\tau(x) = \varphi(x)$ pour tout $x \in E \setminus \{x_1, \cdots, x_r\}$ et on a $\tau \circ \sigma \circ \tau^{-1} = (\tau(x_1), \cdots, \tau(x_r)) = (x'_1, \cdots, x'_r) = \sigma'$. □

Le résultat précédent se traduit en disant que, pour tout entier r compris entre 2 et $\text{card}(E)$, le groupe $\mathcal{S}(E)$ agit par conjugaison de façon transitive sur l'ensemble des r-cycles.

En faisant agir $\mathcal{S}(E)$ par conjugaison sur l'ensemble des cycles, l'orbite d'un r-cycle pour cette action est l'ensemble de tous les r-cycles et son cardinal est $\frac{A_n^r}{r} = (r-1)!\binom{n}{r}$.

Lemme 2.3 *Le centre du groupe de $\mathcal{S}(E)$ est :*

$$Z(\mathcal{S}(E)) = \begin{cases} \mathcal{S}(E) & si \ \text{card}(E) = 2 \\ \{Id_E\} & si \ \text{card}(E) \geq 3 \end{cases}$$

Preuve. Si $\text{card}(E) = 2$, le groupe $\mathcal{S}(E)$ est commutatif et $Z(\mathcal{S}(E)) = \mathcal{S}(E)$. On suppose que $\text{card}(E) \geq 3$ et on se donne σ dans $Z(\mathcal{S}(E))$. Pour $x \neq y$ dans E, on a $(\sigma(x), \sigma(y)) = \sigma(x,y)\sigma^{-1} = (x,y)\sigma\sigma^{-1} = (x,y)$, donc $\sigma\{x,y\} = \{x,y\}$. Pour $\text{card}(E) \geq 3$, on peut trouver, pour tout $x \in E$ deux éléments $y \neq z$ distincts de x et avec $\{x\} = \{x,y\} \cap \{x,z\}$, on déduit que :

$$\begin{aligned} \{\sigma(x)\} &= \sigma(\{x\}) = \sigma(\{x,y\} \cap \{x,z\}) \\ &= \sigma(\{x,y\}) \cap \sigma(\{x,z\}) = \{x,y\} \cap \{x,z\} = \{x\} \end{aligned}$$

ce qui donne $\sigma(x) = x$. On a donc $\sigma = Id_E$. Le centre de $\mathcal{S}(E)$ est donc réduit à $\{Id\}$. □

Ce théorème nous dit aussi que $\mathcal{S}(E)$ n'est pas commutatif pour $n \geq 3$.

2.2 Les groupes symétriques $\mathcal{S}_n$

Théorème 2.1.

Si E, F sont deux ensembles non vides et φ est une bijection de E sur F, les groupes $\mathcal{S}(E)$ et $\mathcal{S}(F)$ sont alors isomorphes.

Preuve. L'application $\psi : \sigma \in \mathcal{S}(E) \mapsto \varphi \circ \sigma \circ \varphi^{-1} \in \mathcal{S}(F)$ est un isomorphisme de groupes. En effet, pour $\sigma \in \mathcal{S}(E)$, $\psi(\sigma) \in \mathcal{S}(F)$ comme composée de bijections et pour σ_1, σ_2 dans $\mathcal{S}(E)$, on a :

$$\psi(\sigma_1 \circ \sigma_2) = \varphi \circ \sigma_1 \circ \sigma_2 \circ \varphi^{-1} = \left(\varphi \circ \sigma_1 \circ \varphi^{-1}\right) \circ \left(\varphi \circ \sigma_2 \circ \varphi^{-1}\right) = \psi(\sigma_1) \circ \psi(\sigma_2)$$

c'est-à-dire que ψ est un morphisme de groupes de $\mathcal{S}(E)$ dans $\mathcal{S}(F)$. Pour σ dans $\ker(\psi)$, on a $\varphi \circ \sigma \circ \varphi^{-1} = Id_F$ et $\sigma = \varphi^{-1} \circ Id_F \circ \varphi = Id_E$, donc ψ est injective. Pour $\sigma' \in \mathcal{S}(F)$, l'application $\sigma = \varphi^{-1} \circ \sigma' \circ \varphi$ est dans $\mathcal{S}(E)$ et on a $\psi(\sigma) = \sigma'$, donc ψ est surjective. □

Donc tout groupe de permutations d'un ensemble E à n éléments est isomorphe au groupe symétrique $\mathcal{S}_n$ des permutations de $\{1, 2, \cdots, n\}$.

Théorème 2.2.

Pour E de cardinal $n \geq 1$, on a $\operatorname{card}(\mathcal{S}(E)) = n!$

Preuve. Pour $n = 1$ c'est clair puisque $\mathcal{S}(E) = \{Id_E\}$. Supposons le résultat acquis pour les ensembles à $n-1 \geq 1$ éléments et soit $E = \{x_1, \cdots, x_n\}$ un ensemble à $n \geq 2$ éléments. On désigne par H le sous-ensemble de $\mathcal{S}(E)$ formé des permutations de E qui laissent stable x_n. On vérifie facilement H est un sous-groupe de $\mathcal{S}(E)$. En effet, on a $Id \in H$ et pour tous σ_1, σ_2 dans H, on a $\sigma_1\sigma_2^{-1}(x_n) = \sigma_1(x_n) = x_n$, donc $\sigma_1\sigma_2^{-1} \in H$ et H est un sous-groupe de $\mathcal{S}(E)$. L'application qui associe à $\sigma \in H$ sa restriction à $F = \{x_1, \cdots, x_{n-1}\}$ réalise alors un isomorphisme de H sur $\mathcal{S}(F)$. En désignant, pour tout entier k compris entre 1 et $n-1$, par τ_k la permutation $\tau_k = (x_k, x_n)$, on a $\mathcal{S}(E)/H = \{\tau_1 H, \cdots, \tau_{n-1}H, H\}$. En effet, pour tout $\sigma \in \mathcal{S}(E)$, il existe $k \in \{1, \cdots, n\}$ tel que $\sigma(x_n) = x_k$ et en notant $\tau_n = Id$, on a $\tau_k^{-1}\sigma(x_n) = \tau_k^{-1}(x_k) = x_n$, donc $\tau_k^{-1}\sigma \in H$ et $\sigma H = \tau_k H$. On a donc $\mathcal{S}(E)/H = \{\tau_1 H, \cdots, \tau_n H\}$ avec $\tau_j H \neq \tau_k H$ pour $k \neq j$ (pour $1 \leq k < j \leq n$, on a $\tau_k^{-1}\tau_j(x_n) = \tau_k(x_j) \neq x_n$, donc $\tau_k^{-1}\tau_j \notin H$). En utilisant l'hypothèse de récurrence, on en déduit que :

$$\begin{aligned}\operatorname{card}(\mathcal{S}(E)) &= \operatorname{card}(\mathcal{S}(E)/H)\operatorname{card}(H) = \operatorname{card}(\mathcal{S}(E)/H)\operatorname{card}(\mathcal{S}(F)) \\ &= n \cdot (n-1)! = n!\end{aligned}$$

□

On peut aussi montrer le théorème précédent en utilisant l'action naturelle de $\mathcal{S}(E)$ sur E (exercice 1.15).

2.3 Support et orbites d'une permutation

Définition 2.4. *Le support d'une permutation $\sigma \in \mathcal{S}(E)$ est le complémentaire dans E de l'ensemble de ses points fixes, soit l'ensemble :*

$$\operatorname{Supp}(\sigma) = \{x \in E \mid \sigma(x) \neq x\}$$

Le support d'un cycle $\sigma = (x_1, \cdots, x_r)$ est $\{x_1, \cdots, x_r\}$.

Théorème 2.3.

Soient σ, σ' dans $\mathcal{S}(E)$.

1. $\sigma(\operatorname{Supp}(\sigma)) = \operatorname{Supp}(\sigma)$.
2. $\operatorname{Supp}(\sigma) = \operatorname{Supp}(\sigma^{-1})$.
3. *Pour tout $r \in \mathbb{Z}$, on a* $\operatorname{Supp}(\sigma^r) \subset \operatorname{Supp}(\sigma)$.
4. *Si* $\operatorname{Supp}(\sigma) \cap \operatorname{Supp}(\sigma') = \emptyset$, *on a alors* $\sigma \circ \sigma' = \sigma' \circ \sigma$.

Preuve.

1. Soit $x \in \operatorname{Supp}(\sigma)$. De $\sigma(x) \neq x$ on déduit que $\sigma(\sigma(x)) \neq \sigma(x)$ (puisque σ est injective) et $\sigma(x) \in \operatorname{Supp}(\sigma)$. On a donc $\sigma(\operatorname{Supp}(\sigma)) \subset \operatorname{Supp}(\sigma)$ (dans

le cas où E est fini, on a l'égalité puisque ces ensembles ont le même nombre d'éléments). Comme σ est surjective, tout $x \in \text{Supp}(\sigma)$ s'écrit $x = \sigma(x')$ et $\sigma(x) = \sigma(\sigma(x')) \neq x = \sigma(x')$ nous impose $\sigma(x') \neq x'$, donc $x' \in \text{Supp}(\sigma)$ et $x \in \sigma(\text{Supp}(\sigma))$. On a donc $\text{Supp}(\sigma) \subset \sigma(\text{Supp}(\sigma))$ et l'égalité $\sigma(\text{Supp}(\sigma)) = \text{Supp}(\sigma)$.

2. De $\sigma(x) = x$ équivalent à $x = \sigma^{-1}(x)$, on déduit que $x \in \text{Supp}(\sigma)$ si, et seulement si, $x \in \text{Supp}\left(\sigma^{-1}\right)$ et donc $\text{Supp}(\sigma) = \text{Supp}\left(\sigma^{-1}\right)$.
3. L'égalité $\sigma(x) = x$ entraîne $\sigma^r(x) = x$ pour tout $r \in \mathbb{Z}$, donc $\sigma^r(x) \neq x$ entraîne $\sigma(x) \neq x$ et $\text{Supp}(\sigma^r) \subset \text{Supp}(\sigma)$.
4. Soient σ, σ' telles que $\text{Supp}(\sigma) \cap \text{Supp}(\sigma') = \emptyset$ et $x \in E$. Si $\sigma(x) = x = \sigma'(x)$, on a alors $\sigma' \circ \sigma(x) = \sigma'(x) = x = \sigma(x) = \sigma \circ \sigma'(x)$. Si $x \in \text{Supp}(\sigma)$, alors $x \notin \text{Supp}(\sigma')$ et $\sigma'(x) = x$, donc $\sigma \circ \sigma'(x) = \sigma(x)$. Mais on a aussi $\sigma(x) \in \text{Supp}(\sigma)$, donc $\sigma(x) \notin \text{Supp}(\sigma')$ et $\sigma' \circ \sigma(x) = \sigma(x) = \sigma \circ \sigma'(x)$. De manière analogue, on vérifie que $\sigma' \circ \sigma(x) = \sigma'(x) = \sigma \circ \sigma'(x)$ pour tout $x \in \text{Supp}(\sigma')$ (on permute les rôles de σ et σ'). On a donc $\sigma \circ \sigma' = \sigma' \circ \sigma$.

□

La réciproque du point **4.** est fausse (prendre $\sigma \neq Id_E$ et $\sigma' = \sigma^{-1}$).

Pour la suite de ce paragraphe et les suivants, E est fini de cardinal $n \geq 2$.

Soit $\sigma \in \mathcal{S}(E)$. On a une action naturelle du groupe cyclique $H = \langle\sigma\rangle$ sur E définie par $\left(\sigma^k, x\right) \mapsto \sigma^k \cdot x = \sigma^k(x)$. Les orbites (ou σ-orbites) pour cette action, sont les ensembles $H \cdot x = \{\gamma \cdot x \mid \gamma \in H\} = \left\{\sigma^k(x) \mid k \in \mathbb{Z}\right\}$, où x décrit E. On notera $Orb_\sigma(x)$ une telle orbite. On rappelle que ces orbites sont aussi les classes d'équivalence pour la relation d'équivalence définie sur E par :

$$(x \mathcal{R}_\sigma y) \Leftrightarrow \left(\exists k \in \mathbb{Z} \mid y = \sigma^k(x)\right)$$

et les orbites deux à deux distinctes forment une partition de E.

Une σ-orbite $Orb_\sigma(x)$ est réduite à un point si, et seulement si, $\sigma(x) = x$ et les orbites non réduites à un point forment une partition du support de σ.

Lemme 2.4 *Soient $\sigma \in \mathcal{S}(E) \setminus \{Id_E\}$ et O une σ-orbite de cardinal $r \geq 2$. Pour tout $x \in O$, r est le plus petit entier naturel non nul tel que $\sigma^r(x) = x$ et :*

$$O = Orb_\sigma(x) = \left\{x, \sigma(x), \cdots, \sigma^{r-1}(x)\right\}$$

Preuve. Comme $\sigma \neq Id_E$, il existe une orbite O non réduite à un point. Il existe $y \in E$ tel que $O = Orb_\sigma(y) = \left\{\sigma^k(y) \mid k \in \mathbb{Z}\right\}$. Si $x \in O$, il existe alors un entier k tel que $x = \sigma^k(y)$ et :

$$Orb_\sigma(x) = \left\{\sigma^j(x) \mid j \in \mathbb{Z}\right\} = \left\{\sigma^{j+k}(y) \mid j \in \mathbb{Z}\right\} = \left\{\sigma^i(y) \mid i \in \mathbb{Z}\right\} = O$$

Si $\sigma^k(x) \neq x$ pour tout $k \geq 1$, on a alors $\sigma^i(x) \neq \sigma^j(x)$ pour tous $i \neq j$ dans $\mathbb{Z}$ et O est infini, ce qui n'est pas. Il existe donc un plus petit entier naturel non nul s tel que $\sigma^s(x) = x$. Comme $O = Orb_\sigma(x)$ est de cardinal $r \geq 2$, elle n'est pas réduite à un point et $\sigma(x) \neq x$. On a donc $s \geq 2$. En utilisant le théorème de division euclidienne, tout entier $k \in \mathbb{Z}$ s'écrit $k = qs + j$ avec $q \in \mathbb{Z}$ et $0 \leq j \leq s-1$, ce qui donne $\sigma^k(x) = \sigma^j(x)$ et $O = \left\{x, \sigma(x), \cdots, \sigma^{s-1}(x)\right\}$. Avec $\sigma^i(x) \neq \sigma^j(x)$ pour tous $i \neq j$ dans $\{0, 1, \cdots, s-1\}$ (caractère minimal de s), on déduit que $\text{card}(O) = s$ et $s = r$. □

Théorème 2.4.

Une permutation $\sigma \in \mathcal{S}(E)$ est un cycle d'ordre $r \geq 2$ si, et seulement si, il n'y a qu'une seule σ-orbite non réduite à un point.

