# Sur un théorème d'Hurwitz

Molina Julien

Dans le cadre des TIPE de l'université Claude Bernard Lyon 1

Semestre de printemps 2016

# Table des matières

**Remerciements** **1**

**Introduction** **2**

**1 Groupes et théorie des représentations** **5**
1.1 Théorie des groupes . . . . . 5
1.1.1 Premières définitions . . . . . 5
1.1.2 Relations d'équivalence : formalisme . . . . . 6
1.1.3 Groupes distingués et groupes quotients . . . . . 7
1.1.4 Autres notions de groupe . . . . . 9
1.2 Théorie des représentations linéaires des groupes . . . . . 11
1.2.1 Représentations linéaires . . . . . 11
1.2.2 Caractères . . . . . 14
1.2.3 Groupes abéliens . . . . . 21

**2 Matrices d'Hurwitz** **22**

**3 Démonstration via l'algèbre linéaire** **25**

**4 Démonstration via la théorie des groupes** **28**

**5 Ouvertures et questionnements** **33**

# Remerciements

# Introduction

Jamais je n'aurai imaginé qu'un jour je puisse rédiger un Travail d'Initiative Personelle Encadré (TIPE) de mathématiques.

Arrivé dans le bureau de Philippe Caldero afin de parler des TIPE, je lui ai fait part de ma préférence pour les thèmes relatifs à l'algèbre. Il me présenta alors un document. Je le feuilletai et ne vis que des symboles et autres formules mathématiques méconnus pour moi à l'époque. Il me lança : "Ça te dirait de travailler sur ce document ?". Ayant envie de travailler sur des thèmes mathématiques nouveaux, je lui rétorquai que ce serait avec plaisir. Et c'est ainsi que débuta mon TIPE qui eu pour fil conducteur le document de Keith CONRAD, *The Hurwitz theorem on sums of squares*. Ce document traite d'un théorème particulier qu'énonça Adolf HURWITZ en 1898 et cherche à le démontrer de plusieurs manières. Tout d'abord grâce à de l'algèbre linéaire, puis avec la théorie des groupes et des représentations de groupes. Le document se termine sur une considération concrète du théorème d'Hurwitz par rapport au produit vectoriel. Dans ce TIPE, nous ne nous intéresserons pas à cette dernière partie, mais uniquement aux démonstrations.

Il nous faut donc maintenant considérer le théorème en lui-même :

**Théorème** (Hurwitz, 1898)**.** *Soit* $\mathbb{K}$ *un corps de caractéristique différente de* 2*. Si*

$$(x_1^2 + x_2^2 + ... + x_n^2)(y_1^2 + y_2^2 + ... + y_n^2) = z_1^2 + z_2^2 + ... + z_n^2$$

*pour tout* $x_1, x_2, ..., x_n, y_1, y_2, ..., y_n$ *dans* $\mathbb{K}$ *et où les* $z_1, z_2, ..., z_n$ *sont des formes bilinéaires sur* $\mathbb{K}$ *dépendant des* $x_i$ *et des* $y_i$ *pour* $i \in [\![1, n]\!]$*, alors* $n = 1, 2, 4$ *ou* 8*.*

Essayons d'expliquer plus concrètement ce théorème. On sait que dans $\mathbb{R}$ nous avons l'égalité suivante :

$$x^2y^2 = (xy)^2 \tag{1}$$

Cela est dû à la commutativité du produit dans $\mathbb{R}$. Mais il est plus intéressant de considérer les relations suivantes qui sont les homologues de (1) pour deux et quatre carrés :

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2 \tag{2}$$

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \quad = \quad & (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 + \\ & (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2 + \\ & (x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2)^2 + \\ & (x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2)^2\end{aligned} \tag{3}$$

Il suffirait simplement de développer les égalités (2) et (3) pour valider leur véracité. De plus, nous remarquons assez rapidement que les membres de droites, pour les relations (2) et (3), sont des formes bilinéaires.

Un peu d'histoire avant d'aller plus loin, la relation (3) fut d'abord découverte par Leonhard EULER au XVIIIe siècle. Celle-ci a disparu dans les méandres scientifiques pour finalement être "re"découverte par William HAMILTON lors de ces travaux sur les quaternions au XIXe siècle. Peu après, Arthur CAYLEY fit une découverte similaire avec une somme de huit carrés. Tout ceci sera traité plus en détail dans le chapitre 4 : Ouvertures et approfondissements.

Cela dit, tout mathématicien aurait reconnu que la progression du nombre de carré dans la somme est celle des puissances de 2 (2,4,8,...). Alors pourquoi ne pas tenter pour 16 ?

Hurwitz le tenta et donna naissance a son fameux $1, 2, 4, 8$-théorème qui montre que d'autres relations de ce type ne sont guère possibles. Suivons alors notre document et cherchons à démontrer ce théorème.

# Chapitre 1

# Groupes et théorie des représentations

Avant de commencer les différentes démonstrations du théorème d'Hurwitz, j'ai voulu

## 1.1 Théorie des groupes

### 1.1.1 Premières définitions

**Définition** (Groupe)**.** *Soit $G$ un ensemble non vide muni d'une loi de composition interne $\oplus$, c'est-à-dire d'une application $\oplus : G \times G \longrightarrow G$ vérifiant les trois axiomes suivants :*

1. $\forall x, y, z \in G,\ (x \oplus y) \oplus z = x \oplus (y \oplus z)$ *(associativité)*
2. *$\forall x \in G$, il existe un élément $e \in G$, appelé élément neutre tel que $x \oplus e = e \oplus x = x$.*
3. *$\forall x \in G$, il existe un élément $x' \in G$, appelé élément symétrique vérifiant $x \oplus x' = x' \oplus x = e$.*

*On dit alors que $\oplus$ définit **une structure de groupe** sur $G$ ou que $(G, \oplus)$ est un **groupe**.*
*Si $G$ est un groupe de cardinal fini, on note $|G|$ son cardinal qu'on appelle aussi **l'ordre**.*

En guise de remarque, on peut ajouter que si $\oplus$ vérifie $\forall x, y \in G,\ x \oplus y = y \oplus x$, alors la loi est dite **commutative** et on dit que $(G, \oplus)$ est un groupe **commutatif** ou un groupe **abélien**.

