Faculté des sciences
Département de Mathématiques
HLMA501

Année 2020–2021

Introduction à la théorie des groupes et algèbre linéaire

Polycopié de cours et d'exercices

P.-L. Montagard

Ce polycopié distribué en début de semestre contient à la fois le cours et les exercices de TD. Concernant le cours, je rappelle que toutes les définitions, les énoncés des théorèmes et propriétés et les démonstrations sont à connaître pour tous les contrôles. Sur chacun de ces contrôles, il y aura au moins 8 points (sur 20) qui seront attribués sur des questions de cours.

Pour les exercices de TD, ils sont rassemblés à chaque fin de section. Il sont classés en trois catégories :

- ⓔ pour entraînement : ce sont des petits exercices d'application directe du cours, que vous devez chercher et résoudre tout seul au fur et à mesure de l'avancée dans le cours ; dans cette catégorie se trouve également les démonstrations qui sont laissées en exercice ;
- ⓒ pour classique : ce sont les exercices qui seront corrigés en priorité par votre chargé de TD ; la méthode utilisée pour la résolution de ces exercices et les résultats obtenus sont à connaître impérativement ;
- ⓐ pour approfondissement : des exercices un peu plus longs et pour certains un peu plus difficiles. Ils sont à faire une fois la section correspondante du cours complètement traitée ; ils ne seront pas forcément corrigés en totalité en TD, mais votre chargé de TD peut vous donner des pistes de résolution.

Beaucoup de ces exercices sont tirés du site internet **exo7**. On peut donc les retrouver, parmi bien d'autres (ainsi que des indications supplémentaires et une correction) à l'adresse suivante : `http://exo7.emath.fr`.

Table des matières

Chapitre 1

Introduction à la théorie des Groupes

1.1 Définitions, exemples, théorème de Lagrange

Nous allons commencer par définir la notion de groupe, ainsi que les notions associées, puis après avoir défini quelques exemples, nous montrerons les premiers résultats sur les cardinaux des groupes finis. À cette occasion, nous verrons que l'arithmétique de $\mathbb{Z}$ intervient de manière importante dans l'étude des groupes finis.

1.1.1 Loi sur un ensemble

Avant de définir la notion de groupe, nous allons rappeler la notion générale de loi sur un ensemble.

Définition 1.1.1. On dit qu'un ensemble G est muni d'une loi, s'il existe une application :

$$\begin{array}{rccc} \varphi : & G \times G & \to & G \\ & (s,t) & \mapsto & \varphi(s,t) \end{array}.$$

On notera sous forme de couple (G, φ) un tel ensemble.

Une loi sur un ensemble est donc simplement une procédure qui à partir de deux éléments de G en construit un troisième. On peut facilement donner des exemples.

Exemple(s) 1.1.1.

1. Si $G = \{e\}$ est un ensemble à un seul élément, alors il existe une seule loi sur $\{e\}$ définie par $\varphi(e, e) = e$.
2. Sur l'ensemble des réels $\mathbb{R}$, on peut définir les deux lois suivantes : pour tout $(x, y) \in \mathbb{R}$, $\varphi(x, y) = x + y$ et $\varphi(x, y) = xy$. On peut remplacer $\mathbb{R}$ par un autre corps $\mathbb{Q}, \mathbb{C}$ ou par un anneau $\mathbb{Z}, \mathbb{D}$.
3. Soient $\mathbb{K}$ un corps et E un espace vectoriel sur $\mathbb{K}$, l'addition des vecteurs est une loi. Par contre, la multiplication par un scalaire n'est pas une loi au sens de la définition vue ici. On utilise la dénomination loi *externe*.
4. Soient X un ensemble et $E = \mathrm{End}(X)$ l'ensemble des applications de X dans lui-même, alors la composition qui à tout couple $(f, g) \in E$ associe l'élément $\varphi(f, g) = f \circ g$ est une loi sur E.
5. Soit X un ensemble, l'ensemble des suites finies d'éléments de X, noté $\mathscr{M}(X)$ s'appelle l'ensemble des mots en l'alphabet X. Le nombre de termes de la suite est appelé longueur du mot. Par exemple si $X = \{a, b\}$ alors les éléments aba et $abba$ sont des mots de longueur respectives 3 et 4. Notons qu'il existe un mot de longueur 0, c'est le mot vide. Sur l'ensemble $G = \mathscr{M}(X)$, on peut définir une loi par juxtaposition (on dit aussi concaténation) ; par exemple $\varphi(aba, abba) = abaabba$. Ceci définit bien une loi sur G.

Remarque(s) 1.1.1. En général, tout comme dans les exemples ci-dessus, on utilise plutôt une notation « binaire » du type $x * y, x + y, xy, x \times y$ pour désigner l'élément $\varphi(x, y)$.

1.1.2 Définition de groupe

Nous allons maintenant définir la notion de groupe.

Définition 1.1.2. Soit $(G, *)$ un ensemble muni d'une loi. On dit que G est un groupe, si les trois axiomes suivants sont vérifiés :

1. Il existe un élément $e \in G$, appelé l'élément neutre de G tel que pour tout $g \in G$: $g * e = e * g = g$.
2. Soit e un élément neutre pour G, alors pour tout élément $s \in G$ il existe un élément $t \in G$, que tel que $s * t = t * s = e$; un tel élément est appelé un inverse de s.
3. Pour tout triplet $(s, t, u) \in G^3$ l'égalité suivante est vérifiée :
$$(s * t) * u = s * (t * u) \ ;$$
on dit que la loi $*$ est associative.

Si de plus, pour tout $(s, t) \in G^2$ on a l'égalité $s * t = t * s$ on dira que $(G, *)$ est un groupe commutatif (ou abélien).

Comme nous allons le voir dans la propriété qui suit, le choix de l'élément neutre e pour énoncer l'existence d'un élément symétrique est superflu.

Propriété 1.1.1. *Soit $(G, *)$ un groupe, alors on a les deux propriétés suivantes :*

1. *Il existe un unique élément neutre dans G.*
2. *Tout élément $s \in G$ admet un unique inverse.*

Démonstration. Soit $e, e' \in G$ deux éléments neutres ; alors par définition pour tout $g \in G$, on a : $e * g = g * e = g$ et $e' * g = g * e' = g$. En particulier, $e * e' = e$ et $e * e' = e'$ ce qui montre le premier point. Pour le deuxième point, soient $s \in G$ et t, t' deux inverses de s. On a donc les égalités : $s * t = t * s = e$ et $s * t' = t' * s = e$; on en déduit les deux égalités suivantes : $t * (s * t') = t * e = t$ et : $(t * s) * t' = e * t' = t'$.

Mais par la propriété d'associativité $t * (s * t') = (t * s) * t'$ d'où $t = t'$. □

Dans le même ordre d'idée, pour vérifier que s est l'inverse de t une seule égalité suffit.

Propriété 1.1.2. *Soient $(G, *)$ un groupe et $(s, t) \in G^2$ tel que $s * t = e$, alors $t * s = e$ et donc $s = t^{-1}$.*

Démonstration. Comme dans la preuve de la proposition précédente, on calcule $s * t * s$ de deux façons. D'une part $s * t * s = (s * t) * s = s$ et $s * t * s = s * (t * s)$. D'où $s = s * (t * s)$ et on conclut en multipliant à gauche par s^{-1}. □

Exemple(s) 1.1.2. Parmi les exemples d'ensemble muni d'une loi, certains sont des groupes.

1. Tout ensemble muni d'un seul élément $\{e\}$ avec la loi $e * e = e$ est un groupe. Ce groupe est appelé le groupe trivial.
2. L'ensemble des réels muni de l'addition est un groupe ; 0 est l'élément neutre et l'inverse de $x \in \mathbb{R}$ est l'opposé $-x$.

   Par contre $\mathbb{R}$ muni de la multiplication n'est pas un groupe ; 0 n'a pas d'inverse ; mais l'ensemble $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ est bien un groupe avec 1 comme élément neutre. Ici on peut remplacer $\mathbb{R}$ par n'importe quel corps comme $\mathbb{Q}$ ou $\mathbb{C}$.

   Pour un anneau $\mathbb{A}$, la situation est légèrement différente : les couples $(\mathbb{A}, +)$ et $(\mathbb{A}^\times, \times)$ sont des groupes, où $\mathbb{A}^\times$ est l'ensemble des éléments inversibles de $\mathbb{A}$ pour la multiplication, par exemple $\mathbb{Z}^\times = \{\pm 1\}$.

3. Si V est un espace vectoriel sur un corps $\mathbb{K}$, alors l'addition est une loi de groupe commutatif sur V.
4. Si X est un ensemble, alors l'ensemble $E = \mathrm{End}(X)$ muni de la loi de composition des applications n'est pas un groupe ; mais le sous-ensemble de E des applications bijectives de X dans lui-même est bien un groupe pour cette loi. Cet ensemble sera noté $\mathrm{Bij}(X)$ ou Σ_X. L'élément neutre est l'application identité que l'on notera $\mathbb{1}_X$, et l'inverse de $f \in \Sigma_X$ est l'application réciproque de f.
5. Les premiers exemples sont des groupes commutatifs (on dit aussi groupes abéliens) ; par contre, si le cardinal de X est plus grand que 3 alors Σ_X n'est pas commutatif (voir l'exercice 4).

Remarque(s) 1.1.2. 1. En pratique, la notation $*$ est rarement employée. En général, la loi est notée avec un point, ou même par simple juxtaposition (le produit de a par b est noté ab). Dans ce cas, on peut aussi utiliser le symbole 1 pour l'unité. L'inverse d'un élément a est noté a^{-1} et si n est un entier positif, a^n désigne le produit de a par lui-même n fois. En posant $a^{-n} = (a^{-1})^n$, et $a^0 = e$ on étend cette notation à tous les entiers relatifs. Les relations usuelles sur les puissances entières pour $\mathbb{R}$ sont vraies dans un groupe, à savoir :

$$a^n a^m = a^{n+m} \text{ et } (a^n)^m = a^{nm}.$$

On utilise aussi fréquemment le symbole $+$, mais l'usage de celui-ci est réservé aux lois commutatives. Dans ce cas, on note 0 l'élément neutre et na la composition de a avec lui-même n fois.

2. Le cardinal de l'ensemble G s'appelle aussi l'ordre du groupe $(G, *)$. On le notera ici : $|G|$.
3. *Quelques règles de calculs.* Soit G un groupe dont la loi est notée par concaténation et d'élément neutre e. Voici quelques règles à retenir :
   (i) Produits de n termes : soit $(g_1, \ldots, g_n) \in G^n$, alors par associativité, dans le produit $(((\cdots(g_1g_2)g_3)\cdots)g_n)$, on peut modifier à sa guise les parenthèses. Tous ces produits sont égaux et seront notés $g_1 \ldots g_n$.
   (ii) Simplification à droite : pour tout $(g, s, t) \in G^3$, $gs = ts \Leftrightarrow g = t$;
   (iii) Simplification à gauche : pour tout $(g, s, t) \in G^3$, $sg = st \Leftrightarrow g = t$;
   (iv) Inverse d'un produit : Pour tout $(s, t) \in G^2$, l'inverse du produit st est égal au produit $t^{-1}s^{-1}$. Plus généralement l'inverse du produit $g_1 \ldots g_n$ est égal à $g_n^{-1} \ldots g_1^{-1}$ (attention à l'ordre des facteurs dans l'inverse).

1.1.3 Sous-groupe, morphismes, produit

Si G est un groupe, et H un sous-ensemble de G, on peut se demander si H lui-même est un sous-groupe (muni de la restriction de la loi sur G), ce qui conduit à la définition suivante.

Définition 1.1.3. Soient $(G, *)$ un groupe et H une partie de G. On dit que H est un sous-groupe de G si H est non vide et si pour tout $(s, t) \in H^2$, on a $st^{-1} \in H$.

Remarque(s) 1.1.3. 1. La condition de stabilité peut être découplée en deux conditions. En effet il y a équivalence :

$$\forall (s,t) \in H^2,\ st^{-1} \in H \quad \Leftrightarrow \quad (\forall (s,t) \in H^2,\ st \in H) \text{ et } (\forall s \in H, s^{-1} \in H).$$

2. On peut donc paraphraser cette définition, en disant qu'une partie H de G est un sous-groupe si H est non vide, stable par multiplication et par passage à l'inverse.

3. Si H est un sous-groupe, alors la restriction de la loi de G à H est bien définie et fait de H un groupe d'élément neutre e, l'élément neutre de G.

   Si on doit vérifier qu'une partie H est un sous-groupe, il est pratique de regarder si l'élément neutre e appartient à G. Si ce n'est pas le cas H n'est pas un sous-groupe ; si c'est le cas, on a montré que H est non vide et il reste à vérifier la stabilité de la multiplication et par passage à l'inverse.

4. Pour montrer qu'un ensemble est un groupe, très souvent on montre que c'est un sous-groupe. Voici un exemple typique : si on considère V un espace vectoriel et $G = \mathrm{GL}(V)$ l'ensemble des applications linéaires et bijectives de V dans lui-même, alors G est un sous-ensemble de Σ_V, non vide puisqu'il contient l'identité, et comme la composée et l'inverse d'une application linéaire sont des applications linéaires, G est un sous-groupe de Σ_V, donc un groupe.

Comme pour les espaces vectoriels, la notion de sous-groupe se comporte bien par rapport aux intersections. On a la propriété suivante :

Propriété 1.1.3. *Soient G un groupe, I un ensemble et $(H_i)_{i\in I}$ un ensemble de sous-groupes de G, alors : $\cap_{i\in I} H_i$ est un sous-groupe de G.*

Démonstration. Comme $\cap_{i\in I} H_i$ contient l'identité, cet ensemble est non vide.

Soit $(x, y) \in \cap_{i\in I} H_i$, alors comme chacun des H_i est un sous groupe, pour tout $i \in I$, on a : $x \in H_i$ et $y^{-1} \in H_i$, et donc $\forall i \in I\ xy^{-1} \in H_i$, c'est à dire $xy^{-1} \in \cap_{i\in I} H_i$. □

Par contre, en général l'union de deux sous-groupes n'est pas un sous-groupe (voir l'exercice 7).

Grâce à cette propriété sur l'intersection de deux sous-groupes, nous allons pouvoir définir le sous-groupe engendré par une partie. Commençons par un théorème.

Propriété 1.1.4. *Soit G un groupe et X une partie de G. Alors l'intersection de tous les sous-groupes contenant X est l'unique plus petit (pour l'inclusion) sous-groupe de G contenant X.*

Démonstration. Notons H l'intersection des sous-groupes contenant X. D'après la propriété 1.1.3, H est un sous-groupe. Soit H' un sous-groupe contenant X, alors par définition de H, on a $H \subset H'$. On en déduit immédiatement l'unicité de H. □

On peut donc parler du plus petit sous-groupe de G contenant X, on le notera $< X >_G$. En algèbre linéaire l'espace vectoriel engendré par une partie peut être défini de deux manières : d'une part comme le plus petit sous-espace contenant cette partie, d'autre part comme l'ensemble des combinaisons linéaires d'éléments de la partie. Nous allons voir un analogue de cette deuxième définition. Si X est une partie d'un groupe G, nous noterons X^{-1}, la partie définie par : $X^{-1} = \{g^{-1} \mid g \in X\}$. Enfin si X est une partie de G, alors l'ensemble des mots sur l'alphabet X peut être vu comme un élément de G si on remplace la juxtaposition par le produit de G. Par convention, le mot vide correspond à l'élément neutre de G. Par un abus de notation, ces mots en $X \subset G$, vus comme éléments de G seront notés de la même façon. On a le théorème suivant :

Théorème 1. *Soit X une partie d'un groupe G, alors le sous-groupe engendré par X est égal à l'ensemble des mots dans l'alphabet $X \cup X^{-1}$. Autrement dit,*

$$< X >_G = \mathscr{M}(X \cup X^{-1}).$$

Démonstration. On vérifie tout d'abord que $\mathscr{M}(X \cup X^{-1})$ est un sous-groupe. Soient x, y deux éléments de $\mathscr{M}(X \cup X^{-1})$, alors il existe deux entiers n et m, deux suites d'éléments de X : $s_1, \ldots, s_n$ et $t_1, \ldots, t_m$ et deux suites d'éléments de l'ensemble $\{\pm 1\}$: $\varepsilon_1, \ldots, \varepsilon_n$ et

$\varepsilon'_1, \ldots, \varepsilon'_m$ tels que $x = s_1^{\varepsilon_1} \ldots s_n^{\varepsilon_n}$ et $y = t_1^{\varepsilon'_1} \ldots t_m^{\varepsilon'_m}$. Alors $y^{-1} = t_m^{-\varepsilon'_m} \ldots t_1^{-\varepsilon'_1}$ et $xy^{-1} = s_1^{\varepsilon_1} \ldots s_n^{\varepsilon_n} t_m^{-\varepsilon'_m} \ldots t_1^{-\varepsilon'_1}$ appartient à $\mathscr{M}(X \cup X^{-1})$. Par minimalité de $< X >_G$, on a l'inclusion $< X >_G \subset \mathscr{M}(X \cup X^{-1})$. Réciproquement, $< X >_G$ étant un sous-groupe qui contient X, il contient tous les éléments de X ainsi que leur inverse, et tous les produits de ces éléments, c'est à dire $\mathscr{M}(X \cup X^{-1})$. □

Remarque(s) 1.1.4. Dans le cas où $X = \{g\}$, les mots en l'alphabet $\{g, g^{-1}\}$ sont les puissances de g. On en déduit que $< g >= \{g^m \mid m \in \mathbb{Z}\}$.

Nous allons maintenant définir les applications entre deux groupes qui sont compatibles avec les lois de ces deux groupes.

Définition 1.1.4. Soient $(G, *)$, $(K, .)$ deux groupes et f une application de G dans K. On dit que f est un morphisme de groupe, si pour tout $(s, t) \in G$, on a : $f(s * t) = f(s).f(t)$.

Exemple(s) 1.1.3. Donnons quelques exemples.

1. Si E et F sont deux espaces vectoriels, et si f est une application linéaire de E dans F, alors en particulier f est un morphisme de groupe pour l'addition sur E et F.
2. Si H est une partie de G, alors H est un sous-groupe de G si et seulement si l'application inclusion de H dans G est un morphisme de groupe (exercice).
3. Si V est un espace vectoriel de dimension finie sur un corps $\mathbb{K}$ et G le groupe $\mathrm{GL}(V)$ défini ci-dessus, on peut considérer l'application déterminant :
$$\begin{array}{rccc} \det : & G & \to & \mathbb{K}^* \\ & A & \mapsto & \det(A). \end{array}$$
Rappelons que pour tout $(A, B) \in \mathrm{GL}(V)$, on a $\det(AB) = \det(A).\det(B)$, ce qui se traduit par : l'application ci-dessus est un morphisme de groupe entre $\mathrm{GL}(V)$ et $\mathbb{K}^*$.
4. Soient G un groupe et $g \in G$, alors l'application de G dans lui-même définie par $\varphi_g(s) = gsg^{-1}$ est un morphisme de groupe (exercice).

Voici quelques propriétés des morphismes.

Propriété 1.1.5. *Soient G_1, G_2 deux groupes, f un morphisme de G_1 dans G_2 ;*

1. *Si e_1, e_2 sont les éléments neutres respectifs de G_1, G_2 alors $f(e_1) = e_2$.*
2. *Si $s \in G_1$ alors $f(s^{-1}) = f(s)^{-1}$.*
3. *Si H_1 un sous-groupe de G_1 et H_2 un sous-groupe de G_2, alors $f(H_1)$ est un sous-groupe de G_2 est $f^{-1}(H_2)$ est un sous-groupe de G_1.*

Démonstration.

1. Il suffit d'écrire $f(e_1) = f(e_1 e_1) = f(e_1)^2$, et en simplifiant par $f(e_1)$ on obtient $e_2 = f(e_1)$.
2. En utilisant le point 1, et le fait que f soit un morphisme, on a :
$$e_2 = f(e_1) = f(ss^{-1}) = f(s)f(s^{-1}).$$
Et donc $f(s^{-1})$ est l'inverse de $f(s)$, c'est à dire $f(s^{-1}) = f(s)^{-1}$.
3. Tout d'abord puisque H_1 est non vide, $f(H_1)$ est également non vide ; soient s_2, t_2 deux éléments de $f(H_1)$, on doit montrer que $s_2 t_2^{-1}$ appartient à $f(H_1)$. Par définition de $f(H_1)$, il existe s_1, t_1 dans H_1 tels que $f(s_1) = s_2$ et $f(t_1) = t_2$. D'autre part, comme f est un morphisme de groupe et d'après les points précédents, on a les égalités :
$$s_2 t_2^{-1} = f(s_1)f(t_1)^{-1} = f(s_1)f(t_1^{-1}) = f(s_1 t_1^{-1}).$$
Comme H_1 est un sous-groupe l'élément $u_1 = s_1 t_1^{-1} \in H_1$ et donc $s_2 t_2^{-1} = f(u_1)$ appartient à H_2. La preuve de l'autre énoncé du point 3 est laissée en exercice.

□

En particulier la pré-image de l'élément neutre $e_2 \in G_2$ est un sous-groupe. Dans le cas d'une application linéaire, c'est un espace vectoriel noté $\ker f$, on garde cette notation dans le cas des morphismes de groupes, c'est à dire :

$$\ker f = \{g \in G_1 \mid f(g) = e_2\}.$$

Comme dans le cas linéaire, l'injectivité de f peut se caractériser par son noyau.

Propriété 1.1.6. *Soient G_1, G_2 deux groupes et f un morphisme de G_1 dans G_2, alors f est injective si et seulement si* $\ker f = \{e_1\}$.

Démonstration. Si f est injective, alors la pré-image de tout élément de G_2 est vide ou réduite à un élément. Mais comme $e_1 \in \ker f$ on a bien l'égalité $\{e_1\} = \ker f$. Réciproquement, supposons que $\ker f = \{e_1\}$. Soit $(s,t) \in G_1^2$ tel que $f(s) = f(t)$, alors on a $f(s)f(t)^{-1} = e_2$. Comme f est un morphisme de groupe, on a donc $f(st^{-1}) = e_2$, c'est à dire st^{-1} appartient à $\ker f$, et donc $st^{-1} = e_1$, *i.e.* $s = t$. □

Voici une propriété très utile des morphismes bijectifs de groupes.

Propriété 1.1.7. *Soient G_1, G_2 deux groupes, f un morphisme bijectif de G_1 dans G_2, alors f^{-1} est un morphisme de groupe.*

Démonstration. Soit $(s_2, t_2) \in G_2^2$, on doit montrer que $f^{-1}(s_2)f^{-1}(t_2) = f^{-1}(s_2t_2)$. Pour cela puisque f est bijective, il existe $(s_1, t_1) \in G_1^2$ tels que $f(s_1) = s_2$ et $f(t_1) = t_2$. On a les égalités suivantes :

$$f^{-1}(s_2t_2) = f^{-1}(f(s_1)f(t_1)) = f^{-1}(f(s_1t_1)) = s_1t_1 = f^{-1}(s_2)f^{-1}(t_2).$$

Vérifier que vous savez justifier chacune des égalités ci-dessus ! □

Cette propriété est à rapprocher d'une propriété semblable en algèbre linéaire : la réciproque d'une application linéaire bijective est linéaire. Mais ce type d'énoncé n'est pas vrai dans tous les contextes. Par exemple, en topologie, la réciproque d'une application continue bijective n'est pas forcément continue.

Concernant les morphismes de groupes, on retrouve la même terminologie que pour les applications linéaires. Un morphisme bijectif de groupe de G_1 dans G_2 est appelé un *isomorphisme*. Lorsqu'il existe un isomorphisme entre deux groupes G_1 et G_2, on dit que les deux groupes sont isomorphes. Ils ne sont pas forcément égaux en tant qu'ensemble, mais en tant que groupe ils sont « identiques », c'est à dire que toutes les propriétés de G_1 en tant que groupe seront vraies pour G_2 (et réciproquement). Par exemple si G_1 est commutatif, G_2 l'est aussi, s'il existe un élément $x_1 \in G_1$ tel que $x_1^n = e$ alors il existe un élément $x_2 \in G_2$ avec la même propriété, etc.

On rencontre aussi le terme *endomorphisme* pour désigner un morphisme de G dans lui-même. Et enfin un endomorphisme bijectif est un *automorphisme*. On notera $\mathrm{Mor}(G_1, G_2)$ l'ensemble des morphismes de G_1 dans G_2 et $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G dans lui-même. Les morphismes définis dans l'exemple 1.1.3.4 sont des automorphismes (le vérifier) ; on les appellent les automorphismes intérieurs de G. On note $\mathrm{Int}(G) = \{\varphi_g \mid g \in G\}$, l'ensemble des automorphismes intérieurs.

L'ensemble des automorphismes de G est un groupe. On a en effet les propriétés suivantes.

Propriété 1.1.8. *Soit G un groupe, on a les trois assertions suivantes.*

(i) Soient φ, ψ deux automorphismes de G, alors $\varphi \circ \psi$ est un automorphisme de G.

(ii) $\mathrm{Aut}(G)$ *est un groupe (pour la composition des applications).*

(iii) $\mathrm{Int}(G)$ *est un sous-groupe de* $\mathrm{Aut}(G)$.

Démonstration.

(i) La preuve de ce point est laissée en exercice.

(ii) On va utiliser la méthode évoquée dans l'exemple 1.1.2. L'ensemble $\mathrm{Aut}(G)$ est un sous-ensemble du groupe : $\mathrm{Bij}(G)$. Montrons que c'est un sous-groupe. Soient φ, ψ deux automorphismes. Alors on a déjà vu que ψ^{-1} est un automorphisme de G (voir la proposition 1.1.7). Ensuite, grâce au point (i), $\varphi \circ \psi$ est un automorphisme de groupe.

(iii) On considère l'application suivante :

$$\begin{array}{rcccl} \Theta & : & G & \to & \mathrm{Int}(G) \\ & & g & \mapsto & \varphi_g \end{array}$$

où pour tout $s \in G$, $\varphi_g(s) = gsg^{-1}$. Alors d'une part, par définition $\mathrm{Im}\,\Theta = \mathrm{Int}(G)$ et d'autre part Θ est un morphisme de groupe (le vérifier). Et donc par la propriété 1.1.5, $\mathrm{Int}(G)$ est un sous-groupe.

□

Terminons cette section en introduisant la notion de produit de groupes.

Propriété 1.1.9. *Soit n un entier naturel non nul, et soient n groupes :*

$$(G_1, *_1), (G_2, *_2), \ldots, (G_n, *_n).$$

Alors le produit cartésien $\prod_{i=1}^{n} G_i$ est un groupe pour la loi produit définie par :

$$(s_1, s_2, \ldots, s_n) * (t_1, t_2, \ldots, t_n) = (s_1 *_1 t_1, s_2 *_2 t_2, \ldots, s_n *_n t_n).$$

Pour cette loi de groupe, les n projections π_j de $\prod_{i=1}^{n} G_i$ dans G_j sont des morphismes de groupes.

Démonstration. La preuve est laissée en exercice. □

1.1.4 Rappels sur les relations d'équivalence

Soit X un ensemble ; une relation sur X est un sous-ensemble $\mathscr{R} \subset X \times X$. En général, $(x, y) \in \mathscr{R}$ est noté $x \sim y$. On va ici s'intéresser aux relations d'équivalence.

Définition 1.1.5. Soit X un ensemble muni d'une relation $\sim$. Cette relation sera appelée relation d'équivalence si les trois propriétés suivantes sont vérifiées :

1. La relation est réflexive : pour tout $x \in X$ $x \sim x$.
2. La relation est symétrique : pour tout couple $(x, y) \in X^2$, $x \sim y$ implique $y \sim x$.
3. La relation est transitive : pour tout $(x, y, z) \in X^3$, $x \sim y$ et $y \sim z$ implique $x \sim z$.

Exemple(s) 1.1.4. Voici quelques exemples de relations d'équivalences.

1. Sur tout ensemble X, on peut définir la relation telle que tout élément n'est en relation qu'avec lui-même (c'est la relation définie par l'égalité).
2. Toujours sur un ensemble X quelconque, on peut définir la relation où pour tout couple $(x, y) \in X$, $x \sim y$.
3. Soit n un entier positif ou nul ; sur l'ensemble $\mathbb{Z}$, on définit $p \sim q$ si et seulement si $p - q$ est un multiple de n (donc $p = q$ si $n = 0$). Cela définit bien une relation d'équivalence (exercice).

4. Si f est une application entre deux ensembles : $f : X \to Y$, alors on peut définir la relation suivante sur X : $x \sim y$ si et seulement si $f(x) = f(y)$. C'est une relation d'équivalence (exercice).

Si X est un ensemble muni d'une relation d'équivalence, et si $x \in X$ alors on définit la classe d'équivalence de x ou la classe d'équivalence passant par x le sous-ensemble de X défini par

$\overline{x} = \{y \in X \,|\, y \sim x\}$.

On dit aussi que x est un représentant de la classe $\overline{x}$. Ces classes vérifient les propriétés suivantes.

Propriété 1.1.10. *Soit X muni d'une relation d'équivalence $\sim$, soit $(x, y) \in X^2$, on a équivalence entre les propriétés suivantes :*

(i) $\overline{x} = \overline{y}$;

(ii) $x \in \overline{y}$;

(iii) $y \in \overline{x}$;

(iv) $\overline{x} \cap \overline{y} \neq \emptyset$;

(v) $x \sim y$.

Démonstration.

$(i) \Rightarrow (ii)$ Remarquons d'abord que puisque la relation est réflexive, $x \in \overline{x}$. Donc si $\overline{x} = \overline{y}$, alors $x \in \overline{y}$ et donc $x \sim y$.

$(ii) \Rightarrow (iii)$ Si $x \in \overline{y}$, alors $x \sim y$ et donc par symétrie $y \in \overline{x}$.

$(iii) \Rightarrow (iv)$ Si $y \in \overline{x}$, alors $y \in \overline{x} \cap \overline{y}$ et donc $\overline{x} \cap \overline{y}$ est non vide.

$(iv) \Rightarrow (v)$ Supposons que $\overline{x} \cap \overline{y} \neq \emptyset$, alors il existe $z \in \overline{x} \cap \overline{y}$, et donc par définition $x \sim z$ et $y \sim z$, et par les propriétés de réflexivité et de transitivité des relations d'équivalence, on a bien $x \sim y$.

$(v) \Rightarrow (i)$ Supposons $x \sim y$, et soit $z \in \overline{x}$, alors $z \sim x$ et donc $z \sim y$, d'où $z \in \overline{y}$ et on a $\overline{x} \subset \overline{y}$. L'autre inclusion se montre de la même façon.

□

Rappelons que si X est un ensemble et que si $\mathscr{P} \subset \mathscr{P}(X)$ est un ensemble de parties de X deux à deux disjointes qui recouvrent X, on dit que $\mathscr{P}$ est une partition de X. La propriété précédente montre que l'ensemble des classes d'équivalence forme une partition de X. Réciproquement, si on se donne une partition de X, alors on peut définir une relation d'équivalence, en définissant $x \sim y$ si et seulement s'il existe un sous-ensemble de X de la partition qui contienne x et y.

On va maintenant donner un nom à cette partition définie par une relation d'équivalence, c'est la notion d'ensemble quotient qui va nous être très utile pour la suite.

Définition 1.1.6. Soit X un ensemble muni d'une relation d'équivalence. L'ensemble quotient $X/\sim$ est le sous-ensemble de $\mathscr{P}(X)$ défini par :

$$X/\sim = \{\overline{x} \,|\, x \in X\}.$$

On définit l'application quotient :

$$\begin{array}{rccc} \pi & : & X & \to & X/\sim \\ & & x & \mapsto & \overline{x} \end{array}.$$

D'après les remarques précédentes, l'application π est bien définie et surjective (exercice).

Exemple(s) 1.1.5. Reprenons maintenant les quatre exemples de relations d'équivalence donnés précédemment et pour chacun d'eux calculer l'ensemble et l'application quotient.

1. Si les éléments de X ne sont en relation qu'avec eux-même, dans ce cas pour tout $x \in X$, on a $\overline{x} = \{x\}$ et l'application quotient est dans ce cas une bijection.
2. Si deux éléments quelconques de X sont en relation, alors la partition $X/\sim$ contient un seul élément qui est X lui-même.
3. Si n est un entier positif ou nul, et $X = \mathbb{Z}$ muni de la relation de congruence : $p \sim q$ si et seulement si $p - q$ est un multiple de n. Alors la classe d'équivalence de p est définie par $\overline{p} = \{p + kn \,|, k \in \mathbb{Z}\}$; si $n = 0$ les classes d'équivalence contiennent un seul élément, et on se retrouve dans un cas particulier du premier exemple. Si $n \neq 0$, en utilisant la division euclidienne de p par n, chaque classe contient un entier compris entre 0 et $n-1$. La partition réalisée par la relation d'équivalence est donc la suivante :

   $$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \ldots \cup \overline{n-1}.$$

   et l'application quotient $\pi(p)$ peut s'interpréter comme le reste modulo n de l'entier p. Notons que l'on a fait le choix ici de représenter chaque classe par un entier compris entre 0 et $n - 1$, mais on aurait très bien pu choisir un autre paramétrage de l'espace quotient, par exemple les entiers entre n et $2n - 1$.
4. Soit f de X dans Y, et la relation définie par $x \sim y$ si $f(x) = f(y)$. Alors la classe d'équivalence $\overline{x}$ est l'ensemble des y qui ont la même image que x. Rappelons que cet ensemble s'appelle aussi la fibre de f passant par x. L'ensemble $X/\sim$ est donc l'ensemble des fibres de f.