Preuve. On a déjà vu qu'un r-cycle a une seule orbite non réduite à un point. Réciproquement si σ a une seule orbite non réduite à un point :

$$O = \left\{x, \sigma(x), \cdots, \sigma^{r-1}(x)\right\} = \{x_1, x_2, \cdots, x_r\}$$

avec $r \geq 2$, on a alors :

$$\begin{cases} \sigma(x_k) = x_{k+1} \ (1 \leq k \leq r-1) \\ \sigma(x_r) = x_1 \\ \sigma(x) = x \text{ si } x \in E \setminus \{x_1, \cdots, x_r\} \end{cases}$$

et σ est le r-cycle $(x_1, x_2, \cdots, x_r)$. □

On déduit du résultat précédent qu'une permutation $\sigma \in \mathcal{S}(E)$ est un cycle d'ordre $r \geq 2$ si, et seulement si, il existe $x \in E$ tel que $\text{Supp}(\sigma) = Orb_\sigma(x)$.

La composée de deux cycles n'est pas un cycle en général. Par exemple pour $\sigma = (1,2,3,4)$ dans $\mathcal{S}_4$, on a $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ avec $Orb_{\sigma^2}(1) = \{1,3\}$ et $Orb_{\sigma^2}(2) = \{2,4\}$, donc σ^2 n'est pas un cycle.

2.4 Décomposition d'une permutation en produit de cycles

Comme précisé au paragraphe précédent, E est fini de cardinal $n \geq 2$. Pour toute permutation $\sigma \in \mathcal{S}(E)$, on note $\theta(\sigma)$ son ordre dans le groupe $\mathcal{S}(E)$.

Définition 2.5. *On dit que deux cycles σ et σ' dans $\mathcal{S}(E)$ sont disjoints, si leurs supports sont disjoints dans E.*

En utilisant le fait que les σ-orbites forment une partition de E et que chaque σ-orbite non réduite à un point permet de définir un cycle, on obtient le résultat suivant qui nous donne un premier système de générateurs de $\mathcal{S}(E)$.

Théorème 2.5.

Toute permutation $\sigma \in \mathcal{S}(E) \setminus \{Id_E\}$ se décompose en produit de cycles deux à deux disjoints (le groupe $\mathcal{S}(E)$ est engendré par les cycles). Cette décomposition est unique à l'ordre près. Si $\sigma = \gamma_1 \cdots \gamma_p$ est une telle décomposition, on a alors la partition $\text{Supp}(\sigma) = \bigcup_{k=1}^{p} \text{Supp}(\gamma_k)$ et $\theta(\sigma) = \text{ppcm}(\theta(\gamma_1), \cdots, \theta(\gamma_p))$.

Preuve. Soient $\sigma \in \mathcal{S}(E) \setminus \{Id_E\}$ et $O_1, \cdots, O_p, \cdots, O_r$ les σ-orbites deux à deux distinctes avec $r_k = \text{card}(O_k) \geq 2$ pour $k = 1, \cdots, p$ et $\text{card}(O_k) = 1$ pour $k = p+1, \cdots, r$ (s'il en existe). On a alors la partition $E = \bigcup_{k=1}^{r} O_k$.

Pour tout entier k compris entre 1 et r, on désigne par γ_k la permutation de E définie par :

$$\forall x \in E,\ \gamma_k(x) = \begin{cases} \sigma(x) \text{ si } x \in O_k \\ x \text{ si } x \notin O_k \end{cases}$$

(γ_k est bien une permutation de E car la restriction de σ à une orbite O_k est une permutation de O_k). Si O_k est réduite à un point, alors $\gamma_k = Id_E$, sinon γ_k est un r_k-cycle : en effet, pour $x \notin O_k$, on a $\gamma_k(x) = x$ et $Orb_{\gamma_k}(x) = \{x\}$ et pour $x \in O_k$, on a :

$$Orb_{\gamma_k}(x) = \left\{\gamma_k^j(x) \mid j \in \mathbb{Z}\right\} = \left\{\sigma^j(x) \mid j \in \mathbb{Z}\right\} = Orb_\sigma(x) = O_k$$

donc γ_k a bien une seule orbite non réduite à un point. On vérifie alors que $\sigma = \prod_{j=1}^{r} \gamma_j = \prod_{j=1}^{p} \gamma_j$. En effet, pour $x \in E$ il existe un unique indice k compris entre 1 et r tel que $x \in O_k$ et on a $\gamma_k(x) = \sigma(x)$, $\gamma_j(x) = x$ pour $j \neq k$ (puisque $x \notin O_j$) et tenant compte du fait que les γ_j commutent (leurs supports sont deux à deux disjoints), on en déduit que :

$$\left(\prod_{j=1}^{r} \gamma_j\right)(x) = \left(\gamma_k \prod_{\substack{j=1 \\ j \neq k}}^{r} \gamma_j\right)(x) = \gamma_k(x) = \sigma(x)$$

Il reste à montrer l'unicité, à l'ordre près, d'une telle décomposition. Soit $\sigma = \prod_{k=1}^{p'} \gamma'_k$ est une autre décomposition en cycles deux à deux disjoints. En notant $O'_1, \cdots, O'_{p'}$ les supports de ces cycles, pour $k \in \{1, \cdots, p'\}$ et $x \in O'_k$, on a $\sigma(x) = \gamma'_k(x)$ ($x \notin O'_j$ pour $j \neq k$ et les cycles commutent), donc $O'_k = Orb_{\gamma'_k}(x) = Orb_\sigma(x)$. Les orbites O'_k sont donc les orbites non réduites à un point de σ et $p' = p$. On a donc $O'_k = O_j$ pour un unique j compris entre 1 et p. Pour $x \in O'_k$, on a $\gamma'_k(x) = \sigma(x) = \gamma_j(x)$ et pour $x \notin O'_k$, $\gamma'_k(x) = x = \gamma_j(x)$, ce qui donne $\gamma'_k = \gamma_j$ et l'unicité de la décomposition à l'ordre près. La réunion $\bigcup_{k=1}^{p} \text{Supp}(\gamma_k)$ est la réunion des orbites O_k non réduites à un point, soit le support de σ. Notons $\mu = \text{ppcm}(\theta(\gamma_1), \cdots, \theta(\gamma_p))$. Comme les cycles γ_k commutent, on a $\sigma^k = \gamma_1^k \cdots \gamma_p^k$ pour tout entier naturel k et $\sigma^k = Id_E$ si, et seulement si, $\gamma_j^k = Id_E$ pour tout j compris entre 1 et p. En effet, il est clair que la condition est suffisante et si $\sigma^k = Id_E$, on a alors pour tout $x \in O_j$ ($O_1, \cdots, O_p$ sont toutes les σ-orbites) $\gamma_j^k(x) = \sigma^k(x) = x$ et aussi $\gamma_j^k(x) = x$ pour $x \notin O_j$, donc $\gamma_j^k = Id_E$. Il en résulte que l'ordre de σ est un multiple commun des ordres des σ_j et c'est un multiple de μ qui lui même est multiple de l'ordre de σ puisque $\sigma^\mu = Id_E$. D'où l'égalité. □

On convient que l'identité est produit de 0 cycle : $Id_E = \gamma^0$ pour tout cycle γ.

Comme l'ordre d'un cycle est égal à sa longueur, l'ordre de σ est aussi le ppcm des longueurs des cycles γ_j.

Pour $E = \{1, 2, \cdots, n\}$, une telle décomposition s'obtient en prenant, dans le cas où il n'est pas fixe, les images de 1 par $\sigma, \sigma^2, \cdots$, jusqu'au moment où on retombe sur 1 (l'orbite de 1), puis on recommence avec le plus petit entier dans $E \setminus Orb_\sigma(1)$ qui n'est pas fixe et ainsi de suite.

Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix}$, on a $\sigma(1) = 2$, $\sigma^2(1) = 3$, $\sigma^3(1) = 4$, $\sigma^4(1) = 5$, $\sigma^5(1) = 1$, ce qui donne le premier cycle $(1, 2, 3, 4, 5)$, puis $\sigma(6) = 7$, $\sigma^2(6) = 6$ et $\sigma(8) = 8$, donc $\sigma = (1, 2, 3, 4, 5)(6, 7)$.

2.5 Systèmes de générateurs de $\mathcal{S}(E)$

On a déjà vu que $\mathcal{S}(E)$ est engendré par les cycles.

Lemme 2.5 *Pour $2 \leq r \leq n$, tout r-cycle dans $\mathcal{S}(E)$ s'écrit comme produit de $r-1$ transpositions.*

Preuve. Résulte de $(x_1, x_2, \cdots, x_r) = (x_1, x_2)(x_2, x_3)\cdots(x_{r-1}, , x_r)$. □

Théorème 2.6.

Toute permutation $\sigma \in \mathcal{S}(E)$ se décompose en produit de transpositions (le groupe $\mathcal{S}(E)$ est engendré par les transpositions).

Preuve. On a $Id_E = \tau^2$ pour toute transposition et toute permutation σ dans $\mathcal{S}(E) \setminus \{Id_E\}$ est produit de cycles et un cycle est produit de transpositions. □

Dans la décomposition d'une permutation en produit de transpositions, il n'y a pas unicité et les transpositions ne commutent pas nécessairement. Par exemple, on a $(2, 3) = (1, 2)(1, 3)(1, 2)$ et $(1, 2)(2, 3) = (1, 2, 3) \neq (2, 3)(1, 2) = (3, 2, 1)$.

Exemple 2.1 *Pour* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} = (1, 2, 3, 4, 5)(6, 7)$, *on a* $\sigma = (1, 2)(2, 3)(3, 4)(4, 5)(6, 7)$.

Comme $\mathcal{S}(E)$ est isomorphe à $\mathcal{S}_n$, on se contente maintenant de décrire des générateurs de $\mathcal{S}_n$.

Lemme 2.6 *$\mathcal{S}_n$ est engendré par les $n-1$ transpositions $(1, k)$ où $2 \leq k \leq n$.*

Preuve. Soit (i, j) une transposition avec $1 \leq i \neq j \leq n$. Si $i = 1$ ou $j = 1$, il n'y a rien à faire ($(i, j) = (j, i)$) et pour $i \neq 1$, $j \neq 1$, on a :

$$(i, j) = (1, i)(1, j)(1, i)^{-1} = (1, i)(1, j)(1, i)$$

(lemme 2.2). Le résultat se déduit alors du fait que $\mathcal{S}_n$ est engendré par les transpositions. □

Il n'est pas possible d'enlever une de ces transpositions $(1,k)$ du fait que pour $2 \leq k \leq n$ et $2 \leq j \neq k \leq n$, toutes les transposition $(1,j)$ laissent fixe k.

Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} = (1,2)(2,3)(3,4)(4,5)(6,7)$, on a :

$$\begin{aligned} \sigma &= (1,2)(1,2)(1,3)(1,2)(1,3)(1,4)(1,3)(1,4)(1,5)(1,4)(1,6)(1,7)(1,6) \\ &= (1,3)(1,2)(1,3)(1,4)(1,3)(1,4)(1,5)(1,4)(1,6)(1,7)(1,6) \end{aligned}$$

Lemme 2.7 *$\mathcal{S}_n$ est engendré par les $n-1$ transpositions $(k,k+1)$ où k est compris entre 1 et $n-1$.*

Preuve. Comme $\mathcal{S}_n$ est engendré par les transpositions $(1,k)$ où $2 \leq k \leq n$, il suffit d'écrire chaque transposition $(1,k)$ comme produit de transpositions du type $(i,i+1)$. Pour $3 \leq k \leq n$, on a :

$$(1,k) = (k-1,k)(1,k-1)(k-1,k)^{-1} = (k-1,k)(1,k-1)(k-1,k)$$

(encore le lemme 2.2). Pour $k=3$, on a $(1,k-1) = (1,2)$ et c'est terminé, sinon on écrit $(1,k-1) = (k-2,k-1)(1,k-2)(k-2,k-1)$ et on continue ainsi de suite si nécessaire. Pour $k=2$, la transposition $(1,k) = (1,2)$ est de la forme souhaitée. □

Il n'est pas possible d'enlever une de ces transpositions $(k,k+1)$ du fait que pour $1 \leq k \leq n-1$ et $1 \leq j \neq k \leq n-1$, toutes les transposition $(j,j+1)$ laissent globalement invariant la partie $\{1,\cdots,k\}$.

Lemme 2.8 *$\mathcal{S}_n$ est engendré par $(1,2)$ et $(1,2,\cdots,n)$.*

Preuve. Comme $\mathcal{S}_n$ est engendré par les transpositions $(k,k+1)$ où k est compris entre 1 et $n-1$, il suffit de montrer que chaque transposition $(k,k+1)$ est dans le sous-groupe G de $\mathcal{S}_n$ engendré par $\tau = (1,2)$ et $\gamma = (1,2,\cdots,n)$. On a déjà $(1,2) \in G$ et, pour $n \geq 3$:

$$\begin{cases} \gamma(1,2)\gamma^{-1} = (\gamma(1),\gamma(2)) = (2,3) \\ \gamma(2,3)\gamma^{-1} = (\gamma(2),\gamma(3)) = (3,4) \\ \vdots \\ \gamma(n-2,n-1)\gamma^{-1} = (\gamma(n-2),\gamma(n-1)) = (n-1,n) \end{cases}$$

soit $(k,k+1) = \gamma^{k-1}(1,2)\left(\gamma^{k-1}\right)^{-1}$ pour $1 \leq k \leq n-1$. □

2.6 Signature d'une permutation

Pour toute permutation $\sigma \in \mathcal{S}(E)$, on note $\mu(\sigma)$ le nombre de σ-orbites distinctes.

Si $\sigma = \prod_{k=1}^{p} \sigma_k$ est la décomposition de σ en produit de cycles deux à deux disjoints, on a vu que p est le nombre de σ-orbites non réduites à un point et $\mu(\sigma) = p + \varphi(\sigma)$ où $\varphi(\sigma)$ est le nombre de points fixes de σ.

Définition 2.6. *La signature d'une permutation $\sigma \in \mathcal{S}(E)$ est l'élément $\varepsilon(\sigma)$ de $\{-1,1\}$ défini par $\varepsilon(\sigma) = (-1)^{n-\mu(\sigma)}$.*

Exemples 2.1

1. *L'identité a n orbites réduites à un point et $\varepsilon(Id_E) = 1$.*
2. *Si σ est un r-cycle, il a une orbite non réduite à un point et $n-r$ orbites réduites à un point, donc $\mu(\sigma) = n-r+1$ et $\varepsilon(\sigma) = (-1)^{r-1}$.*
3. *Si τ est une transposition, on a $\varepsilon(\sigma) = -1$.*

Lemme 2.9 *Pour toute permutation $\sigma \in \mathcal{S}(E)$ et toute transposition $\tau \in \mathcal{S}(E)$, on a $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$.*

Preuve. Soient $\tau = (x,y)$ une transposition dans $\mathcal{S}(E)$ avec $x \neq y$ et $\sigma' = \tau\sigma$. Si $\sigma = Id_E$, on a alors $\tau\sigma = \tau$ et $\varepsilon(\tau\sigma) = -1$. Pour $\sigma \neq Id_E$, on a la décomposition en produit de cycles deux à deux disjoints, $\sigma = \sigma_1 \cdots \sigma_p$, où les $O_k = \text{Supp}(\sigma_k)$, pour k compris entre 1 et p, sont toutes les orbites non réduites à un point.