Comme toute structure algébrique, on peut aussi définir la notion de **sous-groupe** :

**Définition.** *Soit $(G, \cdot)$ un groupe et soit $H$ un sous-ensemble de $G$. On dit que $H$ **est un sous-groupe** de $G$ si :*

1. *$H$ est non-vide - contient l'élément neutre de $G$*
2. *$H$ est stable pour la loi de composition interne définie, ie $\forall\ h_1, h_2 \in H,\ h_1 \cdot h_2 \in H$*
3. *$H$ est stable par inverse, ie $\forall h \in H,\ h^{-1} \in H$*

*Ainsi $H$ définit une structure de sous-groupe. Mais on peut aussi dire que $H$ est un groupe à part entière si on oublie qu'il est sous-ensemble d'un plus "grand" ensemble au sens de l'inclusion.*

Puis on peut aussi définir un autre groupe particulier que nous utiliserons dans ce TIPE :

**Définition.** *Soit $(G, \cdot)$ un groupe et soit $A$ un partie de $G$. Il existe un plus petit sous-groupe de $G$ qui contient $A$. On peut le décrire de deux manières :*

1. *C'est l'intersection de tous les sous-groupe de $G$ contenant $A$.*
2. *On peut le voir comme l'ensemble des $a_1, .., a_n \in G$ tel que pour tout $i \in [\![1, n]\!]$, $a_i \in A$ ou $a_i^{-1} \in A$.*

*On note ce groupe $\langle A \rangle$ et on l'appelle* ***le sous-groupe de $G$ engendré par $A$.***

*Démonstration :*

1. On pose $\{H_i\}_i$ la famille des sous-groupes de $G$ qui contiennent $A$. On sait que l'intersection $H = \bigcap_i H_i$ est un sous-groupe de $G$. On voit de suite que $H$ contient $A$ puisqu'il est intersection de tous les sous-groupe contenant $A$. Et de plus, tout sous-groupe $J$ contenant $A$ fait parti des $H_i$ et donc contient $H$ qui est leur intersection. Ainsi, $h$ est le plus petit sous-groupe, au sens de l'inclusion, contenant $A$.
2. Considérons maintenant l'ensemble $P$ des produits $a_1...a_n \in G$ avec $n \in \mathbb{N}$ et pour tout $i$, $a_i \in A$ ou $a_i^{-1} \in A$. Cet ensemble contient $e$. Mais encore, si on prend deux éléments $a_1...a_n$ et $b_1...b_m$, il est évident que leur produit $a_1...a_n b_1...b_m$ est encore dans $P$ puisque c'est un produit d'un certain nombre d'éléments appartenant, eux-même ou leur inverse, à $A$. Puis, l'inverse de $a_1...a_n$ est $(a_n)^{-1}...(a_1)^{-1}$ qui est encore un élément de $P$. Puis, il vient que $P$ est un sous-groupe de $G$ contenant $A$. Cela dit, si un sous-groupe $H$ de $G$ contient $A$, alors grâce aux propriétés des sous-groupes, il contient tous les inverses de $A$ et aussi tous les produits d'un certain nombre d'éléments de $A$ et d'inverses d'éléments de $A$. D'où $H$ contient $P$. Ce qui montre que $E$ est le plus petit sous-groupe de $G$, pour l'inclusion, contenant $A$ □

### 1.1.2 Relations d'équivalence : formalisme

Un petit aparté sur la théorie des ensembles sera le bienvenu avant d'appliquer ces futurs nouveaux acquis à la théorie des groupes.

Nous allons introduire **la relation d'équivalence**, objet fondamental de la théorie de ensemble qui a pour but de mettre en relation les objets d'un ensemble qui sont analogues selon une certaine propriété.

**Définition.** *Soit $E$ un ensemble. On définit la relation d'équivalence $\sim$ sur $E$ par une relation binaire qui vérifie les propriétés suivantes :*

1. *Réflexivité : Pour tout $x \in E$, $x \sim x$.*
2. *Symétrie : Pour tout $x, y \in E$, on a $x \sim y$ et $y \sim x$.*
3. *Transitivité : Pour tout $x, y, z \in E$, si $x \sim y$ et $y \sim z$, alors $x \sim z$.*

Par suite, nous définissons ce qu'est une **classe d'équivalence** :

**Définition.** *Soit $E$ un ensemble et $\sim$ une relation d'équivalence sur $E$.*
*On définit la classe d'équivalence $[x]$ d'un élément $x$ de $E$ par l'ensemble suivant :*

$$[x] = \{y \in E \mid x \sim y\}$$

On peut citer une petit propriété :

**Proposition.** *Soit $E$ un ensemble, $\sim$ une relation d'équivalence sur $E$ et $x, y \in E$*

1. *On a : $x \sim y \equiv [x] = [y]$*
2. *Les classes d'équivalences $[x]$ et $[y]$ sont soit disjointes soit confondues.*

*Démonstration* :

1. Il faut utiliser la propriété de transitivité de la relation d'équivalence $\sim$.

2. 1er cas : $[x] \cap [y] = \varnothing$. Alors les classes d'équivalences sont disjointes.
   2ème cas : $[x] \cap [y] \neq \varnothing$. Soit $z \in [x] \cap [y]$. Alors cet élément vérifie $x \sim z$ et $y \sim z$. Ainsi par symétrie et transitivité, on a $x \sim y$. On obtient donc que $y$ appartient à la classe d'équivalence de $x$, ie $y \in [x]$.
   Montrons maintenant que la classe de $y$ est contenue dans la classe de $x$. Soit $z_1 \in [y]$. On a $y \sim z_1$ et $x \sim y$, puis par transitivité $x \sim z_1$. Ainsi $z_1 \in [x]$ d'où $[y] \subset [x]$.
   On montre de manière similaire en deux étapes que $[x] \subset [y]$.
   Finalement $[x] = [y]$

□

**Corollaire.** *Soit $E$ un ensemble et $\sim$ une relation d'équivalence sur $E$. Alors les classes d'équivalence pour $\sim$ forment une partition de $E$.*

*Démonstration* : Tout d'abord grâce à la réflexivité, tout élément de $E$ appartient à sa classe d'équivalence. ainsi les classes d'équivalence sont non-vides et recouvrent entièrement $E$. Puis, avec la proposition précédente, les classes d'équivalence de deux éléments sont soit disjointes soit confondues. Finalement, les clases d'équivalence forment bien une partition de $E$, ie $E = \bigsqcup_i [x_i]$.