   Remarquons que par définition de la relation si $\overline{x} = \overline{y}$, alors $f(x) = f(y)$, ou autrement dit l'application f ne dépend pas du représentant choisi dans $\overline{x}$, on peut donc définir une application :

   $$\begin{array}{rcccc} \overline{f} & : & X/\sim & \to & Y \\ & & \overline{x} & \mapsto & f(x) \end{array}$$

   Comme exercice, vérifier que $\overline{f}$ est une application injective.

La situation du dernier exemple ci-dessus conduit à considérer le problème plus général suivant. Soit X un ensemble muni d'une relation d'équivalence $\sim$, soit g une application de X dans un ensemble Y. Quand peut-on définir une application $\overline{g}$ par l'égalité : $\overline{g}(\overline{x}) = g(x)$? Si g est quelconque, l'application $\overline{g}$ n'est pas bien définie, en effet on peut avoir $\overline{x} = \overline{y}$ et $g(x) \neq g(y)$. Ce qui conduit à la définition suivante :

Définition 1.1.7. Soit X un ensemble muni d'une relation d'équivalence $\sim$, soit g une application de X dans un ensemble Y. On suppose que g est constante sur les classes d'équivalences de $\sim$, c'est à dire que $\forall (x, y) \in X^2$, $x \sim y \Rightarrow g(x) = g(y)$, alors il existe une application $\overline{g}$ de $X/\sim$ dans Y définie par $\overline{g}(\overline{x}) = g(x)$.

Lorsque la fonction $\overline{g}$ est définie, on dit que la fonction g « passe » au quotient. Terminons cette section par un résultat dans le cas particulier où l'ensemble X est de cardinal fini.

Propriété 1.1.11. *Soit X un ensemble fini muni d'une relation d'équivalence $\sim$, alors $X/\sim$ et toutes les classes d'équivalence de $\sim$ sont de cardinal fini, et on a :*

$$|X| = \sum_{C \in X/\sim} |C|.$$

Démonstration. Comme toutes les classes sont incluses dans X elles sont de cardinal fini, et comme ces classes sont distinctes, il ne peut pas y en avoir un nombre infini. La deuxième assertion est la simple conséquence du partitionnement de X par les classes d'équivalence. □

1.1.5 Rappels sur $\mathbb{Z}$, ses sous-groupes, ses quotients

L'ensemble des entiers relatifs muni de l'addition est un groupe. On peut facilement donner la liste de tous les sous-groupes de $\mathbb{Z}$. Commençons par une remarque simple. Soit $n \in \mathbb{N}$, alors l'ensemble $n\mathbb{Z}$ des multiples de n est un sous-groupe de $\mathbb{Z}$. En effet, si p et q sont deux multiples de n, alors $p - q$ est évidemment un multiple de n. En fait il n'y a pas d'autres sous-groupes de $\mathbb{Z}$.

Théorème 2. *Soit H un sous-groupe de $\mathbb{Z}$, alors il existe un unique entier $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.*

Démonstration. Montrons l'existence de n : soit H un sous-groupe de $\mathbb{Z}$; si $H = \{0\}$, alors $H = 0\mathbb{Z}$ et c'est terminé dans ce cas. Supposons donc que $H \neq \{0\}$. On sait que si $h \in H$ alors $-h \in H$, donc $H \cap \mathbb{N}^* \neq \emptyset$, et soit $n = \min H \cap \mathbb{N}^*$. Maintenant considérons $h \in H$; effectuons la division euclidienne de h par n : il existe un couple $(q, r) \in \mathbb{Z}$ tel que $0 \leq r < n$ et $h = nq + r$. Comme $n \in H$, alors nq qui est la somme de n avec lui-même q fois est dans H, et donc $r = h - nq$ appartient à H également. Si r est non nul alors $r \in H \cap \mathbb{N}^*$, ce qui amène une contradiction entre la définition de n et la condition $r < n$. Donc $r = 0$ et $h = nq \in \mathbb{Z}$.

L'unicité est laissée en exercice. □

Remarque(s) 1.1.5. Rappelons qu'il est facile de déterminer si deux tels sous-groupes de $\mathbb{Z}$ sont inclus. En effet $m\mathbb{Z} \subset n\mathbb{Z}$ si et seulement si n divise m (attention au sens).

Pour chaque sous-groupe de $\mathbb{Z}$, nous allons définir une relation d'équivalence.

Définition 1.1.8. Soit $n \in \mathbb{N}^*$ et soit $(p, q) \in \mathbb{Z}^2$, on pose $p \sim_n q$ si $p - q \in n\mathbb{Z}$.

Cette relation a déjà été considérée (voir les exemples 1.1.4). L'ensemble quotient $\mathbb{Z}/\sim_n$ que l'on note aussi $\mathbb{Z}/n\mathbb{Z}$ est un groupe. En effet, on a le théorème suivant.

Théorème 3. *L'addition dans $\mathbb{Z}$ définit une loi sur $\mathbb{Z}/n\mathbb{Z}$, et $\mathbb{Z}/n\mathbb{Z}$ muni de cette loi est un groupe.*

Démonstration. La loi $+$ sur $\mathbb{Z}$ passe au quotient, en effet si $p \sim_n p'$ et si $q \sim_n q'$ alors $p+q \sim_n p'+q'$, on peut donc définir : $\overline{p}\bar{+}\overline{q} = \overline{p+q}$. Ensuite, on vérifie facilement les propriétés nécessaires à partir des propriétés sur $\mathbb{Z}$. Par exemple pour l'associativité, si $\overline{p}, \overline{q}, \overline{r}$ sont trois éléments de $\mathbb{Z}/n\mathbb{Z}$, on peut écrire :

$$(\overline{p}\bar{+}\overline{q})\bar{+}\overline{r} = (\overline{p+q})\bar{+}\overline{r} = \overline{(p+q)+r} = \overline{p+(q+r)} = \overline{p}\bar{+}\overline{q+r} = \overline{p}\bar{+}(\overline{q}\bar{+}\overline{r}).$$

On vérifie ensuite que $\overline{0}$ est l'élément neutre et que si $\overline{p} \in \mathbb{Z}/n\mathbb{Z}$ alors $\overline{-p}$ est son inverse (exercice). □

Finissons cette section en rappelant un autre résultat vu l'année dernière, en donnant un énoncé qui utilise la théorie des groupes.

Théorème 4. Le théorème des restes chinois. *Soient n, m deux entiers non nuls et premiers entre eux. Alors il existe un isomorphisme de groupes entre $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/nm\mathbb{Z}$.*

Démonstration. Si $l \in \mathbb{Z}$ et $r \in \mathbb{N}^*$, dans cette preuve nous noterons $\bar{l}^{\{r\}}$ la classe de l modulo r. On définit l'application suivante :

$$\begin{array}{rccc} \Psi & : & \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & & l & \mapsto & (\bar{l}^{\{n\}}, \bar{l}^{\{m\}}). \end{array}$$

Cette application est un morphisme de groupe. De plus, si $\overline{l}^{\{mn\}} = \overline{s}^{\{mn\}}$ alors $l - s$ est un multiple de mn donc de m et de n ; on en déduit que $\Psi(l) = \Psi(s)$. On peut donc définir une application définie sur le quotient $\mathbb{Z}/nm\mathbb{Z}$:

$$\begin{array}{rccc} \overline{\Psi} & : & \mathbb{Z}/nm\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & & \overline{l}^{\{mn\}} & \mapsto & \overline{\Psi}(\overline{l}^{\{mn\}}) = \Psi(l). \end{array}$$

Cette application est un morphisme de groupe (car Ψ est un morphisme de groupe). Calculons son noyau :

$$\ker \overline{\Psi} = \left\{ \overline{l}^{\{mn\}} \,|\, \overline{l}^{\{n\}} = \overline{0}^{\{n\}} \text{ et } \overline{l}^{\{m\}} = \overline{0}^{\{m\}} \right\}.$$

Mais si un entier l est divisible par deux nombres n et m premiers entre eux, alors il est divisible par leur produit mn. Donc $\overline{l}^{\{mn\}} = \overline{0}^{\{mn\}}$ et $\overline{\Psi}$ est injective. Comme les ensembles de départ et d'arrivée sont de même cardinal *fini*, $\overline{\Psi}$ est bijective, ce qui achève la preuve. □

Remarque(s) 1.1.6.

1. En fait le produit dans $\mathbb{Z}$ permet de définir une multiplication dans $\mathbb{Z}/nm\mathbb{Z}$ et dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ qui fait de ces deux groupes des anneaux. Et le morphisme $\overline{\Psi}$ ci-dessus est un morphisme d'anneau.
2. Par une récurrence très simple, on peut étendre ce résultat au cas de r entiers $n_1, n_2, \ldots, n_r$ premiers deux à deux.

1.1.6 L'ordre d'un élément, ordre et indice d'un sous-groupe

Rappelons qu'il est d'usage dans la théorie des groupes d'appeler ordre d'un groupe G son cardinal et que celui-ci est noté $|G|$. Définissons maintenant l'ordre d'un élément de G.

Définition 1.1.9. Soit G un groupe et $g \in G$, on appelle ordre de g (noté $o(g)$) l'ordre du groupe engendré par g, c'est à dire $o(g) = | < g > |$.

Évidemment l'ordre d'un groupe ou d'un élément n'est pas forcément fini, on dit alors que le groupe ou l'élément est d'ordre infini.

Exemple(s) 1.1.6.

1. Si G est quelconque alors son élément neutre e est d'ordre 1 ; en effet on a $< e >= e$. Réciproquement, si $g \in G$ est d'ordre 1, alors $< g >= \{e\}$ et donc g est égal à e.
2. Soit $X = \{1, 2, 3\}$, $G = \Sigma_X$ et σ l'élément de G qui échange 1 et 2 et qui laisse 3 invariant. Il est immédiat de vérifier que $\sigma = \sigma^{-1}$ et que pour tout $m \in \mathbb{Z}$, $\sigma^{2m} = e$ et $\sigma^{2m+1} = \sigma$. On en déduit que $< \sigma >= \{\sigma^n \,|\, n \in \mathbb{Z}\} = \{e, \sigma\}$ et σ est d'ordre 2.
3. Soit G le groupe $\mathbb{Z}$ et $m \in \mathbb{Z}$; on a vu que si $m = 0$, alors il est d'ordre 1. Si $m \neq 0$, alors $< m >= |m|\mathbb{Z}$ et m est d'ordre infini.
4. Soit $G = \mathbb{Z}/4\mathbb{Z}$, alors G a quatre éléments $G = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. On a vu que $\overline{0}$ est l'élément neutre de G donc d'ordre 1. Les éléments $\overline{1}$ et $\overline{3}$ sont d'ordre 4, et $\overline{2}$ est d'ordre 2 (exercice).

Nous allons voir maintenant une autre façon de calculer l'ordre d'un élément. Commençons par une remarque : soit G un groupe dont la loi est notée par simple concaténation, et soit $g \in G$, on a vu précédemment que pour tout $(m, n) \in \mathbb{Z}$, on a l'égalité : $g^m g^n = g^{m+n}$. Ceci peut se traduire par la propriété qui suit.

Propriété 1.1.12. *Soient G et $g \in G$ comme ci-dessus, et soit ψ_g l'application de $\mathbb{Z}$ dans G définie par $\psi_g(m) = g^m$. L'application ψ_g est un morphisme de groupe, et de plus* $\operatorname{Im} \psi_g =< g >$.

Démonstration. Il reste à vérifier la deuxième assertion. Pour cela, on se souvient que $< g >$ est l'ensemble des mots en l'alphabet $\{g\}$ et donc $< g >= \{g^n \mid n \in \mathbb{Z}\}$. $\square$

Le noyau du morphisme ψ_g est directement lié à l'ordre de g. En effet, on a la propriété suivante.

Théorème 5. *Soient G, $g \in G$ et ψ_g comme ci dessus. Soit $n \in \mathbb{N}$ tel que $\ker \psi_g = n\mathbb{Z}$ Alors on a les assertions suivantes :*

(i) Si $n = 0$, alors l'application ψ_g est un isomorphisme de groupe entre $\mathbb{Z}$ et $\operatorname{Im} \psi_g$; si $n \neq 0$ alors l'application ψ_g induit un isomorphisme entre $\mathbb{Z}/n\mathbb{Z}$ et $\operatorname{Im} \psi_g$.

(ii) On a $\ker(\psi_g) \neq \{0\}$ si et seulement si g est d'ordre fini et dans ce cas on a $n = o(g)$.

Démonstration.

(i) Si $n = 0$, alors $\ker \psi_g = \{0\}$ et l'application ψ_g est injective, d'où l'assertion.
Si $n \neq 0$, alors considérons l'application suivante :

$$\begin{array}{rccc} \overline{\psi_g} & : & \mathbb{Z}/n\mathbb{Z} & \to & < g > \\ & & \overline{m} & \mapsto \psi_g(m). & \end{array}$$

Cette application est bien définie ; en effet si $\overline{m} = \overline{l}$, alors $m - l$ est un multiple de n, c'est à dire qu'il existe un $k \in \mathbb{Z}$ tel que $l = m + kn$, mais alors :

$$\psi_g(l) = \psi_g(m + kn) = \psi_g(m)\psi_g(n)^k = \psi_g(m)$$

puisque $n \in \ker \psi_g$ et donc $\psi_g(n) = e$.
Cette application est surjective, puisque $< g >= \{g^m \mid m \in \mathbb{Z}\}$.
Son noyau est réduit à $\{\overline{0}\}$, en effet si $\overline{\psi_g}(\overline{m}) = \psi_g(m) = e$, alors $m \in \ker \psi_g$ et donc $\overline{m} = \overline{0}$, cette application est donc bijective.
Finalement, c'est un morphisme de groupe. En effet soit $(m, l) \in \mathbb{Z}^2$, alors :

$$\overline{\psi}_g(\overline{m} + \overline{l}) = \overline{\psi}_g(\overline{m + l}) = \psi_g(m + l) = \psi_g(m)\psi_g(l) = \overline{\psi}_g(\overline{m})\overline{\psi}_g(\overline{l}).$$

L'application $\overline{\psi}_g$ est donc un isomorphisme entre $\mathbb{Z}/n\mathbb{Z}$ et $\operatorname{Im} \psi_g =< g >$.

(ii) Si $\ker \psi_g \neq \{0\}$, alors grâce au point précédent, on a :

$$o(g) = | < g > | = |\mathbb{Z}/n\mathbb{Z}| = n.$$

Réciproquement si $\ker \psi_g = \{0\}$, alors dans ce cas l'application ψ_g est injective et on a un isomorphisme entre $\mathbb{Z}$ et $< g >$, et g est d'ordre infini.

$\square$

À partir de cette caractérisation de l'ordre d'un élément, on peut en obtenir quelques propriétés.

Propriété 1.1.13. *Soient G un groupe et g un élément de G d'ordre fini égal à n. On a les propriétés suivantes.*

(i) Si $g^m = e$, alors n divise m ;

(ii) $n = \min\{m \in \mathbb{N}^* \text{ tel que } g^m = e\}$.

Démonstration.

(i) D'après la propriété précédente, $\ker\ \psi_g = o(g)\mathbb{Z}$; soit m tel que $g^m = e$, par définition de $\ker \psi_g$ on a donc $m \in \ker \psi_g$, et comme $\ker \psi_g$ est un groupe on a l'inclusion $m\mathbb{Z} \subset \ker \psi_g = o(g)\mathbb{Z}$ ce qui implique $n \mid m$ d'après la remarque 1.1.5.

(ii) Il suffit de remarquer que n est le plus petit multiple positif non nul de n.

□

Remarque(s) 1.1.7. 1. Attention à la conclusion du du point (i) : une erreur classique est d'écrire que si $g^m = e$, alors g est d'ordre m ce qui évidemment faux.

2. Par contre si on montre qu'il existe n un entier tel que $g^m = e$ si et seulement m est un multiple de n, alors par définition n est égal à l'ordre de g.

L'application ψ_g permet de classer à isomorphismes près les groupes qui sont engendrés par un seul élément. Commençons par définir ces sous-groupes.

Définition 1.1.10. Soit G un groupe. S'il existe $g \in G$ tel que $G =< g >$, on dit que G est monogène. Si de plus G est d'ordre fini, on dit que G est cyclique.

Propriété 1.1.14. *Soit G un groupe monogène ; alors si G est d'ordre infini, G est isomorphe à $\mathbb{Z}$ et si G est cyclique, alors il existe $n \in \mathbb{N}^*$ tel que G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration. Soit $g \in G$ tel que $G =< g >$; alors on a égalité : $\operatorname{Im} \psi_g = G$ et donc si g est d'ordre infini, ψ_g est un isomorphisme entre $\mathbb{Z}$ et G, et si g est d'ordre fini égal à n, $\overline{\psi_g}$ est un isomorphisme entre $\mathbb{Z}/n\mathbb{Z}$ et G. □

Exemple(s) 1.1.7. Toutes les assertions de cet exemple sont à montrer en exercice.

Soit $n \in \mathbb{N}^*$; on définit l'ensemble des racines n-ièmes de l'unité :

$$\mathbb{U}_n = \{z \in \mathbb{C} \,|\, z^n = 1\}.$$

L'ensemble $\mathbb{U}_n$ est un sous-groupe de $\mathbb{C}^*$ de cardinal n, de plus il est engendré par l'élément $\exp(\frac{2i\pi}{n})$ et donc $\mathbb{U}_n$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

1.1.7 Le théorème de Lagrange

Nous allons maintenant énoncer et démontrer le théorème de Lagrange. Soient G un groupe et H un sous-groupe, nous allons commencer par définir une relation d'équivalence sur G.

Définition 1.1.11. Soit H un sous-groupe de G, on définit la relation suivante : pour tout $(s,t) \in G^2$, $s \sim_H t$ si et seulement si $st^{-1} \in H$.

Propriété 1.1.15. *La relation $\sim_H$ est une relation d'équivalence.*

Démonstration. On vérifie les trois propriétés qui définissent une relation d'équivalence. D'abord comme $ss^{-1} = e \in H$, la relation est réflexive. Ensuite si $s \sim_H t$ alors $st^{-1} \in H$, mais H étant un sous-groupe, $ts^{-1} \in H$ et donc $t \sim_H s$, la relation est symétrique. Enfin si $s \sim_H t$ et $t \sim_H u$, alors $st^{-1} \in H$ et $tu^{-1} \in H$, mais alors $st^{-1}tu^{-1} = su^{-1} \in H$, *i.e.* $s \sim_H u$, la relation est transitive. □

On peut maintenant définir l'indice de H dans G.

Définition 1.1.12. Soient G un groupe, H un sous-groupe et $\sim_H$ la relation définie ci-dessus. Alors le cardinal de $G/\sim_H$ est appelé l'indice de H dans G. Cet indice est noté $[G : H]$.

La preuve du théorème de Lagrange repose essentiellement sur la propriété qui suit.

Propriété 1.1.16. *Soit C_e la classe d'équivalence passant par l'identité et C une autre classe d'équivalence ; alors $C_e = H$, et il existe une bijection entre C_e et C. En conséquence, toutes les classes d'équivalence ont donc le même cardinal que celui de H.*

Démonstration.

Soit C_e la classe d'équivalence contenant l'identité. Si $t \in C_e$, alors par définition $t \sim_H e$ et donc $te^{-1} = t \in H$. Et donc $C_e \subset H$. Réciproquement si $t \in H$ alors $te^{-1} \in H$ et $t \sim e$. Soit C une classe d'équivalence (qui est non vide par définition), et soit $s \in C$. Alors on définit l'application suivante :

$$\begin{array}{rccc} \Theta & : & C_e & \to & G \\ & & h & \mapsto & hs \end{array}$$

On vérifie d'abord que $\operatorname{Im}\Theta = C$. C'est une simple traduction, en effet :

$$t \in \operatorname{Im}\Theta \Leftrightarrow (\exists h \in H) \text{ tel que } t = hs \Leftrightarrow ts^{-1} = h \in H \Leftrightarrow t \sim_H s \Leftrightarrow t \in C.$$

On peut donc considérer l'application Θ comme une application de C_e dans C. Par définition elle est surjective. Soient maintenant h et h' tels que $\Theta(h) = \Theta(h')$ alors $hs = h's$, et donc $h = h'$ et Θ est bijective. □

Théorème 6. *Théorème de Lagrange.*

Soient G un groupe fini et H un sous-groupe. Alors l'ordre et l'indice de H sont finis et on a l'égalité :

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

En conséquence $|H|$ et $[G : H]$ divise l'ordre de G. En particulier l'ordre de tout élément de G divise l'ordre de G.

Démonstration. Comme $H \subset G$, H est de cardinal fini. De même, il y a un nombre fini de classes d'équivalence de $\sim_H$ dans G et donc $[G : H]$ est fini. Ensuite, la propriété 1.1.11 sur les relations d'équivalence permet d'écrire :

$$|G| = \sum_{C \in G/\sim_H} |C|.$$

Mais on a vu que toutes les classes avaient le même cardinal que le cardinal de H, et donc la somme ci-dessus est simplement la somme de $[G : H]$ termes égaux à $|H|$, soit $|G| = |H|[G : H]$. La dernière remarque provient de la propriété 1.1.13 qui affirme que l'ordre d'un élément est égal à l'ordre du groupe engendré par cet élément. □

Avec l'aide de ce théorème, on a maintenant un outil puissant pour commencer à classifier les groupes d'ordre finis. Par exemple, il est maintenant facile de montrer que les groupes d'ordre un nombre premier sont cycliques, ou bien qu'il existe, à isomorphisme près deux groupes d'ordre 6 (exercice).

Pour les groupes d'ordre 8 la situation est un peu plus compliquée : vous verrez dans l'exercice 34, qu'à isomorphisme près, il y a trois groupes commutatifs distincts et deux groupes non commutatifs d'ordre 8. L'un de ces groupe est le groupe des quaternions que nous allons maintenant définir. Considérons les quatre éléments suivants de $\mathrm{Mat}_2(\mathbb{C})$:

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} ; I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} ; J = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} ; K = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}.$$

Définition 1.1.13. On définit l'ensemble suivant :

$$Q_8 = \{\pm\mathbb{1}, \pm I, \pm J, \pm K\}.$$

On vérifie par un simple calcul que $I^2 = J^2 = K^2 = -\mathbb{1}$ et que $IJ = -JI = K$; de ces égalités on déduit que les trois éléments I, J et K sont d'ordre 4 et que Q_8 est un groupe non commutatif d'ordre 8.

1.1.8 Exercices

Exercice 1 ⓔ

Pour une partie H d'un groupe G montrer l'équivalence :

$$\forall (s,t) \in H^2,\ st^{-1} \in H \quad \Leftrightarrow \quad (\forall (s,t) \in H^2,\ st \in H) \text{ et } (\forall s \in H, s^{-1} \in H)$$

Exercice 2 ⓒ

Parmi les paires $(G, \cdot)$ ci-dessous, déterminer celles qui sont des groupes :

(i) $\mathbb{Q}^\times$, $x \cdot y = xy$;

(ii) $\{2^n \mid n \in \mathbb{Z}\}$, $x \cdot y = xy$;

(iii) $\{\frac{1+2m}{1+2n} \mid n, m \in \mathbb{Z}\}$, $x \cdot y = xy$.

Exercice 3 ⓐ

On considère l'ensemble E des matrices carrées à coefficients réels de la forme

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, \quad a \in \mathbb{R}^\times, \quad b \in \mathbb{R}$$

muni du produit des matrices.

(i) Montrer que E est ainsi muni d'une loi de composition interne associative.

(ii) Déterminer tous les éléments neutres à droite de E.

(iii) Montrer que E n'admet pas d'élément neutre à gauche.

(iv) Soit e un élément neutre à droite. Montrer que tout élément de E possède un inverse à gauche pour cet élément neutre, i.e.

$$\forall g \in E \quad \exists h \in E \quad hg = e.$$

Exercice 4 ⓒ

Déterminer (à isomorphisme près) tous les groupes d'ordre ≤ 5 (On fera cet exercice sans utiliser le théorème de Lagrange). En déduire qu'un groupe non commutatif possède au moins 6 éléments. Montrer que le groupe symétrique Σ_3 est non commutatif.

Exercice 5 ⓔ

Soit G un groupe dans lequel tout élément x vérifie $x^2 = e$. Montrer que G est commutatif.

Exercice 6 ⓒ

Montrer que dans un groupe G, toute partie X non vide finie stable par la loi de composition est un sous-groupe (*Si $x \in X$, considérer l'ensemble des puissances de x.*)

Donner un contre-exemple à la propriété précédente dans le cas d'une partie infinie.

Exercice 7 ⓒ

Soit G un groupe et H, K deux sous-groupes de G. Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

Exercice 8 ⓔ

Soit G un groupe tel que l'application $x \to x^{-1}$ soit un morphisme. Montrer que G est commutatif.

Exercice 9 ⓔ

Montrer que l'application exponentielle $\exp : (\mathbb{R}, +) \to (\mathbb{R}_+^*, \times)$ est un isomorphisme de groupes. Qu'en est-il de l'application $\exp : (\mathbb{C}, +) \to (\mathbb{C}^*, \times)$?

Exercice 10 ⓒ

Sur $\mathbb{R}^2$, on considère la relation suivante : $(a, b) \sim (c, d)$ si et seulement si : $a^2+b^2 = c^2+d^2$.

(i) Montrer que la relation ci-dessus est une relation d'équivalence.

(ii) Décrire les classes d'équivalence.

(iii) Décrire géométriquement l'espace quotient.

Exercice 11 ⓒ

Soit G un groupe d'ordre pair. Montrer qu'il existe un élément $x \in G$, $x \neq e$ tel que $x^2 = e$. (Indication : considérer la partition de G en sous-ensembles du type $\{x, x^{-1}\}$.)

Exercice 12 ⓔ

Montrer qu'un groupe fini dont l'ordre est un nombre premier est cyclique.

Exercice 13 ⓒ

Soit G un groupe. Soient a et b deux éléments de G. Montrer que si ab est d'ordre fini, alors ba l'est également et son ordre est celui de ab.

Exercice 14 ⓒ

Soient G un groupe et H et K deux sous-groupes de G. On note $HK := \{hk \mid h \in H, k \in K\}$.

(i) Montrer sur un exemple dans $G = \Sigma_3$ qu'en général les ensembles HK et KH ne sont pas égaux et ne sont pas des sous-groupes de G.

(ii) Montrer que HK est un sous-groupe de G si et seulement si $HK = KH$.

(iii) Montrer que si H et K sont finis alors $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$.

Indication : on pourra définir une application surjective de $H \times K$ dans HK, puis dénombrer les éléments dans les classes d'équivalence de la relation induite par cette application.

Exercice 15 ⓔ

Déterminer tous les sous-groupes de Q_8 (voir la définition 1.1.13).

Exercice 16 ⓔ

Soit G un groupe, e l'élément neutre de G, et $x \in G$ un élément d'ordre fini r.

(i) Montrer que pour tout $m \in \mathbb{Z}$ on a $x^m = e$ si, et seulement si, r divise m.

(ii) Montrer que pour tout $n \in \mathbb{Z}$ l'ordre de l'élément x^n est égal à r/d, où $d = \mathrm{pgcd}(r, n)$. (*On pourra commencer par montrer que l'ordre de x^n divise r/d.*)

Exercice 17 ⓐ(**d'après une partie du sujet du contrôle continu 2018-2019**)

(i) Soit G un groupe d'ordre fini n, et H_1, H_2 deux sous-groupes de G même ordre un nombre premier p. Quelle peut être l'intersection $H_1 \cap H_2$?

(ii) Soit G un groupe d'ordre cyclique d'ordre 35, montrer que G contient un élément d'ordre 5 et un élément d'ordre 7.

(iii) Montrer que l'assertion ci-dessus reste vraie si G est d'ordre 35, mais non forcément cyclique.

1.2 Actions de groupes, ensembles quotients

Définition 1.2.1. Soient G un groupe et X un ensemble. On dit que G agit sur X (ou que X est un G-ensemble) s'il existe une application φ de $G \times X$ dans X telle que :

(i) pour tout $x \in X$, $\varphi(e, x) = x$;

(ii) pour tout $(s, t) \in G^2$ et pour tout $x \in X$, on a : $\varphi(st, x) = \varphi(s, \varphi(t, x))$.

Remarque(s) 1.2.1.

1. Nous allons dans ce cours plutôt utiliser la notation $g.x$ pour $\varphi(g, x)$. Avec cette notation, les axiomes de la définition deviennent : pour tout $x \in X$ et pour tout $(s, t) \in G^2$, $e.x = x$ et $s.(t.x) = (st).x$.
2. Nous avons en fait défini la notion d'action *à gauche*. On peut aussi définir la notion d'action *à droite*. Par souci de simplification, nous considérerons ici uniquement des actions à gauche.

Donnons maintenant des exemples.

Exemple(s) 1.2.1.

1. Si G est un groupe et X un ensemble, on peut toujours définir une action de G sur X en posant pour tout $(g, x) \in G \times X$, $g.x = x$. Ceci définit bien une action (le vérifier), on dit que c'est l'action triviale.
2. Soient E un espace vectoriel et $\mathscr{E}$ un espace affine de direction E, alors à tout couple $(v, P) \in E \times \mathscr{E}$ on peut associer le point $Q = P + v$ (la translation de vecteur v). Ceci définit une action du groupe additif sous-jacent à E sur $\mathscr{E}$.
3. Si G est un groupe et H un sous-groupe, alors on peut définir trois actions de H sur G : par multiplication à droite, par multiplication à gauche et par conjugaison. On différencie ces trois actions par un indice sous le point, avec la convention suivante : γ pour gauche, δ pour droite et κ pour la conjugaison.
   (i) L'action de H sur G par multiplication à gauche (on dit aussi par translation à gauche) est définie en posant pour tout $(h, g) \in H \times G$, $h._\gamma g = hg$.
   (ii) L'action de H sur G par multiplication à droite (on dit aussi par translation à droite) est définie en posant pour tout $(h, g) \in H \times G$, $h._\delta g = gh^{-1}$.
   (iii) L'action de H sur G par conjugaison est définie en posant pour tout $(h, g) \in H \times G$, $h._\kappa g = hgh^{-1}$.

   Comme exercice, vous vérifierez que chacun des trois exemples ci-dessus est bien une action, ce qui vous permettra notamment de comprendre la nécessité de considérer l'inverse pour l'action par multiplication à droite.
4. Si G agit sur X et si H est un sous-groupe de G alors par restriction, H agit sur X.
5. Soient X un ensemble et $G = \mathrm{Bij}(X)$ alors G agit sur X, en posant pour tout $(g, x) \in G \times X$, $g.x = g(x)$. Cela est bien défini puisque si $g \in G$, alors par définition g est une application (bijective) de X dans lui-même.
6. Soit V un espace vectoriel sur un corps $\mathbb{K}$, alors le groupe $\mathrm{GL}(V)$ agit sur V par restriction de l'action de $\mathrm{Bij}(V)$ sur V définie ci-dessus.

À partir d'une action de G sur un ensemble X, on peut définir une relation d'équivalence.

Propriété 1.2.1. *Soient G un groupe et X un ensemble sur lequel agit G, alors la relation sur X définit par $\forall (x, y) \in X^2$, $x \sim y \Leftrightarrow \exists g \in G$ tel que $g.x = y$ est une relation d'équivalence.*

Démonstration. D'après la première propriété d'une action de groupe, pour tout $x \in X$ $e.x = x$ et donc la relation est réflexive.

Si $x \sim y$, alors il existe $g \in G$ tel que $g.x = y$ mais alors, d'après la deuxième propriété d'une action de groupe : $g^{-1}.y = g^{-1}.(g.x) = (g^{-1}g).x = x$; la relation est donc symétrique.

Pour finir si $x \sim y$ et $y \sim z$ alors il existe $(s,t) \in G^2$ tel que $y = s.x$ et $z = t.y$. On en déduit $(ts).x = t.(s.x) = t.y = z$ et donc $z \sim x$, ce qui montre la transitivité. □

Lorsque G agit sur X, les classes d'équivalence sont appelées les orbites de G dans X. L'orbite passant par un point $x \in X$ sera noté O_x ; par définition, on a :

$$O_x = \{g.x \mid g \in G\}.$$

On trouve aussi la notation $G.x$ pour O_x. La propriété qui suit est une simple, mais utile traduction de la propriété 1.1.10 dans le cas particulier de la relation d'équivalence induite par l'action d'un groupe.