Si $\{x,y\} \cap \bigcup_{k=1}^{p} O_k = \emptyset$, le nombre de points fixes de σ' est alors $\varphi(\sigma') = \varphi(\sigma) - 2$ et le nombre de σ'-orbites est $\mu(\sigma') = p + 1 + \varphi(\sigma) - 2 = \mu(\sigma) - 1$, ce qui donne $\varepsilon(\sigma') = -\varepsilon(\sigma)$.

Si $\{x,y\}$ est contenu dans l'une des σ-orbites O_k, comme les cycles σ_j commutent, on a $\sigma' = \tau\sigma_k \prod_{\substack{j=1 \\ j\neq k}}^{p} \sigma_j$ avec :

$$y \in O_k = Orb_\sigma(x) = \left\{x, \sigma(x), \cdots, \sigma^{r_k-1}(x)\right\} = \{x_1, \cdots, x_{r_k}\}$$

Il existe donc $j \in \{2, \cdots, r_k\}$ tel que $y = x_j$ et :

$$\tau\sigma_k = (x_1, x_j)(x_1, \cdots, x_j, \cdots, x_{r_k}) = (x_1, \cdots, x_{j-1})(x_j, \cdots, x_{r_k}) = \sigma'_k\sigma''_k$$

(pour $j = r_k$, $\sigma''_k = Id_E$), ce qui donne la décomposition en produit de cycles deux à deux disjoints, $\sigma' = \sigma'_k\sigma''_k \prod_{\substack{j=1 \\ j\neq k}}^{p} \sigma_j$. On a donc, $\mu(\sigma') = \mu(\sigma) + 1$ (pour $j = r_k$, le nombre de cycles est inchangé, mais x_{r_k} est un point fixe de plus) et $\varepsilon(\sigma') = -\varepsilon(\sigma)$.

Si x, y sont dans deux orbites distinctes, soit $\{x,y\} \cap O_k = \{x\}$, $\{x,y\} \cap O_j = \{y\}$ avec $j \neq k$, on a alors :

$$O_k = Orb_\sigma(x) = \left\{x, \sigma(x), \cdots, \sigma^{r_k-1}(x)\right\} = \{x_1, \cdots, x_{r_k}\}$$

et $O_j = Orb_\sigma(y) = \left\{y, \sigma(y), \cdots, \sigma^{r_j-1}(y)\right\} = \left\{y_1, \cdots, y_{r_j}\right\}$, donc :

$$\begin{aligned}
\tau\sigma_k\sigma_j &= (x_1, y_1)(x_1, \cdots, x_{r_k})\left(y_1, \cdots, y_{r_j}\right) = (y_1, x_1)(x_1, \cdots, x_{r_k})\left(y_1, \cdots, y_{r_j}\right) \\
&= (y_1, x_1, \cdots, x_{r_k})\left(y_1, \cdots, y_{r_j}\right) = (x_1, \cdots, x_{r_k}, y_1)\left(y_1, \cdots, y_{r_j}\right) \\
&= \left(x_1, \cdots, x_{r_k}, y_1, \cdots, y_{r_j}\right) = \sigma'_k
\end{aligned}$$

et la décomposition en produit de cycles deux à deux disjoints :

$$\sigma' = \tau\sigma_k\sigma_j \prod_{\substack{i=1 \\ i\notin\{j,k\}}}^{p} \sigma_i = \sigma'_k \prod_{\substack{i=1 \\ i\notin\{j,k\}}}^{p} \sigma_i$$

On a donc, $\mu(\sigma') = \mu(\sigma) - 1$ et $\varepsilon(\sigma') = -\varepsilon(\sigma)$.

Enfin, la dernière possibilité est que x [resp. y] soit dans l'une des orbites O_k et y [resp. x] en dehors de la réunion de toutes les orbites. On a alors $\varphi(\sigma') = \varphi(\sigma)+1$ et $O_k = Orb_\sigma(x) = \left\{x, \sigma(x), \cdots, \sigma^{r_k-1}(x)\right\} = \{x_1, \cdots, x_{r_k}\}$, donc :

$$\tau\sigma_k = (x_1, y)(x_1, \cdots, x_{r_k}) = (y, x_1, \cdots, x_{r_k})$$

et $\mu(\sigma') = \mu(\sigma) + 1$, ce qui donne $\varepsilon(\sigma') = -\varepsilon(\sigma)$. □

On en déduit le théorème qui suit qui nous donne une définition équivalente de la signature d'une permutation.

Théorème 2.7.

Si $\sigma \in \mathcal{S}(E)$ est produit de p transpositions, on a alors $\varepsilon(\sigma) = (-1)^p$ (la parité de p est donc uniquement déterminée par σ).

Preuve. C'est une conséquence immédiate du lemme précédent et du fait que $\varepsilon(\tau) = -1$ pour toute transposition τ. □

Théorème 2.8.

Les seuls morphismes de groupes de $(\mathcal{S}(E), \circ)$ dans $(\mathbb{R}^*, \cdot)$ sont l'application constante égale à 1 et la signature ε. La signature étant surjective de $\mathcal{S}(E)$ sur $\{-1, 1\}$.

Preuve. Montrons tout d'abord que ε est un morphisme de groupes surjectif de $(\mathcal{S}(E), \circ)$ sur $\{-1, 1\}$.

On a vu que ε est à valeurs dans $\{-1, 1\}$ et avec $\varepsilon(Id_E) = 1$, $\varepsilon(\tau) = -1$ pour toute transposition τ (E a au moins deux éléments), on déduit que σ est surjectif.

Si σ, σ' sont deux permutations elles s'écrivent respectivement comme produit de p et q transpositions, ce qui permet d'écrire $\sigma\sigma'$ comme produit de $p+q$ transpositions et on a $\varepsilon(\sigma\sigma') = (-1)^{p+q} = \varepsilon(\sigma)\varepsilon(\sigma')$. Donc ε est un morphisme de groupes.

Soit φ un morphisme de groupe de $\mathcal{S}(E)$ dans $\mathbb{R}^*$. Si τ_1, τ_2 sont deux transpositions, il existe une permutation σ telle que $\tau_2 = \sigma\tau_1\sigma^{-1}$ (lemme 2.2) et comme le groupe multiplicatif $\mathbb{R}^*$ est commutatif, on a :

$$\varphi(\tau_2) = \varphi(\sigma)\varphi(\tau_1)\varphi(\sigma)^{-1} = \varphi(\sigma)\varphi(\sigma)^{-1}\varphi(\tau_1) = \varphi(\tau_1)$$

c'est-à-dire que φ est constant sur les transpositions. Avec $\varphi(Id_E) = \varphi\left(\tau^2\right) = (\varphi(\tau))^2$ pour toute transposition τ, on déduit que $\varphi(\tau) = 1$ pour toute transposition τ ou $\varphi(\tau) = -1$ pour toute transposition τ. Dans le premier cas, on a $\varphi(\sigma) = 1$ pour toute permutation σ puisque les transpositions engendrent $\mathcal{S}(E)$

et dans le second cas, comme toute permutation $\sigma \in \mathcal{S}(E)$ s'écrit $\sigma = \prod_{k=1}^{p} \tau_k$ où les τ_k sont des transpositions, on a $\varphi(\sigma) = \prod_{k=1}^{p} \varphi(\tau_k) = (-1)^p = \varepsilon(\sigma)$. □

Le résultat qui suit nous donne une autre définition de la signature d'une permutation $\sigma \in \mathcal{S}_n$.

Théorème 2.9.

Pour toute permutation $\sigma \in \mathcal{S}_n$, on a $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$.

Preuve. Soit φ l'application définie sur $\mathcal{S}_n$ par $\varphi(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$. Pour montrer que $\varphi = \varepsilon$, il suffit de montrer que φ est un morphisme de groupes non constant de $\mathcal{S}_n$ dans $\mathbb{R}^*$. Comme σ est bijective, on a $\varphi(\sigma) \in \mathbb{R}^*$ pour tout $\sigma \in \mathcal{S}_n$. Pour σ_1, σ_2 dans $\mathcal{S}_n$, on a :

$$\begin{aligned}
\varphi(\sigma_1\sigma_2) &= \prod_{1 \leq i < j \leq n} \frac{\sigma_1(\sigma_2(j)) - \sigma_1(\sigma_2(i))}{\sigma_2(j) - \sigma_2(i)} \frac{\sigma_2(j) - \sigma_2(i)}{j - i} \\
&= \prod_{1 \leq i < j \leq n} \frac{\sigma_1(\sigma_2(j)) - \sigma_1(\sigma_2(i))}{\sigma_2(j) - \sigma_2(i)} \prod_{1 \leq i < j \leq n} \frac{\sigma_2(j) - \sigma_2(i)}{j - i} \\
&= \prod_{1 \leq i' < j' \leq n} \frac{\sigma_1(j') - \sigma_1(i')}{j' - i'} \prod_{1 \leq i < j \leq n} \frac{\sigma_2(j) - \sigma_2(i)}{j - i}
\end{aligned}$$

puisque σ_2 est bijective de $\{1, \cdots, n\}$ sur $\{1, \cdots, n\}$, ce qui donne $\varphi(\sigma_1\sigma_2) = \varphi(\sigma_1)\varphi(\sigma_2)$. On a $\varphi(Id_E) = 1$ et pour $\tau = (1, 2)$:

$$\begin{aligned}
\varphi(\tau) &= \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} \frac{\tau(j) - \tau(i)}{j - i} \\
&= \prod_{j=2}^{n} \frac{\tau(j) - 2}{j - 1} \prod_{j=3}^{n} \frac{j - 1}{j - 2} = -\prod_{j=3}^{n} \frac{j - 2}{j - 1} \frac{j - 1}{j - 2} = -1
\end{aligned}$$

donc φ est non constant et c'est la signature. □

Du théorème précédent, on déduit que $\varepsilon(\sigma) = (-1)^{\nu(\sigma)}$, où :

$$\nu(\sigma) = \operatorname{card}\left\{(i, j) \in \mathbb{N}^2 \mid 1 \leq i < j \leq n \text{ et } \sigma(j) < \sigma(i)\right\}$$

est le nombre d'inversions de σ. Ce qui nous donne une définition supplémentaire de la signature.

Exemple 2.2 *Pour* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 2 & 3 & 4 & 7 & 6 & 8 \end{pmatrix}$, *on a* 5 *inversions, donc* $\varepsilon(\sigma) = (-1)^5 = -1$.

2.7 Le groupe alterné

Définition 2.7. *On dit qu'une permutation $\sigma \in \mathcal{S}(E)$ est paire [resp. est impaire] si $\varepsilon(\sigma) = 1$ [resp. $\varepsilon(\sigma) = -1$].*

Exemple 2.3 *Les cycles de longueur paire [resp. impaire] sont des permutations impaires [resp. paires].*

Définition 2.8. *Le groupe alterné est le sous-ensemble de $\mathcal{S}(E)$ formé des permutations paires. On le note $\mathcal{A}(E)$.*

Pour $E = \{1, 2, \cdots, n\}$, on note $\mathcal{A}_n$ le groupe alterné.

$\mathcal{A}(E)$ est un sous-groupe distingué de $\mathcal{S}(E)$ (c'est le noyau du morphisme ε), il est d'indice 2 ($\text{card}\left(\dfrac{\mathcal{S}(E)}{\mathcal{A}(E)}\right) = \text{card}\{-1, 1\} = 2$) et $\text{card}(\mathcal{A}(E)) = \dfrac{n!}{2}$.

Pour $n = 2$, on a $\mathcal{A}(E) = \{Id_E\}$.

$\mathcal{A}_3$ est cyclique engendré par $\gamma_1 = (1, 2, 3)$. En effet $\text{card}(\mathcal{A}_3) = \dfrac{3!}{2} = 3$ et le cycle γ_1 est d'ordre 3 dans $\mathcal{A}_3$.

On suppose, pour ce qui suit que $n \geq 3$.

Lemme 2.10 *Le produit de deux transpositions est un produit de 3-cycles. Précisément, pour x, y, z, t deux à distincts dans E, on a :*

$$(x, y)(x, z) = (x, z, y) \text{ et } (x, y)(z, t) = (x, y, z)(y, z, t).$$

Preuve. Soient τ_1 et τ_2 deux transpositions.

Si $\tau_1 = \tau_2$, on a alors $\tau_1\tau_2 = Id_E = \gamma^3$ pour n'importe quel 3-cycle. Si $\tau_1 \neq \tau_2$, on a alors deux possibilités. Soit $\text{Supp}(\tau_1) \cap \text{Supp}(\tau_2) = \{x\}$, donc $\tau_1 = (x, y)$, $\tau_2 = (x, z)$ avec x, y, z distincts et $\tau_1\tau_2 = (y, x)(x, z) = (y, x, z) = (x, z, y)$ (exercice 2.3), soit $\text{Supp}(\tau_1) \cap \text{Supp}(\tau_2) = \emptyset$, donc $\tau_1 = (x, y)$, $\tau_2 = (z, t)$ avec x, y, z, t distincts et $\tau_1\tau_2 = (x, y)(z, t) = (x, y)(y, z)(y, z)(z, t) = (x, y, z)(y, z, t)$. □

Théorème 2.10.

Pour $n \geq 3$, $\mathcal{A}(E)$ est engendré par les 3-cycles.

Preuve. Comme $\mathcal{S}(E)$ est engendré par les transpositions, on déduit du théorème 2.7 qu'une permutation paire est le produit d'un nombre pair de transpositions et le lemme qui précède nous dit que ce produit s'écrit comme produit de 3-cycles. □

Théorème 2.11.

Pour $n \geq 5$, les sous-groupes distingués de $\mathcal{S}(E)$ sont $\{Id\}$, $\mathcal{A}(E)$ et $\mathcal{S}(E)$.

Preuve. Soit H un sous-groupe distingué non trivial de $\mathcal{S}(E)$ (*i.e.* distinct de $\{Id\}$ et de $\mathcal{S}(E)$). Pour montrer que $H = \mathcal{A}(E)$, il suffit de montrer que H contient

un 3-cycle (il les contient alors tous puisqu'ils sont conjugués dans $\mathcal{S}(E)$, donc $\mathcal{A}(E) \subset H$ et $H = \mathcal{A}(E)$ puisque les 3-cycles engendrent $\mathcal{A}(E)$ et $H \neq \mathcal{S}(E)$: en effet, on a $\mathcal{A}(E) \subset H \subset \mathcal{S}(E)$, donc $\text{card}(H) = p\frac{n!}{2} = p\frac{q\,\text{card}(H)}{2}$ et $pq = 2$, soit $p = 1$ et $H = \mathcal{A}(E)$ ou $p = 2$ et $H = \mathcal{S}(E)$).