□

**Définition.** *Soit $E$ un ensemble et $\sim$ une relation d'équivalence sur $E$. On note $[x]$ la classe d'équivalence de $x \in E$ selon $\sim$. On appelle* ***représentant de la classe*** *$[x]$ tout élément fixé au préalable appartenant à $[x]$ qui sera désigné comme élément "modèle" de cette classe.*

*En effet, nous entendons par là que, puisque tous les éléments de $[x]$ sont similaires pour la relation $\sim$, il nous faut fixer un élément de cette classe qui nous servira d'élément de travail.*

Puis finalement, une définition très importante relative aux relations d'équivalence :

**Définition.** *On se donne un ensemble $E$ et une relation d'équivalence sur $E$ $\sim$. On définit* ***l'ensemble quotient de $E$ par la relation $\sim$****, noté $E\backslash\sim$, par :*

$$E\backslash\sim = \{[x] \mid x \in E\}$$

L'idée de cet ensemble quotient est de pouvoir travailler dans $E\backslash\sim$ comme dans $E$ mais sans distinguer les éléments en fonction de leur classe d'équivalence.

### 1.1.3 Groupes distingués et groupes quotients

Dans toute cette partie, on se donne un groupe $(G, \cdot)$ qui sera multiplicatif.

Pour débuter, on va donner définition-théorème à propos une relation d'équivalence qui sera utile pour toute la théorie des groupes :

**Définition.** *Pour tout sous-groupe $H$ de $G$, la relation suivante :*

$$g_1 \sim g_2 \iff g_1^{-1} g_2 \in H$$

*définie une relation d'équivalence sur $G$.*

*Démonstration :* Tout d'abord, pour $g$ dans $G$, on a $g^{-1}g = 1 \in H$. Ainsi $\sim$ est réflexive.

Ensuite, si $g_1, g_2$ dans $G$ sont tels que $g_1^{-1}g_2 \in H$, on a donc $(g_1^{-1}g_2)^{-1} = g_2^{-1}g_1 \in H$. Ainsi, on a aussi $g_2 \sim g_1$. Donc $\sim$ est symétrique.

Puis, si $g_1, g_2, g_3$ dans $G$ sont tels que $g_1^{-1}g_2 \in H$ et $g_2^{-1}g_3 \in H$, on a donc $g_1^{-1}g_3 = (g_1^{-1}g_2)(g_2^{-1}g_3) \in H$. La relation $\sim$ est donc aussi transitive. Par ces trois propriétés, $\sim$ définie bien sur $G$ une relation d'équivalence. □

On note alors pour tout $g \in G$, $\overline{g}$ la classe d'équivalence de $g$ modulo/selon la relation $\sim$. Dans la théorie des groupes, cette relation est centrale. Ainsi, on dit aussi que $\overline{g}$ est **la classe à gauche modulo $H$ de $g$.**

On a donc, pour tout $g \in G$ :

$$h \in \overline{g} \iff g \sim h \iff g^{-1}h \in H \iff \exists k \in H,\ h = gk \iff h \in gH$$

Autrement dit, $\overline{g} = gH$. On peut de plus remarquer que $\overline{1} = H$ et que $\overline{g} = H$ si et seulement si $g \in H$.

On invoque une autre notation : l'ensemble de toutes les classes d'équivalence est noté $G/H$ et s'appelle **l'ensemble des classes à gauche modulo $H$**. Autrement dit,

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

$\longrightarrow$ On peut aussi définir de manière équivalente une relation d'équivalence $g_1 \equiv g_2 \iff g_1 g_2^{-1} \in H$, et on obtiendrait l'ensemble $H/G = \{Hg \mid g \in G\}$ qu'on appelle **l'ensemble des classes à droite modulo $H$**.

**Théorème.** *Si $H$ est un sous-groupe de $G$, alors l'ensemble des classes à gauche (à droite) modulo $H$ forment une partition de $G$.*

*Démonstration :* Il ne s'agit que d'un cas particulier du cas général démontré dans la partie précédente sur les relations d'équivalence. □

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

$$(g\mathcal{R}g') \implies (gh\mathcal{R}g'h \ \ et \ \ hg\mathcal{R}hg')$$

On va ici introduire un théorème majeur :

**Théorème.** *Si $H$ est un sous-groupe de $G$, alors la relation d'équivalence $\sim$ définie au début associée à $H$ est compatible avec la loi de composition de $G$ si et seulement si $gH = Hg$ pour tout $g \in G$.*

*Démonstration :*

$\implies$ Supposons $\sim$ compatible avec la loi de composition de $G$. Pour tout $k \in gH$, on a $g^{-1}k \sim 1$ et grâce à la compatibilité à gauche et à droite de la relation $\sim$, on en déduit que $g(g^{-1}k) \sim g$ et $g(g^{-1}k)g^{-1} \sim gg^{-1}$, d'où $kg^{-1} \sim 1$, ce qui revient à $k \in Hg$. On a donc $gH \subset Hg$. On montrerait de manière analogue que $Hg \subset gH$. Finalement, on a bien $gH = Hg$.

$\impliedby$ Supposons que $gH = Hg$ pour tout $g \in G$. Si $g \sim g'$ et $h \in G$, on a alors $(gh)^{-1}g'h = h^{-1}g^{-1}g'h$ avec $g^{-1}g' \in H$. Donc $g^{-1}g'h \in Hh = hH$ et ainsi $(gh)^{-1}g'h = h^{-1}hk = k \in H$, autrement dit que $gh \sim g'h$. Mais aussi $(hg)^{-1}hg' = g^{-1}h^{-1}hg' = g^{-1}g' \in H$, ce qui signifie que $hg \sim hg'$. Donc $\sim$ est compatible avec la loi de composition de $G$.

On donne maintenant une définition très importante :

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

*On note ceci $H \triangleleft G$*

On voit donc que, pour pouvoir quotienter un groupe par un certain sous-groupe, il faut que celui-ci soit distingué pour pouvoir travailler dans le groupe quotient avec la même loi de composition.

### 1.1.4 Autres notions de groupe

On va définir ici d'autres notions de groupes et un fameux théorème sur les groupes.