Propriété 1.2.2. *Soient G un groupe et X un ensemble muni d'une action de G, soit $(x,y) \in X^2$, on a équivalence entre les propriétés suivantes :*

(i) $O_x = O_y$;

(ii) $x \in O_y$;

(iii) $y \in O_x$;

(iv) $O_x \cap O_y \neq \emptyset$;

(v) $x \sim y$.

L'ensemble des orbites réalisent donc une partition de X, cette partition est appelée le quotient de X par G, quotient noté X/G. Comme dans le cas des relations d'équivalence, on définit l'application quotient π de X dans X/G, qui à tout $x \in X$ fait correspondre $\pi(x) = O_x$.

À tout $x \in X$, on associe l'ensemble suivant : $G_x = \{g \in G \mid g.x = x\}$. Cet ensemble est un sous-groupe de G ; on a en effet la propriété qui suit.

Propriété 1.2.3. *Soient X un ensemble et G un groupe agissant sur X, alors pour tout $x \in X$ l'ensemble G_x est un sous-groupe de G. Ce groupe est appelée le stabilisateur de x ou le sous-groupe d'isotropie en x.*

Démonstration. Cette preuve est laissée en exercice. □

On va voir qu'une action d'un groupe G sur un ensemble X est équivalent à se donner un morphisme de G dans $\mathrm{Bij}(X)$.

En effet, d'une part si ρ est un morphisme de groupe de G dans $\mathrm{Bij}(X)$, alors G agit sur X, en posant : $g.x = \rho(g)(x)$. (Il est immédiat de vérifier que cela définit bien une action).

D'autre part si G agit sur X, alors on peut définir une application ρ de G dans $\mathrm{Bij}(X)$ en posant : $\rho(g)(x) = g.x$. On a la propriété suivante :

Propriété 1.2.4. *Dans la situation précédente, l'application ρ est un morphisme de groupe.*

Démonstration. Soit $(s,t) \in G^2$, alors pour tout $x \in X$, on a les égalités suivantes :

$$\rho(st)(x) = (st).x = s.(t.x) = s.\rho(t)(x) = \rho(s) \circ \rho(t)(x).$$

La deuxième égalité se déduit de la seconde propriété vérifiée par une action de groupe ; les autres proviennent de la définition de ρ. On a donc $\rho(st) = \rho(s) \circ \rho(t)$, l'application ρ est bien un morphisme. □

Propriété 1.2.5. *Soient X un ensemble et G un groupe agissant sur X et soit ρ le morphisme de G dans $\mathrm{Bij}(X)$ associé, alors on a l'égalité :*

$$\ker \rho = \bigcap_{x \in X} G_x.$$

Démonstration. Soit $g \in G$; l'égalité provient des équivalences suivantes :

$$g \in \bigcap_{x \in X} G_x \Leftrightarrow \forall x \in X,\ g.x = x \Leftrightarrow \forall x \in X,\ \rho(g)(x) = x \Leftrightarrow \rho(g) = \mathbb{1}_X \Leftrightarrow g \in \ker \rho.$$

□

Voici maintenant un peu de vocabulaire. Soient X un ensemble et G un groupe agissant sur X.

Soit $x \in X$, si pour tout $g \in G$, on a $g.x = x$, on dit que x est un point fixe pour l'action de G (on dit aussi que x est invariant). L'ensemble des points fixes de X est noté X^G. Plus généralement si H est une partie de G (pas forcément un sous-groupe), on note X^H l'ensemble des éléments invariants par H, c'est à dire :

$$X^H = \{x \in X \,|\, \forall h \in H,\ h.x = x\}.$$

Par définition on a égalité :

$$X^G = \{x \in X \text{ tel que } |O_x| = 1\}$$

(exercice).

Soit Y une partie de X. On dit que Y est stable par G (ou G-stable), si pour tout $(g, y) \in G \times Y$, $g.y \in Y$. Remarquons que les orbites sont les « atomes » des parties G-stables, au sens qu'une orbite est G-stable et qu'une partie G-stable est une union d'orbites. En particulier si Y ne contient que des points fixes, alors Y est stable. Mais il peut exister des parties G-stables dont les éléments ne sont pas tous invariants.

Soit Z un autre ensemble muni d'une action de G et Ψ une application de X dans Z. On dit que Ψ est équivariante (ou un G-morphisme), si pour tout $(g, x) \in G \times X$, on a : $\Psi(g.x) = g.\Psi(x)$.

Si X contient une seule orbite, on dit que G agit transitivement sur X.

Si pour tout x, le sous-groupe d'isotropie en x est réduit à l'élément neutre, on dit que G agit librement ou que l'action de G sur X est libre.

Lorsque le morphisme ρ défini ci-dessus est injectif, on dit que l'action est fidèle, on trouve aussi parfois le terme d'action effective.

Grâce à la propriété 1.2.5, on constate que si l'action est libre, alors elle est fidèle, mais la réciproque est fausse (voir les exemples ci-après).

Exemple(s) 1.2.2.

1. L'action de G sur lui-même par multiplication à droite est une action fidèle, libre et transitive, de plus $G^G = \{e\}$. Et on a exactement les mêmes propriétés pour l'action de G sur lui-même par multiplication à gauche.
2. Le groupe $\mathrm{GL}(V)$ agit fidèlement sur l'espace V. Le groupe G a deux orbites dans V : $\{0\}$ et $V \setminus \{0\}$. Cette action n'est pas libre et on a l'égalité $V^{\mathrm{GL}(V)} = \{0\}$.

1.2.1 Étude détaillée des trois actions d'un sous-groupe H sur G.

On rappelle que dans la situation où H est un sous-groupe de G, on a défini trois actions de H dans G. Nous allons les étudier plus précisément ici.

L'action par conjugaison

Commençons par l'action par conjugaison. Par souci de simplification, on va supposer $H = G$; l'action est définie de la façon suivante : pour tout $(s, t) \in G^2$, $s._\kappa t = sts^{-1}$. Si $t \in G$,

l'orbite de $t \in G$ pour cette action s'écrit $O(t) = \{sts^{-1} \,|\, s \in G\}$; on l'appelle la classe de conjugaison de t. Le stabilisateur d'un élément $t \in G$ s'écrit :

$$G_t = \{s \in G \,|\, sts^{-1} = t\}.$$

C'est donc l'ensemble des éléments qui commutent avec t, on l'appelle le centralisateur de t dans G et on le note $Z(t)$.

Cette action n'est pas fidèle en général, son noyau est appelée le centre de G, on le note $Z(G)$ et comme d'après la propriété 1.2.5 il est égal à l'intersection de tous les stabilisateurs, on a l'égalité :

$$Z(G) = \{s \in G \,|\, \forall t \in G,\ sts^{-1} = t\}.$$

Le centre de G est donc l'ensemble des éléments de G qui commutent à tous les éléments de G.

Notons que $Z(G)$ est également l'ensemble des points fixes de G, c'est à dire $Z(G) = G^G$. L'origine de cette double interprétation de $Z(G)$ provient du fait que nous sommes ici dans une situation particulière où G est à la fois le groupe qui agit et l'ensemble X muni de l'action de G. Dans la première définition $Z(G)$ est défini comme un sous-groupe de G ; dans la deuxième définition $Z(G)$ est un simple sous-ensemble de G.

Rappelons que dans le cas où le groupe est commutatif, cette action par conjugaison est triviale. Les classes de conjugaison sont réduites à un élément, le centralisateur de tout élément et le centre de G sont égaux à G.

Pour finir avec cette action, notons qu'elle peut s'étendre à l'ensemble $\mathscr{G}$ des sous-groupe de G. En effet, si $s \in G$ et H est un sous-groupe de G, alors l'ensemble suivant :

$$sHs^{-1} = \{shs^{-1} \,|\, h \in H\}$$

est un sous-groupe de G (le vérifier). On en déduit une action de G sur $\mathscr{G}$ définie comme suit :

$$\begin{array}{ccc} G \times \mathscr{G} & \to & \mathscr{G} \\ (s, H) & \mapsto & sHs^{-1} \end{array}.$$

Cette action va permettre d'associer à tout sous-groupe H deux sous-groupes de G. Tout d'abord le stabilisateur de H pour l'action ci-dessus qui est appelé le normalisateur de H dans G ; il est défini par :

$$\mathrm{Nor}(H) = \{s \in G \,|\, sHs^{-1} = H\}.$$

On définit également le centralisateur de H dans G (noté $\mathrm{Z}(H)$) comme l'ensemble des points fixes de H :

$$\mathrm{Z}(H) = G^H = \{s \in G \,|\, \forall h \in H, hsh^{-1} = s\}.$$

Les éléments de G^H sont donc les éléments de G qui commutent avec tous les éléments de H. On vérifie directement que $\mathrm{Z}(H)$ et H sont des sous-groupes de $\mathrm{Nor}(H)$.

L'action par multiplication à gauche

Rappelons que si H est un sous-groupe de G, on a défini l'action suivante de H sur G :

$$\begin{array}{ccc} H \times G & \to & G \\ (h, t) & \mapsto & h.\gamma t = ht \end{array}$$

Pour cette action, l'orbite contenant l'élément $t \in G$ s'écrit :

$$O_t^\gamma = \{ht \,|\, h \in H\} = Ht.$$

Ces orbites s'appellent les classes à droite de H dans G (l'inversion des termes entre droite et gauche peut paraître surprenante, mais l'usage s'est imposé dans ce sens). Rappelons qu'à une action, on peut associer une relation d'équivalence. Ici cette relation s'écrit, pour tout $(s,t) \in G^2$, $s \sim_{H^\gamma} t$ si et seulement si $s \in Ht$ que l'on peut re-écrire $st^{-1} \in H$.

On reconnaît ici la relation d'équivalence utilisée pour démontrer le théorème de Lagrange ! Par conséquent, si on note $G/^\gamma H$ l'ensemble quotient pour cette action, alors ce quotient qui est donc égal l'ensemble des classes à droite est aussi égal à l'ensemble $G/\sim_H$ vu dans la propriété 1.1.16. Il y a donc $[G : H]$ classes à droite, et dans le cas où H est fini, chacune d'elles contient le même nombre d'éléments, à savoir le cardinal de H.

Les classes à droites étant des classes d'équivalence, on peut traduire la propriété 1.1.10 sur les conditions d'égalité de deux classes dans ce cas particulier.

Propriété 1.2.6. *Soient G un groupe, H un sous-groupe de G et $(s,t) \in G^2$, alors les assertions suivantes sont équivalentes :*

(i) $Ht = Hs$;

(ii) $t \in Hs$;

(iii) $s \in Ht$;

(iv) $Ht \cap Hs \neq \emptyset$

(v) *s et t sont dans la même orbite pour l'action par multiplication à gauche de H dans G.*

L'ensemble $G/^\gamma H$ de toutes les classes à droite est muni d'une action du groupe G, (action qui provient de l'action de G sur lui-même par multiplication à droite).

$$\begin{array}{ccc} G \times G/^\gamma H & \to & G/^\gamma H \\ (g, Hs) & \mapsto & Hsg^{-1} \end{array}.$$

En exercice, vérifier que cette action est transitive et que le stabilisateur de la classe $eH = H$ est le groupe H lui-même.

L'action par multiplication à droite

Cette action est définie par :

$$\begin{array}{ccc} H \times G & \to & G \\ (h,t) & \mapsto & h._\delta t = th^{-1} \end{array}.$$

Pour cette action, l'orbite passant par l'élément $t \in G$ s'écrit :

$$O_t^\gamma = \{th^{-1} \,|\, h \in H\} = \{th \,|\, h \in H\} = tH.$$

Ces orbites s'appellent les classes à gauche de H dans G et l'ensemble quotient $G/^\delta H$ est l'ensemble de toutes les classes à gauche. On a l'équivalent de la propriété 1.2.6 sur l'égalité des classes et on a également une action du groupe G sur l'ensemble des classes à gauche :

$$\begin{array}{ccc} G \times G/^\delta H & \to & G/^\delta H \\ (g, sH) & \mapsto & gsH \end{array},$$

et comme pour les classes à droite, cette action est transitive, et l'isotropie de la classe H est H lui-même.

Comparaison des classes à gauche et à droite

Une question naturelle à ce stade est de se demander si la classe à droite Hs et la classe à droite sH sont égales. Évidemment si le groupe est commutatif c'est le cas, mais ce n'est pas toujours vrai, comme on le verra plus tard. Pourtant les deux ensembles quotients $G/^{\gamma}H$ et $G/^{\delta}H$ ne sont pas vraiment différents. Pour les comparer nous allons introduire la notion de G-isomorphisme.

Définition 1.2.2. Soit G un groupe et soient X, Y deux ensembles munis d'une action de G. On dit que X et Y sont G-isomorphes s'il existe une application Θ de X dans Y bijective et G-équivariante.

Remarque(s) 1.2.2. (i) On peut faire la même remarque que dans le cas de deux groupes isomorphes : si deux ensembles sont G-isomorphes, ils ne sont pas égaux, mais les propriétés liées à l'action de G sont exactement les mêmes sur les deux ensembles.

(ii) Il est facile de montrer que si Θ est un G-isomorphisme alors l'application réciproque Θ^{-1} est également G-équivariante, et donc un G-isomorphisme. Ceci est similaire à la propriété 1.1.7 que l'on a rencontrée au sujet des morphismes de groupes bijectifs.

Propriété 1.2.7. *Les ensembles quotients $G/^{\gamma}H$ et $G/^{\delta}H$ sont G-isomorphes.*

Démonstration. C'est l'inversion dans le groupe qui va permettre de définir l'application recherchée. Pour définir cette application, nous avons besoin d'un premier résultat. Soit $(s,t) \in G^2$, alors si $sH = tH$, on a $Hs^{-1} = Ht^{-1}$. En effet, si $sH = tH$, alors $s \in tH$, et donc $s^{-1} \in Ht^{-1}$, soit $Hs^{-1} = Ht^{-1}$. Le même raisonnement montre que si $Hs = Ht$, alors $s^{-1}H = t^{-1}H$. Ces deux remarques permettent de définir deux applications :

$$\begin{array}{rccc} \Theta : & G/^{\delta}H & \to & G/^{\gamma}H \\ & sH & \mapsto & Hs^{-1} \end{array}$$

et

$$\begin{array}{rccc} \Psi : & G/^{\gamma}H & \to & G/^{\delta}H \\ & Hs & \mapsto & s^{-1}H \end{array}.$$

Ces deux applications sont évidemment réciproques l'une de l'autre, ce sont bien des bijections. Il reste à vérifier que Θ est équivariante. Soit $(g,s) \in G^2$, alors d'une part, on a :

$$\Theta(g.sH) = \Theta(gsH) = Hs^{-1}g^{-1}$$

et d'autre part :

$$g.\Theta(sH) = g.Hs^{-1} = Hs^{-1}g^{-1}.$$

On a bien égalité entre ces deux termes et Θ est équivariante. □

Pour alléger les notations, j'utiliserais la notation simplifiée G/H qui par convention désignera $G/^{\delta}H$ c'est à dire l'ensemble des classes à gauche :

$$G/H = \{gH \mid g \in G\}.$$

Nous allons voir maintenant que chacune des orbites d'une action d'un groupe est G-isomorphe à un ensemble G/H.

Propriété 1.2.8. *Soient X un ensemble et G un groupe agissant sur X ; soient $x \in X$, G_x et O_x respectivement le stabilisateur de x et l'orbite passant par x. Alors les ensembles G/G_x et O_x sont G-isomorphes.*

Démonstration. On commence par définir l'application Ψ suivante :

$$\begin{array}{rccc} \Psi : & G & \to & O_x \\ & g & \mapsto & g.x \end{array}.$$

Cette application est surjective par définition. Elle est G-équivariante où G agit sur lui-même par multiplication à gauche :

$$s.\Psi(g) = s.(g.x) = (sg).x = \Psi(sg) = \Psi(s.g).$$

Comme G_x stabilise x, pour tout $(g, g') \in G^2$ si $gG_x = g'G_x$, alors $\Psi(g) = \Psi(g')$, l'application Ψ passe au quotient, et il existe donc une application :

$$\begin{array}{rccc} \overline{\Psi} : & G/G_x & \to & O_x \\ & gG_x & \mapsto & g.x \end{array}.$$

L'application $\overline{\Psi}$ hérite de Ψ les propriétés de surjectivité et de G-équivariance. Il reste à vérifier que $\overline{\Psi}$ est injective. Soit $(g, g') \in G^2$ tel que $\overline{\Psi}(gG_x) = \overline{\Psi}(g'G_x)$, alors $g.x = g'.x$, c'est à dire $g'^{-1}g.x = x$, et donc $g'^{-1}g \in G_x$, d'où $g \in g'G_x$ et $gG_x = g'G_x$. □

Une conséquence de cette propriété est que le cardinal de l'orbite passant par $x \in X$ est égal au cardinal de G/G_x (c'est à dire $[G : G_x]$) et ce cardinal ne dépend donc pas de x mais de l'orbite à laquelle il appartient. Rappelons que si G est fini alors $[G : G_x] = |G/G_x| = |G|/|G_x|$.

Voyons une simple application de cela dans l'exemple qui suit.

Exemple(s) 1.2.3. Reprenons la dernière question de l'exercice 14. Il s'agit de montrer que si H et K sont deux sous-groupes finis d'un groupe G, alors

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Pour cela, on définit une action du groupe produit $H \times K$ sur HK :

$$\begin{array}{ccc} H \times K \times HK & \to & HK \\ (h, k, h'k') & \mapsto & hh'k'k^{-1} \end{array}.$$

On vérifie que cette action est transitive, en effet $e \in HK$ et $\forall (h, k) \in H \times K$, $(h, k^{-1}).e = hk$, et donc tous les éléments de HK sont dans la même orbite que e. Calculons maintenant l'isotropie du point e :

$$(H \times K)_e = \{(h, k) \,|\, hk^{-1} = e\} = \{(h, h \,|\, h \in H \cap K)\}.$$

Ce groupe d'isotropie est donc isomorphe à $H \cap K$, on en déduit immédiatement l'égalité demandée.

Le résultat de la propriété 1.2.8 va être également utilisé pour écrire l'équation aux classes qui permet de calculer le nombre d'éléments d'un ensemble fini X muni d'une action d'un groupe.

Théorème 7. Équation aux classes. *Soient X un ensemble de cardinal fini et G un groupe d'ordre fini agissant sur X. Alors on a égalité :*

$$|X| = \sum_{O \in X/G} |O|.$$

De plus pour tout $O \in X/H$, et pour $x \in O$, on a égalité : $|O| = [G : G_x] = |G|/|G_x|$, en particulier $|O|$ divise $|G|$.

Démonstration. La première égalité est une simple application de la propriété 1.1.11. La seconde égalité est une conséquence de la propriété 1.2.8. □

Exemple(s) 1.2.4. Nous allons donner deux exemples d'application de ce résultat.

1. Lorsque G agit librement sur X, toutes les orbites sont de cardinal $|G|$, et comme il y a $|X/G|$ orbites, l'équation aux classes s'écrit :

$$|X| = |X/G||G|.$$

   ceci permet de redémontrer le théorème de Lagrange. En effet soient G un groupe fini et H un sous-groupe agissant sur G par multiplication à droite. Alors l'action est libre (exercice) ; on en déduit que

$$|G| = |G/^{\delta}H||H|.$$

   On retrouve bien le théorème de Lagrange, en se rappelant que $|G/^{\delta}H|$ est égal à $[G : H]$.

2. Soit p un nombre premier ; on dit qu'un groupe G est un p-groupe si son cardinal est une puissance positive de p. En particulier le groupe trivial est un p-groupe pour tout p. Évidemment, les p-groupes qui vont nous intéresser sont les p-groupes non triviaux.

   Nous allons montrer qu'un p-groupe non trivial admet un centre non trivial. Supposons donc $|G| = p^n$, avec $n \geq 1$ et considérons l'action de G sur lui-même par conjugaison, c'est à dire $\forall (s,t) \in G^2$, $s._{\kappa}t = sts^{-1}$. Séparons les orbites en deux sous-ensembles : celles qui sont de cardinal un d'un côté, puis les autres. Les orbites de cardinal un sont des points fixes qui correspondent aux éléments de $Z(G)$. Il y a donc $|Z(G)|$ orbites de cardinal un. Soit r le nombre d'orbites de cardinal plus grand ou égal à deux. Alors on peut supposer que $r \geq 1$ car si $r = 0$, $Z(G) = G$ est l'assertion est démontrée. Appelons $O_1, \ldots, O_r$ ces orbites, alors d'après le théorème 7, on a l'égalité :

$$|G| = p^n = |Z(G)| + \sum_{i=1}^{r} |O_i|.$$

   Pour tout $i = 1, \ldots, r$ $|O_i|$ divise p^n, mais comme $|O_i| \geq 2$, pour tout $i = 1, \ldots, r$ $|O_i|$ est divisible par p. Comme p divise aussi $|G|$, il divise $|Z(G)|$ ce qui permet de conclure.

1.2.2 Exercices

Exercice 18 ⓒ

Parmi les applications ψ définies ci-dessous, déterminer celles qui définissent une action de G sur E, et dans ce cas décrire les orbites :

1. $G = n\mathbb{Z}$, $E = \mathbb{Z}$, $\psi : (nk, a) \mapsto a + nk$.
2. $G = \mathbb{Z}$, $E = \mathbb{R}$, $\psi : (n, x) \mapsto x + n$.
3. $G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, a \in \mathbb{C}^*, b \in \mathbb{C} \right\}$, $E = \mathbb{C}$, $\psi : \left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, z \right) \mapsto az^2 + b$.

Exercice 19 ⓒ

Soit G un groupe agissant sur un ensemble X.

1. Montrer que pour tout $g \in G$ et tout $x \in X$, $G_{g.x} = gG_xg^{-1}$.
2. Si G est abélien et si l'action est transitive et fidèle, montrer qu'elle est aussi libre. [On rappelle qu'une action est dite libre si tous les stabilisateurs sont triviaux. Elle est dite fidèle si le morphisme de G dans Σ_X est injectif.]

Exercice 20 ⓒ

Montrer que la relation d'équivalence de l'exercice 10 de la section précédente provient d'une action du groupe suivant :

$$\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}.$$

Calculer les sous-groupes d'isotropies pour cette action. Indication : penser à l'identification de $\mathbb{R}^2$ avec $\mathbb{C}$.

Exercice 21 ⓒ

Montrer que tout groupe fini G est isomorphe à un sous-groupe de Σ_n, où n est l'ordre de G. Indication : faire agir G sur lui-même par translations, en déduire un morphisme de groupes $\varphi : G \to \Sigma_G$ puis montrer que φ est injectif.

Exercice 22 ⓒ

Soit G un groupe fini agissant sur un ensemble fini X.

1. On suppose que toute orbite contient au moins deux éléments, que $|G| = 15$ et que $\mathrm{card}(X) = 17$. Déterminer le nombre d'orbites et le cardinal de chacune.
2. On suppose que $|G| = 33$ et $\mathrm{card}(X) = 19$. Montrer qu'il existe au moins une orbite réduite à un élément.

Exercice 23 ⓐ

Le but de cet exercice est de démontrer le théorème de Cauchy : si p est un nombre premier et si G est un groupe d'ordre divisible par p, alors G a un élément d'ordre p. On considère l'ensemble E des p-uplets $(g_1, \ldots, g_p)$ d'éléments de G tels que $g_1 g_2 \ldots g_p = e$.

$$E = \{(g_1, \ldots, g_p) \in G^p \mid g_1 g_2 \ldots g_p = e\}$$

1. Calculer le cardinal de E. (C'est une puissance du cardinal de G.)
2. Montrer que si $(g_1, \ldots, g_p)$ appartient à E, alors $(g_2, g_3, \ldots, g_p, g_1)$ appartient aussi à E.
3. En déduire une action naturelle de $\mathbb{Z}/p\mathbb{Z}$ sur E.
4. Quels peuvent être les cardinaux des orbites ?
5. Montrer que le nombre d'orbites de cardinal 1 est divisible par p.
6. En déduire le théorème de Cauchy. [Remarquer que $(e, e, \ldots, e)$ est un point fixe. Il en existe donc au moins un autre.]

Exercice 24 ⓐ

On veut montrer ici que tout groupe G d'ordre 15 est commutatif. On considère l'action de G sur lui-même par conjugaison.

1. Montrer que les orbites sont de cardinal 1, 3 ou 5.
2. Montrer que le centre $Z(G)$ est à la fois l'ensemble des points fixes, et l'intersection de tous les stabilisateurs.
3. Supposons que $|Z(G)| = 3$.
   (a) Montrer qu'il y a sept orbites : trois de cardinal 1 et quatre de cardinal 3.
   (b) Pour $x \notin Z(G)$, calculer $|G_x|$ et aboutir à une contradiction.
4. Supposons que $|Z(G)| = 5$.
   (a) Déterminer le nombre d'orbites de chaque cardinal.
   (b) Pour $x \notin Z(G)$, calculer $|G_x|$ et aboutir à une contradiction.
5. Supposons que $|Z(G)| = 1$.
   (a) Déterminer le nombre d'orbites de chaque cardinal.
   (b) Étudier les ordres des éléments dans chacune de ces orbites et aboutir à une contradiction. [Indication : vérifier qu'une orbite contient des éléments de même ordre, puis compter le nombre d'éléments d'éléments d'ordre 3 et 5 de plusieurs façons.]
6. En déduire que $Z(G) = G$. Conclure.

1.3 Sous-groupes distingués, groupes quotients, théorèmes d'isomorphismes

1.3.1 Motivations

Soient G un groupe et H un sous-groupe de G ; le but de cette section est de regarder à quelles conditions le quotient G/H peut être muni d'une structure de groupe. Plus précisément, on cherche une loi de groupe sur G/H telle que l'application quotient π de G dans G/H soit un morphisme de groupe.

Pour cela regardons l'exemple que nous avons déjà à notre disposition. Si $G = \mathbb{Z}$, alors le groupe $\mathbb{Z}/n\mathbb{Z}$ a été défini (en L2) comme l'ensemble des classes d'équivalence de $\mathbb{Z}$ pour la relation suivante : $p \sim_n q$ si et seulement si $p - q$ est un multiple de n. On a vu cette année que $\mathbb{Z}/n\mathbb{Z}$ est aussi l'ensemble des classes à gauche (ou à droite) du sous-groupe $n\mathbb{Z}$ dans $\mathbb{Z}$, où l'ensemble des orbites pour le sous-groupe $n\mathbb{Z}$ agissant sur $\mathbb{Z}$ par translation à gauche (ou à droite). C'est ce qui explique d'ailleurs la notation $\mathbb{Z}/n\mathbb{Z}$ plutôt que $\mathbb{Z}/\sim_n$. Regardons précisément la loi sur le quotient. Soit $(p, q) \in \mathbb{Z}^2$, et considérons les deux classes à gauche $p + n\mathbb{Z}$ et $q + n\mathbb{Z}$. Alors la somme de ces deux classes à gauche est définie par :

$$p + n\mathbb{Z} + q + n\mathbb{Z} = p + q + n\mathbb{Z}.$$

Pour justifier cette égalité, on utilise le fait que $q + n\mathbb{Z} = n\mathbb{Z} + q$, c'est à dire que pour tout $q \in \mathbb{Z}$ la classe à gauche $q + n\mathbb{Z}$ est égale à la classe à droite $n\mathbb{Z} + q$. Ceci est vrai dans notre cas puisque $\mathbb{Z}$ est commutatif. Mais pour un groupe non commutatif, cette égalité n'est plus vraie en général (voir le numéro 3 des exemples 1.3.1 ci-dessous). Cette remarque va nous conduire à définir la notion de sous-groupe distingué ou sous-groupe normal.

1.3.2 Sous-groupe distingué et groupe quotient

Commençons donc par une définition.

Définition 1.3.1. Soient G un groupe et K un sous-groupe de G ; on dit que K est distingué dans G, ou que K est un sous-groupe normal de G, si pour tout $s \in G$, on a $sK = Ks$.

Lorsque K est un sous-groupe distingué de G, on note $K \triangleleft G$.

Exemple(s) 1.3.1.

1. Si G est commutatif alors tous les sous-groupes de G sont distingués.
2. Les sous-groupes triviaux $\{e\}$ et G sont distingués.
3. Considérons $G = \Sigma_3$ le groupe des permutations de l'ensemble $\{1, 2, 3\}$. Soient $\tau = (12)$ et $\sigma = (123)$. Soit K le groupe engendré par σ, ce groupe est d'ordre 3, il y a donc deux classes à droites ainsi que deux classes à gauche. La partie K est une classe à droite ainsi qu'une classe à gauche. Et si $a \in G$, $a \notin K$ alors aK est une classe à gauche distincte de K et Ka est une classe à droite distincte de K. Comme les classes à droite (et à gauche) réalisent une partition de G, on a $aK = G \setminus K = Ka$ et K est distingué.

   Soit H le groupe engendré par τ ; celui-ci est d'ordre 2, il existe donc 3 classes à gauche et 3 classes à droite qui contiennent chacune deux éléments. Les classes à gauche sont les suivantes :

   $$\Big\{H,\ (13)H = \{(13), (123)\},\ (23)H = \{(23), (132)\}\Big\}\ ;$$

   et voici les classes à droites :

   $$\Big\{H,\ H(13) = \{(13), (132)\},\ H(23) = \{(23), (123)\}\Big\}.$$

On constate que les classes à gauche et à droite contenant (13) sont distinctes et H n'est donc pas distingué.

On peut maintenant utiliser la notion de groupe distingué pour définir une structure de groupe sur le quotient.

Théorème 8. *Soient G un groupe et K un sous-groupe distingué de G ; on note G/K l'ensemble des classes à gauche, et π l'application quotient de G dans G/K. Il existe sur le quotient G/K une unique structure de groupe telle que l'application π soit un morphisme.*

Démonstration. On commence par définir une loi sur G/K. Pour cela montrons d'abord que pour tout $(s, s', t, t') \in G^4$ tel que $sK = s'K$ et $tK = t'K$ alors $stK = s't'K$. En effet comme $sK = s'K$, $s' \in sK$ et de même $t' \in tK$. On en déduit que $s't' \in sKtK$, mais comme $tK = Kt$ et que $KK = K$ (car K est un sous-groupe), on a $s't' \in stK$, c'est à dire $s't'K = stK$. On peut donc définir le produit suivant sur les classes à gauche : $sK * tK = stK$.

Montrons que cette loi $*$ définit une structure de groupe sur G/K. Commençons par montrer que $K = eK$ est un élément neutre. Pour cela, soit $s \in G$, alors $sK * K = seK = sK = esK = K * sK$.

Pour tout $s \in G$, l'inverse de sK est simplement $s^{-1}K$ en effet $sK * s^{-1}K = ss^{-1}K = K = s^{-1}sK = s^{-1}K * sK$.

L'associativité découle de l'associativité de la loi sur G ; soit $(s, t, u) \in G^3$, alors

$$(sK * tK) * uK = (st)K * uK = (st)uK = s(tu)K = sK * (tK * uK).$$

Comme l'application π de G dans G/K est définie par $\pi(s) = sK$, pour tout $(s, t) \in G^2$, on a l'égalité : $\pi(st) = \pi(s) * \pi(t)$, π est bien un morphisme de groupe.

Il nous reste à vérifier l'unicité de la loi $*$. Supposons qu'il existe une loi $\circledast$ sur G/K telle que l'application π soit un morphisme. Alors pour tout $(s, t) \in G^2$, on peut écrire :

$$sK \circledast tK = \pi(s) \circledast \pi(t) = \pi(st) = \pi(s) * \pi(t) = sK * tK.$$

Les deux lois sont identiques, ce qui termine la preuve. □

Remarque(s) 1.3.1.

1. Par définition, l'application π est surjective, et son noyau est égal à K.
2. Si K st quelconque, alors on peut considérer le produit de deux classes à gauche $sKtK = \{sktk' \mid (k, k') \in K^2\}$. Si K est distingué alors $sKtK = stK$. On peut donc noter sans ambiguïté le produit de sK et tK dans G/K sous la forme $sKtK$ au lieu de $sK * tK$.

   Par contre, si K n'est pas distingué, en général $sKtK \neq stK$. On peut le vérifier en reprenant l'exemple 3 de la remarque 1.3.1 et en constatant que le produit $(13)K(23)K$ contient strictement la classe $(13)(23)K$.
3. Nous ferons plus tard avec des outils supplémentaires des calculs de groupes quotients ; mais dès maintenant, nous pouvons remarquer que si $H = G$, alors G/G contient un seul élément et le groupe quotient est le groupe trivial.
4. À l'opposé si $H = \{e\}$, alors $G/\{e\}$ est en bijection avec les parties à un élément de G (ou autrement dit toutes les classes à droites de $\{e\}$ dans G contiennent un seul élément) et le quotient $G/\{e\}$ est isomorphe à G.