Soient $\sigma \in H \setminus \{Id\}$ et $\tau = (x, y)$ une transposition ne commutant pas à σ (exercice 2.3). H étant distingué dans $\mathcal{S}(E)$, on a $\sigma' = \tau\sigma\tau\sigma^{-1} = \left(\tau\sigma\tau^{-1}\right)\sigma^{-1}$ qui est dans H et en écrivant que $\sigma' = (x, y)\left(\sigma(x, y)\,\sigma^{-1}\right) = (x, y)\,(\sigma(x), \sigma(y))$, on voit que σ' est produit de deux transpositions. L'égalité $\sigma' = Id$ est réalisée si, et seulement si, $\tau\sigma\tau\sigma^{-1} = Id$, soit $\tau\sigma = \sigma\tau^{-1} = \sigma\tau$, ce qui n'est pas. Si $\{x, y\} \cap \{\sigma(x), \sigma(y)\}$ est réduit à un point, alors σ' est un 3-cycle et dans ce cas $H = \mathcal{A}(E)$, sinon cette intersection est vide et en prenant z dans $E \setminus \{x, y, \sigma(x), \sigma(y)\}$ (on a $n \geq 5$), le groupe H contient $(x, y)\,(\sigma(x), z)$ puisque le produit de deux transpositions de supports disjoints sont conjugués dans $\mathcal{S}(E)$ et H est distingué. Il en résulte que H contient :

$$(x, y)\,(\sigma(x), \sigma(y))\,(x, y)\,(\sigma(x), z) = (\sigma(x), \sigma(y))\,(\sigma(x), z)$$

qui est le 3-cycle $(\sigma(y), \sigma(x), z)$. □

En utilisant les groupes de Sylow, on peut montrer qu'un groupe simple d'ordre 60 est isomorphe à $\mathcal{A}_5$. Plus généralement, on a le résultat suivant.

Théorème 2.12.

Pour $n = 3$ ou $n \geq 5$ le groupe $\mathcal{A}(E)$ est simple (i.e. n'a pas de sous-groupes distingués autres que lui même et $\{Id\}$).

Preuve. Pour $n = 3$, $\mathcal{A}(E)$ est cyclique d'ordre 3 et n'a pas de sous-groupe trivial. On suppose $n \geq 5$ et on se donne un sous-groupe distingué H de $\mathcal{A}(E)$ distinct de $\{Id\}$. Pour montrer que $H = \mathcal{A}(E)$, il suffit de montrer que H contient un 3-cycle puisqu'ils sont tous conjugués dans $\mathcal{A}(E)$ et l'engendrent. On se donne $\sigma \in H \setminus \{Id\}$ et $\gamma = (x, z, y) \in \mathcal{A}(E)$ un 3-cycle avec $y = \sigma(x)$ qui ne commute pas à σ (voir l'exercice 2.23). Comme H est un sous-groupe distingué de $\mathcal{A}(E)$, on a $\sigma' = \sigma\gamma\sigma^{-1}\gamma^{-1} = \sigma\left(\gamma\sigma^{-1}\gamma^{-1}\right) \in H$ et en écrivant que :

$$\begin{aligned}\sigma' &= \left(\sigma(x, z, y)\,\sigma^{-1}\right)(y, z, x) = (\sigma(x), \sigma(z), \sigma(y))\,(y, z, x)\\ &= (y, \sigma(z), \sigma(y))\,(y, z, x)\end{aligned}$$

on voit que σ' est produit de deux 3-cycles qui agissent sur $F = \{x, y, z, \sigma(y), \sigma(z)\}$ formé d'au plus 5 éléments (tous les points de $E \setminus F$ sont fixes). L'égalité $\sigma' = Id$ est réalisée si, et seulement si, $\sigma\gamma\sigma^{-1}\gamma^{-1} = Id$, soit $\tau\sigma = \gamma\sigma$, ce qui n'est pas, donc $\sigma' \neq Id$. Dans $\mathcal{S}(F)$ la permutation σ' s'écrit comme produit de cycles de supports disjoints, cette décomposition étant celle de $\mathcal{S}(E)$ et comme $\sigma' \in \mathcal{A}(E)$, il n'y a que trois possibilités : σ' est soit un 3-cycle, soit un produit de deux transpositions de supports disjoints, soit un 5-cycle. Dans le premier cas c'est terminé, dans le second on a $\sigma' = (x_1, x_2)\,(x_3, x_4)$ et, choisissant $x_5 \in E \setminus \{x_1, x_2, x_3, x_4\}$, en notant $\tau = (x_1, x_2, x_5) \in \mathcal{A}(E)$, on vérifie que le commutateur $\sigma'' = [\sigma', \tau] = \sigma'\left(\tau\left(\sigma'\right)^{-1}\tau^{-1}\right)$ qui est dans H est un 3-cycle et

c'est terminé. En effet, on a :

$$\begin{aligned}\sigma'' &= \left(\sigma'\tau\left(\sigma'\right)^{-1}\right)\tau^{-1} = \left(\sigma'\left(x_1\right),\sigma'\left(x_2\right),\sigma'\left(x_5\right)\right)\left(x_5,x_2,x_1\right)\\ &= \left(x_2,x_1,x_5\right)\left(x_5,x_2,x_1\right) = \left(x_2,x_5,x_1\right)\end{aligned}$$

Dans le troisième cas, on a $\sigma' = (x_1,x_2,x_3,x_4,x_5)$ et, en notant $\tau = (x_1,x_2,x_3) \in \mathcal{A}(E)$, on vérifie que le commutateur $\sigma'' = [\sigma',\tau]$ qui est dans H est un 3-cycle et c'est terminé. En effet, on a :

$$\begin{aligned}\sigma'' &= \left(\sigma'\tau\left(\sigma'\right)^{-1}\right)\tau^{-1} = \left(\sigma'\left(x_1\right),\sigma'\left(x_2\right),\sigma'\left(x_3\right)\right)\left(x_3,x_2,x_1\right)\\ &= \left(x_2,x_3,x_4\right)\left(x_3,x_2,x_1\right) = \left(x_1,x_4,x_2\right)\end{aligned}$$

□

2.8 Quelques exemples d'utilisation du groupe symétrique

2.8.1 Dérangements d'un ensemble fini

On note $I_n = \{1,2,\cdots,n\}$ pour tout entier $n \geq 2$.

Définition 2.9. *On appelle dérangement de I_n toute permutation σ de cet ensemble n'ayant aucun point fixe (i.e. telle que $\sigma(i) \neq i$ pour tout $i \in I_n$).*

Pour tout entier naturel non nul p, on note δ_p le nombre de dérangements de I_p. On a $\delta_1 = 0$ et, par convention, on pose $\delta_0 = 1$.

Lemme 2.11 (Formule d'inversion de Pascal) *Si $(f_n)_{n\in\mathbb{N}}$ et $(g_n)_{n\in\mathbb{N}}$ sont deux suites réelles telles que $f_n = \sum_{k=0}^{n}\binom{n}{k}g_k$ pour tout $n \in \mathbb{N}$, on a alors*

$$\forall n \in \mathbb{N},\ g_n = \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}f_k$$

Preuve. On peut montrer cette formule en utilisant un argument d'algèbre linéaire. Pour $n = 0$, c'est clair. En supposant $n \geq 1$, on note F et G les vecteurs de $\mathbb{R}^{n+1}$ définis par $F = (f_k)_{0\leq k\leq n}$, $G = (g_k)_{0\leq k\leq n}$ et on a $F = PG$, où P est la matrice carrée d'ordre $n+1$:

$$P = \begin{pmatrix} \binom{0}{0} & 0 & \cdots & \cdots & 0\\ \binom{1}{0} & \binom{1}{1} & 0 & \cdots & 0\\ \binom{2}{0} & \binom{2}{1} & \binom{2}{2} & \ddots & 0\\ \vdots & \vdots & \ddots & \ddots & 0\\ \binom{n}{0} & \binom{n}{1} & \cdots & \binom{n}{n-1} & \binom{n}{n} \end{pmatrix}$$

(matrice de Pascal). Cette matrice P est inversible (on a $\det P) = 1$) et il s'agit alors de calculer son inverse.

En écrivant, pour $0 \leq k \leq n$, l'égalité $(1+X)^k = \sum_{j=0}^{k} \binom{k}{j} X^j$ dans $\mathbb{R}_n[X]$, on remarque que $P = {}^tQ$, où $Q = \begin{pmatrix} \binom{0}{0} & \binom{1}{0} & \binom{2}{0} & \cdots & \binom{n}{0} \\ 0 & \binom{1}{1} & \binom{2}{1} & \cdots & \binom{n}{1} \\ 0 & 0 & \binom{2}{2} & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \binom{n}{n-1} \\ 0 & 0 & \cdots & 0 & \binom{n}{n} \end{pmatrix}$ est la matrice de passage de la base canonique $\left(X^k\right)_{0\leq k\leq n}$ de $\mathbb{R}_n[X]$ à la base $\left((1+X)^k\right)_{0\leq k\leq n}$. La matrice Q est inversible et son inverse est la matrice de passage de la base $\left((1+X)^k\right)_{0\leq k\leq n}$ à $\left(X^k\right)_{0\leq k\leq n}$, qui s'obtient avec :

$$X^k = (1+X-1)^k = \sum_{j=0}^{k} \binom{k}{j} (1+X)^j (-1)^{k-j}$$

On a donc $Q^{-1} = \begin{pmatrix} \binom{0}{0} & -\binom{1}{0} & \binom{2}{0} & \cdots & (-1)^n \binom{n}{0} \\ 0 & \binom{1}{1} & -\binom{2}{1} & \cdots & (-1)^{n-1} \binom{n}{1} \\ 0 & 0 & \binom{2}{2} & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & (-1)\binom{n}{n-1} \\ 0 & 0 & \cdots & 0 & \binom{n}{n} \end{pmatrix}$ et :

$$P^{-1} = {}^tQ^{-1} = \begin{pmatrix} \binom{0}{0} & 0 & \cdots & \cdots & 0 \\ -\binom{1}{0} & \binom{1}{1} & 0 & \cdots & 0 \\ \binom{2}{0} & -\binom{2}{1} & \binom{2}{2} & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & 0 \\ (-1)^n \binom{n}{0} & (-1)^{n-1} \binom{n}{1} & \cdots & (-1)\binom{n}{n-1} & \binom{n}{n} \end{pmatrix}$$

L'égalité $G = P^{-1}F$ nous donne alors $g_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f_k$. □

Lemme 2.12 *On a :*

$$\forall n \in \mathbb{N},\ n! = \sum_{k=0}^{n} \binom{n}{k} \delta_k \tag{2.1}$$

Preuve. Pour $n = 0$ c'est clair vu les conventions $0! = \delta_0 = 1$. Pour $n \geq 1$, on a la partition $\mathcal{S}_n = \bigcup_{k=0}^{n} \mathcal{S}_{n,k}$, où $\mathcal{S}_{n,k}$ est le sous-ensemble de $\mathcal{S}_n$ formé des permutations de I_n qui ont exactement k points fixes (pour $k = n$, on a $\mathcal{S}_{n,n} = \{Id\}$ et pour $k = n-1$, on a $\mathcal{S}_{n,n-1} = \emptyset$ puisqu'une permutation qui a $n-1$ points fixes en a

obligatoirement n, il n'en n'existe donc pas qui ont exactement $n-1$ points fixes). Il en résulte que $n! = \operatorname{card}(\mathcal{S}_n) = \sum_{k=0}^{n} \operatorname{card}(\mathcal{S}_{n,k})$.

En choisissant un ensemble de k points fixes dans I_n, il y a δ_{n-k} dérangements possibles pour les $n-k$ points restants et comme il y a $\binom{n}{k}$ façons de choisir ces k points fixes, on déduit que $\operatorname{card}(\mathcal{S}_{n,k}) = \binom{n}{k}\delta_{n-k}$ (on a bien $\operatorname{card}(\mathcal{S}_{n,n-1}) = 0$ puisque $\delta_1 = 0$ et la convention $\delta_0 = 1$ est justifiée par $\operatorname{card}(\mathcal{S}_{n,n}) = 1$) donc :

$$n! = \sum_{k=0}^{n} \binom{n}{k}\delta_{n-k} = \sum_{k=0}^{n} \binom{n}{n-k}\delta_k = \sum_{k=0}^{n} \binom{n}{k}\delta_k$$

□

Théorème 2.13.

Pour tout $n \in \mathbb{N}$, le nombre de dérangements de I_n est $\delta_n = n!\sum_{k=0}^{n} \frac{(-1)^k}{k!}$.

Preuve. En utilisant la formule d'inversion de Pascal, on déduit du lemme précédent que $\delta_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k! = n!\sum_{k=0}^{n} \frac{(-1)^k}{k!}$. □

Corollaire 2.1. *Pour tout $n \in \mathbb{N}$, le nombre de permutations de I_n ayant exactement r points fixes, pour $0 \leq r \leq n$, est $\binom{n}{r}\delta_{n-r} = \frac{n!}{r!}\sum_{k=0}^{n-r} \frac{(-1)^k}{k!}$.*

Preuve. Pour un ensemble de r points fixes choisi il y a δ_{n-r} dérangements des autres points et on peut choisir ces points fixes de $\binom{n}{r}$ façons. □

2.8.2 Le théorème de Cayley

Théorème 2.14. Cayley

Tout groupe G est isomorphe à un sous-groupe de $\mathcal{S}(G)$.

Preuve. Soit G un groupe. Pour tout $g \in G$, l'application $\varphi(g) : h \mapsto g \cdot h$ est dans $\mathcal{S}(G)$. En effet, pour tout $k \in G$, l'équation $g \cdot h = k$ a une unique solution donnée par $h = g^{-1}k$, ce qui signifie que $\varphi(g)$ est une bijection de G sur lui même. Avec $\varphi(gg')(h) = gg'h = \varphi(g)(\varphi(g')(h)) = \varphi(g) \circ \varphi(g')(h)$ pour tous g, g', h dans G, on déduit que $\varphi(gg') = \varphi(g) \circ \varphi(g')$ pour tous g, g' dans G, ce qui signifie que φ est un morphisme de groupes. Enfin, si $g \in \ker(\varphi)$, on a $g \cdot h = h$ pour tout $h \in G$ et $g = 1$, donc φ est injectif et réalise un isomorphisme de G sur $\operatorname{Im}(\varphi)$ qui est un sous-groupe de $\mathcal{S}(G)$. □

2.8.3 Matrices de permutation

On désigne par $\mathbb{K}$ un corps commutatif et à toute permutation $\sigma \in \mathcal{S}_n$, on associe la matrice de passage P_σ de la base canonique $\mathcal{B} = (e_j)_{1\leq j\leq n}$ de $\mathbb{K}^n$ à la base $\mathcal{B}_\sigma = \left(e_{\sigma(j)}\right)_{1\leq j\leq n}$. On dit que P_σ est la matrice de permutation associée à σ. On peut remarquer que $P_\sigma e_j = e_{\sigma(j)}$ pour tout j compris entre 1 et n et en conséquence, pour tout vecteur $x = (x_i)_{1\leq i\leq n}$, on a $P_\sigma x = \left(x_{\sigma^{-1}(i)}\right)_{1\leq i\leq n}$. En effet, en écrivant que $x = \sum_{j=1}^{n} x_j e_j$, on a $P_\sigma x = \sum_{j=1}^{n} x_j P_\sigma e_j = \sum_{j=1}^{n} x_j e_{\sigma(j)}$et le changement d'indice $k = \sigma(j)$ (σ est bijective), donne $P_\sigma x = \sum_{k=1}^{n} x_{\sigma^{-1}(k)} e_k$.

Théorème 2.15.