**Définition.** *On appelle **commutateur** de $g$ et $h$, éléments de $(G, \cdot)$ par :*

$$[g, h] = g \cdot h \cdot g^{-1} \cdot h^{-1}$$

*On peut remarquer que $g$ et $h$ commutent si $[g, h] = e$, où $e$ est l'élément neutre du groupe.*

**Définition.** *On appelle le **sous-groupe dérivé de** $(G, \cdot)$ le groupe suivant :*

$$D(G) = [G, G] = \langle\ \{[g, h],\ \mid g, h \in G\}\ \rangle$$

*Autrement dit c'est le sous-groupe engendré par les commutateurs de $G$.*

On peut citer deux petites propriétés de ce groupe :

**Proposition.** *Soit $(G, \cdot)$ un groupe.*

1. *$D(G)$ est distingué dans $G$*
2. *Pour tout sous-groupe normal $H$ de $G$, $G \setminus H$ est abélien si et seulement si $D(G) \subset H$.*

*Démonstration :*

1. Prenons un élément de $D(G)$, par exemple $[g, h]$ avec $g, h \in G$. Soit $s \in$. On a :

$$\begin{aligned}
[sgs^{-1}, shs^{-1}] &= sgs^{-1}shs^{-1}(sgs^{-1})^{-1}(shs^{-1})^{-1} \\
&= sgs^{-1}shs^{-1}sg^{-1}s^{-1}sh^{-1}s^{-1} \\
&= sghg^{-1}h^{-1}s^{-1} \\
&= s[g, h]s^{-1}
\end{aligned}$$

   Ainsi, par définition $D(G)$ est distingué dans $G$.

2.

$$\begin{aligned}
G \setminus H \text{ abélien} &\iff \text{pour tout } x, y \in G,\ \overline{xy} = \overline{yx} \text{ avec } \overline{x} = xH \text{ et } \overline{y} = yH \\
&\iff \text{pour tout } x, y \in G,\ \overline{xyx}^{-1}\overline{y}^{-1} = \overline{e} \\
&\iff \text{pour tout } x, y \in G,\ [x, y] \in H \\
&\iff D(G) \subset H
\end{aligned}$$

□

**Définition.** *Soit $(G, \cdot)$ un groupe. On appelle* ***le centre*** *de $G$, le groupe noté $Z_G$ défini par :*

$$Z_G = \{g \in G \mid g \cdot h = h \cdot g, \ \forall h \in G\}$$

*Autrement dit, c'est le groupe des éléments qui commutent avec tous les autres éléments du groupe.*

**Définition.** *Soit $G$ un groupe. On appelle* ***classe de conjugaison de*** *$g \in G$ l'ensemble suivant :*

$$C_g = \{hgh^{-1} \mid h \in G\}$$

Maintenant nous allons donner un des théorèmes les plus importants dans la théorie des groupes :

**Théorème** (Théorème de Lagrange)**.** *Soit $(G, \cdot)$ un groupe et $H$ un sous-groupe de $G$. Alors :*

1. *$|H|$ divise $|G|$.*
2. *soit $g \in G$ et $n$ le plus petit entier strictement positif tel que $g^n = e$ où $e$ est le neutre de $G$. Alors $n|\ |G|$.*

*Démonstration :*

1. Soient $g, g' \in G$. On a alors que soit $gH = g'H$ soit que $gH \cap g'H = \varnothing$.
   En effet, soit $k \in gH \cap g'H$, alors il existe $h, h' \in H$ tels que $k = gh = g'h'$. Il vient alors $g = g'h'h^{-1} = g'(h'h^{-1})$. Or $h'h^{-1}$ appartient à $H$ donc $g'h'h^{-1} \in g'H$. Ainsi, par égalité $g$ appartient aussi à $g'H$. Donc $gH \subset g'H$.
   On montre de la même manière que $g'H \subset gH$. Ainsi, on a bien $gH = g'H$.
   De plus, tout élément $g$ de $G$ appartient à une classe du type $gH$, celle de $g = ge$. Ainsi $G$ est une réunion disjointe des $gH$.
   De plus, on sait que les $gH$ sont en bijection avec $H = eH$. Pour se faire, on vérifie simplement que $\varphi_g : H \longrightarrow gH, h \longmapsto gh$ est bijective en montrant que $\varphi_g \circ \varphi_{g^{-1}} = Id_{gH}$ et que $\varphi_{g^{-1}} \circ \varphi_g = Id_H$.
   Ainsi, comme $G$ est une réunion disjointe des $gH$, on a $|G| = \sum |gH| = \sum |H|$ puisque les $gH$ sont en bijection avec $H$.
   D'où $|G|$ est un multiple de $|H|$.
2. Soit $g \in G$. On considère la suite $(g^k)_{k \in \mathbb{N}}$. Cette suite est bien finie puisque $G$ est lui-même fini.
   Alors il existe $k, k' \in \mathbb{N}$ différents tels que $g^k = g^{k'}$ par non-injectivité de l'application $\mathbb{Z} \longrightarrow G, k \longmapsto g^k$, $\mathbb{Z}$ étant infini et $G$ fini. D'où, $g^{k-k'} = e$, quitte à prendre l'inverse, on peut supposer $k > k'$.
   Il existe un $m > 0$ tel que $g^m = e$ et on le suppose comme étant minimal, toute partie non vide de $\mathbb{N}$ étant minorée. On pose alors : $H = \{e, g, g^2, ..., g^{m-1}\}$. Montrons $H$ est bien un sous-groupe de $G$ et $|H| = m$.
   En effet, soit $k \in \mathbb{Z}$, on pose $k = mq + r$, avec $0 \leqslant r < m$. On a alors : $g^k = g^{mq+r} = (g^m)^q \times g^r = e^q \times g^r = g^r \in H$. Ainsi cela montre que $H$ est un sous-groupe de $G$.
   De plus, on suppose $0 \leqslant i < j < m$. On va montrer que $g^i \neq g^j$. Supposons que $g^i = g^j$ alors $g^{j-i} = e$ avec $0 < j - i < m$. Ce qui est absurde par minimalité de $m$. Ainsi par le (1) puis que $H$ est un sous-groupe de $G$ de cardinal $m$, on a bien $m \mid |G|$.

□

## 1.2 Théorie des représentations linéaires des groupes

Dans cette partie, nous allons nous intéresser plus théoriquement aux représentations linéaires des groupes finis. Nous étudierons d'abord les représentations en elles-mêmes, et ensuite nous évoquerons la théorie des caractères des représentations.

### 1.2.1 Représentations linéaires

#### a) Définitions

Prenons un groupe $(G,\cdot)$ fini.