On va maintenant énoncer plusieurs caractérisations des sous-groupes distingués.

Propriété 1.3.1. *Soient G un groupe et K un sous-groupe ; alors on a équivalence entre les assertions suivantes :*

(i) le sous-groupe K est distingué dans G ;

(ii) pour tout $s \in G$, on a égalité $sKs^{-1} = K$;

(iii) pour tout $s \in G$, on a l'inclusion $sKs^{-1} \subset K$;

(iv) on a égalité entre les classes à droite et les classes à gauche de K dans G, autrement dit on a : $G/^{\delta}K = G/^{\gamma}K$.

(v) il existe un groupe H, un morphisme de groupe ψ de G dans H tel que $K = \ker \psi$.

(vi) L'action de K sur $G/^{\delta}K$ par multiplication à gauche est triviale.

(vii) L'action de K sur $G/^{\gamma}K$ par multiplication à droite est triviale.

Démonstration. L'équivalence $(i) \Leftrightarrow (ii)$ est quasi immédiate (la multiplication par s^{-1} à droite préserve l'égalité). Nous allons montrer les autres équivalences par une preuve « circulaire ».

$(iv) \Rightarrow (iii)$ Supposons $G/^{\delta}K = G/^{\gamma}K$, alors pour tout $s \in G$ la classe à gauche sK est une classe à droite, et donc il existe $t \in G$ tel que $sK = Kt$. Mais $s \in sK = Kt$, et donc $Ks = Kt$ et $sK = Ks$ pour tout $s \in G$, et donc $sKs^{-1} \subset K$.

$(iii) \Rightarrow (i)$ Si pour tout $s \in G$, $sKs^{-1} \subset K$, alors en multipliant à gauche par s^{-1} puis à droite par s, on obtient : $Ks^{-1} \subset s^{-1}K$ et $sK \subset Ks$. Ces inclusions étant vraies pour tout $s \in G$, on a bien $sK = Ks$ pour tout $s \in G$.

$(i) \Rightarrow (v)$ Si K est distingué, alors d'après la propriété 8, il existe une structure de groupe sur G/K et un morphisme de groupe surjectif π de G dans G/K. D'après une des remarques 1.3.1, K est égal au noyau de π.

$(v) \Rightarrow (vi)$ Soient $k \in K$ et $s \in G$, l'action en question est définie par l'égalité suivante : $k.sK = ksK$. Supposons donc que $K = \ker \psi$, alors on peut écrire :

$$k.sK = ksK = ks \ker \psi = s(s^{-1}ks) \ker \psi.$$

Mais comme

$$\psi(sks^{-1}) = \psi(s)\psi(k)\psi(s^{-1}) = \psi(s)\psi(s^{-1}) = e,$$

l'élément $s^{-1}ks$ appartient à $\ker \psi$ qui est un sous-groupe et donc

$$ksK = s \ker \psi \ker \psi = s \ker \psi = sK.$$

L'action est bien triviale.

$(vi) \Rightarrow (vii)$ D'après la propriété 1.2.7 l'ensemble des classes à gauche est G-isomorphe (et donc K-isomorphe) à l'ensemble des classes à droite. La trivialité de l'action $G/^{\gamma}K$ est donc équivalente à la trivialité de l'action sur $G/^{\delta}K$.

$(vii) \Rightarrow (iv)$ Ici l'action est définie comme suit : pour tout $k \in K$ et pour tout $s \in G$, on a $k.Ks = Ksk^{-1}$. Si cette action est triviale alors pour tout $k \in K$ et pour tout $s \in G$, on a l'égalité : $Ksk^{-1} = Ks$. On en déduit : $sk^{-1} \in Ks$ et donc $sK = Ks$, les deux ensembles $G/^{\delta}K$ et $G/^{\gamma}K$ sont égaux.

□

Remarque(s) 1.3.2. Évidemment si le groupe G est commutatif, alors tous ses sous-groupes sont distingués. Attention, la réciproque de cette assertion est fausse. En effet, tous les sous-groupes de Q_8 (voir l'exemple 1.1.13) sont distingués (exercice) et pourtant Q_8 n'est pas commutatif.

Nous allons maintenant voir comment se comporte la notion de sous-groupe distingué par image directe et image réciproque d'un morphisme.

Propriété 1.3.2. *Soient G et H deux groupes et ψ un morphisme de G dans H. Soient K un sous-groupe distingué de G et N un sous-groupe distingué de H. Alors $\psi(K)$ est distingué dans $\operatorname{Im}\psi$ et $\psi^{-1}(N)$ est distingué dans G.*

Démonstration. Montrons la première assertion. Soient $h \in \psi(K)$ et $t \in \operatorname{Im}\psi$; on doit montrer que $tht^{-1} \in \psi(K)$. Pour cela, considérons $k \in K$ et $g \in G$ tels que $\psi(k) = h$ et $\psi(g) = t$. On a les égalités suivantes :

$$tht^{-1} = \psi(g)\psi(k)\psi(t^{-1}) = \psi(gkg^{-1}).$$

Comme K est distingué dans G, $gkg^{-1} \in K$ et $tht^{-1} \in \psi(K)$.

Pour la deuxième assertion, considérons $s \in \psi^{-1}(N)$ et $g \in G$, on doit montrer que $gsg^{-1} \in \psi^{-1}(N)$. On a l'égalité suivante :

$$\psi(gsg^{-1}) = \psi(g)\psi(s)\psi(g)^{-1}.$$

Mais comme $\psi(s) \in N$ et que N est distingué dans H $\psi(g)\psi(s)\psi(g)^{-1} \in N$ ce qui achève la démonstration. □

Remarque(s) 1.3.3. De la propriété précédente, on en déduit que si ψ est surjective, $\psi(K)$ est distingué dans H. La surjectivité de ψ est nécessaire. En effet dans l'exercice 26, on a un exemple de sous-groupes K et H de G tel que $K \triangleleft H$ et $H \triangleleft G$ mais K n'est pas distingué dans G. Cela fournit un contre-exemple à l'assertion ci-dessus, en considérant le morphisme inclusion i de H dans G.

1.3.3 Théorèmes d'isomorphismes, factorisation

Nous avons vu dans les exemples 1.1.5 qu'une relation d'équivalence bien choisie permet de « rendre » injective une application. Nous allons voir que ce résultat reste vrai si on considère des morphismes de groupe. Ceci est le premier théorème d'isomorphisme.

Théorème 9. Premier théorème d'isomorphisme

Soient G et H deux groupes et ψ un morphisme de groupe de G dans H ; soit π l'application quotient de G dans $G/\ker\psi$. Alors, il existe un unique morphisme $\overline{\psi}$ de $G/\ker\psi$ dans H telle que $\overline{\psi} \circ \pi = \psi$. Cet morphisme est injectif et induit un isomorphisme entre $G/\ker\psi$ et $\operatorname{Im}\psi$.

Démonstration. Remarquons d'abord que pour tout $(s,t) \in G^2$, si $s\ker\psi = t\ker\psi$, alors $\psi(s) = \psi(t)$. On peut donc définir une application $\overline{\psi}$ de $G/\ker\psi$ dans H, en posant pour tout $s \in G$, $\overline{\psi}(s\ker\psi) = \psi(s)$.

Vérifions que $\overline{\psi}$ est un morphisme ; posons $K = \ker\psi$ et soit $(s,t) \in G^2$, on a les égalités suivantes :

$$\overline{\psi(sK * tK)} = \overline{\psi}(stK) = \psi(st) = \psi(s)\psi(t) = \overline{\psi}(sK)\overline{\psi}(tK).$$

Montrons l'unicité de $\overline{\psi}$: supposons qu'il existe une application α de G/K dans H telle que $\alpha \circ \pi = \psi$, alors pour tout $s \in G$, on a : $\alpha \circ \pi(s) = \psi(s)$, soit $\alpha(sK) = \psi(s)$ et $\alpha = \overline{\psi}$.

Pour finir vérifions que $\overline{\psi}$ est injective ; soit $s \in G$ tel que $\overline{\psi(sK)} = e$, c'est à dire $\psi(s) = e$, on en déduit que $s \in K = \ker\psi$, et donc $sK = K$ est l'élément neutre de G/K. Donc $\overline{\psi}$ est un isomorphisme entre G/K et $\operatorname{Im}\overline{\psi}$, mais comme $\overline{\psi} \circ \pi = \psi$ et que π est surjective, on a l'égalité $\operatorname{Im}\overline{\psi} = \operatorname{Im}\psi$. □

Nous allons maintenant pouvoir donner d'autres exemples de groupes distingués et calculer le groupe quotient associé.

Exemple(s) 1.3.2. 1. Soient G un groupe et $g \in G$, dans la propriété 1.1.12 on a défini une application ψ_g de $\mathbb{Z}$ dans G en posant $\psi_g(m) = g^m$. Par définition, $\operatorname{Im}\psi_g$ est égale au groupe $< g >$ engendré par g. Le noyau de ψ_g est un sous-groupe de $\mathbb{Z}$, et donc d'après la propriété 2, il existe $n \in \mathbb{N}$ tel que $\ker\psi_g = n\mathbb{Z}$. Le premier théorème d'isomorphisme fournit un isomorphisme entre $\mathbb{Z}/n\mathbb{Z}$ et $< g >$ et on retrouve les résultats du théorème 5 : si $n = 0$ alors $< g >$ est isomorphe à $\mathbb{Z}/\{0\}$, c'est à dire isomorphe à $\mathbb{Z}$; si $n \neq 0$, le groupe $< g >$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et g est d'ordre fini égal à n.

2. Soit V un espace vectoriel sur un corps $\mathbb{K}$ de dimension finie. On a vu que le déterminant définit un morphisme, noté det de $\mathrm{GL}(V)$ dans $\mathbb{K}^*$. Son noyau est le groupe des matrices de déterminant égal à 1, c'est donc un sous-groupe distingué de $\mathrm{GL}(V)$ appelé le groupe spécial linéaire et noté SL(V). D'après le premier théorème d'isomorphisme, il existe un morphisme injectif $\overline{\det}$ de $\mathrm{GL}(V)/\mathrm{SL}(V)$ dans $\mathbb{K}^*$. Mais comme l'application det est surjective, $\overline{\det}$ l'est également et $\mathrm{GL}(V)/\mathrm{SL}(V)$ est isomorphe à $\mathbb{K}^*$.

3. Dans la preuve de la propriété 1.1.8, on a défini le morphisme suivant :

$$\begin{array}{rccc} \Theta & : & G & \to & \mathrm{Aut}(G) \\ & & g & \mapsto & \varphi_g \end{array}.$$

où φ_g est l'automorphisme intérieur défini par $\varphi_g(s) = gsg^{-1}$. Par définition, l'image de Θ est le groupe $\mathrm{Int}(G)$ des automorphismes intérieurs. Le noyau de Θ est égal au centre $Z(G)$ (le vérifier), et donc $Z(G)$ est distingué dans G (on peut aussi vérifier ce fait directement).

En appliquant le premier théorème d'isomorphisme, on obtient un morphisme injectif $\overline{\Theta}$ de $G/Z(G)$ dans $\mathrm{Aut}(G)$. Comme l'image de Θ est égale à $\mathrm{Int}(G)$, les groupes $G/Z(G)$ et $\mathrm{Int}(G)$ sont isomorphes.

4. Le groupe $\mathrm{Int}(G)$ est un sous-groupe du groupe des automorphismes de G (voir la propriété 1.1.8). Ce sous-groupe est en fait distingué, en effet, soient ψ un automorphisme φ_g un automorphisme intérieur et $s \in G$; on a les égalités suivantes :

$$\begin{array}{rcc} \psi \circ \varphi_g \circ \psi^{-1}(s) & = & \psi(g\psi^{-1}(s)g^{-1}) \\ & = & \psi(g)\psi(\psi^{-1}(s))\psi(g^{-1}) \\ & = & \psi(g)s\psi(g^{-1}) \\ & = & \varphi_{\psi(g)}(s) \end{array}.$$

Et donc $\psi \circ \varphi_g \circ \psi^{-1} = \varphi_{\psi(g)}$ et $\mathrm{Int}(G)$ est distingué dans $\mathrm{Aut}(G)$.

Pour généraliser ce premier théorème sous forme de résultat de factorisation, on a besoin d'une première propriété sur les sous-groupes d'un quotient.

Propriété 1.3.3. *Soient G un groupe, K un sous-groupe distingué et H un sous-groupe de G contenant K, alors H/K est un sous-groupe de G/K.*

Démonstration. En écrivant la définition des deux ensembles,

$$H/K = \{hK \mid h \in H\} \text{ et } G/K = \{gK \mid g \in G\},$$

on vérifie qu'on a bien l'inclusion. Pour montrer que H/K est un sous-groupe, on remarque que H/K est l'image du sous-groupe H par le morphisme quotient π de G dans G/K. □

Théorème 10. Théorème de factorisation *Soient G et H deux groupes, K un sous-groupe distingué de G et π l'application quotient de G dans G/K ; soient ψ un morphisme de G dans H. Alors il existe un morphisme $\overline{\psi}$ de G/K dans H tel que $\overline{\psi} \circ \pi = \psi$ si et seulement si $K \subset \ker\psi$. Dans ce cas le morphisme $\overline{\psi}$ est unique et on a $\ker\overline{\psi} = \ker\psi/K$ et $\operatorname{Im}\overline{\psi} = \operatorname{Im}\psi$.*

Démonstration. Supposons qu'il existe un morphisme $\overline{\psi}$ vérifiant $\overline{\psi} \circ \pi = \psi$. Et soit $k \in K$, alors $\psi(k) = \overline{\psi} \circ \pi(k)$, or $\pi(k) = e$ et donc $k \in \ker \psi$.

Réciproquement si $K \subset \ker \psi$, alors on suit le même raisonnement que dans la preuve du théorème 9. On vérifie d'abord que pour tout $(s,t) \in G^2$ tels que $sK = tK$, on a $\psi(sK) = \psi(tK)$. On définit $\overline{\psi}$ en posant $\overline{\psi}(tK) = \psi(t)$, puis on montre que $\overline{\psi}$ est un morphisme qui vérifie l'identité $\overline{\psi} \circ \pi = \psi$. Et cette identité implique l'unicité et l'égalité entre les images : $\operatorname{Im} \overline{\psi} = \operatorname{Im} \psi$.

Il reste donc à calculer le noyau de $\overline{\psi}$; pour cela soit $t \in G$ tel que $\overline{\psi}(tK) = e$, on en déduit $\psi(t) = e$, c'est à dire $t \in \ker \psi$ et donc $tK \in \ker \psi / K$ (voir la propriété 1.3.3). □

Nous allons maintenant énoncer et démontrer le deuxième théorème d'isomorphisme.

Théorème 11. Deuxième théorème d'isomorphisme

Soient G un groupe, H et K deux sous-groupes ; de plus nous supposerons que K est distingué dans G. Alors on a les assertions suivantes :

(i) HK est un sous-groupe de G ;

(ii) $H \cap K$ est distingué dans H ;

(iii) K est distingué dans HK ;

(iv) les groupes HK/K et $H/H \cap K$ sont isomorphes.

Démonstration.

(i) Remarquons d'abord que $HK = KH$, en effet soit $(h,k) \in H \times K$, alors on peut écrire : $hk = hkh^{-1}h$. Mais comme K est distingué, l'élément hkh^{-1} appartient à K et donc $hk \in KH$. L'inclusion réciproque provient de l'égalité $kh = hh^{-1}kh$. Dans l'exercice 14, on a vu que $HK = KH$ si et seulement si HK est un groupe, le point (i) est donc démontré.

(ii) Soient $k \in H \cap K$ et $h \in H$, on doit montrer que $hkh^{-1} \in H \cap K$; mais comme K est distingué $hkh^{-1} \in K$ et comme c'est le produit de trois éléments de H, hkh^{-1} appartient à H.

(iii) Cette assertion est claire.

(iv) Appelons i l'application de H dans HK définie par $i(h) = h$ et π l'application quotient de HK dans HK/K, alors la composée $\alpha = \pi \circ i$ est une application de H dans HK/K définie par $\alpha(h) = hK$. Comme π et i sont des morphismes, α est également un morphisme de groupes. De plus α est surjective, en effet toutes les classes à gauches de K dans HK s'écrivent hkK pour un couple $(h,k) \in H \times K$; mais $hkK = hK = \alpha(h)$. Calculons maintenant le noyau de α ; soit $h \in H$ tel que $h \in \ker \alpha$, alors $\alpha(h) = e$ est équivalent à $i(h) = h \in \ker \pi = K$, donc $\ker \alpha = H \cap K$. On conclut en appliquant le premier théorème d'isomorphisme.

□

Voyons maintenant le troisième et dernier théorème d'isomorphisme.

Théorème 12. Troisième théorème d'isomorphisme *Soient G un groupe et K et N deux sous-groupes distingués de G tels que $N \subset K$. On a alors les assertions suivantes :*

(i) N est un sous-groupe distingué de K et K/N est un sous groupe distingué de G/N.

(ii) Le quotient $(G/N)/(K/N)$ est isomorphe à G/K.

Démonstration.

(i) La première partie de l'assertion est évidente. Notons π le morphisme quotient de G dans G/N ; comme π est surjectif et $K/N = \pi(K)$, K/N est distingué dans G/N d'après la propriété 1.3.2.

(ii) Considérons l'application quotient θ de G dans G/K. Comme N est un sous-groupe de K, d'après le théorème 10 le morphisme θ se factorise : il existe un morphisme $\overline{\theta}$ de G/N dans K/N tel que $\theta = \overline{\theta} \circ \pi$; comme θ est surjectif, $\overline{\theta}$ l'est également. Et son noyau est égal à $\ker \theta/N$ soit K/N. Il reste à appliquer le premier théorème d'isomorphisme (le théorème 9) pour obtenir l'isomorphisme demandé.

□

1.3.4 Les sous-groupes d'un quotient

Soient G un groupe et K un sous-groupe distingué de G, on va décrire ici les sous-groupes du quotient G/K, puis nous appliquerons ce résultat à l'étude des sous-groupes d'un groupe cyclique. Nous noterons comme d'habitude π le morphisme quotient de G dans G/K. Nous noterons $\mathscr{G}_K$ l'ensemble des sous-groupes de G contenant K et $\mathscr{G}^K$ l'ensemble des sous-groupes du quotient G/K.

Théorème 13. *Soient G un groupe, et K un sous-groupe distingué, alors les applications suivantes :*

$$\Pi : \begin{array}{ccc} \mathscr{G}_K & \to & \mathscr{G}^K \\ H & \mapsto & \pi(H) \end{array} \quad et$$

$$\Theta : \begin{array}{ccc} \mathscr{G}^K & \to & \mathscr{G}_K \\ L & \mapsto & \pi^{-1}(L) \end{array} .$$

sont bien définies et réciproques l'une de l'autre. Par conséquent l'ensemble des sous-groupes du quotient G/K est en bijection avec l'ensembles des sous-groupes de G contenant K. De plus, le sous-groupe H contenant K est distingué dans G si et seulement si $\pi(H)$ est distingué dans G/K.

Démonstration. Les applications Π et Θ sont bien définies, car d'une part on a vu dans la propriété 1.1.5 que l'image directe et réciproque d'un sous-groupe par un morphisme est un sous-groupe, et d'autre part on a l'inclusion $K = \pi^{-1}(e) \subset \pi^{-1}(L)$.

Montrons qu'elles sont réciproques l'une de l'autre. Tout d'abord, puisque π est surjective, pour tout sous-groupe L de G/K on a l'égalité : $\pi(\pi^{-1}(L)) = L$ et donc $\Pi \circ \Theta = \mathbb{1}_{\mathscr{G}^K}$.

Montrons maintenant $\Theta \circ \Pi = \mathbb{1}_{\mathscr{G}_K}$. Pour cela considérons H un sous-groupe de G contenant K ; on doit montrer que $\pi^{-1}(\pi(H)) = H$. On a bien évidemment $H \subset \pi^{-1}(\pi(H))$; considérons donc un élément $g \in \pi^{-1}(\pi(H))$. Par définition $\pi(g) \in \pi(H)$, il existe donc $h \in H$ tel que $\pi(g) = \pi(h)$, mais alors $gh^{-1} \in \ker \pi = K$ et comme $K \subset H$ l'élément $g = gh^{-1}h$ appartient à H.

La dernière partie du théorème est une simple conséquence de la surjectivité de π et des résultats de la propriété 1.3.2. □

Voici une application directe de ce théorème.

Théorème 14. *Soient $n \in \mathbb{N}^*$ et G un groupe cyclique d'ordre n. Alors pour tout diviseur d de n, il existe un unique sous-groupe de G d'ordre d et ce sous-groupe est cyclique.*

Démonstration. On a vu que G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ (voir la propriété 1.1.14) ; il suffit donc de montrer le théorème dans le cas où $G = \mathbb{Z}/n\mathbb{Z}$; d'après le théorème précédent, l'ensemble des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ est en bijection avec l'ensemble des sous-groupes de $\mathbb{Z}$ contenant $n\mathbb{Z}$. D'après le théorème 2 et la remarque qui suit, l'ensemble de ces sous-groupes est en bijection avec les entiers positifs m qui divisent n. Réciproquement, à un sous-groupe $m\mathbb{Z}$ avec m qui divise n correspond le sous-groupe $m\mathbb{Z}/n\mathbb{Z}$. Montrons que ce sous-groupe est d'ordre d avec $d = n/m$ et isomorphe à $\mathbb{Z}/d\mathbb{Z}$ ce qui conclura la preuve. Posons $n = md$ et considérons la composition des morphismes suivants :

$$\begin{array}{ccccc} \mathbb{Z} & \to & m\mathbb{Z} & \to & m\mathbb{Z}/n\mathbb{Z} \\ p & \mapsto & pm & \mapsto & pm + n\mathbb{Z}. \end{array}$$

Cette composée est un morphisme de groupe surjectif, et son noyau est égal à $d\mathbb{Z}$, on conclut grâce au premier théorème d'isomorphisme (théorème 9). $\square$

1.3.5 Exercices

Exercice 25 ⓒ

Montrer qu'un sous-groupe d'indice 2 est toujours distingué.

Exercice 26 ⓒ

Soient G un groupe et $K \subset H \subset G$ deux sous-groupes. On suppose que H est distingué dans G et que K est caractéristique dans H (i.e. stable par tout automorphisme de H). Montrer qu'alors K est distingué dans G.

Donner un exemple de groupe G et de deux sous-groupes $K \subset H \subset G$, H étant distingué dans G et K étant distingué dans H, mais K n'étant pas distingué dans G.

Exercice 27 ⓐ

Soient G un groupe et $\sim$ une relation d'équivalence sur G. On suppose que cette relation est compatible avec la loi de groupe, c'est-à-dire que

$$\forall (s,t) \in G^2 \quad \forall (s',t') \in G^2 \quad s \sim s' \quad \text{et} \quad t \sim t' \quad \text{alors} \quad st \sim s't'$$

Montrer que la classe H de l'élément neutre 1 est un sous-groupe distingué de G et que

$$\forall (s,s') \in G \quad s \sim s' \quad \text{est} \quad \text{équivalent} \quad \text{à} \quad s's^{-1} \in H$$

Exercice 28 ⓒ

1. Soient G un groupe et H un sous groupe distingué de G d'indice n. Montrer que pour tout $a \in G$, $a^n \in H$. Donner un exemple de sous-groupe H non distingué de G pour lequel la conclusion précédente est fausse.
2. Soient G un groupe fini et H un sous-groupe distingué d'ordre n et d'indice m. On suppose que m et n sont premiers entre eux. Montrer que H est l'unique sous-groupe de G d'ordre n.
3. Montrer qu'un sous-groupe d'indice n de $\mathbb{C}^*$ est égal à $\mathbb{C}^*$.

Exercice 29 ⓐ

On considère ici deux groupes finis G, H et $f : G \to H$ un morphisme de groupes.

1. Soit G' un sous-groupe de G. Montrer que l'ordre de $f(G')$ divise les ordres de G' et de H.
2. En déduire que si G' un sous-groupe de G d'ordre premier à l'ordre de H, alors $G' \subset \ker(f)$.
3. Retrouver le résultat de la deuxième question de l'exercice 28.

Exercice 30 ⓒ

1. Soient G un groupe et H un sous-groupe contenu dans le centre $Z(G)$ de G. Montrer que H est distingué dans G et que, si le groupe quotient G/H est cyclique, alors G est commutatif.

2. En déduire qu'un groupe d'ordre p^2 où p est un nombre premier est commutatif. (Indication : on utilisera que le centre d'un p-groupe différent de l'identité est non trivial, voir cours)

Exercice 31 ⓐ

On considère les groupes suivants :

$$\mathbb{U} = \{z \in \mathbb{C} \,|\, |z| = 1\} \quad \mathbb{U}_n = \{z \in \mathbb{C} \,|\, z^n = 1\} \quad \mathbb{U}_\infty = \{z \in \mathbb{C} \,|\, \exists n \quad z^n = 1\}$$

Un groupe est dit de type fini, s'il existe un ensemble de cardinal fini $X \subset G$ tel que $G =< X >$.

1. Montrer les isomorphismes qui suivent.
   (i) $\mathbb{R}/\mathbb{Z} \simeq \mathbb{U}$;
   (ii) $\mathbb{C}^\times/\mathbb{R}^\times_{>0} \simeq \mathbb{U}$;
   (iii) $\mathbb{C}^\times/\mathbb{R}^\times \simeq \mathbb{U}$;
   (iv) $\mathbb{U}/\mathbb{U}_n \simeq \mathbb{U}$;
   (v) $\mathbb{C}^\times/\mathbb{U}_n \simeq \mathbb{C}^\times$.
2. Montrer que $\mathbb{U}_\infty \simeq \mathbb{Q}/\mathbb{Z}$. Quels sont les sous-groupes finis de $\mathbb{U}_\infty$?
3. Montrer qu'un sous-groupe de type fini de $\mathbb{Q}$ contenant $\mathbb{Z}$ est de la forme $\frac{1}{q}\mathbb{Z}$. En déduire la forme des sous-groupes de type fini de $\mathbb{Q}/\mathbb{Z}$ et de $\mathbb{U}_\infty$.
4. Soit p un nombre premier. Montrer que $\mathbb{U}_{p^\infty} = \{z \in \mathbb{C} \,|\, \exists n \in \mathbb{N} \quad z^{p^n} = 1\}$ est un sous-groupe de $\mathbb{U}_\infty$. Est-il de type fini ?

Exercice 32 ⓒ

Soient G un groupe, et H et K deux sous-groupes de G. On suppose dans cet exercice que K est distingué, que $G = KH$ et que $K \cap H = \{e\}$. On dit alors que G est le produit semi-direct (interne) de K par H et on note $G = K \rtimes H$.

(a) Montrer que pour tout $g \in G$, il existe un unique couple $(k, h) \in K \times H$ tel que $g = kh$. En déduire que l'application suivante :

$$m : \begin{array}{ccc} K \times H & \to & G \\ (k,h) & \mapsto & kh \end{array}.$$

est une bijection.

De même, montrer que pour tout $g \in G$ il existe un unique couple $(k', h') \in K \times H$ tel que $g = h'k'$.

(b) Si $h \in H$, montrer que l'automorphisme intérieur :

$$\varphi_h : \begin{array}{ccc} G & \to & G \\ g & \mapsto & hgh^{-1} \end{array}$$

laisse stable le groupe K.

(c) Montrer que pour tout $(k, h) \in K \times H$ et pour tout $(k', h') \in K \times H$, on a :

$$khk'h' = k\varphi_h(k')hh'$$

(d) Montrer que l'application m est un morphisme de groupe si et seulement si H est distingué (dans ce cas G est donc isomorphe au produit direct).

(e) Montrer que le groupe symétrique Σ_n est le produit semi-direct de A_n par le groupe engendré par une transposition.

Exercice 33 ⓒ

Soient $n \in \mathbb{N}$, $n \geq 2$ et $\mathscr{P}_n$ un polygone régulier du plan euclidien centré en l'origine et à n sommets (par exemple celui dont les sommets ont pour affixe les racines n-ièmes de l'unité). On note D_n l'ensemble des isométries directes et indirectes du plan préservant $\mathscr{P}_n$.

À toute fin utile, on rappelle que l'ensemble des isométries linéaires du plan est un groupe, le groupe orthogonal $\mathrm{O}_2(\mathbb{R})$. *Les éléments dans* $\mathrm{O}_2(\mathbb{R})$ *sont de deux sortes : les isométries directes qui sont de déterminant* 1 *et qui sont des rotations, et les indirectes qui sont de déterminant* -1 *et qui sont des symétries axiales (et qui sont donc d'ordre* 2*)*

(a) Montrer que D_n est un sous-groupe du groupe orthogonal. On l'appelle le groupe diédral.

(b) Montrer que le sous-groupe D_n^+ constitué des isométries directes est cyclique d'ordre n et qu'il est distingué dans D_n.

(c) Montrer que D_n contient exactement n rotations et n symétries, et qu'il est donc d'ordre $2n$.

(d) Montrer que D_n est le produit semi-direct de D_n^+ par le sous-groupe d'ordre 2 engendré par une symétrie axiale de D_n. En particulier D_2 est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ et D_3 est isomorphe à Σ_3.

Exercice 34 ⓐ

Avec tout ce qui a été vu en cours et en TD jusqu'à présent, classifier les groupes d'ordre 8. On montrera qu'à isomorphisme près il y a trois groupes commutatifs et deux non commutatifs à savoir D_4 (voir l'exercice 33) et Q_8 (voir la définition 1.1.13).

1.4 Théorèmes de Sylow

1.4.1 Motivations

Le dernier théorème de la section précédente peut-être vu comme une réciproque du théorème de Lagrange : dans un groupe cyclique, pour tout diviseur d de l'ordre du groupe, on peut trouver un sous-groupe d'ordre d.

Pour un groupe quelconque, une telle réciproque n'est pas vraie en général. Cependant il existe des diviseurs d de l'ordre du groupe pour lequel on est assuré de l'existence d'un sous-groupe d'ordre d, c'est lorsque d est une puissance d'un nombre premier. Il n'y a pas unicité, mais lorsque la puissance de p est la plus grande possible alors tous les sous-groupes obtenus sont conjugués.

Ces deux résultats font partie d'une série de trois résultats connus sous le nom de théorèmes de Sylow. Pour les énoncer et les démontrer, nous avons besoin de quelques définitions et résultats préalables.

Rappelons qu'un p-groupe est un groupe d'ordre une puissance positive de p. Si G est un sous-groupe et si p est un diviseur de $|G|$, un p-sous-groupe de G est un sous-groupe de G qui est un p-groupe. Enfin, si n est l'ordre de G, et si $n = p^r m$ avec $r > 0$ et m non divisible par p, un sous-groupe d'ordre p^r est appelé un p-sous groupe de Sylow (que l'on abrège fréquemment en p-Sylow). Autrement dit, un p-Sylow est un p-groupe de G de cardinal maximal. En particulier le sous-groupe trivial (réduit à l'identité) est un p-sous-groupe de G (pour tout p premier). De même, ce sous-groupe trivial est également un p-sous-groupe de Sylow si p est un nombre premier ne divisant pas l'ordre de G.

Nous allons commencer par quelques résultats préliminaires.

1.4.2 Résultats préliminaires

Nous allons maintenant énoncer et démontrer le théorème de Cauchy dans le cas plus simple des groupes commutatifs. Dans l'exercice 23, il y a une preuve de ce théorème pour un

groupe non forcément commutatif.

Propriété 1.4.1. Théorème de Cauchy pour les groupes abéliens
Soient G un groupe fini et commutatif et p un nombre premier divisant l'ordre de G, alors il existe dans G un élément d'ordre p.

Démonstration. S'il existe un élément g dont l'ordre est divisible par p, alors cet ordre s'écrit $p^r m$ avec $r > 0$ et m non divisible par p. On considère l'élément $s = g^{p^{r-1}m}$, alors $s \neq e$ (sinon g ne serait pas d'ordre $p^r m$) et $s^p = e$, et donc s est d'ordre p.

Supposons donc qu'il n'existe pas d'élément dont l'ordre est divisible par p, ce qui va nous conduire à une contradiction. Soit $\{h_1, h_2, \ldots, h_s\}$ une partie de G qui engendre G (cela existe puisque G est fini). Pour tout $i \in \{1, \ldots, s\}$ appelons H_i le groupe engendré par h_i. Par hypothèse, pour tout $i \in \{1, \ldots, s\}$, H_i est d'ordre premier à p. Considérons l'application suivante :

$$\begin{array}{ccc} \prod_{i=1}^{s} H_i & \to & G \\ (g_1, g_2, \ldots, g_s) & \mapsto & g_1 g_2 \ldots g_s \end{array}.$$

Cette application est un morphisme (puisque G est commutatif) surjectif (puisque $\{h_1, h_2, \ldots, h_s\}$ engendre G). Et donc d'après le premier théorème d'isomorphisme (le théorème 9), l'ordre de G divise l'ordre de $\prod_{i=1}^{s} H_i$, mais ceci n'est pas possible puisque p divise G, mais pas l'ordre de $\prod_{i=1}^{s} H_i$. □

Énonçons maintenant un résultat pratique, qui est une conséquence directe de l'équation aux classes.