L'application $P : \sigma \mapsto P_\sigma$ est un morphisme de groupes injectif de $\mathcal{S}_n$ dans $GL_n(\mathbb{K})$ et pour toute permutation $\sigma \in \mathcal{S}_n$, on a $\det(P_\sigma) = \varepsilon(\sigma)$.

Preuve. On a bien $P_\sigma \in GL_n(\mathbb{K})$ pour toute permutation $\sigma \in \mathcal{S}_n$. Pour σ, σ' dans $\mathcal{S}_n$ et $1 \leq j \leq n$, on a $P_\sigma(P_{\sigma'} e_j) = P_\sigma e_{\sigma'(j)} = e_{\sigma(\sigma'(j))} = e_{\sigma\sigma'(j)} = P_{\sigma\sigma'} e_j$, donc $P_\sigma P_{\sigma'} = P_{\sigma\sigma'}$ et P est un morphisme de groupes.

Si $\sigma \in \ker(P)$, on a $P_\sigma = I_n$ et $e_j = e_{\sigma(j)}$ pour tout j, ce qui revient à dire que $j = \sigma(j)$ pour tout j et donc que $\sigma = Id$. Le morphisme P est donc injectif.

Si τ est une transposition, la matrice P_τ est déduite de I_n en permutant deux colonnes et utilisant les propriétés du déterminant (qui peut se définir avec les opérations élémentaires et sans référence au groupe symétrique), on en déduit que $\det(P_\tau) = -\det(I_n) = -1$ (sous-entendu $-1_\mathbb{K}$). En écrivant $\sigma \in \mathcal{S}_n$ comme produit de p transpositions et en utilisant le fait que P est un morphisme de groupes, on en déduit que $\det(P_\sigma) = (-1)^p = \varepsilon(\sigma)$ (sous-entendu $\varepsilon(\sigma)\,1_\mathbb{K}$). □

Prenant $\mathbb{K} = \mathbb{R}$, le résultat précédent nous donne une définition équivalent de la signature, dans la mesure où on a défini le déterminant d'une matrice carrée sans référence au groupe symétrique.

Corollaire 2.2. *Tout groupe fini d'ordre $n \geq 1$ est isomorphe à un sous-groupe de $GL_n(\mathbb{F}_p)$ où $\mathbb{F}_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ et $p \geq 2$ est un nombre premier.*

Preuve. Le théorème de Cayley (théorème 5.1) nous dit que G est isomorphe à un sous-groupe de $\mathcal{S}_n$ (qui est isomorphe à $\mathcal{S}(G)$ pour G d'ordre n) et le théorème précédent que $\mathcal{S}_n$ est isomorphe à un sous-groupe de $GL_n(\mathbb{F}_p)$. Il en résulte que G est isomorphe à un sous-groupe de $GL_n(\mathbb{F}_p)$. □

2.8.4 Isométries laissant une partie invariante

Voir le paragraphe 3.4

2.8.5 Polynômes symétriques

$\mathbb{K}$ est un corps commutatif de caractéristique différente de 2.

Un polynôme $P = \sum a_{i_1,\cdots,i_n} X_1^{i_1} \cdots X_n^{i_n} \in \mathbb{K}[X_1, \cdots, X_n]$ est dit de degré égal à d si $a_{i_1,\cdots,i_n} = 0$ pour toute liste $(i_1, \cdots, i_n) \in \{1, \cdots, n\}^n$ telle que $\sum_{k=1}^{n} i_k > d$ et s'il existe une liste $(i_1, \cdots, i_n)$ telle que $\sum_{k=1}^{n} i_k = d$ et $a_{i_1,\cdots,i_n} \neq 0$.

Définition 2.10. *On dit qu'un polynôme $P \in \mathbb{K}[X_1, \cdots, X_n]$ est symétrique si $P\left(X_{\sigma(1)}, \cdots, X_{\sigma(n)}\right) = P(X_1, \cdots, X_n)$ pour toute permutation $\sigma \in \mathcal{S}_n$.*

Les polynômes $\Sigma_{k,n} = \sum_{1 \leq i_1 < \cdots < i_k \leq n} X_{i_1} \cdots X_{i_k}$, où k est compris entre 1 et n, sont les polynômes symétriques élémentaires.

On a $\Sigma_{1,n} = \sum_{i=1}^{n} X_i$, $\Sigma_{2,n} = \sum_{1 \leq i < j \leq n} X_i X_j, \cdots, \Sigma_{n,n} = X_1 \cdots X_n$ et :

$$\Sigma_{k,n}(X_1, \cdots, X_{n-1}, 0) = \Sigma_{k,n-1}(X_1, \cdots, X_{n-1}) \ (1 \leq k \leq n-1) \tag{2.2}$$

Théorème 2.16.

Si $P \in \mathbb{K}[X_1, \cdots, X_n]$ est symétrique, il existe alors un unique polynôme $Q \in \mathbb{K}[X_1, \cdots, X_n]$ tel que $P(X_1, \cdots, X_n) = Q(\Sigma_{1,n}, \cdots, \Sigma_{n,n})$.

Preuve. L'existence se montre par une double récurrence sur $n \geq 1$ et sur le degré $d \geq 0$ de $P \in \mathbb{K}[X_1, \cdots, X_n]$. Pour $n = 1$, on a $\Sigma_{1,1} = X_1$ et le résultat est acquis pour tous les degrés avec $Q = P$. Supposons le résultat acquis pour $n - 1 \geq 1$. Si $P \in \mathbb{K}[X_1, \cdots, X_n]$ est un polynôme constant, le polynôme $Q = P$ convient. Supposons que le résultat soit acquis pour tous les polynômes symétriques dans $\mathbb{K}[X_1, \cdots, X_n]$ de degré au plus égal à $d-1$ avec $d \geq 1$ et soit $P \in \mathbb{K}[X_1, \cdots, X_n]$ symétrique de degré d. Le polynôme $P(X_1, \cdots, X_{n-1}, 0)$ étant symétrique dans $\mathbb{K}[X_1, \cdots, X_{n-1}]$, il existe $Q_1 \in \mathbb{K}[X_1, \cdots, X_{n-1}]$ tel que :

$$\begin{aligned} P(X_1, \cdots, X_{n-1}, 0) &= Q_1(\Sigma_{1,n-1}, \cdots, \Sigma_{n-1,n-1}) \\ &= Q_1(\Sigma_{1,n}(X_1, \cdots, X_{n-1}, 0), \cdots, \Sigma_{n-1,n}(X_1, \cdots, X_{n-1}, 0)) \end{aligned}$$

Le polynôme $P_1(X_1, \cdots, X_n) = P(X_1, \cdots, X_n) - Q_1(\Sigma_{1,n}, \cdots, \Sigma_{n-1,n})$ est, comme le polynôme P, symétrique de degré inférieur ou égal à d dans $\mathbb{K}[X_1, \cdots, X_n]$. Comme $P_1(X_1, \cdots, X_{n-1}, 0) = 0$, on a $P_1 = \sum a_{i_1,\cdots,i_n} X_1^{i_1} \cdots X_{n-1}^{i_{n-1}} X_n^{i_n}$ où les coefficients $a_{i_1,\cdots,i_n}$ sont non nuls et les exposants i_n qui apparaissent dans cette écriture sont tous non nuls. En notant τ_k la transposition (k, n), pour $1 \leq k \leq n-1$, on a :

$$\begin{aligned} P_1\left(X_{\tau_k(1)}, \cdots, X_{\tau_k(n)}\right) &= P_1(X_1, \cdots, X_{k-1}, X_n, X_{k+1}, \cdots, X_{n-1}, X_k) \\ &= P_1(X_1, \cdots, X_n) \end{aligned}$$

et $X_n = 0$ donne $P_1(X_1, \cdots, X_{k-1}, 0, X_{k+1}, \cdots, X_{n-1}, X_k) = 0$, donc les exposants i_k, pour k compris entre 1 et n, sont tous non nuls et on a :

$$P_1 = \left(\sum a_{i_1,\cdots,i_n} X_1^{i_1-1} \cdots X_n^{i_n-1}\right) X_1 \cdots X_n = P_2 \Sigma_{n,n}$$

Pour toute permutation $\sigma \in \mathcal{S}_n$, on a :

$$\begin{aligned} P_2(X_1, \cdots, X_n)\Sigma_{n,n} &= P_1(X_1, \cdots, X_n) = P_1\left(X_{\sigma(1)}, \cdots, X_{\sigma(n)}\right) \\ &= P_2\left(X_{\sigma(1)}, \cdots, X_{\sigma(n)}\right)\Sigma_{n,n} \end{aligned}$$

ce qui entraîne que $P_2\left(X_{\sigma(1)}, \cdots, X_{\sigma(n)}\right) = P_2(X_1, \cdots, X_n)$ puisque l'anneau $\mathbb{K}[X_1, \cdots, X_n]$ est intègre. Le polynôme P_2 est donc symétrique de degré strictement inférieur à d. L'hypothèse de récurrence (sur d) nous assure de l'existence d'un polynôme $Q_2 \in \mathbb{K}[X_1, \cdots, X_n]$ tel que $P_2(X_1, \cdots, X_n) = Q_2(\Sigma_{1,n}, \cdots, \Sigma_{n,n})$ et finalement :

$$\begin{aligned} P(X_1, \cdots, X_n) &= P_1(X_1, \cdots, X_n) + Q_1(\Sigma_{1,n}, \cdots, \Sigma_{n-1,n}) \\ &= Q_2(\Sigma_{1,n}, \cdots, \Sigma_{n,n})\Sigma_{n,n} + Q_1(\Sigma_{1,n}, \cdots, \Sigma_{n-1,n}) \\ &= Q(\Sigma_{1,n}, \cdots, \Sigma_{n,n}) \end{aligned}$$

où $Q \in \mathbb{K}[X_1, \cdots, X_n]$.

Montrer l'unicité d'un tel polynôme Q est équivalent à montrer que l'égalité $Q(\Sigma_{1,n}, \cdots, \Sigma_{n,n}) = 0$ est uniquement réalisée pour le polynôme nul. Pour ce faire, on raisonne par récurrence sur $n \geq 1$. Pour $n = 1$, c'est clair puisque $\Sigma_{1,1} = X_1$. Supposons le résultat acquis pour $n - 1 \geq 1$ et raisonnons par récurrence sur le degré d de $Q(\Sigma_{1,n}, \cdots, \Sigma_{n,n})$. Pour Q constant c'est clair. En supposant le résultat acquis pour les polynômes à n variables de degré au plus égal à $d - 1 \geq 0$, on se donne $Q \in \mathbb{K}[X_1, \cdots, X_n]$ de degré d tel que $Q(\Sigma_{1,n}, \cdots, \Sigma_{n,n}) = 0$. La division euclidienne dans $\mathbb{K}[X_1, \cdots, X_{n-1}][X_n]$ de Q par X_n s'écrit :

$$Q(X_1, \cdots, X_n) = S(X_1, \cdots, X_n)X_n + R(X_1, \cdots, X_{n-1})$$

et la condition $Q(\Sigma_{1,n}, \cdots, \Sigma_{n,n}) = 0$ nous donne par évaluation en $X_n = 0$, tenant compte de (2.2), $0 = Q(\Sigma_{1,n-1}, \cdots, \Sigma_{n-1,n-1}, 0) = R(\Sigma_{1,n-1}, \cdots, \Sigma_{n-1,n-1})$ et en conséquence $R = 0$ (hypothèse de récurrence sur n). On a alors :

$$0 = Q(\Sigma_{1,n}, \cdots, \Sigma_{n,n}) = S(\Sigma_{1,n}, \cdots, \Sigma_{n,n})\Sigma_{n,n}$$

soit $S(\Sigma_{1,n}, \cdots, \Sigma_{n,n}) = 0$ avec S de degré au plus égal à $d-1$, ce qui équivaut à $S = 0$ (hypothèse de récurrence sur d). D'où l'unicité de Q. □

2.9 Exercices

Exercice 2.1. *Montrer que si l'ensemble E a au moins 3 éléments, alors le groupe $\mathcal{S}(E)$ n'est pas commutatif (voir aussi le lemme 2.3).*

Solution. Soient x_1, x_2, x_3 distincts dans E et $\tau_1 = (x_1, x_2), \tau_2 = (x_2, x_3)$. On a $\tau_2 \circ \tau_1(x_1) = x_3$ et $\tau_1 \circ \tau_2(x_1) = x_2 \neq x_3$. Donc $\tau_2 \circ \tau_1 \neq \tau_1 \circ \tau_2$ et $\mathcal{S}(E)$ n'est pas commutatif.

Exercice 2.2. *On suppose que* $\operatorname{card}(E) = n \geq 2$. *Montrer que, pour* $2 \leq r \leq n$, *dans* $\mathcal{S}(E)$ *il y a* $\binom{n}{r}(r-1)! = \dfrac{n!}{r(n-r)!}$ *cycles d'ordre* r *distincts.*

Solution. Pour définir un r-cycle, on choisit d'abord une liste $(x_1, \cdots, x_r)$ dans E, il y a $A_n^r = r!\binom{n}{r} = \dfrac{n!}{(n-r)!}$ possibilités. Pour un tel choix de la partie $\{x_1, \cdots, x_r\}$ de E, les r permutations circulaires :

$$(x_1, \cdots, x_r),\ (x_2, x_3, \cdots, x_r, x_1),\ , (x_r, x_1, \cdots, x_{r-1})$$

donnent le même cycle, les autres permutations donnant des cycles différents, il y a donc $\dfrac{A_n^r}{r} = (r-1)!\binom{n}{r}$ possibilités.

Exercice 2.3. *Montrer que si* σ, σ' *sont deux cycles tels que l'intersection* $\operatorname{Supp}(\sigma) \cap \operatorname{Supp}(\sigma')$ *soit réduite à un point, alors* $\sigma\sigma'$ *est un cycle.*

Solution. Soient $\sigma = (x_1, x_2, \cdots, x_r)$ et $\sigma' = (x'_1, x'_2, \cdots, x'_s)$ deux cycles tels que $\operatorname{Supp}(\sigma) \cap \operatorname{Supp}(\sigma) = \{x_k\}$. Si j est l'entier compris entre 1 et s tel que $x_k = x'_j$, on a alors :

$$\begin{aligned}\sigma\sigma' &= (x_{k+1}, \cdots, x_r, x_1, \cdots, x_k)\left(x_k, x'_{j+1}, \cdots, x'_s, x'_1, \cdots, x'_{j-1}\right)\\ &= \left(x_{k+1}, \cdots, x_r, x_1, \cdots, x_k, x'_{j+1}, \cdots, x'_s, x'_1, \cdots, x'_{j-1}\right)\end{aligned}$$

Exercice 2.4. *On suppose que* $\operatorname{card}(E) \geq 3$. *Montrer que pour toute permutation* $\sigma \in \mathcal{S}(E) \setminus \{Id_E\}$, *il existe une transposition qui ne commute pas à* σ. *On a donc* $\sigma \notin Z(\mathcal{S}(E))$ *et on retrouve le fait que* $Z(\mathcal{S}(E)) = \{Id_E\}$.