**Définition** (Représentation linéaire)**.** *Une* ***représentation linéaire de*** $G$ ***dans*** $E$*, où* $E$ *est un* $\mathbb{C}$*-espace vectoriel, est un homomorphisme* $\rho$ *de* $G$ *dans le groupe* $(\boldsymbol{GL}_n(E), \circ)$*. Autrement dit, à tout élément* $g$ *de* $G$*, on associe* $\rho_g$ *de* $\boldsymbol{GL}_n(E)$ *de telle sorte que :*

$$\rho_{gh} = \rho_g \circ \rho_h \qquad \forall g, h \in G$$

D'autres définitions terminologiques s'ajoutent à celle-ci.

**Définition.** *Considérons* $(G,\cdot)$ *un groupe, et* $\rho : G \longrightarrow \boldsymbol{GL}_n(E), \rho' : G \longrightarrow \boldsymbol{GL}_n(F)$ *deux représentations linéaires de* $G$*, où* $E$ *et* $F$ *sont deux* $\mathbb{C}$*-espaces vectoriels.*

1. *On appelle* $E$ ***un espace de représentation de*** $G$ *ou par abus, une représentation de* $G$*, ou encore un* $G$***-module****.*
2. *On appelle* ***degré*** *de la représentation* $\rho$*, la dimension de* $E$*, dans le cas où* $\dim(E) < \infty$*.*
3. *Une représentation est dite* ***fidèle*** *s'il est injective.*
4. *On dit que* $\rho$ *et* $\rho'$ *sont* ***isomorphes*** *s'il existe un isomorphisme* $\varphi : E \longrightarrow F$ *tel que :*

$$\forall g \in G, \quad \varphi \circ \rho_g = \rho'_g \circ \rho$$

*On appelle* $\varphi$ *un* ***morphisme de représentations*** *ou un* ***opérateur d'entrelacement****.*

Ici, une petite propriété s'offre à nous.

**Proposition.** *Soit* $\rho$ *une représentation du groupe* $(G,\cdot)$ *dans* $(\boldsymbol{GL}_n(E), \circ)$ *où* $E$ *est un* $\mathbb{C}$*-espace vectoriel.*
*On a alors* $\rho_g^{-1} = \rho_{g^{-1}}$ *pour tout* $g \in G$

<u>*Démonstration*</u> : Regardons l'élément $\rho_1$.
On a alors $\rho_1 = \rho_{g\cdot g^{-1}} = \rho_g \circ \rho_{g^{-1}}$ par définition d'une représentation linéaire de $G$. De plus, $\rho$ étant un homomorphisme, l'élément neutre est envoyé sur l'autre élément neutre, d'où $\rho_1 = Id_n$.
On a donc $\rho_1 = Id_n = \rho_g \circ \rho_{g^{-1}}$ et $\rho_{g^{-1}} = \rho_g^{-1}$ □

#### b) Représentations particulières

Nous allons maintenant parler de deux représentations particulières qui ont des caractéristiques assez puissantes dans la théorie de représentation.

Considérons une représentation $\rho : G \longrightarrow \mathbf{GL}_n(E)$ du groupe $(G,\cdot)$ dans $E$, un $\mathbb{C}$-espace vectoriel. Prenons $F$ un sous-espace vectoriel de $E$, stable par opérations de $G$, *ie* pour $x \in F$, $\rho_g(x) \in F$, pour tout $g \in G$. Regardons maintenant la restriction de $\rho$ à $F$. On a, par stabilité de

$F$, que $\rho_{|F}$ est un automorphisme. De plus, par les propriétés de $\rho$, on a que $\rho_{gh|F} = \rho_{g|F} \circ \rho_{h|F}$ pour $g, h \in G$.

On en conclut donc que $\rho_{|F} : G \longrightarrow \mathbf{GL}_n(F)$ est une représentation linéaire de $G$ sur $F$ et on dit aussi que $\rho_{|F}$ ou $F$ est une **sous-représentation** de $\rho$ ou $E$.

On en tire alors un théorème fondamental qu'est celui de Maschke :

**Théorème** (Théorème de Maschke)**.** *Soient $\rho : G \longrightarrow \boldsymbol{GL}_n(E)$ une représentation linéaire du groupe $(G, \cdot)$ dans $E$ et $F$ un sous-espace vectoriel de $E$ $G$-stable.*

*Il existe alors un supplémentaire de $F$ dans $E$ qui est $G$-stable.*

*Démonstration :* Par simple considération d'algèbre linaire, on a de suite l'existence d'un supplémentaire de $F$ dans $E$, à l'aide du théorème de la base incomplète. Notons-le $H$. De plus, notons $p_0$ le projecteur de $E$ sur $F$ parallèlement à $H$.

Cependant, rien ne nous montre, *a priori*, que $H$ est $G-$stable. Pour ce faire considérons l'application de $E$ dans $E$ définie par :

$$p = \frac{1}{|G|} \sum_{g \in G} \rho_g \circ p_0 \circ \rho_{g^{-1}}$$

Tachons alors de montrer que $p$ est un projecteur sur $F$.

En effet, soit $x \in E$, on a :

$$p(x) = \frac{1}{|G|} \sum_{g \in G} (\rho_g \circ p_0 \circ \rho_{g^{-1}})(x)$$

On a que $p_0 \circ \rho_{g^{-1}}(x)$ appartient à $F$ puisque $\mathrm{Im}(p_0) = F$.
De même, $\rho_g \circ p_0 \circ \rho_{g^{-1}}(x)$ appartient à $F$ puisque $F$ est $G-$stable.
Ainsi, par sommation, $p(x) \in F$. On en déduit que $\mathrm{Im}(p) \subset F$.

Prenons maintenant un élément $f \in F$. Par $G-$stabilité de $F$ et que $p_0$ est un projecteur sur $F$, on a :

$$\begin{aligned}
p(f) &= \frac{1}{|G|} \sum_{g \in G} (\rho_g \circ p_0 \circ \rho_{g^{-1}})(f) \\
&= \frac{1}{|G|} \sum_{g \in G} (\rho_g \circ \rho_{g^{-1}})(f) \\
&= \frac{1}{|G|} \sum_{g \in G} \rho_{g \cdot g^{-1}}(f) \\
&= \frac{1}{|G|} \sum_{g \in G} \rho_1(f) \\
&= \frac{1}{|G|} \sum_{g \in G} f \\
&= \frac{1}{|G|} |G| f \\
&= f
\end{aligned}$$

Ce qui montre que $F \subset \mathrm{Im}(p)$. On obtient donc $F = \mathrm{Im}(p)$.