Propriété 1.4.2. *Soit p un nombre premier et soit G un groupe agissant sur un ensemble fini X ; supposons que pour tout orbite O non réduite à un point, le cardinal de O est divisible par p (cet hypothèse est vérifiée en particulier si G est un p-groupe) alors on a la congruence :*

$$|X| \equiv |X^G| \pmod{p}.$$

Démonstration. On écrit l'équation aux classes, en notant $O_1, \ldots, O_r$ les orbites de cardinal supérieur où égal à deux.

$$|X| = |X^G| + \sum_{i=1}^{r} |O_i|.$$

Par hypothèse, pour tout $i \in \{1, 2, \ldots, r\}$ p divise $|O_i|$ et donc $\sum_{i=1}^{r} |O_i| \equiv 0 \pmod{p}$, ce qui achève la preuve. □

1.4.3 Les théorèmes de Sylow

Nous pouvons maintenant énoncer les théorèmes de Sylow, que nous rassemblons ici en un seul théorème.

Théorème 15. Les théorèmes de Sylow
Soient G un groupe fini d'ordre n et p un nombre premier tel que $n = p^r m$ avec $r \geq 0$ et m et p premier entre eux. Alors, on a les assertions suivantes :

(i) Pour tout $i \in \{0, 1, \ldots, r\}$ il existe un sous-groupe de G d'ordre p^i, en particulier il existe un p-Sylow.

(ii) Soit H un sous-groupe d'ordre p^i avec $i \in \{0, 1, \ldots, r\}$, et soit S un p-Sylow de G, alors il existe $g \in G$ tel que $gHg^{-1} \subset S$. En particulier tous les p-Sylow sont conjugués, et tous les p-sous-groupes de G sont inclus dans un p-Sylow.

(iii) Soit n_p le nombre de p-Sylow de G, alors n_p est congru à 1 modulo p et divise m.

Démonstration.

(i) C'est le point le plus délicat à montrer et il y a plusieurs preuves possibles. Nous allons le faire ici par récurrence sur l'ordre de G. L'énoncé est évidemment vrai pour $n = 1$, puisque par convention, pour tout nombre premier p le groupe trivial est un p-sous-groupe de Sylow de lui-même.

Supposons maintenant que le point (i) est vrai pour tout groupe fini dont l'ordre est strictement plus petit que n. Soit G un groupe d'ordre n et p un nombre premier tel que $n = p^r m$ avec p qui ne divise pas m. Si $r = 0$, alors le résultat est évident.

Supposons donc maintenant que $r > 0$. Si G contient un sous-groupe strict L d'indice non divisible par p, alors on peut écrire $|L| = p^r m'$ avec m' premier à p et divisant m. Par hypothèse de récurrence L contient des sous-groupes d'ordre p^i pour $i \in \{1, 2, \ldots, r\}$ et ces sous-groupes sont également des sous-groupes de G.

Supposons donc que tous les sous-groupes stricts de G ont un indice divisible par p. Dans ce cas on considère l'action de G sur lui-même par conjugaison. Rappelons que l'ensemble des points fixes pour cette action est égal à $Z(G)$ le centre de G ; notons $O_1, O_2, \ldots, O_r$ l'ensemble des orbites de cardinal supérieur où égal à deux. Chacun des O_i est l'indice d'un sous-groupe strict de G, donc divisible par p d'après l'hypothèse ; on peut donc appliquer la propriété 1.4.2 : $|Z(G)|$ est congru à $|G|$ modulo p, $|Z(G)|$ est donc divisible par p. Comme $Z(G)$ est commutatif, on peut appliquer le théorème de Cauchy rappelé ci-dessus : il existe un élément d'ordre p dans $Z(G)$; soit K le groupe engendré par cet élément. Alors comme K est un sous-groupe du centre de G, il est distingué et G/K et d'ordre $p^{r-1}m$. D'après l'hypothèse de récurrence, pour tout $i \in \{0, 1, \ldots, r-1\}$ il existe dans G/K des sous-groupes d'ordre p^i. Considérons l'image réciproque de ces sous-groupes par le morphisme quotient π de G dans G/K, on obtient des sous-groupes d'ordre p^i pour $i \in \{1, 2, \ldots, r\}$, le premier point est démontré.

(ii) Soient H et S vérifiant les hypothèses. On fait agir H sur l'espace des classes à gauche G/S en posant :

$$\begin{array}{ccc} H \times G/S & \to & G/S \\ (h, gS) & \mapsto & hgS \end{array}.$$

Comme H est un p-groupe et que G/S est de cardinal m qui est non nul modulo p, d'après la propriété 1.4.2 le cardinal de l'ensemble des points fixes est aussi non nul modulo p, l'ensemble des points fixes est donc non vide. Soit $g \in G$ tel que la classe gS soit fixe par H, alors pour tout $h \in H$, $hgS = gS$ soit $hg \in gS$, c'est à dire $h \in gSg^{-1}$. On a donc montré que $H \subset gSg^{-1}$. Dans le cas où H est lui-même un p-Sylow, par cardinalité, on a l'égalité $H = gSg^{-1}$, ce qui termine la preuve de ce point.

(iii) Soient S un p-Sylow et $\mathrm{Conj}(S)$ l'ensemble des sous-groupes conjugués de S dans G. Autrement dit :

$$\mathrm{Conj}(S) = \{gSg^{-1} \mid g \in G\}.$$

D'après le point *(ii)*, $\mathrm{Conj}(S)$ contient tous les p-Sylow ; il est donc de cardinal n_p. Par restriction, le groupe S agit sur $\mathrm{Conj}(S)$ par conjugaison. Cherchons les points fixes pour cette action. Soit $L \in \mathrm{Conj}(S)^S$, alors pour tout $s \in S$, $sLs^{-1} = L$. On en déduit que $SL = LS$ et donc d'après l'exercice 14, SL est un sous-groupe de cardinal $\frac{|S|\,|L|}{|S \cap L|}$. C'est donc un p-groupe qui contient les p-Sylow S et L. Par maximalité de S et L on a donc $S = SL = L$. Le seul point fixe pour cette action est donc le groupe S et en appliquant le résultat de la propriété 1.4.2, on en déduit que :

$$n_p = |\mathrm{Conj}(S)| \overset{(p)}{\equiv} |\mathrm{Conj}(S)^S| = 1.$$

Pour finir, considérons maintenant l'action par conjugaison du groupe G sur $\mathrm{Conj}(S)$. D'après le point précédent, il y a une seule orbite pour cette action, qui est de cardinal n_p et donc $n_p \mid |G| = n$. Mais comme n_p est premier à p, nécessairement $n_p \mid m$.

□

Exemple(s) 1.4.1. Nous verrons beaucoup d'applications de ce théorème en TD ; nous allons ici en donner une seule, en montrant qu'un groupe d'ordre 200 admet un sous-groupe distingué non trivial (on dit qu'un tel groupe n'est pas simple). La décomposition en facteurs premiers de 200 s'écrit : $200 = 2^3 5^2$. Calculons n_5 le nombre de 5-Sylow. D'après les théorèmes de Sylow, on sait que $n_5 \mid 8$ et donc $n_5 = 1, 2, 4, 8$. Mais on doit avoir aussi $n_5 \equiv 1 \pmod 5$, ce qui implique $n_5 = 1$, il y a donc un seul 5-Sylow qui est distingué.

1.4.4 Exercices

Exercice 35 ⓒ

Soit G un groupe d'ordre 399.

(a) Montrer que G admet un unique 19-Sylow P qui est distingué dans G.

(b) Soit Q un 7-Sylow. Montrer que $N = PQ$ est un sous-groupe d'ordre 133 de G et que ce groupe est cyclique.

(c) On suppose que Q n'est pas distingué dans G. Montrer que G admet 57 sous-groupes cycliques d'ordre 133 distincts deux à deux. En vérifiant que le groupe cyclique d'ordre 133 admet au moins 8 générateurs, aboutir à une contradiction. En déduire que Q est distingué dans G et que N est distingué dans G.

(d) Montrer que $G = NR$, où R est un 3-Sylow. En déduire que G est isomorphe au produit semi-direct d'un groupe cyclique d'ordre 133 par un groupe cyclique d'ordre 3.

Exercice 36 ⓒ

Soient $p < q$ deux nombres premiers distincts et G un groupe d'ordre pq. Montrer que G admet un unique q-Sylow Q qui est distingué et que $G = QP$, où P est un p-Sylow de G. En déduire que G est isomorphe au produit semi-direct d'un groupe cyclique d'ordre q par un groupe cyclique d'ordre p. Montrer que si $q-1$ n'est pas divisible par p, ce produit semi-direct est en fait un produit direct.

Exercice 37 ⓒ

Soient p et q deux nombres premiers et G d'ordre p^2q. On veut montrer que G n'est pas simple.

(a) Rappeler pourquoi si $p = q$, le groupe n'est pas simple.

(b) Si $p > q$, en supposant que G est simple, trouver une contradiction.

(c) Supposons maintenant que $p < q$ et que G soit simple. En calculant le nombre n_q de q-Sylow, montrer qu'on a forcément $p = 2$ et $q = 3$. En déduire une contradiction.

Exercice 38 ⓒ

Soient p, q, r trois nombres premiers tels que $p < q < r$ et G un groupe d'ordre pqr. En estimant les nombres de p-Sylow, q-Sylow et r-Sylow puis les nombres d'éléments d'ordre respectifs p, q et r, montrer que G ne peut pas être simple.

Exercice 39 ⓐ

Soit G un groupe d'ordre $2^s 3$ avec $s \geq 2$, on veut montrer que G n'est pas simple. En supposant que G est simple et en considérant l'action de G sur l'ensemble des 2-Sylow, déduire une contradiction.

Exercice 40 ⓐ

En utilisant les quatre exercices précédents, montrer qu'il n'existe pas de groupe simple non cyclique d'ordre strictement inférieur à 60. (Il reste deux cas à considérer)

1.5 Étude détaillée du groupe symétrique, simplicité du groupe alterné

1.5.1 Premières propriétés

Soit X un ensemble, on a défini dans l'exemple 1.1.2.4 le groupe des bijections de X dans lui-même noté $\mathrm{Bij}(X)$ ou également Σ_X. Remarquons d'abord que ce groupe ne dépend pas vraiment de X.

Propriété 1.5.1. *Soient X et Y deux ensembles : supposons qu'il existe une bijection entre X et Y. Alors les groupes* $\mathrm{Bij}(X)$ *et* $\mathrm{Bij}(Y)$ *sont isomorphes.*

Démonstration. Appelons f la bijection de X dans Y et considérons les applications suivantes :

$$\begin{array}{ccc} \mathrm{Bij(X)} & \to & \mathrm{Bij(Y)} \\ \sigma & \mapsto & f \circ \sigma \circ f^{-1} \end{array}$$

et

$$\begin{array}{ccc} \mathrm{Bij(Y)} & \to & \mathrm{Bij(X)} \\ \tau & \mapsto & f^{-1} \circ \tau \circ f. \end{array}$$

On vérifie immédiatement que ces deux applications sont bien définies, que ce sont des morphismes de groupes et qu'elles sont réciproques l'une de l'autre. □

Nous allons nous intéresser ici au cas où X est un ensemble fini non vide. D'après la propriété précédente, on peut supposer que $X = X_n = \{1, 2, \ldots, n\}$ (avec $n \in \mathbb{N}^*$) et on notera le groupe Σ_n au lieu de $\mathrm{Bij}(X_n)$. Ce groupe est appelé le groupe symétrique, et vous l'avez étudié en L2. Nous rappelons ici rapidement quelques propriétés déjà vues et parfois déjà utilisées cette année en cours ou en TD. Rappelons que les éléments de Σ_n sont usuellement appelés des permutations.

Comme on l'a vu dans l'exemple 1.2.1.5, le groupe Σ_n agit naturellement sur l'ensemble X_n, en posant pour tout $(\sigma, j) \in \Sigma_n \times X_n$, $\sigma.j = \sigma(j)$. Cette action permet de définir nombre de notions associées au groupe Σ_n. Par exemple si $\sigma \in \Sigma_n$, on appelle le *support* de σ l'ensemble des points non fixés par σ : $X^n \setminus (X^n)^\sigma$. Par définition du support, deux éléments de Σ_n qui ont des supports disjoints commutent.

Rappelons la définition des cycles qui sont des permutations particulières.

Définition 1.5.1. Soit $\sigma \in \Sigma_n$; s'il existe $(i_1, i_2, \ldots, i_t)$ un t-uplets d'éléments distincts deux à deux de X_n tel que $\sigma(i_j) = i_{j+1}$ pour $j \in \{1, 2, \ldots t-1\}$ et $\sigma(i_t) = i_1$, on dit que σ est un cycle de taille t et de support $\{i_1, i_2, \ldots, i_t\}$. Un tel cycle se note $(i_1 i_2 \ldots i_t)$.

L'entier t s'appelle la taille du cycle ; un cycle de taille 2 s'appelle une transposition.

L'intérêt de la notion de cycle apparaît clairement dans la propriété qui suit.

Propriété 1.5.2. *Soit σ une permutation de X_n, alors il existe un entier r, et des cycles $c_1, c_2, \ldots c_r$ à supports disjoints tel que $\sigma = c_1 c_2 \ldots c_r$. De plus, les cycles $c_1, c_2, \ldots c_r$ commutent deux à deux et cette décomposition de σ en produit est unique à l'ordre près des facteurs. On l'appelle la décomposition de σ en (produit de) cycles.*

Démonstration. On peut retrouver ce résultat déjà vu en L2, en considérant l'action du groupe $H =< \sigma >$ sur X_n. On considère les orbites $O_1, O_2, \ldots, O_r$ pour cette action. On s'intéresse à la restriction de l'action de σ sur chaque orbite O_i. D'après la propriété 1.2.4, on en déduit un morphisme :

$$\begin{array}{rccc} \theta_i : & H & \to & \mathrm{Bij}(O_i) \\ & \sigma & \mapsto & \sigma_{|O_i} \end{array}.$$

Comme σ est d'ordre fini, l'image de θ est égale à $\{\mathbb{1}_{O_i}, \sigma_{|O_i}, \ldots \sigma_{|O_i}^{t_i-1}\}$ avec $\sigma_{|O_i}^{t_i} = \mathbb{1}_{O_i}$, où t_i est l'ordre de $\sigma_{|O_i}$ (exercice : n est un diviseur de l'ordre de σ).

D'autre part comme O_i est une orbite, pour tout point $x_i \in O_i$, on a les égalités :

$$O_i = \mathrm{Im}\,\theta(x_i) = \{x_i, \sigma_{|O_i}(x_i), \ldots \sigma_{|O_i}^{t_i-1}(x_i)\},$$

de plus $\sigma_{|O_i}^{t_i}(x_i) = \mathbb{1}_{O_i}(x_i) = x_i$, et donc la restriction de σ à O_i est bien un cycle.

La commutation des cycles et l'unicité de la décomposition découle directement du fait que les orbites réalisent une partition de X_n. □

Les points fixes sont des cycles de longueur 1. Parfois ces cycles de longueur 1 sont omis quand on considère la décomposition d'une permutation en produits de cycles. D'autre part dans l'écriture d'un cycle, $c = (i_1 i_2 \ldots i_t)$, on peut faire une permutation circulaire des $i_1, i_2, \ldots, i_t$ sans changer le cycle. Très souvent, on choisit l'entier i_1 comme étant le plus petit parmi les entiers $i_1, i_2, \ldots, i_t$.

Nous allons maintenant définir le type d'une permutation.

Définition 1.5.2. Soient $\sigma \in \Sigma_n$ et $\sigma = c_1 \ldots c_r$ sa décomposition en cycle ; pour tout $i \in \{1, \ldots, r\}$ soit t_i la taille du cycle c_i ; on peut supposer que $t_1 \geq t_2 \geq \ldots \geq t_r$, on appelle type de σ le r-uplet $\pi_\sigma = (t_1, t_2, \ldots, t_r)$.

Par définition, si $\sigma \in \Sigma_n$, et si $\pi_\sigma = (t_1, t_2, \ldots, t_r)$, alors la somme $t_1 + t_2 + \ldots + t_r$ est égal à n.

Un r-uplet $\pi = (\pi_1, \ldots, \pi_r)$ avec $\pi_1 \geq \pi_2 \ldots \geq \pi_r > 0$ tels que $\sum \pi_i = n$ est appelé une partition de n. Les π_i sont les parts de la partition, l'entier n est le poids de la partition et l'entier r est appelé la longueur de la partition. Il est d'usage de regrouper dans la partition les parts égales en utilisant un exposant. Par exemple $\pi = (3^2, 2^4, 1) = (3, 3, 2, 2, 2, 2, 1)$ est une partition de 15.

Nous allons voir que le type d'une permutation détermine son ordre et sa classe de conjugaison. Commençons par l'ordre.

Propriété 1.5.3. *(i) Soit c un cycle de taille t de Σ_n, alors c est d'ordre t.*

(ii) Soient σ un élément de Σ_n et $(t_1, t_2, \ldots, t_r)$ son type, alors l'ordre de σ est égal au ppcm de $t_1, t_2, \ldots, t_r$.

Démonstration. Cette preuve est laissée en exercice. □

Pour ce qui est de la classe de conjugaison, commençons par rappeler un résultat déjà vu en L2 qui calcule le conjugué d'un cycle.

Propriété 1.5.4. *Soit $\sigma \in \Sigma_n$ et $c = (i_1 i_2 \ldots i_t)$ un cycle ; alors on a l'égalité :*

$$\sigma c \sigma^{-1} = (\sigma(i_1)\sigma(i_2) \ldots \sigma(i_t)).$$

Démonstration. Exercice. □

Nous pouvons maintenant faire le lien entre le type d'une permutation et sa classe de conjugaison.

Théorème 16. *Deux permutations de Σ_n sont conjuguées si et seulement si elles sont du même type.*

Démonstration. Soient σ, σ' deux permutations ; supposons qu'elles sont conjuguées, c'est à dire qu'il existe $\tau \in \Sigma_n$ tel que $\sigma' = \tau\sigma\tau^{-1}$; soient $\sigma = c_1c_2\dots c_r$ la décomposition de σ en produit de cycles à supports disjoints. On a les égalités :

$$\tau\sigma\tau^{-1} = \tau c_1c_2\dots c_r\tau^{-1} = \tau c_1\tau^{-1}\tau c_2\tau^{-1}\dots\tau c_r\tau^{-1} = c'_1c'_2\dots c'_r,$$

où on a posé pour tout $i \in \{1, 2, \dots, r\}$ $c'_i = \tau c_i\tau^{-1}$. D'après la propriété 1.5.4, pour tout $i \in \{1, 2, \dots, r\}$, c'_i est un cycle de support l'image du support de c_i par τ, et donc les c'_i sont des cycles à supports disjoints et de même taille que les c_i. Par unicité de la décomposition en produit de cycles à supports disjoints, $\sigma' = c'_1c'_2\dots c'_r$ est la décomposition en cycles de supports disjoints de σ' qui a donc le même type que σ.

Réciproquement supposons que σ et σ' sont de même type. Écrivons la décomposition en cycle de ces deux permutations :

$$\sigma = c_1c_2\dots c_r \text{ et } \sigma' = c'_1c'_2\dots c'_s.$$

Comme elles sont de même type, on a $s = r$ et on peut supposer que pour tout $i \in \{1, 2, \dots, r\}$, c_i et c'_i sont de même taille t_i. On va montrer que $\sigma' = \tau\sigma\tau^{-1}$, où τ est une permutation dont le support est inclus dans le support de σ. On fait une récurrence sur r. Si $r = 1$, alors $\sigma = c_1 = (i_1, \dots, i_{t_1})$ et $\sigma' = c'_1 = (i'_1, \dots, i'_{t_1})$; considérons la permutation τ définie par $\tau(i_k) = i'_k$ pour $k \in \{1, 2, \dots, t_1\}$ et $\tau(m) = m$ si $m \in \{1, 2, \dots, n\} \setminus \{i_1, \dots, i_{t_1}\}$. Alors le support de τ est bien inclus dans $\{i_1, \dots, i_{t_1}\}$ qui est le support de σ et grâce à la propriété 1.5.4, on a bien : $\tau c_1\tau^{-1} = c'_1$.

Supposons l'assertion vraie jusqu'au rang $r-1$. D'après l'hypothèse de récurrence il existe μ tel que $\mu c_2c_3\dots cr\mu^{-1} = c'_2c'_3\dots c'_r$ avec le support de μ inclus dans le support du produit $c_2c_3\dots c_r$. De même, il existe τ tel que $\tau c_1\tau^{-1}$ tel que le support de τ est inclus dans le support de c_1. Avec ces hypothèses, on en déduit que les permutations τ et μ sont à supports disjoints donc elles commutent ; de même τ commute avec le produit $c_2c_3\dots c_r$ et μ commute avec c_1. On en déduit :

$$(\tau\mu)c_1c_2\dots c_r(\tau\mu)^{-1} = \tau\mu c_1c_2\dots c_r\mu^{-1}\tau^{-1} = \tau c_1\tau^{-1}\mu c_2\dots c_r\mu^{-1} = c'_1c'_2\dots c'_r = \sigma',$$

ce qui achève la preuve. □

1.5.2 Des ensembles générateurs de Σ_n

Nous allons donner plusieurs sous-ensembles qui sont générateurs de Σ_n. Rappelons qu'une partie X d'un groupe G est dite génératrice si $< X >= G$ ou de manière équivalente si tous les éléments de G s'écrivent comme produit d'éléments de X et de leurs inverses (voir la propriété 1.1.4 et le théorème 1). Remarquons que si les éléments de X sont tous d'ordre fini (ce qui est vrai si G est d'ordre fini), alors il n'est pas nécessaire de considérer les inverses des éléments pour calculer le groupe engendré par X, puisque dans ce cas l'inverse d'un élément est égal à une puissance de cet élément.

Théorème 17. *Les ensembles suivants engendrent le groupe symétrique Σ_n :*

(i) L'ensembles des cycles.

(ii) L'ensemble des transpositions.

(iii) L'ensemble des transpositions élémentaires :

$$\{(i, i+1) \mid 1 \leq i \leq n-1\}.$$

(iv) L'ensemble à deux éléments suivants :

$$\{(12), (12\dots n)\}.$$

Démonstration.

(i) On sait que toute permutation s'écrit comme un produit de cycles (voir la propriété 1.5.2), ce qui montre ce point.

(ii) Pour montrer que les transpositions engendrent Σ_n, d'après le point précédent il suffit de montrer que tout cycle $(i_1 \dots i_t)$ s'écrit comme un produit de transpositions. Or, on a l'égalité :

$$(i_1 \dots i_t) = (i_1 i_2)(i_2 i_3) \dots (i_{t-1} i_t). \tag{1.1}$$

(iii) On doit montrer que toute transposition (ab) s'écrit comme un produit de transposition élémentaire. On peut supposer que $b = a + k$ avec $k > 0$; montrons l'assertion par récurrence sur k. Pour $k = 1$, l'assertion est claire. Ensuite l'égalité suivante :

$$(a\, a+k) = (a+k-1\, a+k)(a\, a+k-1)(a+k-1\, a+k)$$

permet de montrer l'assertion au rang k si elle est vraie jusqu'au rang $k-1$.

(iv) Pour tout $i \in \{1, 2, \dots, n-1\}$, on vérifie l'égalité suivante :

$$(i\, i+1) = (12\dots n)^{i-1}(12)(12\dots n)^{-i+1},$$

ce qui montre ce dernier point.

□

1.5.3 La signature d'une permutation

Pour définir la signature d'une permutation, on commence par définir la notion d'inversion. On note T le sous-ensemble de X_n^2 suivant :

$$T = \{(i,j) \in X_n^2 \,|\, i < j\}.$$

Puis pour chaque σ on définit son ensemble d'inversion :

$$I(\sigma) = \{(i,j) \in T \,|\, \sigma(i) > \sigma(j)\}.$$

Exemple(s) 1.5.1. (i) Si e est la permutation identité, alors son ensemble d'inversion est l'ensemble vide. C'est le seul élément de Σ_n qui vérifie cette propriété.

(ii) Si (ab) (avec $a < b$) est une transposition, alors son ensemble d'inversion est égal à :

$$I(ab) = \{a, b\} \cup \{(a,i) \,|\, a < i < b\} \cup \{(i,b) \,|\, a < i < b\}.$$

Notons au passage que le cardinal de $I(ab)$ est impair.

Nous allons maintenant pourvoir définir la signature d'une permutation à partir de son ensemble d'inversion.

Définition 1.5.3. Soit $\sigma \in \Sigma_n$, on définit la signature de σ, notée par $\varepsilon(\sigma)$, par :

$$\varepsilon(\sigma) = (-1)^{|I(\sigma)|}.$$

D'après les exemples précédents, on connaît déjà la signature de l'identité : $\varepsilon(e) = 1$ et la signature d'une transposition τ : $\varepsilon(\tau) = -1$.

Nous allons voir que la signature est un morphisme de groupe. C'est une propriété remarquable, et qui ne se déduit pas aisément de la définition.

Théorème 18. *Pour tout $\sigma \in \Sigma_n$, on a :*

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

Pour tout $(\sigma', \sigma) \in \Sigma_n^2$, on a : $\varepsilon(\sigma'\sigma) = \varepsilon(\sigma')\varepsilon(\sigma)$. Ou autrement dit, la signature est un morphisme du groupe Σ_n dans le groupe ± 1

Démonstration. Soient P l'ensembles des parties à deux éléments de X_n et T l'ensemble défini ci-dessus. Ces deux ensembles sont en bijection, grâce aux applications suivantes :

$$\begin{array}{ccc} T & \to & P \\ (i,j) & \mapsto & \{i,j\} \end{array}$$

de réciproque :

$$\begin{array}{ccc} P & \to & T \\ \{i,j\} & \mapsto & (\min\{i,j\}, \max\{i,j\}). \end{array}$$

Notons également que σ induit une application :

$$S : \begin{array}{ccc} P & \to & P \\ \{i,j\} & \mapsto & \{\sigma(i), \sigma(j)\} \end{array}$$

qui est une bijection.

On peut maintenant calculer :

$$\prod_{(i,j)\in T} j - i = \prod_{\{i,j\}\in P} |j - i| = \prod_{\{i,j\}\in P} |\sigma(j) - \sigma(i)| = \prod_{(i,j)\in T} |\sigma(j) - \sigma(i)|.$$

La première égalité et la troisième sont vraies en utilisant la bijection entre P et T. Pour la deuxième, on utilise la bijection S et le fait que grâce à la valeur absolue, le terme $|\sigma(j) - \sigma(i)|$ ne dépend pas du couple (i,j), mais de l'ensemble $\{i,j\}$.

Par définition, (i,j) est une inversion si et seulement $|\sigma(j) - \sigma(i)| = -(\sigma(j) - \sigma(i))$, et donc :

$$\prod_{(i,j)\in T} |\sigma(j) - \sigma(i)| = (-1)^k \prod_{(i,j)\in T} \sigma(j) - \sigma(i)$$

où k est le nombre d'inversion de σ ce qui conclut la preuve du premier point.

Pour le deuxième point, on doit montrer l'égalité suivante :

$$\prod_{(i,j)\in T} \frac{\sigma'\sigma(j) - \sigma'\sigma(i)}{j - i} = \prod_{(i,j)\in T} \frac{\sigma'(j) - \sigma'(i)}{j - i} \prod_{(i,j)\in T} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Après simplification, on doit vérifier :

$$\prod_{(i,j)\in T} \frac{\sigma'\sigma(j) - \sigma'\sigma(i)}{\sigma(j) - \sigma(i)} = \prod_{(i,j)\in T} \frac{\sigma'(j) - \sigma'(i)}{j - i}.$$

Comme l'expression $\frac{\sigma'(j) - \sigma'(i)}{j - i}$ ne change pas si on permute $\sigma(j)$ et $\sigma(i)$, on peut définir : $\overline{\sigma'}(\{i,j\}) = \frac{\sigma'(j) - \sigma'(i)}{j - i}$. En utilisant la bijection entre T et P (pour la première et troisième égalité) et la bijection S (pour la deuxième égalité), on obtient :

$$\begin{aligned}\prod_{(i,j)\in T}\frac{\sigma'(j)-\sigma'(i)}{j-i} &= \prod_{\{i,j\}\in P}\overline{\sigma'}(\{i,j\})\\ &= \prod_{\{i,j\}\in P}\overline{\sigma'}(\{\sigma(i),\sigma(j)\})\\ &= \prod_{(i,j)\in T}\frac{\sigma'\sigma(j)-\sigma'\sigma(i)}{\sigma(j)-\sigma(i)},\end{aligned}$$

ce qui conclut cette preuve. □

En utilisant ce théorème, on peut calculer la signature d'un produit de r transpositions, elle est égale à $(-1)^r$. Comme tout élément $\sigma \in \Sigma_n$ s'écrit comme un produit de transpositions, si on connaît cette décomposition, on peut calculer rapidement la signature de σ. Remarquons au passage que cette décomposition de σ en produit de transpositions n'est pas unique, par contre d'après la propriété de la signature, la parité du nombre de termes d'une telle décomposition est la même pour toutes les décompositions.

Si on considère un cycle de taille t, sa signature est égale à $(-1)^{t-1}$ (voir l'égalité 1.1 vu dans la preuve du théorème 17). Cette remarque va nous permettre de retrouver la définition de la signature qui a été vue en L2.

Propriété 1.5.5. *Soient $\sigma \in \Sigma_n$ et $\sigma = c_1c_2\dots c_r$ sa décomposition en produit de cycles. Alors $\varepsilon(\sigma) = (-1)^{n-r}$*

Démonstration. Pour $i \in \{1, 2, \dots, r\}$, appelons t_i la taille de c_i. La signature est multiplicative donc :

$$\varepsilon(\sigma) = \prod_{i=1}^{r}\varepsilon(c_i) = \prod_{i=1}^{r}(-1)^{t_{i-1}} = (-1)^{\sum_{i=1}^{r}(t_i-1)}.$$

Mais on a vu à la suite de la définition 1.5.2 que $\sum_{i=1}^{r} t_i = n$ ce qui conclut la preuve. □

Enfin le théorème 18 permet de donner une caractérisation du morphisme signature.

Propriété 1.5.6. *La signature est l'unique morphisme non trivial de Σ_n dans le groupe à deux éléments $\{\pm 1\}$.*

Démonstration. Le fait que la signature vérifie les deux propriétés découle directement du théorème 18 et de la remarque 1.5.1. Vérifions que c'est le bien le seul. Soit φ un morphisme non trivial de Σ_n dans $\{\pm 1\}$. Alors comme Σ_n est engendré par les transpositions, il existe une transposition τ telle que $\varphi(\tau) = -1$ (sinon φ serait trivial). Le morphisme φ étant à valeur dans un groupe commutatif, il est constant sur les classes de conjugaison (le vérifier). Comme toutes les transpositions sont conjuguées, φ prend la valeur -1 pour toutes les transpositions. Et donc $\varphi = \varepsilon$ sur l'ensemble des transpositions. En utilisant encore une fois que les transpositions engendrent Σ_n, on a l'égalité : $\varphi = \varepsilon$. □

Les permutations de signature $+1$ (qui sont appelées les permutations paires) sont par définition les éléments du noyau du morphisme signature. On appelle ce noyau le groupe alterné, nous le noterons ici A_n. Par définition, A_n est donc un sous-groupe *distingué* de Σ_n. Voici quelques propriétés de ce groupe.

Propriété 1.5.7. *(a) Le groupe A_n est de cardinal $n!/2$*

(b) C'est le seul sous-groupe d'indice 2 de Σ_n.

(c) Il est engendré par les 3-cycles.

Démonstration.

(i) On utilise le premier théorème d'isomorphisme appliqué au morphisme signature : le quotient Σ_n/A_n est isomorphe au groupe $\{\pm 1\}$ qui est de cardinal 2, d'ou l'assertion.

(ii) Soit K un sous-groupe de Σ_n d'indice 2. Alors l'exercice 25, K est distingué. Comme Σ_n/K est de cardinal 2, il est isomorphe au groupe $\{\pm 1\}$. En considérant le morphisme quotient π de Σ_n dans Σ_n/K, on donc un morphisme de Σ_n dans $\{\pm 1\}$ et de noyau K. D'après la propriété 1.5.6, ce morphisme est le morphisme signature dont le noyau est A_n, et donc $K = A_n$.

(iii) Voir l'exercice 42.

□

1.5.4 Le groupe A_n est simple

La notion de groupe simple est fondamentale dans l'études des groupes (finis). Commençons par définir cette notion.

Définition 1.5.4. Soit G un groupe, on dit que G est un groupe simple si les seuls sous-groupes distingués de G sont $\{e\}$ et G.