Solution. Si $\sigma \in \mathcal{S}(E) \setminus \{Id\}$, il existe $x \in E$ tel que $y = \sigma(x) \neq x$. On se donne $z \in E \setminus \{x, y\}$ (E a au moins 3 éléments) et τ est la transposition $\tau = (y, z)$. Avec :

$$\sigma\tau(x) = \sigma(x) = y \text{ et } \tau\sigma(x) = \tau(y) = z \neq y$$

on déduit que $\sigma\tau \neq \tau\sigma$ et $\sigma \notin Z(\mathcal{S}(E))$.

Exercice 2.5. *Montrer que* $\mathcal{S}_3$ *est, à isomorphisme près, le seul groupe d'ordre* 6 *non commutatif.*

Solution. Soit G un groupe non commutatif d'ordre 6. Le théorème de Cauchy nous dit qu'on peut trouver dans G, un élément g d'ordre 2 et un élément h d'ordre 3 (ce qui peut se montrer ici directement). On vérifie alors que

$$G = \left\{g^i h^j\ ;\ i = 0, 1 \text{ et } j = 0, 1, 2\right\}$$

Pour cela il suffit de vérifier que les $g^i h^j$ sont deux à deux distincts. Si $g^i h^j = g^{i'} h^{j'}$, on a alors $g^{i-i'} = h^{j'-j} \in \langle g \rangle \cap \langle h \rangle = \{1\}$ ($\langle g \rangle \cap \langle h \rangle$ étant contenu dans $\langle g \rangle$ d'ordre 2 et dans $\langle h \rangle$ d'ordre 3 a un ordre qui divise 2 et 3, cet ordre est donc 1). On a donc $g^{i-i'} = h^{j'-j} = 1$, donc 2 divise $i - i' \in \{-1, 0, 1\}$ et 3 divise $j - j' \in \{-2, -1, 0, 1, 2\}$, ce qui entraîne $i = i'$ et $j = j'$. L'application φ de G dans $\mathcal{S}_3$ définie par $\varphi\left(g^i h^j\right) = \tau_1^i \gamma_1^j$ pour tout $(i, j) \in \{0, 1\} \times (0, 1, 2)$ réalise alors un isomorphisme de groupes de G sur $\mathcal{S}_3$. En effet, cette application est bijective puisque les applications $(i, j) \mapsto g^i h^j$ et $(i, j) \mapsto \tau_1^i \gamma_1^j$ sont bijectives de $\{0, 1\} \times (0, 1, 2)$ sur G et $\mathcal{S}_3$ respectivement. Le fait que c'est un morphisme de groupes provient des égalités $hg = gh^2$ et $h^2 g = gh$ dans G et $\mathcal{S}_3$ (avec $(g, h) = (\tau_1, \gamma_1)$ dans ce cas). En effet, on a $hg \notin \left\{1_G, g, h, h^2, gh\right\}$ (comme g est d'ordre 2 et h d'ordre 3, $hg = 1_G$ donne $h = g$, $hg = g$ donne $h = 1_G$, $hg = h$ donne $g = 1_G$, $hg = h^2$ donne $g = 1_G$ et $hg = gh$ n'est pas possible car G est non commutatif), donc $hg = gh^2$ et $h^2 g = hgh^2 = gh^4 = gh$. Tenant compte de $\varphi\left(g^i h^j\right) = \tau_1^i \gamma_1^j$ pour tout $(i, j) \in \mathbb{Z}^2$, il en résulte que pour $g^i h^j$, $g^{i'} h^{j'}$ dans G, on a :

$$g^i h^j \cdot g^{i'} h^{j'} = \begin{cases} g^i h^{j+j'} \text{ si } i' = 0 \\ g^{i+1} h^{j'} \text{ si } i' = 1 \text{ et } j = 0 \\ g^{i+1} h^{j'+2} \text{ si } i' = 1 \text{ et } j = 1 \\ g^{i+1} h^{j'+1} \text{ si } i' = 1 \text{ et } j = 2 \end{cases}$$

et :

$$\varphi\left(g^i h^j \cdot g^{i'} h^{j'}\right) = \begin{cases} \tau_1^i \gamma_1^{j+j'} = \tau_1^i \gamma_1^j \cdot \gamma_1^{j'} \text{ si } i' = 0 \\ \tau_1^{i+1} \gamma_1^{j'} = \tau_1^i \cdot \tau_1 \gamma_1^{j'} \text{ si } i' = 1 \text{ et } j = 0 \\ \tau_1^{i+1} \gamma_1^{j'+2} = \tau_1^i \tau_1 \gamma_1^2 \gamma_1^{j'} = \tau_1^i \gamma_1 \cdot \tau_1 \gamma_1^{j'} \text{ si } i' = 1 \text{ et } j = 1 \\ \tau_1^{i+1} \gamma_1^{j'+1} = \tau_1^i \tau_1 \gamma_1 \gamma_1^{j'} = \tau_1^i \gamma_1^2 \cdot \tau_1 \gamma_1^{j'} \text{ si } i' = 1 \text{ et } j = 2 \end{cases}$$

$$= \begin{cases} \varphi\left(g^i h^j\right) \varphi\left(h^{j'}\right) \text{ si } i' = 0 \\ \varphi\left(g^i\right) \varphi\left(g h^{j'}\right) \text{ si } i' = 1 \text{ et } j = 0 \\ \varphi\left(g^i h\right) \varphi\left(g h^{j'}\right) \text{ si } i' = 1 \text{ et } j = 1 \\ \varphi\left(g^i h^2\right) \varphi\left(g h^{j'}\right) \text{ si } i' = 1 \text{ et } j = 2 \end{cases} = \varphi\left(g^i h^j\right) \varphi\left(g^{i'} h^{j'}\right)$$

On peut se passer du théorème de Cauchy pour cet exercice. Comme G est non commutatif, il n'y a pas d'élément d'ordre 6 (sinon G est cyclique). Si tous les éléments de $G \setminus \{1_G\}$ sont d'ordre 2, le groupe est alors commutatif. Il existe donc un élément d'ordre 3. Si tous les éléments de $G \setminus \{1_G\}$ sont d'ordre 3, on a alors $g \neq g^{-1}$ pour tout $g \neq 1_G$ et $G \setminus \{1_G\} = \bigcup_{g \neq e} \left\{g, g^{-1}\right\}$ serait de cardinal pair, ce qui est absurde. Il existe donc dans $G \setminus \{1_G\}$ au moins un élément d'ordre 2. En fait, de manière plus général, un groupe d'ordre $2n$ avec $n \geq 1$ a au moins un élément d'ordre 2. En effet, pour $n = 1$, c'est clair et pour $n \geq 2$, s'il n'y a pas d'élément d'ordre 2, on a alors $g \neq g^{-1}$ pour tout $g \neq 1_G$ et $G \setminus \{1_G\} = \bigcup_{g \neq e} \left\{g, g^{-1}\right\}$ serait de cardinal pair, ce qui est en contradiction avec $\operatorname{card}\left(G \setminus \{1_G\}\right) = 2n - 1$.

Exercice 2.6. *Soit $\sigma = (x_1, x_2, \cdots, x_r)$ un cycle de longueur paire. Montrer que σ^2 n'est pas un cycle.*

Solution. Soit $r = 2p$ la longueur de σ avec $p \geq 1$. Pour $p = 1$, $\sigma^2 = Id_E$ n'est pas un cycle et pour $p \geq 2$, on a :

$$Orb_{\sigma^2}(x_1) = \{x_1, x_3, \cdots, x_{2p-1}\} \text{ et } Orb_{\sigma^2}(x_2) = \{x_2, x_4, \cdots, x_{2p}\}$$

et σ^2 n'est pas un cycle.

Exercice 2.7. *Soit $\sigma = (x_1, x_2, \cdots, x_r)$ un cycle de longueur $r \geq 2$.*

1. *Montrer que, pour $x \in \text{Supp}(\sigma)$ et $j \in \mathbb{Z}$, on a :*
$$\left(\sigma^j(x) = x\right) \Leftrightarrow (r \text{ divise } j)$$
2. *Montrer que pour tout entier $m \in \mathbb{Z}$, on a :*
$$\text{Supp}(\sigma^m) = \begin{cases} \emptyset \text{ si } r \text{ divise } m \\ \text{Supp}(\sigma) \text{ si } r \text{ ne divise pas } m \end{cases}$$
3. *Montrer que, pour tout $x \in \text{Supp}(\sigma)$ et tout $m \in \mathbb{Z}$, on a $\text{card}(Orb_{\sigma^m}(x)) = \dfrac{r}{r \wedge m}$.*
4. *Montrer que, pour $m \in \mathbb{Z}$ non multiple de r, σ^m est un cycle si, et seulement si, m est premier avec r.*

Solution.

1. Si r divise j, on a alors $\sigma^j = Id$ et $\sigma^j(x) = x$ pour tout $x \in E$. Réciproquement, supposons que $\sigma^j(x) = x$ pour $x = x_k \in \text{Supp}(\sigma)$. On a alors $\sigma^j(x_k) = \sigma^{j+k-1}(x_1)$ et en effectuant la division euclidienne de $j + k - 1$ par r, on a $j + k - 1 = qr + p$ avec $0 \leq p \leq r - 1$ et $x_k = \sigma^j(x_k) = \sigma^p(x_1) = x_{p+1}$, ce qui équivaut à $p + 1 = k$. Il en résulte que $j + k = qr + p + 1 = qr + k$, soit $j = qr$, c'est-à-dire que r divise j.
2. Si r divise m, on a alors $\sigma^m = Id$ et $\text{Supp}(\sigma^m) = \emptyset$. S'il existe $x \in \text{Supp}(\sigma)$ tel que $x \notin \text{Supp}(\sigma^m)$, on a alors $\sigma^m(x) = x$ et r divise m. Il en résulte que si r ne divise pas m, on a alors $\text{Supp}(\sigma) \subset \text{Supp}(\sigma^m)$ et $\text{Supp}(\sigma) = \text{Supp}(\sigma^m)$ du fait que l'inclusion $\text{Supp}(\sigma^m) \subset \text{Supp}(\sigma)$ est vérifiée pour tout entier relatif m.
3. Si r divise m, on a alors $\sigma^m = Id$, $Orb_{\sigma^m}(x) = \{x\}$, $r \wedge m = r$ et :
$$\text{card}(Orb_{\sigma^m}(x)) = 1 = \frac{r}{r \wedge m}$$
Sinon, $\sigma^m(x) \neq x$ et $\text{card}(Orb_{\sigma^m}(x)) \geq 2$. En notant δ le pgcd de m et r, on a $m = \delta m_1$, $r = \delta r_1$ avec $r_1 \geq 2$ (sinon $r = \delta$ divise m), les entiers r_1 et m_1 étant premiers entre eux, $(\sigma^m)^{r_1}(x) = \sigma^{m_1 \delta r_1}(x) = \sigma^{m_1 r}(x) = x$ et pour k compris entre 1 et $r_1 - 1$, $(\sigma^m)^k(x) = \sigma^{mk}(x) \neq x$ (sinon $r = \delta r_1$ divise $mk = \delta m_1 k$, donc r_1 divise $m_1 k$ et r_1 divise k puisque $r_1 \wedge m_1 = 1$, ce qui est incompatible

avec $1 \leq k \leq r_1 - 1$). On a donc $Orb_{\sigma^m}(x) = \left\{x, \sigma^m(x), \cdots, (\sigma^m)^{r_1-1}(x)\right\}$ et cette orbite est de cardinal $r_1 = \dfrac{r}{r \wedge m}$.

4. Si m est premier avec r, on a alors :

$$\text{Supp}(\sigma^m) = \text{Supp}(\sigma),\ \text{card}(Orb_{\sigma^m}(x_1)) = r = \text{card}(\text{Supp}(\sigma^m))$$

et $Orb_{\sigma^m}(x_1) \subset \text{Supp}(\sigma^m)$, donc $Orb_{\sigma^m}(x_1) = \text{Supp}(\sigma^m)$ et σ^m est un cycle. Sinon on a $2 \leq \text{card}(Orb_{\sigma^m}(x_1)) = \dfrac{r}{r \wedge m} < r = \text{card}(\text{Supp}(\sigma^m))$ et il y a au moins deux σ^m-orbites non réduites à un point, donc σ^m n'est pas un cycle.

Exercice 2.8. *Donner la décomposition en produit de cycles deux à deux disjoints de $\sigma \in \mathcal{S}_n$ définie par $\sigma(k) = n + 1 - k$ pour tout $k \in \{1, \cdots, n\}$ (elle inverse l'ordre des entiers $1, \cdots, n$).*

Solution. On a $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ n & n-1 & n-2 & \cdots & 2 & 1 \end{pmatrix}$. Si n est pair, soit $n = 2p$ avec $p \geq 1$, on a alors $\sigma(k) = 2p + 1 - k$ et $\sigma^2(k) = \sigma(2p + 1 - k) = k$ pour $k = 1, \cdots, p$ (et $2p + 1 - k = 2p, \cdots, p + 1$), ce qui donne :

$$\sigma = (1, 2p)(2, 2p - 1) \cdots (p, p + 1)$$

Si n est impair, soit $n = 2p + 1$ avec $p \geq 1$, on a :

$$\sigma(k) = 2p + 2 - k,\ \sigma^2(k) = \sigma(2p + 2 - k) = k$$

pour $k = 1, \cdots, p$ ($2p + 2 - k = 2p + 1, \cdots, p + 2$) et $\sigma(p + 1) = p + 1$ ce qui donne $\sigma = (1, 2p + 1)(2, 2p) \cdots (p, p + 2)$. Donc σ est produit de transpositions eux à deux disjointes et est d'ordre 2 (ce qui se voit directement sur sa définition).

Exercice 2.9. *Soient σ, γ deux permutations dans $\mathcal{S}(E) \backslash \{Id_E\}$. Exprimer la décomposition en cycles deux à deux disjoints de $\sigma\gamma\sigma^{-1}$ en fonction de celle de γ.*

Solution. Si $\gamma = \prod_{j=1}^{p} \gamma_j$ est la décomposition en cycles disjoints de γ, alors $\sigma\gamma\sigma^{-1} = \prod_{j=1}^{p} \left(\sigma\gamma_j\sigma^{-1}\right)$ est celle de $\sigma\gamma\sigma^{-1}$ puisque pour $\gamma_j = (x_1, \cdots, x_r)$, on a $\sigma\gamma_j\sigma^{-1} = (\sigma(x_1), \cdots, \sigma(x_r))$ et les supports de ces cycles sont 2 à 2 disjoints du fait que σ est bijective.

Exercice 2.10. *Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix}$. Calculer σ^{2009}.*

Solution. $\sigma = (1,2,3,4,5)(6,7) = \gamma\tau$ est d'ordre ppcm $(5,2) = 10$. En effectuant la division euclidienne, on a pour tout entier relatif $m = 10q + r$ où $0 \leq r \leq 9$, $\sigma^m = \sigma^r$. Ce qui donne :

$$\begin{aligned}\sigma^{2009} = \sigma^9 = \gamma^9\tau^9 = \gamma^{-1}\tau = (5,4,3,2,1)(6,7)\\ = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 2 & 3 & 4 & 7 & 6 & 8 \end{pmatrix}\end{aligned}$$

Exercice 2.11. *Quel est l'ordre maximal d'un élément de $\mathcal{S}_5$.*

Solution. La décomposition en cycles disjoints d'un élément de $\mathcal{S}_5 \setminus \{Id\}$ (Id est d'ordre 1) est formée soit d'un r-cycle avec $2 \leq r \leq 5$, soit d'un 2-cycle et d'un cycle d'ordre 2 ou 3 et cet ordre est au maximum 6, qui est atteint pour $(1,2)(3,4,5)$.