Montrons maintenant que $p$ commute avec $\rho_g$ pour tout $g$ dans $G$. En effet, :

$$\begin{aligned}\rho_g \circ p &= \frac{1}{|G|}\sum_{h\in G} \rho_g \circ \rho_h \circ p_0 \circ \rho_{h^{-1}} = \frac{1}{|G|}\sum_{h\in G} \rho_{g\cdot h} \circ p_0 \circ \rho_{h^{-1}} \circ \rho_{g^{-1}\cdot g} \\ &= \frac{1}{|G|}\sum_{h\in G} \rho_{g\cdot h} \circ p_0 \circ \rho_{h^{-1}\cdot g^{-1}} \circ \rho_g = \frac{1}{|G|}\sum_{h\in G} \rho_{g\cdot h} \circ p_0 \circ \rho_{(g\cdot h)^{-1}} \circ \rho_g \\ &= p \circ \rho_g\end{aligned}$$

Il ne reste alors plus qu'à montrer que $\mathrm{Ker}(p)$ est $G-$invariant. En effet, soit $v \in \mathrm{Ker}(p)$, alors pour tout $g \in G$, on a : $p(\rho_g(v)) = \rho_g(p(v)) = \rho_g(0) = 0$.

Finalement, par définition d'une projection, $\mathrm{Im}(p) \cap \mathrm{Ker}(p) = \{0\} = F \cap \mathrm{Ker}(p)$. De plus par le théorème du rang, on obtient que $\dim(E) = \dim(Ker(p)) + \dim(Im(p))$.

Ce qui montre finalement que $E = F \oplus Ker(p)$, avec $\mathrm{Ker}(p)$ $G-$stable. D'où l'existence d'un complémentaire $G-$stable dans $E$ pour $F$. □

Considérons maintenant une représentation linéaire de $G$, $\rho : G \longrightarrow \mathbf{GL}_n(E)$. Si $E$ n'est pas réduit à $\{0\}$ et si aucun sous-espace vectoriel de $E$ est $G-$stable (mis à part $\{0\}$ et $E$), on dit que $\rho$ est **irréductible** ou **simple**. Cette définition est équivalente au fait que $E$ n'est pas somme directe de sous espaces vectoriels.

Avec cette nouvelle définition, on obtient un nouveau théorème :

**Théorème.** *Soit $(G, \cdot)$ un groupe.*

*Toute représentation linéaire de $(G, \cdot)$ est somme directe de représentations irréductibles.*

<u>*Démonstration*</u> : Soit $E$ une représentation de $G$. On va démontrer le théorème par récurrence sur $\dim(E) = n$.

- Initialisation : Supposons $\dim(E) = 0$, le théorème est valide puisque $\{0\}$ est somme directe de la famille vide de représentations linéaires.

- Hérédité : Supposons le théorème vrai pour $n \geqslant 1$. Regardons $E$ pour $\dim(E) = n + 1$.

Si $E$ est déjà irréductible, il n'y à rien à faire.

Sinon, par le théorème de Maschke, on peut décomposer $E$ en directe de $F, G$, c'est-à-dire $E = F \oplus G$. On a de plus que $\dim(F) \leqslant n$ et $\dim(G) \leqslant n$. On peut donc appliquer l'hypothèse de récurrence, et on obtient que $F$ et $G$ sont sommes directes de représentations irréductibles. Il en est donc de même pour $E$.

Ceci termine l'hérédité et achève la récurrence. □

Mais encore, à partir de deux représentations $\rho : G \longrightarrow \mathbf{GL}_n(V)$ et $\sigma : G \longrightarrow \mathbf{GL}_n(W)$ on peut en fabriquer de nouvelles :

— sur l'espace $Hom_{\mathbb{K}}(V, V')$, on fait agir un élément $g$ de $G$ par :

$$\forall \varphi \in Hom_{\mathbb{K}}(V, V'), \quad g \cdot \varphi = \sigma_g \circ \varphi \circ \rho_{g^{-1}}$$

**c) <u>Exemples</u>**

1. Si on prend $E = \mathbb{C}$. On peut alors considérer la représentation appelée **représentation triviale** définie par : $\rho : G \longrightarrow \mathbf{GL}_n(E) = \mathbb{C}^*$, $g \longmapsto 1$. Cette représentation est de degré 1.
2. Soit $G$ un groupe et notons $g$ son cardinal. Soit $E$ un espace vectoriel de dimension égale à $g$ ayant pour une base $(e_t)_{t\in G}$. Prenons un élément $h \in G$ et soit $\rho_h$ l'application linéaire

de $E$ dans $E$ qui transforme $e_h$ en $e_{sh}$. On peut constater que cette application respecte la définition d'une représentation linéaire de $G$. Ainsi, $\rho$ est une représentation linéaire $G$ que l'on appelle la **représentation régulière**. Son degré est égal à $g$.

### 1.2.2 Caractères

A partir de maintenant, on prendra pour convention que le corps $\mathbb{K}$ est inclus dans $\mathbb{C}$.

#### a) Définitions et premières propriétés

Dans cette sous-partie, nous allons présenter l'outil fondamental des représentations qu'est le *caractère* d'une représentation.

**Définition.** *Soit $\rho : G \longrightarrow \boldsymbol{GL}_n(E)$ une représentation de $G$ et $E$ un $\mathbb{K}$-espace vectoriel. On appelle **caractère** de $\rho$ la fonction suivante :*

$$\chi : G \longrightarrow \mathbb{K}, \quad g \longmapsto Tr(\rho_g)$$

Donnons quelques rapides propriétés primaires du caractère :

**Proposition.** *Soit $\chi$ le caractère d'une représentation $\rho$, de $G$ sur $E$, de degré $n$, on a alors :*

1. $\chi(1) = n$
2. $\chi(hgh^{-1}) = \chi(g)$ *pour tout* $g, h \in G$
3. *Soient $\rho : G \longrightarrow \boldsymbol{GL}_n(E_1)$ et $\rho' : G \longrightarrow \boldsymbol{GL}_n(E_2)$ deux représentations de $G$. Notons $\chi_1$ et $\chi_2$ leurs caractères respectifs.*
   *Le caractère $\chi$ de la représentation somme directe $E_1 \oplus E_2$ est $\chi = \chi_1 + \chi_2$.*
4. *Soient $V$ et $V'$ deux représentations de $G$ de caractères respectifs $\chi$ et $\chi'$.*
   *Alors le caractère de $Hom_{\mathbb{K}}(V, V')$ est $\overline{\chi}\chi'$.*

*Démonstration* :