De façon imagée et pour motiver la définition, on peut voir les groupes simples comme des espèces d'atomes constituant la « matière » des groupes. De façon plus concrète, on peut déjà regarder les groupes simples finis et commutatifs.

Exemple(s) 1.5.2. Les groupes d'ordre premier sont simples. Ce sont les seuls groupes finis commutatifs simples.

Nous allons voir que le groupe A_n pour $n \geq 5$ est simple.

Théorème 19. *Pour $n \geq 5$, les 3-cycles de A_n sont conjugués et le groupe A_n est simple.*

Démonstration. Commençons par montrer la première assertion. Soient (abc) et $(a'b'c')$ deux 3-cycles. Ils sont de même type, et d'après la propriété 16 ils sont conjugués dans Σ_n. Il existe donc $\sigma \in \Sigma_n$ tel que $\sigma(abc)\sigma^{-1} = (a'b'c')$. Si $\sigma \in A_n$, on a terminé. Sinon, soient d, e deux éléments de X_n qui n'appartiennent pas à l'ensemble $\{a, b, c\}$ (on utilise ici que $n \geq 5$). Posons $\sigma' = \sigma(de)$, alors on a $\sigma'(abc)\sigma'^{-1} = (a'b'c')$ et $\sigma' \in A_n$, et donc (abc) et $(a'b'c')$ sont conjugués dans A_n.

Soit K un sous-groupe distingué de A_n différent de l'identité. Il s'agit de montrer que $K = A_n$. Mais pour cela il suffit de montrer que K contient un seul 3-cycle. En effet comme les 3-cycles sont conjugués dans A_n et que K est distingué, si K contient un 3-cycle il les contient tous. Et comme ces 3-cycles engendrent A_n, on a bien $A_n = K$.

Montrons donc que K contient un 3-cycle. Soit $\sigma \in K$ tel que le nombre de points fixes de Σ soit maximal parmi les éléments de $K \setminus \{e\}$, et montrons que cet élément est forcément un 3-cycle.

On décompose σ en produit de cycles à supports disjoints. Si dans cette décomposition, tous les cycles sont des transpositions, alors il y a au moins deux transpositions. Supposons que ces deux transpositions s'écrivent (ab) et (cd) avec $\{a, b, c, d\} \in X_n$ distincts. On peut donc écrire $\sigma = (ab)(cd)c_3 \dots c_r$ où $c_3, \dots, c_r$ sont des cycles à supports disjoints de l'ensemble $\{a, b, c, d\}$; notons qu'ici nous n'indiquons que les cycles de taille supérieure ou égale à deux, les points fixes ne sont pas indiqués. Considérons maintenant $e \notin \{a, b, c, d\}$ et le cycle $\tau = (cde)$. Alors $\tau\sigma\tau^{-1} = (ab)(de)c'_3 \dots c'_r$ où les cycles $c'_3, \dots, c'_r$ ont leurs supports disjoints de $\{a, b, d, e\}$. Remarquons que puisque K est distingué, l'élément $\tau\sigma\tau^{-1}$ appartient à K. Soit $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$, c'est aussi un élément de K différent de l'identité. Il fixe a et b, ainsi que

tous les éléments fixés par σ et qui ne sont pas dans l'ensemble $\{a, b, c, d, e\}$. Mais du coup, comme σ ne fixe aucun des points a, b, c, d, l'élément ρ fixe plus de points que σ ce qui est une contradiction.

Supposons maintenant que σ n'est ni un 3-cycle, ni un produit de transpositions. Alors on écrit la décomposition en cycle à supports disjoints : $\sigma = c_1 \dots c_r$. On peut supposer que la taille de c_1 est supérieure où égale à 3. Et on écrit $c_1 = (abc\dots)$. Alors il existe au moins deux éléments distincts d et e non fixés par σ et n'appartenant pas à l'ensemble $\{a, b, c\}$. En effet, si c_1 est un 3-cycle alors par hypothèse $r \geq 2$ et le résultat est clair. De même si $r = 1$, alors la taille de c_1 est plus grande que 5 et on peut choisir deux éléments dans le support de c_1 distincts de a, b, c .

Posons comme précédemment $\tau = (cde)$. Alors $\tau\sigma\tau^{-1} = (abd...)c'_2c'_3 \dots c'_r$. Comme précédemment, l'élément $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$ est un élément non trivial de K qui fixe b ainsi que tous les éléments qui n'appartiennent pas à l'ensemble $\{a, b, c, d, e\}$ et qui sont fixés par σ. Mais comme σ ne fixe aucun des éléments de l'ensemble $\{a, b, c, d, e\}$, l'élément ρ fixe plus d'éléments que σ ce qui est une contradiction. Il reste donc une seule possibilité : σ est un 3-cycle. □

Remarque(s) 1.5.1. Pour $n \leq 4$ la situation est bien comprise. Tout d'abord pour $n = 1$ ou 2 le groupe A_n est réduit à un seul élément, il est donc trivialement simple. Pour $n = 3$, alors A_3 est isomorphe au seul groupe d'ordre 3, le groupe cyclique d'ordre 3 qui est également simple.

Par contre A_4 n'est pas simple. On considère le sous-ensemble de Σ_4 suivant :

$$K = \{e, (12)(34), (13)(24), (14)(23)\}.$$

Il est immédiat de vérifier que K est un sous-groupe de Σ_4, isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$; de plus en utilisant la propriété 1.5.4 on vérifie que K est distingué dans Σ_4. Il est donc distingué dans A_4 qui n'est pas un groupe simple. On aurait donc pu énoncer le théorème sous la forme : pour $n \neq 4$, A_n est simple.

1.5.5 Exercices

Exercice 41 ⓔ

Montrer que toute permutation d'ordre 10 dans Σ_8 est impaire.

Exercice 42 ⓒ

(a) Montrer que le produit de deux transpositions distinctes est un 3-cycle ou un produit de deux 3-cycles. En déduire que A_n est engendré par les 3-cycles.

(b) Montrer que $A_n =< (123), (124), \dots, (12n) >$.

Exercice 43 ⓒ

Montrer que dans Σ_n tout élément σ est conjugué à son inverse. De plus montrer que l'élément qui conjugue σ et σ^{-1} peut être choisi d'ordre 2. En déduire que tout élément de Σ_n s'écrit comme le produit de deux éléments d'ordre 2.

Exercice 44 ⓐ

Soit G un groupe simple d'ordre 60. Le but de cet exercice est de montrer que G est isomorphe à A_5. On note n_2, n_3, n_5 le nombre de 2-Sylow, 3-Sylow et 5-Sylow de G. Soit G un groupe simple d'ordre 60. Le but de cet exercice est de montrer que G est isomorphe à A_5. On note n_2, n_3, n_5 le nombre de 2-Sylow, 3-Sylow et 5-Sylow de G.

(a) Supposons que G agisse non trivialement sur un ensemble à n éléments, montrer qu'il existe un morphisme injectif ψ de G dans Σ_n. En déduire que $n \geq 5$ et que si $n = 5$, alors G est isomorphe à A_5.

(b) Montrer que $n_5 = 6$; en déduire que G admet 24 éléments d'ordre 5.

(c) Montrer que n_3 est égal à 4 ou 10. En utilisant la première question montrer que $n_3 \neq 4$. En déduire que $n_3 = 10$ et que G admet 20 éléments d'ordre 3.

(d) Montrer que $n_2 = 3, 5$ ou 15. Toujours avec la première question, montrer que $n_2 \neq 3$.

(e) Supposons $n_2 = 5$, conclure.

(f) Supposons que $n_2 = 15$. Montrer qu'il existe deux 2-Sylow distincts H_1 et H_2 dont l'intersection contient un élément d'ordre 2. Soit s cet élément, montrer que son centralisateur $C = Z_G(s) = \{g \in G \mid gs = sg\}$ est d'ordre $12, 20$ ou 60. Montrer que la seule possibilité est 12 (en utilisant la première question), et conclure.

Chapitre 2

Algèbre linéaire approfondie

2.1 Endomorphismes et matrices semblables

2.1.1 Motivations

Le but de cette partie est d'étudier les endomorphismes à « changement de base près ». Précisons cela : soit E un espace vectoriel de dimension finie n sur un corps $\mathbb{K}$, et f un endomorphisme de E (une application linéaire de E dans lui-même). Pour chaque choix d'une base $\mathscr{B}$ de E, on obtient une matrice que l'on notera $\mathrm{Mat}_{\mathscr{B}}(f)$. On veut essayer d'apporter des réponses aux questions suivantes :

(i) Est-ce qu'il existe une base $\mathscr{B}$ dans laquelle la matrice $\mathrm{Mat}_{\mathscr{B}}(f)$ est simple ?

(ii) Si $\mathscr{B}$ et $\mathscr{B}'$ sont deux bases, quel est le lien entre $\mathrm{Mat}_{\mathscr{B}}(f)$ et $\mathrm{Mat}_{\mathscr{B}'}(f)$?

(iii) Quelles sont les fonctions « invariantes » par changement de bases ?

Vous connaissez déjà des débuts de réponses. Pour la question (i), vous avez vu en L2 que certains endomorphismes sont diagonalisables, c'est à dire qu'il existe une base dans laquelle la matrice de f est diagonale. Pour les questions (ii) et (iii), vous savez que le déterminant, la trace, le polynôme caractéristique sont invariants par changement de base.

2.1.2 Définitions d'endomorphismes et de matrices semblables

Pour formaliser plus précisément toutes ces questions, nous allons introduire la notion d'endomorphismes semblables. Mais rappelons d'abord quelques notions et notations sur la correspondance entre applications linéaires et bases.

Soient E, F deux espaces vectoriels de dimension respectives n, m sur un corps $\mathbb{K}$ et $f \in \mathscr{L}(E, F)$ une application linéaire de E dans F ; soient $\mathscr{B}$ une base de E et $\mathscr{C}$ une base de F, on note $\mathrm{Mat}_{\mathscr{C},\mathscr{B}}(f)$ la matrice de f dans les bases $\mathscr{B}$ et $\mathscr{C}$. Les colonnes de cette matrice sont les coordonnées dans la base $\mathscr{C}$ de l'image par f des vecteurs de la base $\mathscr{B}$, et donc cette matrice admet m lignes et n colonnes, elle appartient donc à l'espace $\mathrm{M}_{m,n}(\mathbb{K})$.

Lorsque $E = F$ *et* $\mathscr{B} = \mathscr{C}$, on note $\mathrm{Mat}_{\mathscr{B},\mathscr{B}}(f)$ plus simplement par $\mathrm{Mat}_{\mathscr{B}}(f)$.

Rappelons le lien entre applications linéaires et matrices.

Propriété 2.1.1. *Soient E, F deux $\mathbb{K}$-espaces vectoriels de dimension respectives n et m comme ci-dessus et soient $\mathscr{B}$ une base de E et $\mathscr{C}$ une base de F, alors l'application suivante :*

$$\begin{array}{ccc} \mathscr{L}(E,F) & \to & \mathrm{M}_{m,n}(\mathbb{K}) \\ f & \mapsto & \mathrm{Mat}_{\mathscr{C},\mathscr{B}}(f) \end{array}$$

est une application linéaire bijective. De plus, dans le cas où $m = n$, cette application est compatible avec le produit existant sur les deux espaces, et l'endomorphisme f est bijective si et seulement si la matrice $\mathrm{Mat}_{\mathscr{C},\mathscr{B}}(f)$ est inversible.

Rappelons maintenant la formule de changement de base dans ce contexte.

Propriété 2.1.2. *Soient E, F et f comme ci-dessus. Soient $\mathscr{B}, \mathscr{B}'$ deux bases de E et $\mathscr{C}, \mathscr{C}'$ deux bases de F. On a l'égalité suivante :*

$$\mathrm{Mat}_{\mathscr{C}',\mathscr{B}'}(f) = \mathrm{Mat}_{\mathscr{C}',\mathscr{C}}(\mathbb{1}_F)\mathrm{Mat}_{\mathscr{C},\mathscr{B}}(f)\mathrm{Mat}_{\mathscr{B},\mathscr{B}'}(\mathbb{1}_E).$$

Nous allons maintenant pouvoir définir la notion d'endomorphismes semblables.

Définition 2.1.1. Soient $\mathbb{K}$ un corps, $n \in \mathbb{N}$, E un $\mathbb{K}$-espace vectoriel de dimension n, et $(f, g) \in \mathrm{End}(E)$ deux endomorphismes de E. On dit que f et g sont semblables, s'il existe deux bases $\mathscr{B}, \mathscr{B}'$ de E telles que $\mathrm{Mat}_{\mathscr{B}}(f) = \mathrm{Mat}_{\mathscr{B}'}(g)$.

Nous allons voir une autre façon d'énoncer que deux endomorphismes sont semblables et nous en déduirons aisément que cette relation est une relation d'équivalence.

Propriété 2.1.3. *(i) Les endomorphismes f et g sont semblables si et seulement s'il existe une application linéaire inversible $s \in \mathrm{GL}(E)$ telle que $f = sgs^{-1}$.*

(ii) la relation « être semblable à »est une relation d'équivalence.

Démonstration.

(i) Supposons que f et g soient semblables, il existe donc deux bases $\mathscr{B}$ et $\mathscr{B}'$ tels que $\mathrm{Mat}_{\mathscr{B}}(f) = \mathrm{Mat}_{\mathscr{B}'}(g)$. Soit P la matrice de passage suivante : $P = \mathrm{Mat}_{\mathscr{B}',\mathscr{B}}(\mathbb{1}_E)$. Alors P est inversible d'inverse $P^{-1} = \mathrm{Mat}_{\mathscr{B},\mathscr{B}'}(\mathbb{1}_E)$ et d'après la formule de changement de base (propriété 2.1.2), on a l'égalité :

$$\mathrm{Mat}_{\mathscr{B}'}(g) = \mathrm{Mat}_{\mathscr{B}',\mathscr{B}}(\mathbb{1}_E)\mathrm{Mat}_{\mathscr{B}}(g)\mathrm{Mat}_{\mathscr{B},\mathscr{B}'}(\mathbb{1}_E) = P\mathrm{Mat}_{\mathscr{B}}(g)P^{-1}.$$

Et donc nous avons finalement :

$$\mathrm{Mat}_{\mathscr{B}}(f) = P^{-1}\mathrm{Mat}_{\mathscr{B}}(g)P.$$

D'après la propriété 2.1.1, il existe $s \in \mathrm{GL}(E)$ tels que $P = \mathrm{Mat}_{\mathscr{B}}(s)$, et l'égalité ci-dessus devient : $f = sgs^{-1}$.

(ii) Ce point est laissé en exercice.

□

On considère très souvent l'espace vectoriel $E = \mathbb{K}^n$; dans ce cas les endomorphismes de E sont donnés directement par des matrices. Si l'on traduit pour ces endomorphismes particuliers la propriété d'être semblables, on obtient la notion de matrices semblables.

Définition 2.1.2. Soient $n \in \mathbb{N}$ et $(M, N) \in \mathrm{M}_n$ deux matrices carrées de taille n, on dit que M et N sont semblables s'il existe une matrice $P \in \mathrm{M}_n(\mathbb{K})$ *inversible* telle que : $M = PNP^{-1}$.

Pour finir cette introduction, et pour faire le lien avec le chapitre précédent, on peut remarquer que cette équivalence entre endomorphismes ou matrices provient d'une action de groupe. À cet effet, rappelons que l'ensemble $\mathrm{GL}(E)$ des applications linéaires de E dans E (resp. l'ensemble $\mathrm{GL}_n(\mathbb{K})$) est un groupe. Le groupe $\mathrm{GL}(E)$ (resp. $\mathrm{GL}_n(\mathbb{K})$) agit sur l'espace $\mathrm{End}(E)$ (resp. $\mathrm{M_n}(\mathbb{K})$) :

$$\begin{array}{ccc} \mathrm{GL}(E) \times \mathrm{End}(E) & \to & \mathrm{End}(E) \\ (s, f) & \mapsto & sfs^{-1} \end{array}$$

et

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbb{K}) \times \mathrm{M}_n(\mathbb{K}) & \to & \mathrm{M}_n(\mathbb{K}) \\ (P, M) & \mapsto & PMP^{-1} \end{array}.$$

Propriété 2.1.4. *Deux endomorphismes (resp. deux matrices) sont semblables si et seulement s'ils (resp. si elles) sont dans la même orbite pour l'action définie ci-dessus.*

Démonstration. Il suffit d'appliquer les définitions. □

2.1.3 D'autres rappels

Voici quelques rappels du cours de L2.

Définition 2.1.3. Soient E un espace vectoriel de dimension n sur un corps $\mathbb{K}$, et $f \in \mathrm{End}(E)$, on dit que λ est valeur propre s'il existe $v \in E$ non nul tel que $f(v) = \lambda v$. Pour λ une valeur propre, on définit l'ensemble des vecteurs propres de valeur propre λ en posant :

$$E_\lambda = \{v \in E \mid f(v) = \lambda v\} = \ker(f - \lambda \mathbb{1}_E).$$

Rappelons que E_λ est un sous-espace vectoriel (c'est clair par la deuxième égalité) ; on peut le définir même si λ n'est pas une valeur propre, mais dans ce cas $E_\lambda = \{0\}$.

Pour finir avec E_λ remarquons que c'est un sous-espace stable par f, c'est à dire que $f(E_\lambda) \subset E_\lambda$ et que la restriction de f à E_λ est une homothétie de rapport λ.

Pour $f \in \mathrm{End}(E)$, on définit le polynôme caractéristique de f, en posant $P_f(X) = \det(f - X\mathbb{1}_E)$.

Propriété 2.1.5. *Soient $f \in \mathrm{End}(E)$ et $\lambda \in \mathbb{K}$, alors λ est une valeur propre si et seulement si $P_f(\lambda) = 0$.*

Démonstration. Voir le cours de L2. □

L'ensemble des valeurs propres est donc l'ensemble des racines d'un polynôme de degré $n = \dim E$. Pour un tel polynôme, il y a plusieurs façons d'écrire ses racines et la factorisation qui l'accompagne. Si on considère l'ensemble des racines comme un p-uplet : $(\mu_1, \mu_2, \ldots, \mu_p)$ alors la factorisation de P s'écrira :

$$P(X) = Q(X) \prod_{i=1}^{p} (X - \mu_i),$$

avec Q un polynôme n'admettant pas de racines. Ici, on peut avoir $\mu_i = \mu_j$ avec $i \neq j$.

On peut aussi considérer les racines comme un multi-ensemble, c'est à dire l'ensemble support : $\{\lambda_1, \ldots, \lambda_r\}$, et une fonction multiplicité :

$$\begin{array}{ccc} \{\lambda_1, \ldots, \lambda_r\} & \to & \mathbb{N} \\ \lambda_i & \mapsto & n_i \end{array}$$

La factorisation va s'écrire

$$P(X) = Q(X) \prod_{i=1}^{r} (X - \lambda_i)^{n_i},$$

où Q est un polynôme qui n'admet pas de racines dans $\mathbb{K}$. Ici si $i \neq j$ alors $\lambda_i \neq \lambda_j$. Les deux écritures sont dépendantes, par exemple, on a $\sum_{i=1}^{r} n_i = p$.

Dans les deux cas, si le polynôme est scindé (s'il admet n racines comptées avec multiplicités), par exemple si $\mathbb{K} = \mathbb{C}$, alors Q est une constante.

Rappelons que l'ensemble des valeurs propres de $f \in \mathrm{End}(E)$ s'appelle le spectre de E, on le note $\mathrm{spec}(f)$. Les racines du polynôme caractéristique forment donc un multi-ensemble, et on peut écrire la factorisation de ce polynôme sous la forme :

$$P_f(X) = Q(X) \prod_{\lambda \in \mathrm{spec}(f)} (X - \lambda)^{n_\lambda},$$

où Q est un polynôme n'admettant pas de racines dans $\mathbb{K}$.

Rappelons qu'un endomorphisme est diagonalisable, s'il existe une base $\mathscr{B}$ telle que $\mathrm{Mat}_{\mathscr{B}}(f)$ soit une matrice diagonale. On a la propriété suivante :

Propriété 2.1.6. *Soit $f \in \mathrm{End}(E)$, on a équivalence entre :*

(i) L'endomorphisme f est diagonalisable.

(ii) La matrice de f dans une base quelconque est semblable à une matrice diagonale.

(iii) Pour tout $\lambda \in \mathrm{spec}(f)$, on a l'égalité $n_\lambda = \dim E_\lambda$, et le polynôme Q est une constante.

(iv) On a l'égalité :

$$E = \bigoplus_{\lambda \in \mathrm{spec}(f)} E_\lambda.$$

Démonstration. Voir le cours de L2. □

On peut déjà apporter une réponse partielle à une des questions de l'introduction. Pour cela, on considère deux endomorphismes $(f, f') \in \mathrm{End}(E)^2$. Si $\lambda \in \mathrm{spec}(f)$ (resp. $\lambda \in \mathrm{spec}(f')$), nous noterons n_λ la multiplicité de λ dans P_f (resp. n'_λ la multiplicité de λ dans $P_{f'}$).

Propriété 2.1.7. *Soient $(f, f') \in \mathrm{End}(E)^2$ deux endomorphismes diagonalisables, alors f et f' sont semblables si et seulement si $\mathrm{spec}(f) = \mathrm{spec}(f')$ et si pour tout $\lambda \in \mathrm{spec}(f)$, on a l'égalité $n_\lambda = n'_\lambda$.*

Démonstration. Si les deux endomorphismes sont semblables, alors il existe deux bases $\mathscr{B}$ et $\mathscr{B}'$ de E telles que $\mathrm{Mat}_{\mathscr{B}}(f) = \mathrm{Mat}_{\mathscr{B}'}(f')$. En calculant le polynôme caractéristique de f (resp. de f') dans la base $\mathscr{B}$ (resp. de f' dans la base $\mathscr{B}'$), on obtient l'égalité $P_f = P_{f'}$. Et donc f et f' ont même valeur propre comptées avec multiplicités. Remarquons que pour montrer ce sens, nous n'avons pas utiliser le fait que f et f' soient diagonalisables.

Supposons maintenant que $\mathrm{spec}(f) = \mathrm{spec}(f')$ et que pour tout $\lambda \in \mathrm{spec}(f)$, $n_\lambda = n'_\lambda$. Comme f est diagonalisable, il existe une base $\mathscr{B}$ telle que $\mathrm{Mat}_{\mathscr{B}}(f)$ soit une matrice diagonale. Les coefficients sur la diagonale sont les valeurs propres de P_f, c'est à dire les λ, chacune apparaissant n_λ fois. On peut faire la même remarque pour f' : il existe une base $\mathscr{B}'$ telle que $\mathrm{Mat}_{\mathscr{B}'}(f')$ soit diagonale, et d'après l'hypothèse, on a : $\mathrm{Mat}_{\mathscr{B}}(f) = \mathrm{Mat}_{\mathscr{B}'}(f')$, c'est à dire f et f' sont semblables d'après la définition 2.1.1. □

2.1.4 Exercices

Exercice 45 ⓔ

On rappelle qu'un endomorphisme d'un espace vectoriel de dimension finie est trigonalisable, si cet endomorphisme est semblable à une matrice triangulaire (où de manière équivalente, un endomorphisme f est trigonalisable s'il existe une base dans laquelle la matrice de f soit triangulaire).

1. Montrer qu'un endomorphisme est trigonalisable si et seulement si son polynôme caractéristique est scindé.
2. Montrer que deux endomorphismes trigonalisables qui commutent peuvent être trigonalisé dans une même base.

Exercice 46 ⓒ

Soient f et g deux endomorphismes d'un espace vectoriel de dimension finie commutant entre eux et diagonalisables.

1. Montrer que f laisse stable les sous-espaces propres de g.
2. En déduire que f et g sont simultanément diagonalisables(*i.e.* diagonalisables dans une même base).

3. Plus généralement, soit $(f_i)_{i\in I}$ une famille d'endomorphismes qui sont diagonalisables et qui commutent deux à deux ; montrer que tous les éléments de cette famille sont simultanément diagonalisables. Indication : faire une récurrence sur la dimension de l'espace.

Exercice 47 ⓐ

Soient $\mathbb{K}$ un corps et M, N deux matrices appartenant à $\mathrm{M}_{mn}(\mathbb{K})$, on dit que M et N sont équivalentes, s'il existe deux matrices inversibles $(P, Q) \in \mathrm{GL}_m(\mathbb{K}) \times \mathrm{GL}_n(\mathbb{K})$ telles que $M = PNQ$.

1. Montrer que la relation définie ci-dessus est bien une relation d'équivalence.
2. Montrer que cette relation provient d'une action de groupe que l'on déterminera.
3. Montrer que dans le cas où $m = n$, alors si M et N sont semblables, elles sont équivalentes. Que pensez-vous de la réciproque ?
4. Montrer que M et N sont équivalentes si et seulement si elles ont même rang.

2.2 Polynômes d'endomorphismes, polynôme minimal

Notons $\mathbb{K}[X]$ l'ensemble des polynômes sur un corps $\mathbb{K}$; rappelons que cet ensemble est une $\mathbb{K}$-algèbre. Ce qui veut dire que $\mathbb{K}[X]$ est un espace vectoriel (de dimension infinie) et que cet espace est muni d'un produit :

$$\begin{array}{ccc} \mathbb{K}[X] \times \mathbb{K}[X] & \to & \mathbb{K}[X] \\ (P, Q) & \mapsto & PQ \ ; \end{array}$$

cette application est bi-linéaire et de plus ce produit est commutatif et associatif. Une autre ensemble que nous avons rencontré et qui admet une structure d'algèbre est l'espace $\mathrm{End}(E)$; c'est un espace vectoriel sur $\mathbb{K}$ et la composition est un produit qui est associatif, mais non commutatif. Si $f \in \mathrm{End}(E)$, et $P \in \mathbb{K}[X] = \sum_{i=0}^{n} a_i X^i$, alors en considérant les puissances de f comme la composition de f avec lui-même et avec la convention habituelle que $f^0 = \mathbb{1}_E$, on peut calculer $P(f) = \sum_{i=0}^{n} a_i f^i$ qui est un élément de $\mathrm{End}(E)$. On peut donc définir l'application :

$$\Pi_f : \begin{array}{ccc} \mathbb{K}[X] & \to & \mathrm{End}(E) \\ P & \mapsto & P(f) \end{array}.$$

Cette application est linéaire, c'est à dire que pour tout $\lambda \in \mathbb{K}$ et tout $(P, Q) \in \mathbb{K}[X]^2$, on a :

$$\Pi_f(P + Q) = \Pi_f(P) + \Pi_f(Q) \text{ et } \Pi_f(\lambda P) = \lambda \Pi_f(P),$$

ce qui peut s'écrire :

$$(P + Q)(f) = P(f) + Q(f) \text{ et } (\lambda P)(f) = \lambda(P(f)).$$

C'est un peu moins évident, mais cette application est également compatible avec le produit.

Propriété 2.2.1. *Pour tout $(P, Q) \in \mathbb{K}[X]^2$, on a $\Pi_f(PQ) = \Pi_f(P)\Pi_f(Q)$, ou autrement dit $(PQ)(f) = P(f)Q(f)$.*

Démonstration. Comme le produit est linéaire par rapport à chacun des deux termes du produit, on se ramène à montrer l'assertion pour $P = X^s$ et $Q = X^r$, mais pour ces deux monômes, l'égalité est évidente. □

Donnons une application simple et très utile des propriétés des polynômes d'endomorphismes.

Propriété 2.2.2. *Soient $f \in \mathrm{End}(E)$ et $P \in \mathbb{K}[X]$, alors $\ker P(f)$ est stable par f.*

Démonstration. Soit $v \in E$ tel que $v \in \ker P(f)$; alors par définition, on a $P(f)(v) = 0$. Montrons que $f(v) \in \ker P(f)$. Pour cela on effectue le calcul suivant :

$$P(f)(f)(v) = (PX)(f)(v) = (XP)(f)(v) = fP(f)(v) = f(0) = 0.$$

La première et troisième égalité proviennent de la compatibilité du produit dans $\mathbb{K}[X]$ et $\mathrm{End}(E)$, et la deuxième du fait que le produit dans $\mathbb{K}[X]$ est commutatif. □

Voici des propriétés de l'image et du noyau de l'application Π_f.

Propriété 2.2.3. *Soient $f \in \mathrm{End}(E)$ et Π_f l'application définie ci-dessus. On a les propriétés suivantes :*

(i) Le noyau de Π_f est un idéal de $\mathbb{K}[X]$, c'est à dire que $\ker \Pi_f$ est un sous-espace vectoriel et pour tout $P \in \ker \Pi_f$ et pour tout $Q \in \mathbb{K}[X]$, on a $PQ \in \ker \Pi_f$.

(ii) L'image de Π_f est un sous-algèbre de $\mathrm{End}(E)$ qui est commutative.

Démonstration. Le premier point se montre par un calcul direct. Pour le deuxième point, on vérifie en utilisant les propriétés de Π_f que l'image de Π_f est un sous-espace vectoriel et stable par multiplication. De plus, comme le produit sur $\mathbb{K}[X]$ est commutatif, le produit sur l'image de Π_f l'est également. □

Rappelons deux propriétés concernant l'arithmétique des polynômes.

Propriété 2.2.4. *Soit I un idéal différent de 0 de $\mathbb{K}[X]$, alors il existe un unique polynôme unitaire P tel que $I = P\mathbb{K}[X] = \{PQ \mid Q \in \mathbb{K}[X]\}$.*

Démonstration. C'est un résultat que vous avez vu en L2 ; pour vous rafraîchir la mémoire : pensez à la preuve de la propriété sur les sous-groupes de $\mathbb{Z}$ en remplaçant la division euclidienne dans les entiers par la division euclidienne sur les polynômes. □

Propriété 2.2.5. Égalité de Bézout pour les polynômes
Soient P et Q deux polynômes premiers entre eux, c'est à dire que les seuls diviseurs communs de P et Q sont les polynômes constants. Alors il existe deux polynômes $(R, S) \in \mathbb{K}[X]^2$ tels que $RP + SQ = 1$.

Démonstration. Voir également le cours de L2 ; on peut aussi retrouver une preuve : considérer la somme de l'idéal engendré par P et de l'idéal engendré par Q, c'est un idéal, et on peut utiliser la propriété précédente. □

2.2.1 Le polynôme minimal, le polynôme caractéristique

L'application Π_f n'est pas injective, son noyau n'est donc pas réduit à 0, il existe un polynôme unitaire, noté M_f tel que $\ker \Pi_f = M_f\mathbb{K}[X]$. Ce polynôme est appelé le polynôme minimal de f. Notons que si $Q \in \ker \Pi_f$, alors $Q(f) = 0$; on dit que Q est un polynôme annulateur de f. Donnons quelques exemples.

Exemple(s) 2.2.1. (i) Si E est l'espace de dimension 0, alors le noyau de Π_f est égal à $\mathbb{K}[X]$ tout entier, dans ce cas $M_f = 1$,

(ii) Le cas ci-dessus est le seul cas où le polynôme minimal est constant, en effet si $\dim E \geq 0$, M_f est degré au moins égal à 1 et si $\lambda \in \mathbb{K}$, $M_f = X - \lambda$ si et seulement si $f = \lambda \mathbb{1}_E$. On peut voir dans cet exemple que le degré du polynôme minimal peut être beaucoup plus petit que le degré du polynôme caractéristique.

On a la caractérisation suivante de M_f parmi les polynômes annulateurs de f :

Propriété 2.2.6. *Soit $f \in \mathrm{End}(E)$, soit $Q \in \mathbb{K}[X]$ unitaire tel que $Q(f) = 0$, alors on a équivalence entre :*

(i) Pour tout P tel que $P(f) = 0$, alors $Q \mid P$

(ii) $Q = M_f$

Démonstration. Puisque $Q(f) = 0$ on sait déjà que $M_f \mid Q$. Du coup si (i) est vrai alors comme $M_f(f) = 0$, on a $Q \mid M_f$ ce qui implique (ii). La réciproque est évidente. □

Rappelons maintenant un théorème vu l'année dernière.

Théorème 20. Le théorème de Cayley-Hamilton *Soit $f \in \mathrm{End}(E)$ et soit P_f son polynôme caractéristique, alors $P_f(f) = 0$.*

Démonstration. Cette preuve a été vu en L2, par souci de complétude nous la rappellerons dans la partie 2.3. □

Les équivalences suivantes sont directes :

$$M_f \mid P_f \Leftrightarrow P_f \in \ker \Pi_f \Leftrightarrow P_f(f) = 0.$$

On en déduit un énoncé équivalent du théorème précédent.