Exercice 2.12. *Soit σ un cycle de longueur $r \geq 2$ et m un entier relatif non multiple de r. Que dire de la décomposition de σ^m en cycles deux à deux disjoints ? (On peut utiliser l'exercice 2.7).*

Solution. Avec l'exercice 2.7, on a vu que σ^m est un cycle si, et seulement si, $m \wedge r = 1$. Pour $m \wedge r \neq 1$, on a $\text{Supp}(\sigma^m) = \text{Supp}(\sigma)$, et $\text{card}(Orb_{\sigma^m}(x)) = \dfrac{r}{\text{pgcd}(r,m)} \geq 2$ pour tout $x \in \text{Supp}(\sigma)$. Comme les σ^m-orbites non réduites à un point forment une partition de $\text{Supp}(\sigma^m)$, il en résulte que σ^m est produit de $\text{pgcd}(r,m)$ cycles disjoints, tous de longueur $\dfrac{r}{\text{pgcd}(r,m)}$. On retrouve le fait que σ^m est d'ordre $\dfrac{r}{\text{pgcd}(r,m)}$.

Exercice 2.13. *Montrer directement par récurrence sur $n \geq 2$, que $\mathcal{S}(E)$ est engendré par les transpositions.*

Solution. Pour $E = \{x_1, x_2\}$, on a $\mathcal{S}(E) = \{Id_E, (x_1,x_2)\}$. Supposons le résultat acquis pour les ensembles de cardinal $n-1 \geq 2$ et soit E de cardinal n. Soient $\sigma \in \mathcal{S}(E)$. Si $\sigma = Id_E$, on a $\sigma = \tau^2$ pour toute transposition τ. Sinon il existe $x \in E$ tel que $y = \sigma(x) \neq x$. En désignant par τ la transposition $\tau = (x,y)$, on a $\tau\sigma(x) = x$ et la restriction de $\tau\sigma$ à $F = E \setminus \{x\}$ est une permutation de F, elle s'écrit donc comme produit de transpositions et $\tau\sigma = \tau_1 \cdots \tau_r$ où les τ_k sont des transpositions de E qui laissent fixe x. Il en résulte que $\sigma = \tau\tau_1 \cdots \tau_r$ est produit de transpositions.

Cette démonstration montre aussi que si $\{\tau_1, \cdots, \tau_r\}$ est une famille de transpositions qui engendre $\mathcal{S}(E)$, on a nécessairement $r \geq n-1$.

Exercice 2.14. *Montrer que, pour tout entier $n \geq 3$, $\mathcal{S}_n$ est engendré par $(1,2)$ et $(2,3,\cdots,n)$.*

Solution. Comme $\mathcal{S}_n$ est engendré par les $(1,k)$ où $2 \leq k \leq n$, il suffit de montrer que chaque transposition $(1,k)$ est dans le sous-groupe G de $\mathcal{S}_n$ engendré par $(1,2)$ et $(2,3,\cdots,n)$. On a déjà $(1,2) \in G$. En notant $\sigma_k = (2,3,\cdots,n)^{k-2}$ pour $3 \leq k \leq n$, on a $\sigma_k(1) = 1$, $\sigma_k(2) = k$, et $(1,k) = \sigma_k(1,2)\sigma_k^{-1} \in H$.

Exercice 2.15. *Déterminer la signature de la permutation :*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 2 & 3 & 4 & 7 & 6 & 8 \end{pmatrix}$$

Solution. On a $\sigma = (1,5,4,3,2)(6,7)$ et $\varepsilon(\sigma) = (-1)^{5-1}(-1) = -1$. On peut aussi écrire σ comme produit de transpositions, $\sigma = (1,5)(5,4)(4,3)(3,2)(6,7)$ et $\varepsilon(\sigma) = (-1)^5 = -1$.

Exercice 2.16. *Donner la liste de tous les éléments de $\mathcal{A}_4$ en précisant leurs ordres.*

Solution. On note τ_{ij} la transposition (i,j) dans $\mathcal{S}_4$ pour $1 \leq i \neq j \leq 4$. On a dans le groupe $\mathcal{A}_4$ les 12 éléments distincts suivants :

- l'identité ;
- les 3 éléments d'ordre 2 : $\tau_{12} \circ \tau_{34}, \tau_{13} \circ \tau_{24}, \tau_{23} \circ \tau_{14}$ (le produit de deux transpositions de supports disjoints est d'ordre 2 puisque ces transpositions commutent) ;
- les 8 éléments d'ordre 3 : $(2,3,4)$, $(2,4,3)$, $(1,3,4)$, $(1,4,3)$, $(1,2,4)$, $(1,4,2)$, $(1,2,3)$ $(1,3,2)$ (un 3-cycle fixe un élément de $\{1,2,3,4\}$ et il y en a deux qui fixent k, pour $k = 1,2,3,4$)

et on a ainsi tous les éléments puisque $\mathcal{A}_4$ est de cardinal $\dfrac{4!}{2} = 12$.

Exercice 2.17.

1. *Soient G un groupe d'ordre $2n$ et H un sous-groupe de G d'ordre n (donc d'indice 2). Montrer que $g^2 \in H$ pour tout $g \in G$.*
2. *Montrer que $\mathcal{A}_4$ (qui est d'ordre 12) n'a pas de sous-groupe d'ordre 6.*

Solution.

1. Soit $g \in G$. Si $g \in H$, on a alors $g^2 \in H$ puisque H est un groupe. Si $g \notin H$, on a alors $gH \neq H$ et $G/H = \{H, gH\}$, ce qui nous donne la partition $G = H \cup gH$. Si $g^2 \notin H$, il est alors dans gH et s'écrit $g^2 = gk$ avec $k \in H$, ce qui entraîne $g = k \in H$ qui est en contradiction avec $g \notin H$.

2. Si H est un sous-groupe de $\mathcal{A}_4$ d'ordre 6, on a alors $\sigma^2 \in H$ pour tout $\sigma \in \mathcal{A}_4$. Si $\sigma \in \mathcal{A}_n$ est un 3-cycle, il est alors d'ordre 3 et $\sigma^4 = \sigma$, c'est-à-dire que $\sigma = \gamma^2$ avec $\gamma = \sigma^2 = \sigma^{-1} \in \mathcal{A}_n$. Donc H va contenir tous les 3-cycles, soit 8 éléments, ce qui n'est pas possible.

Exercice 2.18. *Montrer que, pour $n \geq 4$, les produits de deux transpositions disjointes sont conjugués dans $\mathcal{A}(E)$.*

Solution. Soient $\sigma = (x_1, x_2)(x_3, x_4)$ et $\sigma' = (x'_1, x'_2)(x'_3, x'_4)$ deux produits de deux transpositions disjointes. En désignant par τ une permutation dans $\mathcal{S}(E)$ telle que $\tau(x_k) = x'_k$ pour $1 \leq k \leq 4$, on a :

$$\begin{aligned}\tau\sigma\tau^{-1} &= \tau(x_1, x_2)\tau^{-1}\tau(x_3, x_4)\tau^{-1} = (\tau(x_1), \tau(x_2))(\tau(x_3), \tau(x_4)) \\ &= (x'_1, x'_2)(x'_3, x'_4) = \sigma'\end{aligned}$$

(ce qui prouve que σ et σ' sont conjuguées dans $\mathcal{S}(E)$). Si $\tau \in \mathcal{A}(E)$ c'est terminé, sinon $\gamma = (x'_3, x'_4)\tau$ est dans $\mathcal{A}(E)$ et :

$$\gamma\sigma\gamma^{-1} = (\gamma(x_1), \gamma(x_2))(\gamma(x_3), \gamma(x_4)) = (x'_1, x'_2)(x'_4, x'_3) = \sigma'$$

Exercice 2.19. *Montrer que $\mathcal{A}(E)$ est stable par tout automorphisme de $\mathcal{S}(E)$.*

Solution. Si φ est un automorphisme de $\mathcal{S}(E)$, alors pour tout 3-cycle $\sigma \in \mathcal{A}(E)$, $\varphi(\sigma)$ est d'ordre 3 dans $\mathcal{S}(E)$. Comme $\varphi(\sigma)$ est produit de cycles et l'ordre de $\varphi(\sigma)$ est le ppcm des longueurs de ces cycles, ils sont nécessairement tous d'ordre 3 et $\varphi(\sigma) \in \mathcal{A}(E)$. De manière plus générale si E, F sont deux ensembles de même cardinal et φ une bijection de E sur F, on lui associe naturellement l'application $\Phi : \sigma \in \mathcal{S}(E) \mapsto \varphi \circ \sigma \circ \varphi^{-1}$ qui réalise un isomorphisme de groupes de $\mathcal{S}(E)$ sur $\mathcal{S}(F)$. Le raisonnement fait avec l'exercice précédent nous montre que la restriction de Φ à $\mathcal{A}(E)$ réalise un isomorphisme de groupes de $\mathcal{A}(E)$ sur $\mathcal{A}(F)$.

Exercice 2.20. *Décomposer en produit de 3-cycles dans $\mathcal{A}_7$ la permutation* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}$.

Solution. On a la décomposition en produit de transpositions :

$$\sigma = (1, 2)(2, 3)(3, 4)(4, 5)(5, 6)(6, 7)$$

donc $\varepsilon(\sigma) = 1$ et $\sigma \in \mathcal{A}_7$. Puis :

$$\sigma = (2, 3, 1)(4, 5, 3)(6, 7, 5) = (1, 2, 3)(3, 4, 5)(5, 6, 7)$$

Exercice 2.21. *Pour $n \geq 3$, montrer que les 3-cycles $\gamma_k = (1,2,k)$ où k est compris entre 3 et n engendrent $\mathcal{A}_n$.*

Solution. Il suffit de montrer que tout 3-cycle peut s'écrire comme produit de cycles du type $(1,2,k)$. Pour i,j,k distincts de $1,2$, on a :

$$(i,j,k) = (1,2,i)(2,j,k)(1,2,i)^{-1} \text{ et } (2,j,k) = (1,2,j)(1,2,k)(1,2,j)^{-1}$$

(exercice 2.2). On peut aussi procéder par récurrence. Pour $n = 3$, c'est vrai ($\mathcal{A}_3 = \langle(1,2,3)\rangle$). Supposons le résultat acquis pour $n \geq 3$ et soit $\sigma \in \mathcal{A}_{n+1}$. Si $\sigma(n+1) = n+1$, alors la restriction de σ à $\{1,\cdots,n\}$ est dans $\mathcal{A}_n$, donc elle s'écrit comme produit de γ_k avec $3 \leq k \leq n$ et il en est de même de σ. Sinon, $\sigma(n+1) = j \leq n$ et avec :

$$\left(\gamma_{n+1}^{-1} \circ \gamma_j \circ \sigma\right)(n+1) = \left(\gamma_{n+1}^{-1} \circ \gamma_j\right)(j) = \left(\gamma_{n+1}^{-1}\right)(1) = n+1$$

on déduit que $\sigma' = \gamma_{n+1}^{-1} \circ \gamma_j \circ \sigma \in \mathcal{A}_{n+1}$ est produit de γ_k avec $3 \leq k \leq n$ et $\sigma = \gamma_j^{-1} \circ \gamma_{n+1} \circ \sigma' = \gamma_j^2 \circ \gamma_{n+1} \circ \sigma'$ est produit de γ_k avec $3 \leq k \leq n+1$.

Exercice 2.22. *Pour $n \geq 3$, montrer que les 3-cycles $(k,k+1,k+2)$ où k est compris entre 1 et $n-2$ engendrent $\mathcal{A}_n$.*

Solution. $\mathcal{A}_n$ étant engendré par les 3-cycles $\gamma_k = (1,2,k)$ où $3 \leq k \leq n$, il suffit d'écrire chaque γ_k comme produit 3-cycles du type $(j,j+1,j+2)$ et $(i,i+1,i+2)^{-1} = (i+2,i+1,i)$ où $1 \leq i,j \leq n-2$. Pour $4 \leq k \leq n$, on a :

$$(1,2,k) = (k-1,k,k+1)(1,2,k-1)(k-1,k,k+1)^{-1}$$

Pour $k = 4$, on a $(1,2,k-1) = (1,2,3)$ et c'est terminé, sinon on utilise l'égalité $(1,2,k-1) = (k-2,k-1,k)(1,2,k-2)(k-2,k-1,k)^{-1}$ et on continue ainsi de suite si nécessaire. Pour $k = 3$, le cycle $(1,2,3)$ est de la forme souhaitée.

Exercice 2.23. *Déterminer, pour $n \geq 4$, le centre $Z(\mathcal{A}(E))$ du groupe $\mathcal{A}(E)$.*

Solution. Si $\sigma \in \mathcal{A}(E) \setminus \{Id\}$, il existe alors $x \in E$ tel que $y = \sigma(x) \neq x$. On se donne $z \in E \setminus \{x, y, \sigma(y)\}$ (E a au moins 4 éléments) et γ est le 3-cycle $\gamma = (x,y,z) \in \mathcal{A}(E)$. On a alors $\sigma\gamma(x) = \sigma(y)$ et $\gamma\sigma(x) = \gamma(y) = z \neq \sigma(y)$, donc $\sigma\gamma \neq \gamma\sigma$ et $\sigma \notin Z(\mathcal{A}(E))$. Le centre de $\mathcal{A}(E)$ est donc réduit à $\{Id\}$. Pour $n = 3$, $\mathcal{A}(E)$ est cyclique, donc commutatif et $Z(\mathcal{A}(E)) = \mathcal{A}(E)$.

Exercice 2.24.

1. *Montrer que, pour $n \geq 5$, deux 3-cycles sont conjugués dans $\mathcal{A}(E)$.*
2. *Vérifier que ce résultat n'est pas vrai pour $\mathcal{A}_4$.*

3. En déduire que, pour $n \geq 5$, le groupe dérivé $D(\mathcal{A}(E))$ de $\mathcal{A}(E)$ (i.e. le groupe engendré par les commutateurs $[\sigma,\tau] = \sigma\tau\sigma^{-1}\tau^{-1}$ où σ et τ sont dans $\mathcal{A}(E)$) est $\mathcal{A}(E)$.

Solution.