1. On a $\rho(1) = \mathrm{id}$. D'où, $Tr(id) = n$ puisque $E$ est de dimension $n$.
2. On sait que pour tout $A, B$ dans $\mathcal{M}_n(\mathbb{K})$, $Tr(AB) = TR(BA)$. Ainsi pour tout $g, h \in G$ : $\chi(hgh^{-1}) = Tr(\rho_{hgh^{-1}}) = Tr(\rho_{hg}\rho_{h^{-1}}) = Tr(\rho_{h^{-1}}\rho_{hg}) = Tr(\rho_{h^{-1}hg}) = Tr(\rho_g) = \chi(g)$.
3. Étudions $\rho$ et $\rho'$ sous forme matricielle, que nous noterons respectivement $R_r$ et $R_{r'}$. En prenant une base bien choisie pour la décomposition $E_1 \oplus E_2$, la représentation de $E_1 \oplus E_2$ sera donnée matriciellement par :

$$R = \begin{pmatrix} R_r & (0) \\ (0) & R_{r'} \end{pmatrix}$$

   On obtient donc que $Tr(R) = Tr(R_r) + Tr(R_{r'})$. En terme de caractères, cela revient à : $\chi = \chi_1 + \chi_2$.
4. Fixons un élément $g$ de $G$. On a alors $g^{|G|} = e$ dans $G$, ainsi : $\rho_g^{|G|} = id_V$. Par suite, $\rho_g$ annule le polynôme scindé à racines simples $x^{|G|} - 1$ et $\rho_g$ est diagonalisable. Posons alors une base de $V$ composée de vecteurs propres de $\rho_g$, notée $(e_1, ..., e_d)$, ainsi que les valeurs propres correspondantes notées $\lambda_1, ..., \lambda_d$. On applique le même raisonnement à $V'$ et on pose une base $(e'_1, ..., e'_{d'})$ composée de vecteurs propres et on note aussi $\lambda'_1, ..., \lambda'_{d'}$ les valeurs propres correspondantes. On a donc :

$$\chi_\rho(g) = \sum_{i=1}^{d} \lambda_i, \qquad \chi_{\rho'}(g) = \sum_{i=1}^{d'} \lambda'_i$$

On choisit alors une base pour $Hom_{\mathbb{K}}(V,V')$. On la note $(c_{jj'})$, où, pour $1 \leqslant j \leqslant d$ et $1 \leqslant j' \leqslant d'$, les $c_{jj'}$ représentent les applications linéaires qui envoient $e_j$ sur $e_{j'}$ et tue $e_k$ si $k \neq j$ ; elles correspondent aux matrices élémentaires. On obtient donc :

$$(\rho'_g \circ c_{jj'} \circ \rho_g^{-1})(e_k) = \rho'_g \circ_{jj'} (\lambda_k^{-1} e_k) = \delta_{jk}\lambda_k^{-1}\rho'_g(e'_{j'}) = \delta_{jk}\overline{\lambda_j}\lambda'_j e'_{j'}$$

On voit donc que $c_{jj'}$ est un vecteur propre pour l'action de $g$ et sa valeur propre est $\overline{\lambda_j}\lambda'_{j'}$. Comme la famille $(c_{jj'})$ constitue une base de $Hom_{\mathbb{K}}(V,V')$ (puisqu'elle correspond aux matrices élémentaires), on en déduite le caractère de $Hom_{\mathbb{K}}(V,V')$ en $g$ :

$$\sum_{j=1}^{d}\sum_{j'=1}^{d'} \overline{\lambda_j}\lambda'_{j'} = \sum_{j=1}^{d}\overline{\lambda_j}\sum_{j'=1}^{d'}\lambda'_{j'} = \overline{\chi(g)}\chi'(g)$$

□

**Lemme de Schur**

Nous allons présenter ici un lemme majeur de la théorie des représentations :

**Lemme** (De Schur)**.** *Soient $\rho^1 : G \longrightarrow \boldsymbol{GL}_n(E_1)$ et $\rho^2 : G \longrightarrow \boldsymbol{GL}_n(E_2)$ deux représentations irréductibles de $G$ et soit $f$ une application linéaire de $E_1$ dans $E_2$ telle que $\rho_g^2 \circ f = f \circ \rho_g^1$ pour tout $g \in G$. On a alors :*

1. *Si $\rho^1$ et $\rho^2$ ne sont pas isomorphes, on a $f = 0$.*
2. *Si $E_1 = E_2$ et $\rho^1 = \rho^2$ alors $f$ est une homothétie.*

*Démonstration* :

1. On va raisonner par contraposée. Supposons $f$ différente de l'application nulle. Soit $x \in \ker(f)$. On a $f(\rho_g^1(x)) = \rho_g^2(f(x)) = 0$. Ainsi $\rho_g^1(x) \in \ker(f)$, d'où $\ker(f)$ est $G$-stable. De plus, $\ker(f)$ est un sous-espace vectoriel de $E_1$, on pourrait alors lui trouver une supplémentaire dans $E_1$ par le théorème de Maschke. Or $E_1$ est irréductible, donc n'est pas somme directe de sous-espaces. Ainsi, soit $E_1 = \ker(f)$, soit $E_1 = \{0\}$. Le premier cas est exclus car il entrainerait que $f = 0$, on a donc que $\ker(f) = \{0\}$. Ceci prouve que $f$ est un isomorphisme de $E_1$ dans $E_2$ vérifiant $\rho_g^2 \circ f = f \circ \rho_g^1$. Donc $\rho^1$ et $\rho^2$ sont isomorphes.
2. Supposons maintenant que $E_1 = E_2$ et $\rho^1 = \rho^2$. Soit $\lambda$ un valeur propre de $f$. On a son existence car on travaille dans le corps $\mathbb{C}$ des complexes. Posons $j = f - \lambda id$. Puisque $\lambda$ est une valeur propre de $f$, $\ker(j)$ n'est pas trivial et d'autre part, on a $\rho_g^2 \circ j = j \circ \rho_g^1$. Or grâce à la démonstration du point 1), la simultanéité de ces conditions implique que $j = 0$, c'est-à-dire que $f = \lambda id$, donc $f$ est une homothétie. □

## b) <u>En route vers LE théorème</u>

Le but de cette sous partie est d'aboutir à un théorème très puissant et qui nous servira dans la démonstration du théorème d'Hurwitz : « Le nombre de représentations irréductibles de $G$, à isomorphisme près, est égal au nombre de classes de conjugaisons de $G$ »

### i) Notations et définitions

Posons $\mathbb{C}^G$ l'ensemble des fonctions de $G$ à valeurs dans $\mathbb{C}$.