Théorème 21. Le théorème de Cayley-Hamilton (deuxième version) *Soient $f \in \mathrm{End}(E)$, M_f et P_f le polynôme minimal et caractéristique de f ; alors M_f divise P_f.*

Un autre lien entre le polynôme minimal et le caractéristique est le suivant :

Propriété 2.2.7. *Soit Q irréductible, tel que $\ker Q(f) \neq 0$, alors $Q \mid M_f$.*

Démonstration. Par l'absurde. Si Q ne divise pas M_f alors comme Q est irréductible Q et M_f sont premiers entre eux. D'après le théorème de Bezout pour les polynômes, (voir la propriété 2.2.5), il existe donc R et S tels que $RQ + SM_f = 1$. Soit $v \in \ker Q(f)$ non nul, alors $RQ(f)(v) + SM_f(f)(v) = v$, mais les deux termes de gauche sont nuls. □

Si on suppose que le polynôme caractéristique de f est scindé, ce qui est toujours le cas si le corps de base est $\mathbb{C}$, alors le polynôme minimal possède les mêmes facteurs irréductibles que le polynôme caractéristiques. En effet, on a la proposition qui suit.

Propriété 2.2.8. *On suppose que le polynôme caractéristique P_f est scindé ; soit Q un facteur irréductible de P_f, alors $Q \mid M_f$.*

Démonstration. Par hypothèse le facteur irréductible Q de P_f est de degré 1, donc de la forme $X - \lambda$; le scalaire λ est une racine de P et une valeur propre de f. Par définition $\ker Q(f)$ est l'espace propre associé à λ, il est donc non nul. On applique la proposition précédente 2.2.7 pour conclure. □

Remarque(s) 2.2.1. Avec un peu plus d'outils, nous verrons que ce résultat reste correct même si le polynôme caractéristique n'est pas scindé : voir le théorème complémentaire 27.

Voici maintenant quelques résultats pratiques sur le polynôme minimal et le polynôme caractéristique d'une somme directe de sous-espace stables.

Propriété 2.2.9. *Soit $f \in \mathrm{End}(E)$; on suppose qu'il existe des sous-espaces vectoriels $E_1, E_2, \ldots, E_s$ stables par f et tels que :*

$$E = \bigoplus_{i=1}^{s} E_i.$$

Pour $i \in \{1, 2, \ldots, s\}$ posons $f_i = f_{E_i}$ et P_i (resp. M_i), le polynôme caractéristique (resp. le polynôme minimal) de f_i. Soient $Q_1, Q_2, \ldots, Q_s$ s polynômes tels que pour tout $i \in \{1, 2, \ldots, s\}$, Q_i soit un polynôme annulateur de f_i et enfin soit Q un polynôme annulateur de chacun des f_i. On a alors les résulats suivants :

(i) *Q est un polynôme annulateur de f.*

(ii) *$Q_1 Q_2 \ldots Q_s$ est un polynôme annulateur de f.*

(iii) $P_f = \prod_{i=1}^{s} P_i$.

(iv) $M_f = \mathrm{ppcm}(M_1, M_2, \ldots, M_s)$.

Démonstration.

(i) Soit $v \in E$, on doit montrer que $Q(f)(v) = 0$; pour cela on décompose v dans la somme directe : $v = \sum_{i=1}^{s} v_i$, où pour tout $i \in \{1, 2; \ldots, s\}$, $v_i \in E_i$. On peut alors calculer :

$$Q(f)(v) = Q(f)\left(\sum_{i=1}^{s} v_i\right) = \sum_{i=1}^{s} Q(f)(v_i).$$

Or chacun des termes de la somme ci-dessus est nul puisque par hypothèse pour tout $i \in \{1, 2, \ldots, s\}$, Q est un polynôme annulateur de f_i et que $Q(f)(v_i) = Q(f_i)(v_i)$.

(ii) Si on pose $Q = Q_1 Q_2 \ldots Q_s$ alors on vérifie que pour tout $i \in \{1, 2, \ldots, s\}$, et pour tout $v_i \in E_i$, on a $Q(v_i) = 0$, et on utilise le point (i).

(iii) Choisissons une base $\mathscr{B} = \mathscr{B}_1 \cup \mathscr{B}_2 \cup \ldots \cup \mathscr{B}_s$ compatible avec la décomposition en somme directe de E. Alors dans cette base la matrice de f est diagonale par blocs et chaque bloc est égal à la matrice d'un endomorphisme f_i :

$$\begin{pmatrix} \mathrm{Mat}_{\mathscr{B}_1}(f_1) & * & * & * \\ * & \mathrm{Mat}_{\mathscr{B}_2}(f_2) & * & * \\ * & * & \ddots & * \\ * & * & * & \mathrm{Mat}_{\mathscr{B}_s}(f_s) \end{pmatrix}$$

où les étoiles remplacent des coefficients égaux à zéro. La matrice $f - X\mathbb{1}_E$ qui permet de calculer P_f est également diagonale par blocs, et chaque bloc diagonal est égal à la matrice de $f_i - X\mathbb{1}_{E_i}$ dans la base $\mathscr{B}_i$; on conclut la preuve du premier point en utilisant que le déterminant d'une matrice diagonale par blocs et égal au produit des déterminants des blocs diagonaux.

(iv) Pour le dernier point, posons $Q = \mathrm{ppmc}(M_1, M_2, \ldots, M_s)$, alors Q est un polynôme annulateur de chacun des f_i et donc un polynôme annulateur de f d'après le point (i). Soit R un polynôme annulateur de f, montrons que R est un multiple de Q. Pour cela il suffit de remarquer que pour $i \in \{1, 2, \ldots, s\}$ R est un polynôme annulateur de f_i et donc $M_i \mid R$. Par définition du ppmc, on a $Q \mid R$.

□

Remarque(s) 2.2.2. Dans la propriété ci-dessus les résultats sont vrais même si un ou plusieurs sous-espaces parmi E_i est de dimension nulle : dans ce cas, le polynôme minimal et le polynôme caractéristique de la restriction est constant et égal à 1.

2.2.2 Le lemme des noyaux

Nous avons vu dans la propriété 2.2.2 que si $f \in \mathrm{End}(E)$ et $Q \in \mathbb{K}[X]$ alors $\ker Q(f)$ est un sous-espace *stable* par f. L'existence d'un sous-espace stable $F \subset E$ conduit à une question naturelle : est-ce qu'il existe un sous-espace supplémentaire de F dans E *stable* par f ? Si f est diagonalisable alors la réponse est oui : pour tout sous-espace stable F il existe un sous-espace supplémentaire G *stable* par f et c'est même une caractérisation des endomorphismes diagonalisables (voir l'exercice 51).

Cependant, même si f n'est pas diagonalisable, on peut produire des sous-espaces stables admettant un supplémentaire : c'est la situation rencontrée dans le lemme des noyaux.

Théorème 22. *Soient $f \in \mathrm{End}(E)$ et P et Q deux polynômes premiers entre eux, alors l'espace $\ker(PQ(f))$ se décompose en somme directe de sous-espaces stables par f de la façon suivante :*

$$\ker(PQ(f)) = \ker P(f) \oplus \ker Q(f).$$

De plus les projecteurs de $ker(PQ(f)$ sur les espaces $\ker P(f)$ et $\ker Q(f)$ sont des polynômes en f.

Démonstration. Remarquons d'abord qu'on a bien l'inclusion $\ker P(f) \subset \ker(PQ)(f)$ (idem pour $\ker Q(f)$) et que d'après la propriété 2.2.2, les deux sous-espaces $\ker P(f)$ et $\ker Q(f)$ sont stables par f. Comme P et Q sont premiers entre eux, d'après l'égalité de Bézout (propriété 2.2.5), il existe deux polynômes $(R, S) \in \mathbb{K}[X]$ tels que $RP + SQ = 1$; et donc $RP(f) + SQ(f) = \mathbb{1}_E$ Soit $v \in \ker P(f) \cap \ker Q(f)$, alors on a $RP(f)(v) + SQ(f)(v) = v$, mais comme $P(f)(v) = Q(f)(v) = 0$, on a $v = 0$.

De même si $v \in \ker PQ(f)$, alors toujours en utilisant Bézout, on peut écrire $v = RP(f)(v) + SQ(f)(v)$; on remarque ensuite que $RP(f)(v) \in \ker Q(f)$ et $SQ(f)(v) \in \ker P(f)$, on a donc bien $\ker(PQ(f)) = \ker P(f) \oplus \ker Q(f)$. Et au passage, on constate que $RP(f)$ (resp. $SQ(f)$ est la projection de $\ker PQ(f)$ sur $\ker Q(f)$ (resp. $\ker P(f)$), et ces deux morphismes sont bien des polynômes en f. □

Dans la suite, nous aurons besoin d'une version du lemme des noyaux plus générale.

Théorème 23. *Soient $f \in \mathrm{End}(E)$ et r un entier supérieur ou égal à 2 et $P_1, P_2, \ldots, P_r$ des polynômes premiers deux à deux, alors l'espace $\ker(P_1 \ldots P_r(f))$ se décompose en somme de directe de sous-espaces stables de la façon suivante :*

$$\ker(P_1 \ldots P_r(f)) = \bigoplus_{i=1}^{r} \ker P_i(f).$$

De plus les projecteurs de $\ker(P_1 \ldots P_r(f))$ sur chacun des termes de la somme sont des polynômes en f.

Démonstration. On fait une récurrence sur r. D'après le théorème précédent, l'assertion est vraie pour $r = 2$. Supposons qu'elle soit vrai jusqu'au rang $r - 1$. Comme P_1 est premier avec tous les P_i pour $i \in \{2, 3, \ldots, r\}$, en appliquant encore une fois le théorème précédent, on a

$$\ker(P_1 \ldots P_r(f)) = \ker P_1(f) \oplus \ker(P_2 \ldots P_r(f)).$$

et la projection sur les deux facteurs est un polynôme en f. On applique ensuite l'hypothèse de récurrence sur $\ker(P_2 \ldots P_r(f))$ pour conclure. □

2.2.3 Sous-espaces caractéristiques

On a vu précédemment (dans la propriété 2.1.6) que si $f \in \mathrm{End}(E)$, alors f est diagonalisable si et seulement si l'espace E s'écrit comme somme directe des sous-espaces propres de f. Lorsque f n'est pas diagonalisable, on va définir pour chaque valeur propre un sous-espace associé qui sera un sous-espace un peu plus « gros » que le sous-espace propre, de sorte que E sera somme directe de ces nouveaux sous-espaces.

Définition 2.2.1. Soient $f \in \mathrm{End}(E)$ et $\mathrm{spec}(f)$ l'ensemble des valeurs propres de f. Pour tout $\lambda \in \mathrm{spec}(f)$, on définit le sous-espace caractéristique associé à λ :

$$E^\lambda = \bigcup_{k\in\mathbb{N}} \ker(f - \lambda \mathbb{1}_E)^k$$

Comme l'union de sous-espaces vectoriels n'est pas forcément un sous-espace vectoriel, il n'est pas clair que E^λ est un sous-espace vectoriel ; nous allons voir que c'est pourtant bien le cas dans la propriété qui suit.

Propriété 2.2.10. *Soit $f \in \mathrm{End}(E)$, alors pour tout $\lambda \in \mathrm{spec}(f)$, E^λ est un sous-espace vectoriel qui contient le sous-espace propre E_λ.*

Démonstration. Les deux assertions de la propriété découlent de la remarque élémentaire suivante : pour tout endomorphisme $g \in \mathrm{End}(E)$ et pour tout $(i, j) \in \mathbb{N}$ tel que $i \leq j$, on a $\ker g^i \subset \ker g^j$. En appliquant cette remarque à l'endomorphisme $g = f - \lambda \mathbb{1}_E$ on obtient que la suite des espaces vectoriels définissant E^λ est croissante pour l'inclusion ce qui entraîne que E^λ est bien un sous-espace qui contient $\ker(f - \lambda \mathbb{1}_E) = E_\lambda$. □

Avec ces outils, nous allons maintenant pouvoir montrer qu'un endomorphisme est diagonalisable si et seulement si son polynôme minimal est scindé et à racines simples. Rappelons qu'un polynôme de $\mathbb{K}[X]$ est scindé sur $\mathbb{K}$ si il s'écrit comme produit de polynôme de degré 1 (sur $\mathbb{C}$ tout polynôme est donc scindé).

On a vu dans la proposition 2.2.8 que si $\lambda \in \mathrm{spec} f$, alors $X - \lambda$ divise M_f ; d'autre part si μ est une racine de M_f, c'est une racine de P_f puisque $M_f \mid P_f$ et donc $\mu \in \mathrm{spec} f$. Si M_f est scindé, on peut donc écrire :

$$M_f = \prod_{\lambda\in\mathrm{spec}(f)} (X - \lambda)^{m_\lambda}.$$

Si de plus, P_f est scindé, alors on a le même genre de décomposition :

$$P_f(X) = (-1)^n \prod_{\lambda\in\mathrm{spec}(f)} (X - \lambda)^{n_\lambda},$$

avec

$$\sum_{\lambda\in\mathrm{spec}(f)} n_\lambda = \deg(P) = \dim E = n.$$

et pour tout $\lambda \in \mathrm{spec} f$, $1 \leq m_\lambda \leq n_\lambda$. Remarquons que si M_f est scindé, on peut montrer que P_f est scindé (voir le théorème 26), mais ce résultat est un peu technique, nous ne voulons pas l'utiliser à ce stade du cours ; d'ailleurs il n'est pas nécessaire pour le résultat principal de cette section : les théorèmes 24 et 25.

Gardons ces notations pour énoncer le théorème qui suit.

Théorème 24.
Décomposition de E en somme directe de sous-espaces caractéristiques
Soit $f \in \mathrm{End}(E)$ tel que M_f soit scindé, on a les assertions suivantes :

(i) Pour tout $\lambda \in \operatorname{spec}(f)$, $E^\lambda = \ker(f - \lambda \mathbb{1}_E)^{m_\lambda}$.

(ii) $E = \bigoplus_{\lambda \in \operatorname{spec}(f)} E^\lambda$.

(iii) Si de plus P_f *est scindé, alors pour tout* $\lambda \in \operatorname{spec}(f)$, $\dim E^\lambda = n_\lambda$.

Démonstration. Avec les notations introduites, on a :

$$M_f = \prod_{\lambda \in \operatorname{spec}(f)} (X - \lambda)^{m_\lambda}$$

Remarquons que par définition $\ker M_f(f) = E$; d'autre part comme les $\lambda \in \operatorname{spec}(f)$ sont distincts, les facteurs du produit ci-dessus sont deux à deux premiers entre eux. On peut donc appliquer le lemme des noyaux, et on obtenir :

$$E = \bigoplus_{\lambda \in \operatorname{spec}(f)} \ker(f - \lambda \mathbb{1}_E)^{m_\lambda},$$

où chacun des sous-espaces $\ker(f - \lambda \mathbb{1}_E)^{m_\lambda}$ est stable par f. Pour tout $\lambda \in \operatorname{spec}(f)$, considérons f_λ la restriction de f à $\ker(f - \lambda \mathbb{1}_E)^{m_\lambda}$.

Alors pour tout $\lambda \in \operatorname{spec}(f)$, le polynôme minimal de f_λ est égal à $(X - \lambda)^{m_\lambda}$. En effet sinon, d'après le point (iv) de la propriété 2.2.9, on obtiendrait un polynôme minimal de degré strictement plus petit que le degré de M_f. La suite des noyaux $\ker(f - \lambda \mathbb{1}_E)^k$ est donc constante dès que $k \geq m_\lambda$, et on a donc montré le point (i) et (ii).

Pour montrer le point (iii), pour tout $\lambda \in \operatorname{spec}(f)$, posons $d_\lambda = \dim E^\lambda$. Alors pour tout λ, le polynôme caractéristique de f_λ divise le polynôme caractéristique de f (d'après la propriété 2.2.9) et admet λ comme seule valeur propre possible, il est donc égal à $\pm(X - \lambda)^{d_\lambda}$ avec $d_\lambda \leq n_\lambda$. Mais comme

$$\sum_{\lambda \in \operatorname{spec}(f)} d_\lambda = n = \sum_{\lambda \in \operatorname{spec}(f)} n_\lambda,$$

pour tout $\lambda \in \operatorname{spec}(f)$, on a nécessairement $d_\lambda = n_\lambda$. □

Grâce à ce théorème sur la décomposition de l'espace en somme directe de sous-espaces caractéristiques, on peut obtenir d'autres caractérisations de la diagonalisabilité d'un endomorphisme.

Théorème 25. *Soit* $f \in \operatorname{End}(E)$, *on a équivalence entre les propriétés suivantes :*

(i) L'endomorphisme f *est diagonalisable.*

(ii) Il existe un polynôme annulateur de f *scindé et à racines simples.*

(iii) Le polynôme minimal M_f *est scindé et à racines simples.*

Démonstration. Supposons (i) et soit S le polynôme suivant :

$$S(X) = \prod_{\lambda \in \operatorname{spec}(f)} (X - \lambda).$$

Alors par construction S est un polynôme annulateur de f restreinte à E_λ pour tout $\lambda \in \operatorname{spec}(f)$, et donc d'après la propriété 2.2.9, S est un polynôme annulateur de f, ce qui montre (ii).

Supposons (ii) et soit Q scindé à racines simples tel que $Q(f) = 0$, alors par définition, M_f divise Q, et M_f est scindé et à racines simples. Supposons (iii), on utilise le théorème 24. Puisque M_f est scindé, on a

$$E = \bigoplus_{\lambda \in \operatorname{spec}(f)} E^\lambda,$$

et puisqu'il est à racines simples, $E^\lambda = E_\lambda$ et donc au final :

$$E = \bigoplus_{\lambda \in \mathrm{spec}(f)} E_\lambda,$$

ce qui implique bien que f est diagonalisable. □

Pour compléter ce cours, nous allons terminer par le résultat annoncé précédemment.

Théorème 26. *Soit $f \in \mathrm{End}(E)$, alors P_f est scindé si et seulement si M_f est scindé.*

Démonstration. Tout d'abord un diviseur d'un polynôme scindé est scindé, donc si P_f est scindé alors M_f l'est également.

Pour la réciproque : soit Q un polynôme irréductible qui divise P_f, alors d'après le théorème qui suit il divise M_f. Si M_f est scindé, Q est donc de degré 1. . □

Il nous reste donc à montrer le résultat suivant :

Théorème 27. *Supposons que $\mathbb{K}$ soit un sous-corps de $\mathbb{C}$, soit E un $\mathbb{K}$-espace vectoriel de dimension finie, et soit $f \in \mathrm{End}(E)$, alors tout polynôme irréductible Q qui divise P_f divise M_f.*

Démonstration. Soit Q un facteur irréductible de P_f ; considérons $Q(f) \in \mathrm{End}(E)$; comme $\mathbb{K} \subset \mathbb{C}$, on peut étendre les scalaires et considérer $E_\mathbb{C}$ l'espace vectoriel des combinaisons linéaires complexes d'une base $\mathscr{B}$ de E. Sur $\mathbb{C}$ le polynôme Q admet une racine λ et on peut écrire $Q = (X - \lambda)R$. Par définition $(E_\mathbb{C})_\lambda$ est non nul et est inclus dans le noyau de $Q(f)$, et donc $\ker Q(f) \neq 0$ sur $E_\mathbb{C}$. Comme ceci se traduit par $\det Q(f) = 0$, on a $\ker Q(f) \neq 0$ sur E, mais alors on a vu dans la propriété 2.2.7 que Q divise alors le polynôme minimal. □

Remarque(s) 2.2.3. L'hypothèse sur le corps $\mathbb{K}$ n'est absolument pas nécessaire ; elle permet juste de donner une démonstration plus rapide. Sans cette hypothèse, on peut utiliser que tout corps $\mathbb{K}$ est un sous-corps d'un (unique) corps algébriquement clos (ce corps s'appelle la clôture algébrique de $\mathbb{K}$). On peut aussi montrer un résultat un peu plus fort sans utiliser cet argument de clôture algébrique : P_f divise M_f^n où $n = \dim E$. Ce résultat est énoncé et démontré ci-après.

Théorème 28. *Soit $f \in \mathrm{End}(E)$, où E est un espace vectoriel de dimension finie égale à n, P_f son polynôme caractéristique, M_f son polynôme minimal. Alors P_f divise M_f^n.*

Démonstration. Remarquons d'abord que si X et Y sont deux indéterminées, et si

$$M_f(X) = \sum_{i=0}^{r} a_i X^i$$

alors

$$M_f(X) - M_f(Y) = (X - Y) \sum_{i=1}^{r} a_i (X - Y)^{i-1}.$$

Évaluons ce polynôme en les endomorphismes $X = f$ et $Y = \lambda \mathbb{1}_E$. (Notons que cette évaluation est bien définie puisque les deux endomorphismes f et $\lambda \mathbb{1}_E$ commutent). On obtient alors :

$$M_f(f) - M_f(\lambda \mathbb{1}_E) = (f - \lambda \mathbb{1}_E) \circ \left(\sum_{i=1}^{r} a_i (f - \lambda \mathbb{1}_E)^{i-1} \right).$$

Comme $M_f(f) = 0$, on obtient finalement l'égalité suivante entre endomorphismes :

$$M_f(\lambda \mathbb{1}_E) = -(f - \lambda \mathbb{1}_E) \circ \left(\sum_{i=1}^{r} a_i (f - \lambda \mathbb{1}_E)^{i-1} \right).$$

Les déterminants des deux endomorphismes de l'égalité ci-dessus sont donc égaux. Calculons-les.

$$\begin{aligned} \det\left(M_f(\lambda \mathbb{1}_E)\right) = \det\left(\sum_{i=0}^{r} a_i (\lambda \mathbb{1}_E)^i \right) &= \det\left(\sum_{i=0}^{r} a_i \lambda^i \mathbb{1}_E \right) \\ &= \det\left(M_f(\lambda) \mathbb{1}_E\right) \\ &= (M_f(\lambda))^n. \end{aligned}$$

D'autre part :

$$\det\left[-(f - \lambda \mathbb{1}_E) \circ \left(\sum_{i=1}^{r} a_i (f - \lambda \mathbb{1}_E)^{i-1} \right) \right] =$$
$$(-1)^n \det(f - \lambda \mathbb{1}_E) \det\left(\sum_{i=1}^{r} a_i (f - \lambda \mathbb{1}_E)^{i-1} \right).$$

Par définition $\det(f - \lambda \mathbb{1}_E) = P_f(\lambda)$ et $Q(\lambda) = (-1)^n \det\left(\sum_{i=1}^{r} a_i (f - \lambda \mathbb{1}_E)^{i-1}\right)$ est un polynôme en λ. Au final, on a donc :

$$(M_f(\lambda))^n = P_f(\lambda) Q(\lambda),$$

d'où le résultat. □

2.2.4 Exercices

Exercice 48 ⓔ

Soient f un endomorphisme d'un $\mathbb{K}$-espace vectoriel et $Q \in \mathbb{K}[X]$ un polynôme irréductible. Montrer que $Q(f)$ est non bijective si et seulement si $Q \mid M_f$ (une implication a déjà été montrée dans le cours, voir la propriété 2.2.7).

Exercice 49 ⓒ

Montrer que si $F \subset E$ est un sous-espace stable par f, alors $M_{f_{|F}}$ divise M_f. En déduire que si P_f est scindé et si on considère la décomposition de E en somme directe de sous-espaces caractéristiques :

$$E = \bigoplus_{\lambda \in \mathrm{spec}(f)} E^\lambda,$$

alors :

$$F = \bigoplus_{\lambda \in \mathrm{spec}(f)} E^\lambda \cap F.$$

Exercice 50 ⓒ

Soit f l'endomorphisme de $\mathbb{R}^3$ dont la matrice dans la base canonique est la matrice A. Pour chacun des cas proposés, décrire les sous-espaces propres, les sous-espaces caractéristiques, et les sous-espaces stables pour f.

1. $A = \begin{pmatrix} 1 & 1 & -1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$

2. $A = \begin{pmatrix} 7 & -1 & 0 \\ 1 & 5 & 0 \\ -5 & -1 & 3 \end{pmatrix}$

Exercice 51 ⓐ

On dit qu'un endomorphisme f est semi-simple si pour tout sous-espace $F \subset E$ stable par f, il existe une supplémentaire de F stable par f. Montrer que si $\mathbb{K} = \mathbb{C}$, alors f est semi-simple si et seulement si f est diagonalisable (indication : utiliser les résultats de l'exercice 49). Que pensez-vous de cette équivalence si $\mathbb{K} = \mathbb{R}$?

2.3 Compléments et rappel (une preuve du théorème de Cayley-Hamilton)

Pour compléter cette partie, nous allons maintenant donner une preuve du théorème de Cayley-Hamilton. Cela sera l'occasion d'introduire (ou de rappeler) deux outils très utiles dans la théorie : le polynôme minimal en un vecteur et la matrice compagnon d'un endomorphisme.

Définition 2.3.1. Soient E un espace vectoriel sur un corps $\mathbb{K}$ et $f \in \mathrm{End}(E)$. À tout vecteur $v \in E$, on associe l'application suivante :

$$\begin{array}{rccc} \Pi_f^v : & \mathbb{K}[X] & \to & E \\ & P & \mapsto & P(f)(v) \end{array}.$$

Cette application est la composée de l'application Π_f définie précédemment et de l'évaluation en v. On en déduit immédiatement la proposition qui suit.

Propriété 2.3.1. *Le noyau de l'application Π_f^v est un idéal non nul de $\mathbb{K}[X]$.*

On peut donc maintenant définir le polynôme minimal de f au point $v \in E$.

Définition 2.3.2. Le polynôme unitaire qui engendre l'idéal $\ker \Pi_f^v$ s'appelle le polynôme minimal de f en v ; ce polynôme est noté M_f^v.

Remarquons que si M_f est le polynôme minimal de f, alors $M_f \in \ker \Pi_f^v$ et donc pour tout $v \in E$, $M_f^v \mid M_f$. Autrement dit M_f^v est le diviseur unitaire de M_f de plus petit degré parmi les polynômes $Q \in \mathbb{K}[X]$, tels que $Q(f)(v) = 0$.

Définissons maintenant la matrice compagnon d'un polynôme.

Définition 2.3.3. Soient $\mathbb{K}$ un corps, n un entier non nul, $(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{K}^n$ et $P(X)$ le polynôme unitaire suivant :

$$P(X) = a_0 + a_1 X + a_2 X^2 + \ldots + a_{n-1} X^{n-1} + X^n.$$

On définit $\mathcal{C}_P$ la matrice compagnon du polynôme P en posant :

$$\mathcal{C}_P = \begin{pmatrix} 0 & 0 & \ldots & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & 1 & 0 & -a_{n-1} \end{pmatrix}.$$

L'explication du terme « compagnon » provient de la proposition suivante :

Propriété 2.3.2. *On considère la matrice $\mathcal{C}_P$ comme un endomorphisme, noté f_P de $\mathbb{K}^n$, alors le polynôme caractéristique de cet endomorphismes est égal à $(-1^n)P$ et son polynôme minimal est égal à P.*

Démonstration. Cette preuve est laissée en exercice.

Idées : pour le polynôme caractéristique, faire une récurrence sur n ; pour le polynôme minimal, considérer la base canonique $(e_1, e_2, \ldots, e_n)$, montrer que la famille

$$(e_1, \mathcal{C}_P(e_1), \ldots, \mathcal{C}_P^{n-1}(e_1))$$

est libre. En déduire que le polynôme minimal $M_{f_P}^{e_1}$ ne peut pas être de degré inférieur ou égal à $n-1$. □

Ces deux notions peuvent être reliées grâce à la proposition qui suit.

Propriété 2.3.3. *Soient E un espace vectoriel de dimension finie sur un corps $\mathbb{K}$, f un endomorphisme de E, et $v \in E$ un vecteur non nul. Soit*

$$M_f^v = a_0 + a_1 X + a_2 X^2 + \ldots + a_{n-1} X^{n-1} + X^n$$

le polynôme minimal en v de f. Pour $i \in \{0, 1, \ldots n-1\}$, notons $e_i = f^i(v)$. Alors la famille

$$\mathscr{B}_v = (e_i)_{i \in \{0,1,\ldots n-1\}}$$

est libre, et engendre un espace stable par f que nous noterons E_v. De plus la matrice de la restriction de f à E_v dans la base $\mathscr{B}_v$ est la matrice compagnon de M_f^v.

Démonstration. Supposons que la famille $\mathscr{B}_v$ soit liée ; il existe donc des scalaires

$$(a_0, a_1, \ldots, a_{n-1})$$

tels que :

$$a_0 v + a_1 f(v) + \cdots + a_{n-1} f^{n-1}(v) = 0.$$

On a donc un polynôme $Q = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$ tel que $Q(f)(v) = 0$, mais comme Q est de degré $n-1$, et que le polynôme minimal M_f^v est de degré n, on obtient une contradiction.

Pour la suite, on calcule l'image par f des éléments de $\mathscr{B}_v$. Pour $i \in \{0, 1, \ldots n-2\}$, on obtient :

$$f(e_i) = f(f^i(v)) = f^{i+1}(v) = e_{i+1}$$

et grâce à la définition de M_f^v, on obtient :

$$f(e_{n-1}) = -(a_0 e_0 + a_1 e_1 + \cdots + a_{n-1} e_{n-1}).$$

On en déduit immédiatement que E_v est stable par f ainsi que la dernière assertion sur la matrice de la restriction de f à E_v dans la base $\mathscr{B}_v$. □

Une preuve du théorème de Cayley-Hamilton

Avec ces deux outils nous pouvons maintenant donner une preuve de Cayley-Hamilton. Soient E un espace vectoriel de dimension finie sur un corps $\mathbb{K}$ et f un endomorphisme de E. Soit P_f le polynôme caractéristique de f ; il s'agit de montrer que pour tout $v \in E$, $P(f)(v) = 0$. Remarquons que cette égalité est vraie si $v = 0$. On peut donc supposer que $v \neq 0$. On reprend les notations de la proposition précédente : soit M_f^v le polynôme minimal en v de f et E_v le sous-espace stable de base $\mathscr{B}_v$. On complète cette base en une base $\mathscr{B}$ de E. Alors puisque E_v est stable par f, dans cette base $\mathscr{B}$ la matrice de f sera triangulaire par blocs de la forme :

$$\begin{pmatrix} \mathcal{C}_{M_f^v} & B \\ 0 & D \end{pmatrix}.$$

Le polynôme caractéristique de f dans cette base $\mathscr{B}$ est donc égal au produit du polynôme caractéristique de f restreint à E_v par le polynôme caractéristique de la matrice carrée D, c'est à dire, d'après la proposition 2.3.2 : $P_f = M_f^v P_D$. Et donc :

$$P_f(f)(v) = \left(M_f^v P_D\right)(f)(v) = \left(P_D M_f^v\right)(f)(v) = \left(P_D(f) \circ M_f^v(f)\right)(v) = 0$$

puisque par définition $M_f^v(f)(v) = 0$.

2.4 Les endomorphismes nilpotents

On a vu que la restriction d'un endomorphisme à un sous-espace caractéristique E_λ n'est pas diagonalisable si et seulement si $E_\lambda \neq E^\lambda$, c'est à dire si et seulement s'il existe $m \geq 0$ tel que $(f_{E_\lambda} - \lambda \mathbb{1}_{E_\lambda})^m \neq 0$ et $(f_{E_\lambda} - \lambda \mathbb{1}_{E_\lambda})^{m+1} = 0$. Autrement dit, l'existence d'une restriction non nulle de f à un sous-espace stable avec une de ces puissance nulle est équivalente à la non diagonalisabilité de f. Nous allons donc étudier plus en détail les endomorphismes dont une puissance est nulle.

Définition 2.4.1. Soit $f \in \mathrm{End}(E)$, on dit que f est nilpotent s'il existe $m \in \mathbb{N}$ tel que $f^m = 0$.

Remarque(s) 2.4.1.

1. L'endomorphisme nul est évidemment nilpotent.
2. Pour tout $a \in \mathbb{K}$, la matrice suivante de $\mathrm{M}_2(\mathbb{K})$:

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}$$

   est la matrice d'un endomorphisme nilpotent.
3. Plus généralement, si A est une matrice triangulaire stricte, alors l'endomorphisme associé est nilpotent (voir la propriété 2.4.1 qui suit).

Définissons maintenant l'indice de nilpotence.

Définition 2.4.2. Soit $f \in \mathrm{End}(E)$ nilpotent. On dit que p est l'indice de nilpotence de f, si $f^p = 0$ et $f^{p-1} \neq 0$.

Autrement dit l'indice de nilpotence est le plus petit entier m tel que $f^m = 0$.

Voici maintenant d'autres caractérisations d'un endomorphisme nilpotent. Remarquons que nous utiliserons le théorème 26 pour la preuve ; nous allons donc faire l'hypothèse que $\mathbb{K} \subset \mathbb{C}$.

Propriété 2.4.1. *Soit $\mathbb{K} \subset \mathbb{C}$, soit E un espace vectoriel de dimension finie sur $\mathbb{K}$, et soit $f \in \mathrm{End}(E)$, alors les conditions suivantes sont équivalentes :*

(i) *f est nilpotent ;*

(ii) *$M_f = X^p$, où p est l'indice de nilpotence de f ;*

(iii) *$P_f = (-1)^n X^n$;*

(iv) *il existe une base $\mathscr{B}$ telle que dans cette base, la matrice de f soit triangulaire supérieure stricte ;*

(v) *f admet comme seule valeur propre 0 de multiplicité n.*

Démonstration.