1. On sait déjà que deux 3-cycles sont conjugués dans $\mathcal{S}(E)$ (exercice 2.2). Soient $\gamma = (x_1, x_2, x_3)$ et $\gamma' = (x'_1, x'_2, x'_3)$ deux 3-cycles. On se donne une permutation $\sigma \in \mathcal{S}(E)$ telle que $\sigma(x_k) = x'_k$ pour $k = 1, 2, 3$ et on a alors $\gamma' = \sigma\gamma\sigma^{-1}$. Si $\sigma \in \mathcal{A}(E)$, c'est terminé, sinon en prenant x_4, x_5 dans $E \setminus \{x_1, x_2, x_3\}$ (E a au moins 5 éléments), la permutation $\sigma' = (x_4, x_5)\sigma$ est dans $\mathcal{A}(E)$ avec $\sigma'(x_k) = x'_k$ pour $k = 1, 2, 3$ et on est ramené au cas précédent.
2. Ce résultat est faux pour $n = 4$. Si $\gamma = (1, 2, 3)$ et $\gamma' = (2, 3, 4)$ sont conjugués dans $\mathcal{A}_4$, il existe alors $\sigma \in \mathcal{A}_4$ telle que $(2, 3, 4) = \sigma\gamma\sigma^{-1} = (\sigma(1), \sigma(2), \sigma(3))$ et on a nécessairement $\sigma(4) = 1$. On parcourant la liste des éléments de $\mathcal{A}_4$ (exercice 2.16), on voit que $\sigma = \tau_{23} \circ \tau_{14}$, ou $\sigma = (1, 3, 4)$, ou $\sigma = (1, 2, 4)$ et $\sigma\gamma\sigma^{-1} = (4, 3, 2) \neq \gamma'$, ou $\sigma\gamma\sigma^{-1} = (3, 2, 4) \neq \gamma'$, ou $\sigma\gamma\sigma^{-1} = (2, 4, 3) \neq \gamma'$. Les cycles γ et γ' ne sont pas conjugués dans $\mathcal{A}_4$.
3. Comme $\mathcal{A}(E)$ est engendré par les 3-cycles, il suffit de montrer que tout 3-cycle est dans $D(\mathcal{A}(E))$. Si γ est un 3-cycle, il en est de même de $\gamma^{-1} = \gamma^2$, donc γ^2 est conjugué à γ dans $\mathcal{A}(E)$, c'est-à-dire qu'il existe $\sigma \in \mathcal{A}(E)$ tel que $\gamma^2 = \sigma^{-1}\gamma\sigma$ et $\gamma = \gamma^{-1}\sigma^{-1}\gamma\sigma \in D(\mathcal{A}(E))$.

Exercice 2.25. *Montrer que, pour $n \geq 2$, $\mathcal{S}_n$ est isomorphe à un sous-groupe de $\mathcal{A}_{n+2}$.*

Solution. On associe à la transposition $\tau = (n+1, n+2)$ l'application :

$$\begin{array}{rccc} \varphi : & \mathcal{S}_n & \to & \mathcal{A}_{n+2} \\ & \sigma & \mapsto & \left\{ \begin{array}{l} \sigma \text{ si } \sigma \in \mathcal{A}_n \\ \tau \circ \sigma \text{ si } \sigma \notin \mathcal{A}_n \end{array} \right. \end{array}$$

On vérifie facilement que φ est un morphisme de groupes. Pour σ, σ' dans $\mathcal{S}_n$, on a :

$$\begin{aligned} \varphi(\sigma\sigma') &= \left\{ \begin{array}{l} \sigma\sigma' \text{ si } (\sigma \in \mathcal{A}_n \text{ et } \sigma' \in \mathcal{A}_n) \text{ ou } (\sigma \notin \mathcal{A}_n \text{ et } \sigma' \notin \mathcal{A}_n) \\ \tau \circ \sigma \circ \sigma' \text{ si } (\sigma \in \mathcal{A}_n \text{ et } \sigma' \notin \mathcal{A}_n) \text{ ou } (\sigma \notin \mathcal{A}_n \text{ et } \sigma' \in \mathcal{A}_n) \end{array} \right. \\ &= \varphi(\sigma)\varphi(\sigma') \end{aligned}$$

puisque τ commute à $\mathcal{S}_n$ et $\tau^2 = Id$. Si $\varphi(\sigma) = Id$, on a $\sigma = Id$ pour $\sigma \in \mathcal{A}_n$ ou $\tau \circ \sigma = Id$ pour $\sigma \notin \mathcal{A}_n$, mais ce dernier cas équivaut à $\sigma = \tau$ qui est impossible puisque σ et τ sont de supports disjoints. Le morphisme φ est donc injectif et $\mathcal{S}_n$ est isomorphe à un sous-groupe de $\mathcal{A}_{n+2}$.

Exercice 2.26. *On se propose de montrer que, pour* $n = 5$, $\mathcal{A}(E)$ *est simple (i.e. n'a pas de sous-groupes distingués autres que lui même et* $\{Id\}$*).*

1. *Donner une description de* $\mathcal{A}(E)$ *en classant ses élément en fonction de leur ordre.*
2. *Montrer que* $\mathcal{A}(E)$ *est simple.*

Solution.

1. Pour $n = 5$, notons $E = \{x_1, x_2, x_3, x_4, x_5\}$ et pour $1 \leq i \neq j \leq 5, \tau_{ij}$ la transposition (x_i, x_j) dans $\mathcal{S}(E)$. On décrit d'abord le groupe $\mathcal{A}(E)$. Dans ce groupe, on a les 60 éléments distincts suivants :
   - l'identité ;
   - $\frac{\binom{5}{2}\binom{3}{2}}{2} = 15$ éléments d'ordre 2 donnés par le produit de deux transpositions de supports disjoints : $\tau_{12} \circ \tau_{34}$, $\tau_{12} \circ \tau_{35}$, $\tau_{12} \circ \tau_{45}$, $\cdots$ (deux transpositions de supports disjoints commutent et leur produit est d'ordre 2) ;
   - $2\binom{5}{3} = 20$ cycles d'ordre 3 distincts (un même support à 3 éléments donne 2 cycles) ;
   - $4! = 24$ cycles d'ordre 5 : $(x_1, x_2, x_3, x_4, x_5)$, $(x_1, x_3, x_4, x_5, x_2)$, $\cdots$ (si $\gamma^5 = 1$, alors $\gamma^{-1} = \gamma^4 \in \mathcal{A}(E)$ et $\gamma \in \mathcal{A}(E)$). On a ainsi tous les éléments puisque $\mathcal{A}(E)$ est de cardinal $\frac{5!}{2} = 60$.
2. Soit H un sous-groupe distingué de $\mathcal{A}(E)$ non réduit à $\{Id\}$. Si H contient un 3-cycle, il les contient alors tous puisqu'ils sont conjugués et $H = \mathcal{A}(E)$ puisque les 3-cycles engendrent $\mathcal{A}(E)$. Si H contient un produit $\sigma = (x, y)(z, t)$ de deux transpositions de supports disjoints, il contient alors, pour $u \in E \setminus \{x, y, z, t\}$, le commutateur :
$$\begin{aligned}\sigma(x, y, u)\sigma^{-1}(x, y, u)^{-1} &= (\sigma(x), \sigma(y), \sigma(u))(u, y, x)\\ &= (y, x, u)(u, y, x) = (x, y, u)\end{aligned}$$
($\sigma \in H$, donc $\sigma^{-1} \in H$ puisque H est un groupe et $(x, y, u)\sigma^{-1}(x, y, u)^{-1} \in H$ puisque H est distingué) qui est un 3-cycle, donc $H = \mathcal{A}(E)$.
Si H contient un 5-cycle $\sigma = (x, y, z, t, u)$, il contient alors le commutateur :
$$\begin{aligned}(x, y, z)\sigma(x, y, z)^{-1}\sigma^{-1} &= (x, y, z)\sigma(z, y, x)\sigma^{-1} = (x, y, z)(\sigma(z), \sigma(y), \sigma(x))\\ &= (x, y, z)(t, z, y) = (y, t, x)\end{aligned}$$
qui est un 3-cycle, donc $H = \mathcal{A}(E)$.

Exercice 2.27. $\operatorname{card}(\mathcal{A}_5) = 60$ *n'étant pas multiple de* $\operatorname{card}(\mathcal{S}_4) = 24$*, il n'existe pas de morphisme de groupes injectif de* $\mathcal{S}_4$ *dans* $\mathcal{A}_5$*. On se propose de montrer avec cet exercice que pour* $n \geq 2$*, il n'existe pas de morphisme de groupes injectif de* $\mathcal{S}_n$ *dans* $\mathcal{A}_{n+1}$*.*

1. *Montrer le résultat pour $n = 2$ et $n = 3$.*
2. *Montrer le résultat pour n pair.*
3. *On suppose que $n = 2p + 1$ est impair avec $p \geq 2$ et qu'il existe un morphisme de groupes injectif φ de $\mathcal{S}_{2p+1}$ dans $\mathcal{A}_{2p+2}$. On note $H = \mathrm{Im}(\varphi)$ et $E = \mathcal{A}_{2p+2}/H$ est l'ensemble quotient des classes à gauche modulo H.*

   (a) Montrer que l'application :

$$\begin{array}{rccc} \psi: & \mathcal{A}_{2p+2} & \to & \mathcal{S}(E) \\ & \sigma & \mapsto & (\gamma H \mapsto \sigma\gamma H) \end{array}$$

   est un morphisme de groupes (action par translation à gauche de $\mathcal{A}_{2p+2}$ sur E).

   (b) Conclure en utilisant le fait que $\mathcal{A}_{2p+2}$ est simple.

Solution.

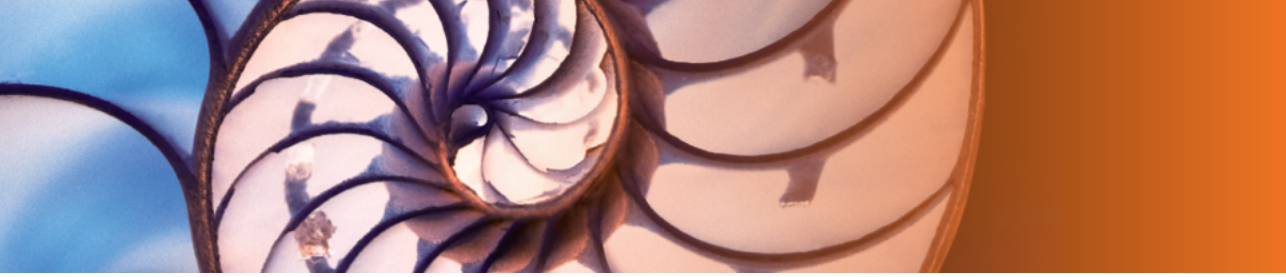
1. Pour $n = 2$, on a $\mathcal{S}_2 = \{Id, (1,2)\}$ qui est d'ordre 2 et $\mathcal{A}_3$ qui est d'ordre 3, il ne peut donc exister de morphisme de groupes injectif de $\mathcal{S}_2$ dans $\mathcal{A}_3$. Pour $n = 3$, $\mathcal{S}_3$ est d'ordre 6 et $\mathcal{A}_4$ n'a pas de sous-groupe d'ordre 6 (exercice 2.17), il ne peut donc exister de morphisme de groupes injectif de $\mathcal{S}_3$ dans $\mathcal{A}_4$.
2. On suppose que $n \geq 4$. Comme $\mathcal{S}_n$ est d'ordre $n!$ et $\mathcal{A}_{n+1}$ d'ordre $\dfrac{(n+1)!}{2}$, une condition nécessaire est que $n!$ divise $\dfrac{(n+1)!}{2}$, ce qui revient à dire que $n+1$ est pair, ou encore que $n = 2p+1$ est impair avec $p \geq 2$.
3. Comme φ est injectif, $H = \mathrm{Im}(\varphi)$ est un sous-groupe d'ordre $(2p+1)!$ de $\mathcal{A}_{2p+2}$ et l'ensemble quotient $E = \mathcal{A}_{2p+2}/H$ des classes à gauche modulo H est de cardinal $\dfrac{(2p+2)!}{2(2p+1)!} = p+1$.

   (a) Pour σ, γ dans $\mathcal{A}_{2p+2}$, $\sigma\gamma H$ est dans E ; $\sigma\gamma H = \sigma\gamma' H$ entraîne $\gamma H = \gamma' H$, donc $\psi(\sigma)$ est injective et $\gamma' H = \sigma\sigma^{-1}\gamma' H$ avec $\sigma^{-1}\gamma' \in \mathcal{A}_{2p+2}$ et $\sigma^{-1}\gamma' H \in E$, donc $\psi(\sigma)$ est surjective et c'est bien un élément de $\mathcal{S}(E)$; pour σ, σ', γ dans $\mathcal{A}_{2p+2}$, on a $\psi(\sigma\sigma')(\gamma H) = \sigma\sigma'\gamma H = \psi(\sigma) \circ \psi(\sigma')(\gamma H)$ et $\psi(\sigma\sigma') = \psi(\sigma) \circ \psi(\sigma')$, donc ψ est bien un morphisme de groupes.

   (b) Comme $\mathcal{A}_{2p+2}$ est simple pour $p \geq 2$, $\ker(\psi)$ qui est distingué dans $\mathcal{A}_{2p+2}$ est $\{Id\}$ ou $\mathcal{A}_{2p+2}$. Avec $\mathrm{card}(\mathcal{S}(E)) = (p+1)!$ et :

$$\mathrm{card}(\mathcal{A}_{2p+2}) = \frac{(2p+2)!}{2} = (p+1)(2p+1)! > (p+1)!$$

   on déduit que ψ ne peut être injectif et $\ker(\psi) = \mathcal{A}_{2p+2}$, ce qui entraîne que pour tout $\sigma \in \mathcal{A}_{2p+2}$, on a $\psi(\sigma)(H) = H$, soit $\sigma H = H$, donc $\sigma \in H$ et $\mathcal{A}_{2p+2} \subset H \subset \mathcal{A}_{2p+2}$, soit $H = \mathcal{A}_{2p+2}$ avec $\mathrm{card}(H) = (2p+1)!$ et $\mathrm{card}(\mathcal{A}_{2p+2}) = (p+1)(2p+1)!$, ce qui est impossible.



Mathématiques pour l'agrégation
Algèbre et géométrie

La préparation des candidats aux concours de l'agrégation interne et externe de mathématiques nécessite des outils et des méthodes spécifiques qu'il leur est souvent bien difficile de se procurer, faute d'une littérature adaptée aux exigences de la situation.

Ce cours d'algèbre et de géométrie est taillé sur mesure pour ces candidats. Les notions indispensables y sont abordées dans le détail et leur assimilation est facilitée par un grand nombre d'exercices corrigés dont beaucoup peuvent être utilisés par les candidats pour leurs leçons à l'épreuve orale.

LES PLUS

- **Parfait complément du volume de Mathématiques pour l'agrégation. Analyse et probabilités**
- **Chaque théorème est suivi d'une série d'applications**
- **Tous les exercices sont intégralement corrigés**

Agrégé de mathématiques, **Jean-Étienne Rombaldi** a enseigné à l'université Grenoble-Alpes, institut Fourier. Membre du jury du CAPES externe et de l'agrégation interne de mathématiques pendant plusieurs années, il a été responsable de la préparation à l'agrégation interne de l'université de Grenoble et préparateur à l'agrégation interne et externe de cette même université ainsi que pour le CNED.

ISBN : 978-2-8073-3220-1

9 782807 332201

deboeck SUPÉRIEUR

www.deboecksuperieur.com

Conception graphique : Primo&Primo®