$(i) \Rightarrow (ii)$ Si f est nilpotente, soit p son indice de nilpotence. Alors comme $X^p = 0$, M_f divise X^p, et comme p est le plus petit m tel que $X^m = 0$ et que M_f est le polynôme minimal de f, on a $M_f = X^p$.

$(ii) \Rightarrow (iii)$ Si $M_f = X^p$, le polynôme minimal est scindé. D'après le théorème 26 le polynôme P_f est scindé, et toutes ses racines sont également des racines de M_f, et donc P_f admet une seule racine qui est zéro avec multiplicité n.

$(iii) \Rightarrow (iv)$ Comme P_f est scindé, d'après l'exercice 45, il existe donc une base $\mathscr{B}$ telle que la matrice de f dans cette base soit triangulaire supérieure. Les coefficients sur la diagonale sont alors les valeurs propres de f, ils sont donc nuls et la matrice de f dans $\mathscr{B}$ est triangulaire supérieure stricte.

$(iv) \Rightarrow (v)$ On se place dans la base dans laquelle la matrice de f est triangulaire. Les valeurs propres de f sont alors les coefficients diagonaux de la matrice ; ils sont tous nuls par hypothèse.

$(v) \Rightarrow (i)$ Si f admet 0 comme valeur propre de multiplicité n, alors $P_f = (-1)^n X^n$, et d'après le théorème de Cayley-Hamilton, on a $f^n = 0$ et f est nilpotent.

□

Remarque(s) 2.4.2. 1. On peut retenir deux conséquences de la preuve de cette dernière propriété. D'abord que si f est nilpotent d'indice de nilpotence p alors $M_f = X^p$. De plus comme $M_f \mid P_f$, on a $p \leq n = \dim E$.

2. Dans la propriété précédente, on peut remplacer triangulaire supérieure stricte à triangulaire inférieure stricte. En effet la matrice de f dans une base $\mathscr{B} = (v_1, v_2, \ldots, v_n)$ est triangulaire supérieure (stricte), la matrice de f dans la base $\mathscr{C} = (v_n, v_{n-1}, \ldots, v_1)$ sera triangulaire inférieure (stricte)

2.4.1 Exercices

Exercice 52 ⓒ

Soient $f, g \in \mathrm{End}(E)$ deux endomorphismes nilpotents qui commutent ; montrer que $f + g$ est nilpotent.

Exercice 53 ⓐ

1. Soit f un endomorphisme nilpotent ; montrer que $\det(f + \mathbb{1}_V) = 1$.
2. Montrer que si f et g commutent et si f est nilpotent alors fg est nilpotent. Le résultat est-il vrai si f et g ne commutent pas ?
3. Montrer que si f et g commutent et si g est inversible alors f et g^{-1} commutent également.
4. Montrer que pour tout endomorphisme h, et pour $x \in \mathbb{K}$, $h + x\mathbb{1}_V$ est inversible sauf pour un nombre fini de valeurs de x.
5. En utilisant les questions précédentes, montrer que si f est nilpotent et commute avec g, alors $\det(g + f) = \det(g)$. Indication : on commencera par considérer le cas où g est inversible.

2.5 La décomposition de Jordan-Chevalley

Nous allons d'abord voir qu'il existe un seul endomorphisme nilpotent et diagonalisable, l'endomorphisme nul. Autrement dit, si un endomorphisme non nul est nilpotent, il n'est pas diagonalisable. On a déjà vu un cas particulier de ce résultat : la restriction d'un endomorphisme à un sous-espace caractéristique de valeur propre λ est diagonalisable si et seulement l'endomorphisme nilpotent $(f - \lambda\mathbb{1}_E)_{|E^\lambda}$ est nul.

Propriété 2.5.1. *Soit $f \in \mathrm{End}(E)$ tel que f soit nilpotent et diagonalisable, alors $f = 0$.*

Démonstration. Si f est nilpotent son polynôme minimal est X^p, mais comme f est diagonalisable, son polynôme minimal est à racines simples, donc $M_f = X$ et $f = 0$. $\square$

Voyons maintenant la décomposition de Jordan-Chevalley. Notons qu'elle est très souvent appelée décomposition de Dunford. Mais cette appellation, même si elle a l'avantage d'éviter la confusion avec la forme réduite de Jordan que nous verrons plus tard est incorrecte : c'est bien Camille Jordan qui a montré pour la première fois cette décomposition et Claude Chevalley l'a généralisée ensuite dans un contexte qui dépasse le cadre de ce cours. Énonçons donc cette décomposition.

Théorème 29. Décomposition de Jordan-Chevalley *Soit $f \in \mathrm{End}(E)$ de polynôme caractéristique P_f scindé, alors il existe un unique couple $(f_D, f_N) \in \mathrm{End}(E)^2$, tel que :*

(i) $f = f_D + f_N$;

(ii) *f_D est diagonalisable et f_N est nilpotent ;*

(iii) $f_N f_D = f_D f_N$;

(iv) *f_N et f_D sont des polynômes en f.*

Démonstration. Comme dans les sections précédentes, on factorise P_f :

$$P_f = (-1)^n \prod_{\lambda \in \mathrm{spec}(f)} (X - \lambda)^{n_\lambda}.$$

et d'après le théorème 24, E est somme directe des sous-espaces caractéristiques de f :

$$E = \bigoplus_{\lambda \in \mathrm{spec}(f)} E^\lambda.$$

De plus, pour tout $\lambda \in \mathrm{spec}(f)$, le projecteur π_λ de E sur E^λ est un polynôme en f. On définit f_D par sa restriction sur E^λ pour tout $\lambda \in \mathrm{spec}(f)$ en posant : $(f_D)_{|E^\lambda} = \lambda \mathbb{1}_{E^\lambda}$. La matrice de f_D est donc diagonale dans une base formée par réunion de bases de E^λ et f_D est diagonalisable. On peut aussi définir f_D comme suit :

$$f_D = \sum_{\lambda \in \mathrm{spec}(f)} \lambda \, \pi_\lambda$$

ce qui assure que f_D est un polynôme en f. Posons maintenant $f_N = f - f_D$. On a alors $f = f_D + f_N$ et comme f_D est un polynôme en f, f_N l'est également. Vérifions que f_N est nilpotent. Pour tout $\lambda \in \mathrm{spec}(f)$, on a :

$$(f_N)_{|E^\lambda} = (f - f_D)_{|E^\lambda} = f_{|E^\lambda} - \lambda \mathbb{1}_{E^\lambda}.$$

Par définition du sous-espace caractéristique, on a donc que pour tout $\lambda \in \mathrm{spec}(f)$, $(f_N)^{m_\lambda}_{|E^\lambda} = 0$, où m_λ es la multiplicité de λ dans M_f. Et donc f_N est bien nilpotent, d'indice de nilpotence $\max\{m_\lambda \mid \lambda \in \mathrm{spec}(f)\}$.

Sur chaque E^λ, $(f_D)_{|E^\lambda}$ est une homothétie et donc commute avec $(f_N)_{|E^\lambda}$, ce qui implique que f_N et f_D commutent.

Il nous reste à vérifier l'unicité du couple (f_D, f_N) pour cela supposons qu'il existe deux couples (f_D, f_N) et (f'_D, f'_N) vérifiant les points (i) à (iv). On a donc :

$$f_D - f'_D = f'_N - f_N.$$

Comme f_D et f'_D sont deux polynômes en f, ils commutent. D'après l'exercice 46, ils sont simultanément diagonalisables, et donc $f_D - f'_D$ est diagonalisable. De même f_N et f'_N commutent, et d'après l'exercice 52, $f'_N - f_N$ est nilpotent. On a vu dans la propriété 2.5.1 que le seul endomorphisme nilpotent et diagonalisable est l'endomorphisme nul, ce qui achève la preuve du théorème. $\square$

Remarque(s) 2.5.1. *(i)* Attention : pour obtenir la décomposition de Jordan, il ne suffit pas de trouver une base $\mathscr{B}$ telle que la matrice de f dans $\mathscr{B}$ soit triangulaire et de poser f_D égale à la partie diagonale de cette matrice (complétée par des 0) et f_N égale à la partie triangulaire stricte (également complétée par des 0). Car il n'est pas toujours vrai que cette partie diagonale va commuter avec la partie triangulaire stricte.

(ii) Attention (bis) : cette décomposition n'induit pas une décomposition en somme directe de sous-espaces. L'ensemble des endomorphismes diagonalisables et l'ensemble des endomorphismes nilpotents ne sont pas des sous-espaces vectoriels de $\mathrm{End}(E)$.

2.5.1 Exercices

Exercice 54 ⓒ

Pour chacune des matrices suivantes donner la décomposition de Jordan-Chevalley :

$$A_1 = \begin{pmatrix} 1 & 2 \\ 0 & -3 \end{pmatrix} A_2 = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix} A_3 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

$$A_4 = \begin{pmatrix} 5 & 0 & 0 & 0 \\ 1 & 4 & 0 & 0 \\ 1 & -1 & 5 & 0 \\ 1 & 0 & 2 & 5 \end{pmatrix} A_5 = \begin{pmatrix} \alpha & x & z \\ 0 & \alpha & y \\ 0 & 0 & \beta \end{pmatrix}$$

pour la dernière, on discutera suivant les valeurs de α, β, x, y, z.

Exercice 55 ⓐ

Rappelons que si $f \in \mathrm{End}(E)$, on note $O(f)$ l'orbite de f pour l'action de $\mathrm{GL}(E)$ sur $\mathrm{End}(E)$ par conjugaison. On va supposer $\mathbb{K} = \mathbb{C}$ et munir l'espace vectoriel $\mathrm{End}(E)$ de la topologie induite par une norme quelconque.

1. Montrer (si cela n'a pas été fait en cours) que si f est nilpotent alors l'endomorphisme nul est dans l'adhérence de $O(f)$. Indication : se ramener au cas d'un bloc de Jordan en utilisant la forme réduite de Jordan de f.
2. Montrer que pour tout f, $\overline{O(f)}$ contient une matrice diagonalisable.
3. En déduire que si $O(f)$ est fermée, alors f est diagonalisable.
4. Supposons f diagonalisable ; montrer que $g \in O(f)$ si et seulement si $P_g = P_f$ et $M_g = M_f$.
5. En déduire que si f est diagonalisable alors $O(f)$ est fermée.

2.6 Forme réduite de Jordan d'une matrice

Il s'agit ici de donner pour tout endomorphisme de polynôme caractéristique scindé une base dans laquelle la matrice de f est très simple. La forme de cette matrice est unique et permet de décider si deux endomorphismes sont semblables ou pas. En utilisant la décomposition de E en somme de sous-espaces caractéristiques, on peut se ramener au cas où l'endomorphisme est nilpotent, nous allons commencer par ce cas.

2.6.1 Le cas nilpotent

Les blocs de Jordan

La brique de base pour définir la forme réduite de Jordan est définie comme suit.

Définition 2.6.1. Soit $q \in \mathbb{N}$, la matrice J_q est la matrice carrée de taille q telle que :

$$\begin{array}{rcll} (J_q)_{i,i+1} & = & 1 & \text{pour } 1 \leq i \leq q-1 \\ & = & 0 & \text{sinon.} \end{array}$$

Pour $\lambda \in \mathbb{K}$, on définit également $J_q(\lambda) = J_q + \lambda \mathbb{1}_V$.

On a par définition $J_q = J_q(0)$. Visuellement $J_q(\lambda)$ est la matrice de taille q dont les coefficients sur la diagonale sont égaux à λ, ceux sur la sur-diagonale sont égaux à 1 et tous les autres sont nuls.

$$J_q(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \lambda & 1 \\ 0 & \dots & \dots & 0 & \lambda \end{pmatrix}$$

Les endomorphismes associés aux blocs de Jordan J_q sont nilpotents. On en effet la propriété qui suit.

Propriété 2.6.1. *Soient $q \in \mathbb{N}$ et J_q la matrice définie ci-dessus. Alors pour tout $i \in \{0, 1, \dots, q\}$, on a l'égalité :* $\dim \ker J_q^i = i$. *En particulier J_q est nilpotente d'indice de nilpotence q.*

Démonstration. Soit f l'endomorphisme de $\mathbb{K}^q$ associé à J_q et $(e_1, e_2, \dots e_q)$ la base canonique de $\mathbb{K}$. On montre par récurrence que pour tout $(i, j) \in \{1, 2, \dots, n\}$, $f^i(e_j) = 0$ si $1 \leq j \leq i$ et $f^i(e_j) = e_{j-i}$ si $i < j \leq q$. On en déduit que le rang de f^i est égal à $q - i$. $\square$

On peut maintenant énoncer le théorème de réduction de Jordan pour les endomorphismes nilpotents.

Théorème 30. *Soit $f \in \mathrm{End}(E)$ un endomorphisme nilpotent, alors il existe une suite d'entiers $d^f = (d_1, d_2, \dots, d_r)$ tels que $d_1 \geq d_2 \geq \dots \geq d_r > 0$ et $\sum_{i=1}^r d_i = n$, et une base $\mathscr{B}$ de E telle que la matrice de f dans $\mathscr{B}$ soit diagonale par blocs, et où les blocs diagonaux sont les matrices $J_{d_1}, J_{d_2}, \dots, J_{d_r}$. De plus la suite d'entiers d^f caractérise la classe de similitude de f : soient $(f, g) \in \mathrm{End}(E)$, alors $d^f = d^g$ si et seulement si f et g sont semblables.*

Avant de faire la preuve de ce théorème, faisons quelques remarques et donnons quelques définitions. Rappelons la définition d'une partition (notion qui a déjà été vue à l'occasion de l'étude des classes de conjugaison dans le groupe symétrique).

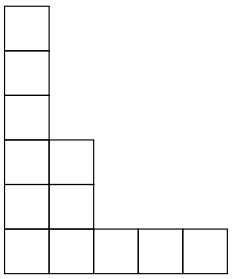
Définition 2.6.2. Une suite décroissante d'entiers strictement positifs

$$\delta = (\delta_1, \delta_2, \dots, \delta_p)$$

dont la somme vaut n est appelée une partition de n. Les entiers δ_i sont appelés les parts de la partition, et le nombre de parts est appelé la longueur de la partition.

Une partition peut s'encoder sous forme de diagramme appelé diagramme (ou tableau) de Young. Si δ est une partition de longueur p, alors son diagramme de Young est un tableau à p lignes, où la i-ième ligne est constituée de δ_i boîtes. Ici nous allons numéroter les lignes en partant du bas, et le colonnes de gauche à droite. Remarquons que par définition, si δ est une partition de n, alors son tableau contient n boîtes.

Donnons un exemple : si $\delta = (5, 2, 2, 1, 1, 1) = (5, 2^2, 1^3)$, son diagramme est égal à :



Nous allons maintenant commencer la preuve de la réduction de Jordan pour les endomorphismes nilpotents. Concernant l'existence de la base $\mathscr{B}$, il y a plusieurs preuves possibles. Nous avons choisi d'en présenter une constructive : c'est à dire que nous pourrons utiliser cette preuve pour calculer explicitement la base dans laquelle une matrice donnée est sous forme de réduite de Jordan.

Pour construire une telle base, l'objet essentiel est la suite des noyaux des itérées de f. On suppose que f est d'indice de nilpotence p et on définit pour $i \in \{0, \dots, p\}$ $K_i = \ker f^i$. On a directement les inclusions :

$$\{0\} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_{p-1} \subset K_p = E.$$

Une telle suite croissante de sous-espaces vectoriels s'appelle un drapeau de E. Pour tout $i \in \{1, \dots, p\}$, considérons un sous-espace vectoriel S_i tel que $K_{i-1} \oplus S_i = K_i$. Voici un premier résultat sur la famille des $(S_i)_{1 \leq i \leq p}$ et sur la restriction de f aux S_i fondamental pour la suite.

Propriété 2.6.2. *On a les assertions suivantes :*

(i) pour tout $i \in \{1, \dots, p\}$, $\bigoplus_{j=1}^{i} S_j = K_i$;

(ii) pour tout $i \in \{2, \dots, p\}$: la restriction de f à S_i est injective ;

(iii) pour tout $i \in \{2, \dots, p\}$: $f(K_i) \subset K_{i-1}$ et $f(S_i) \cap K_{i-2} = \{0\}$.

Démonstration.

On montre le premier point par récurrence sur i. Pour $i = 1$, c'est évident puisque $K_1 = S_1$. Supposons que l'assertion soit vraie pour $i \in \{1, \dots, p\}$. Comme S_{i+1} est un supplémentaire de K_i dans K_{i+1}, on a $S_{i+1} \oplus K_i = K_{i+1}$. Et donc en utilisant l'hypothèse de récurrence, on a :

$$K_{i+1} = K_i \oplus S_{i+1} = \bigoplus_{j=1}^{i} S_j \oplus S_{i+1} = \bigoplus_{j=1}^{i+1} S_j.$$

Comme $K_{i-1} \oplus S_i = K_i$, on a $K_{i-1} \cap S_i = \{0\}$. Mais pour $i = 2, \dots, p$, $\ker f = K_1 \subset K_{i-1}$, donc $\ker f \cap S_i = \{0\}$, ce qui montre la deuxième propriété.

Montrons l'inclusion du dernier point : soit $v \in K_i$, alors $f^i(v) = 0$, soit $f^{i-1}(f(v)) = 0$, donc $f(v) \in K_{i-1}$.

Pour finir, considérons $v \in f(S_i) \cap K_{i-2}$, alors il existe $w \in S_i$ tel que $v = f(w)$. Comme $v \in K_{i-2}$, on a $0 = f^{i-2}(v) = f^{i-1}(w)$, et donc $w \in K_{i-1} \cap S_i$ ce qui implique que $w = 0$ ainsi que $v = f(w) = 0$. □

Définition 2.6.3.
Pour $i \in \{1, \ldots, p\}$, on pose $\delta_i = \dim K_i - \dim K_{i-1}$ et $\delta^f = (\delta_1, \delta_2, \ldots, \delta_p)$.

À cause de l'inclusion des noyaux $(K_i)_{1 \leq i \leq p}$, il est clair que les termes de δ_f sont positifs. Mais cette suite a d'autres propriétés.

Propriété 2.6.3. *Soit δ^f comme ci-dessus ; on a les deux propriétés suivantes :*

1. $\sum_{i=1}^{p} \delta_i = \dim E = n$;
2. *on a les inégalités :* $\delta_1 \geq \delta_2 \geq \cdots \geq \delta_p > 0$.

Démonstration. La première égalité découle directement de la définition des δ_i.

Pour la deuxième assertion, on utilise la propriété précédente. On choisit une famille d'espaces $(S_i)_{1 \leq i \leq p}$ comme ci-dessus ; pour tout $i \in \{1, \ldots, p\}$, on a $\delta_i = \dim S_i$. On a montré que $f(S_i) \cap K_{i-2} = \{0\}$, donc il existe un supplémentaire $\tilde{S}_{i-1}$ de K_{i-2} dans K_{i-1} et contenant $f(S_i)$; ce supplémentaire n'est pas forcément égal à S_{i-1}, mais il ont tous les deux la même dimension. Enfin comme f restreinte à S_i est injective on a :

$$\dim S_i = \dim f(S_i) \leq \dim \tilde{S}_{i-1} = \dim S_{i-1}.$$

□

Remarque(s) 2.6.1. La suite des noyaux $(K_i)_{1 \leq i \leq p}$ est donc une suite croissante, mais les différences de dimension diminuent ; pour se rappeler de cette propriété, il est coutumier de dire que la suite est croissante mais s'essouffle.

On peut maintenant définir la base dans laquelle la matrice de f sera sous la forme réduite de Jordan. Cette base se construit en définissant n vecteurs qui vont remplir le tableau de Young associé à δ_f et qui formeront la base recherchée.

Soient δ_p vecteurs linéairement indépendants dans $V \setminus K^{p-1}$; on définit S_p comme l'espace engendré par ces vecteurs , ce qui assure que S_p est un supplémentaire de K_{p-1} dans E. Avec ces vecteurs, on remplit la ligne du haut (la p-ième). Puis on remplit les colonnes sous chacun de ces vecteurs par l'image des itérées de f, en commençant par les images par f et en finissant par les images par f^{p-1} qui seront donc placées sur la première ligne.

Ensuite, on considère la $(p-1)$-ième ligne, on a déjà δ_p vecteurs linéairement indépendants n'appartenant pas à K^{p-2} ; on complète cette famille par $\delta_{p-1} - \delta_p$ vecteurs pour obtenir une base d'un supplémentaire S_{p-1} de K_{p-2} dans K_{p-1}. Ces vecteurs complètent le remplissage de la $(p-1)$-ième ligne puis on remplit les colonnes sous chacun de ces vecteurs par les images des itérées de f (cette fois la première ligne est remplie par les images de f^{p-2}).

On continue à remplir le tableau successivement lignes à lignes : à la ligne i on a déjà une famille de δ_{i+1} vecteurs qui sont image par f des vecteurs remplissant la $i+1$-ième ligne. Ces vecteurs forment une famille libre d'après le point *(ii)* de la propriété 2.6.2, et n'appartiennent pas à K_{i-1} d'après le point *(iii)* de la propriété 2.6.2. On peut donc compléter cette famille pour obtenir une base d'un supplémentaire S_i de K_{i-1} dans K_i. Ces vecteurs complètent le remplissage de la i-ième ligne, puis on remplit les colonnes en dessous de ces vecteurs par leurs images par les itérées de f.

Une fois le tableau rempli, on le lit de bas en haut et de gauche à droite, ce qui nous donne une famille $\mathscr{B}$ de n vecteurs. On conclut l'existence d'une réduite de Jordan grâce à la propriété qui suit.

Propriété 2.6.4. *La famille $\mathscr{B}$ est une base de E et dans cette base la matrice de f est une réduite de Jordan.*

Démonstration. Par construction l'ensemble des vecteurs remplissant la ligne i est une famille libre et génératrice d'un supplémentaire S_i de K_{i-1} dans K_i. Et d'après le point i de la propriété 2.6.2, la somme directe des $(S_i)_{1\leq i\leq p}$ est égale à E, ce qui montre que l'on a bien obtenu une base de E.

Pour le deuxième point, on remarque que les vecteurs qui remplissent une colonne du tableau forment une famille libre de la forme (en lisant de bas en haut)

$$(f^{q-1}(v), f^{q-2}(v), \ldots, f(v), v)$$

avec $v \in V$ tel que $f^q(v) = 0$, et la matrice de la restriction de f à l'espace engendré par ces vecteurs est un bloc de Jordan de taille q. □

On a donc montré l'existence d'une base dans laquelle la matrice de f est sous la forme de réduite de Jordan.

Montrons maintenant la deuxième partie du théorème. Soient f et g nilpotents tels que $d^f = d^g$; alors f et g ont la même réduite de Jordan, et donc f et g sont semblables d'après la propriété 2.1.3. Réciproquement supposons que f et g soient semblables, alors toujours d'après la propriété 2.1.3, il existe $s \in \mathrm{GL}(E)$ tel que $f = sgs^{-1}$. Comme s est bijective, on en déduit immédiatement que la suite des dimensions des noyaux des itérés de f et de g sont identiques. Les suites δ^f et δ^g sont donc égales. Or la suite d^f (resp. la suite d^g) est obtenue à partir des colonnes du diagramme de Young de δ^f (resp de δ^g), et donc puisque $\delta^f = \delta^g$, on a $d^f = d^g$.

2.6.2 Le cas général

Si f est quelconque, on peut se ramener au cas nilpotent en considérant les restrictions de f aux sous-espaces caractéristiques. On a alors le résultat qui suit.

Théorème 31. *Soit $f \in \mathrm{End}(E)$ de polynôme caractéristique scindé. On suppose comme dans la partie sur la décomposition de Jordan-Chevalley que :*

$$P_f = (-1)^n \prod_{\lambda\in\mathrm{spec}(f)} (X-\lambda)^{n_\lambda} \text{ et } M_f = \prod_{\lambda\in\mathrm{spec}(f)} (X-\lambda)^{m_\lambda}$$

Alors pour tout $\lambda \in \mathrm{spec}(f)$, il existe une suite décroissante d'entiers strictement positifs $d^f_\lambda = (d_1, d_2, \ldots, d_{r_\lambda})$ tels que $\sum_{i=1}^{r_\lambda} d_i = \dim E^\lambda = n_\lambda$ et $d_1 = m_\lambda$ et une base $\mathscr{B}_\lambda$ de E^λ telle que la matrice de la restriction de f à E^λ soit diagonale par blocs et dont les blocs diagonaux sont égaux aux matrices de Jordan $J_{d_1}(\lambda), J_{d_2}(\lambda), \ldots, J_{d_{r_\lambda}}(\lambda)$. Ou plus graphiquement, on a :

$$\mathrm{Mat}_{\mathscr{B}_\lambda}(f) = \begin{pmatrix} J_{d_1}(\lambda) & 0 & \ldots & 0 \\ 0 & J_{d_2}(\lambda) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & J_{d_{r_\lambda}}(\lambda) \end{pmatrix}$$

De plus si f et g sont deux endomorphismes de E, alors f et g sont semblables si et seulement si $\mathrm{spec}(f) = \mathrm{spec}(g)$ et si pour tout $\lambda \in \mathrm{spec}(f)$ on a l'égalité $d^g_\lambda = d^f_\lambda$.

Démonstration. Pour montrer l'existence de la base $\mathscr{B}_\lambda$, on considère la restriction f_λ de f à E^λ. Alors l'endomorphisme $\tilde{f}_\lambda = f_\lambda - \lambda \mathbb{1}_{E^\lambda}$ est nilpotent d'indice de nilpotence n_λ. On applique le théorème précédent à $\tilde{f}_\lambda$: il existe donc une suite $d^f_\lambda = (d_1, d_2, \ldots, d_{r_\lambda})$ telle

que la matrice de $\tilde{f}_\lambda$ dans cette base soit diagonale par blocs, de blocs diagonaux égaux à $J_{d_1}, J_{d_2}, \ldots, J_{d_{r_\lambda}}$. On en déduite que la matrice de $f_\lambda = \lambda \mathbb{1}_{E^\lambda} + \tilde{f}_\lambda$ dans $\mathscr{B}_\lambda$ est bien de la forme énoncée dans le théorème.

Pour la deuxième partie, si on suppose qu'on a égalité entre $\mathrm{spec}(f)$ et $\mathrm{spec}(g)$ et que pour tout $\lambda \in \mathrm{spec}(f)$, on a $d_\lambda^g = d_\lambda^f$, alors f et g ont même réduite de Jordan, ils sont donc semblables d'après la propriété 2.1.3.

Réciproquement, si f et g sont semblables alors toujours d'après la proposition 2.1.3, il existe $s \in \mathrm{GL}(E)$ tel que $g = sfs^{-1}$. On en déduit $P_f = P_g$ et donc $\mathrm{spec}(f) = \mathrm{spec}(g)$. Ensuite, pour tout $\lambda \in \mathrm{spec}(f)$, on définit les deux suites de sous-espaces vectoriels suivantes : $k_i^f(\lambda) = \dim \ker(f - \lambda \mathbb{1}_E)^i$ et $k_i^g(\lambda) = \dim \ker(g - \lambda \mathbb{1}_E)^i$, pour $i \in \{0, 1, \ldots, m_\lambda\}$ et les deux suites décroissantes d'entiers suivantes $\delta_i^f(\lambda) = k_i^f(\lambda) - k_{i-1}^f(\lambda)$ et $\delta_i^g(\lambda) = k_i^g(\lambda) - k_{i-1}^g(\lambda)$, pour $i \in \{1, 2, \ldots, n_\lambda\}$. Comme f et g sont conjugués, alors les suites $k^f(\lambda)$ et $k^g(\lambda)$ sont égales, ainsi que les suites $\delta^f(\lambda)$ et $\delta^g(\lambda)$. Par le même raisonnement que dans le théorème 30, on en déduit que les suites des tailles des blocs de Jordan dans la réduite de f_λ et de g_λ sont égales. $\square$

Le calcul pratique de la réduite de Jordan en général

En pratique, si l'on veut trouver la forme de réduite de Jordan d'un endomorphisme non forcément nilpotent, il faut donc commencer par calculer le polynôme caractéristique, puis les valeurs propres de f. Ensuite pour tout $\lambda \in \mathrm{spec}(f)$, on considère $\tilde{f}_\lambda = f_\lambda - \lambda \mathbb{1}_V$, puis on calcule les noyaux $K(\lambda)_i = \ker \tilde{f}_\lambda^i$. Cette suite est croissante pour l'inclusion et stationne lorsque $\ker \tilde{f}(\lambda)^i = E^\lambda$. On applique ensuite la méthode vue précédemment pour le cas nilpotent à l'application $\tilde{f}_\lambda$ et à la suite croissante :

$$\{0\} = K_0(\lambda) \subset K_1(\lambda) \subset K_2(\lambda) \subset \cdots \subset K_{m_\lambda}(\lambda) = E^\lambda.$$

Ce qui nous permet d'obtenir une base $\mathscr{B}_\lambda$ de E^λ dans laquelle la matrice de $\tilde{f}_\lambda$ (resp de f_λ) sera composée de produits de blocs de Jordan J_q (resp. de produits de blocs de Jordan $J_q(\lambda)$).

Lien entre décomposition de Jordan-Chevalley et réduite de Jordan

Terminons ce cours par un commentaire sur le lien entre décomposition de Jordan et réduction de Jordan. Soit f un endomorphisme de E donné dans une base $\mathscr{C}$. Si l'on connaît la réduction de Jordan de f, alors en se plaçant dans la base $\mathscr{B}$ dans laquelle f est sous sa forme réduite, il est facile de donner la décomposition de Jordan de f. En effet, la partie diagonalisable sera l'endomorphisme diagonal égale à l'homothétie de rapport λ sur chaque sous-espace caractéristique E^λ, et la partie nilpotente sera égal à la matrice diagonale par bloc dont la restriction à E^λ est la forme réduite de $\tilde{f}_\lambda$. Ensuite, si on veut donner la décomposition de Jordan dans la base initiale $\mathscr{C}$, il faut appliquer les formules de changement pour écrire la partie diagonalisable et la partie nilpotente de f dans la base $\mathscr{C}$.

Cependant en pratique, si l'on ne connaît pas la réduite de Jordan de f ni la base dans laquelle la matrice de f est sous la forme d'une réduite de Jordan, il est plutôt maladroit d'essayer de calculer la décomposition de Jordan de f en passant par le calcul de la réduite de Jordan. Vous avez sûrement vu des exemples de calculs plus ou moins directs sans passer par le calcul de la réduite de Jordan en TD lors de la résolution de l'exercice 54. En fait il existe des algorithmes permettant de calculer la décomposition de Jordan-Chevalley de f rapidement et ceci sans calculer les valeurs propres de f, voir par exemple en suivant le lien : `http://math.univ-lyon1.fr/ ressayre/PDFs/newton-dunford.pdf` .

2.6.3 Exercices

Exercice 56 ⓒ

Soit $A \in M_6(\mathbb{C})$. On suppose que $P_A(X) = (X-2)^4(X-3)^2$ et $M_A(X) = (X-2)^2(X-3)$.

1. Que peut-on dire des dimensions des sous-espaces propres (resp. caractéristiques) de A ?
2. Quelles sont les formes de réduite de Jordan possibles pour A ?

Exercice 57 ⓒ

Déterminer toutes les matrices $A \in M_2(\mathbb{R})$ telles que

$$A^3 - 7A^2 + 15A - 9\,\mathbb{1}_2 = 0\ .$$

(Remarque : $X^3 - 7X^2 + 15X - 9 = (X-3)^2(X-1)$.)

Exercice 58 ⓒ

Pour chacune des matrices suivantes, on calculera sa forme réduite de Jordan, puis on donnera une base dans laquelle la matrice est de cette forme.

$$A = \begin{pmatrix} 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad B = \begin{pmatrix} -2 & -1 & 1 & 2 \\ 1 & -4 & 1 & 2 \\ 0 & 0 & -5 & 4 \\ 0 & 0 & -1 & -1 \end{pmatrix}$$

$$C = \begin{pmatrix} 2 & -1 & -1 & 4 & 1 \\ -2 & 1 & 1 & -7 & -1 \\ 4 & -2 & -2 & 14 & 2 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 \end{pmatrix} \quad D = \begin{pmatrix} 0 & 0 & 1 & 0 & -1 \\ 0 & -1 & 2 & -6 & -4 \\ 1 & -1 & 3 & -4 & -4 \\ 0 & 1 & -1 & 4 & 2 \\ 1 & -1 & 2 & -4 & -3 \end{pmatrix}.$$

Indication : la matrice C admet 0 comme valeur propre triple et 1 comme valeur propre double ; la matrice D admet 0 comme valeur propre double et 1 comme valeur propre triple.