**Définition.** *Soit $f \in \mathbb{C}^G$. On dit que $f$ est une **fonction centrale** si :*

$$\forall g, h \in G, \quad f(hgh^{-1}) = f(g)$$

*On notera dorénavant $FC$ l'ensemble des fonctions centrales.*

À partir de cette définition, nous pouvons faire quelques remarques :

— Les caractères sont des fonctions centrales. En effet, on sait que la trace est stable par conjugaison, *ie*, $Tr(ghg^{-1}) = Tr(h)$ pour tout $g, h \in G$.

— Les fonctions centrales sont constantes sur les classes de conjugaison de $G$.

Nous allons maintenant introduire une notation qui nous servira dans toute cette partie.

Soit $G$ un groupe. Prenons deux fonctions $f, h$ de $\mathbb{C}^G$. On pose alors :

$$\langle f, h \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{f(g)} h(g)$$

On remarque avec aisance que nous sommes en présence d'un produit hermitien sur $\mathbb{C}^G$. En effet $\langle \cdot, \cdot \rangle$ est anti-linéaire en son premier argument, linéaire en son deuxième, hermitien et défini positif. Mais nous nous intéresserons plus au fait que $\langle \cdot, \cdot \rangle$ est un produit hermitien sur l'espace $FC$.

**ii) Invariants**

Ce paragraphe donnera naissance à une proposition qui nous servira bientôt.

Considérons $W$ un $G$-module et le sous-espace suivant, appelé sous-espace des invariants par l'action de $G$ :

$$W^G = \{w \in W,\ \forall g \in G,\ g \cdot w = w\}$$

On donne alors la proposition suivante :

**Proposition.** *Soit $W$ un $\mathbb{K}-$espace vectoriel. Soit $\rho : G \longrightarrow \boldsymbol{GL}_n(W)$ une représentation de $G$. Alors l'endomorphisme suivant :*

$$\pi = \frac{1}{|G|} \sum_{g \in G} \rho_g$$

*est un morphisme de représentations et un projecteur dont l'image est $W^G$.*

<u>*Démonstration*</u> : Soit $w \in W^G$, on a donc :

$$\pi(w) = \frac{1}{|G|} \sum_{g \in G} \rho_g(w) = \frac{1}{|G|} \sum_{g \in G} w = w$$

Et ainsi, $\pi_{|W^G} = id_{W^G}$.

A présent, soit $w \in W$. Alors $\forall h \in G$, on a :

$$\pi \circ \rho_h(w) = \frac{1}{|G|} \sum_{g \in G} \rho_{gh}(w) = \frac{1}{|G|} \sum_{g'} \rho_{g'}(w) = \pi(w)$$

et, de même :

$$\rho_h \circ \pi(w) = \frac{1}{|G|} \sum_{g \in G} \rho_{gh}(w) = \frac{1}{|G|} \sum_{g' \in G} \rho_{g'}(w) = \pi(w)$$

On tient alors que : $Im(\pi) \subset W^G$.

Finalement, de cette inclusion et de l'égalité $\pi_{|W^G} = id_{W^G}$, on a que $\pi^2 = \pi$ et $Im(\pi) = W^G$. □

**Proposition.** *Soient $V$ et $V'$ deux représentations d'un groupe $G$ et soient $\chi$ et $\chi'$ leurs caractères respectifs. On a donc :*

$$\langle \chi, \chi' \rangle = \dim(Hom_{\mathbb{K}}(V, V')^G) = \dim(Hom_{\mathbb{C}G}(V, V'))$$

*où $Hom_{\mathbb{C}G}(V, V')$ est le sous-espace des morphismes de représentation de $V$ vers $V'$.*

*Démonstration* : Étudions plus précisément le projecteur défini à la proposition précédente. On sait que pour un projecteur, son rang est égal à sa trace. Appliquons alors ce projecteur à $W = Hom_{\mathbb{K}}(V, V')$ :

$$\begin{aligned}\dim(Hom_{\mathbb{K}}(V,V')^G) &= rg(\pi)\\ &= Tr(\pi)\\ &= \frac{1}{|G|}\sum_{g\in G}\chi_{Hom_{\mathbb{K}}(V,V')}(g)\\ &= \frac{1}{|G|}\sum_{g\in G}\overline{\chi(g)}\chi'(g)\\ &= \langle\chi,\chi'\rangle\end{aligned}$$

Pour la deuxième égalité, soit $\varphi \in Hom_{\mathbb{K}}(V,V')^G$. Par l'action de $G$ sur $Hom_{\mathbb{K}}(V,V')$, on a : $\rho_{V'}(g)\circ\varphi\circ\rho_V(g^{-1}) = \varphi$. Ce qui est équivalent à : $\rho_{V'}(g)\circ\varphi = \varphi\circ\rho_V(g)$. Ce qui montre que $\varphi$ est un morphisme de représentation (un opérateur d'entrelacement). Ainsi $Hom_{\mathbb{K}}(V,V')^G = Hom_{\mathbb{C}G}(V,V')$, d'où $\dim(Hom_{\mathbb{K}}(V,V')^G) = \dim(Hom_{\mathbb{C}G}(V,V'))$

□

**iii) Orthogonalité**

Nous allons montrer ici un théorème qui sera crucial pour le fameux théorème. Nous allons utiliser les propositions précédente pour le démontrer.

**Théorème.** *Soient $\chi$ et $\chi'$ les caractères de deux représentations irréductibles $V$ et $V'$. Alors :*

$$\langle\chi,\chi'\rangle = \begin{cases} 1 \text{ si } V \text{ et } V' \text{ sont isomorphes}\\ 0 \text{ sinon}\end{cases}$$

*Démonstration* : Précédemment, nous avions montré que $\langle\chi,\chi'\rangle = \dim(Hom_{\mathbb{K}}(V,V')^G) = \dim(Hom_{\mathbb{C}G}(V,V'))$ pour deux représentations $V$ et $V'$ **irréductibles**. Appliquons alors le lemme de Schur à cette relation. On a que si $V$ et $V'$ ne sont pas isomorphes alors le morphisme de représentations est l'application nul, autrement dit, dans ce cas-ci $Hom_{\mathbb{C}G}(V,V') = \{0\}$ et donc $\langle\chi,\chi'\rangle = \dim(Hom_{\mathbb{C}G}(V,V')) = 0$.

Dans l'autre cas, si $V = V'$, autrement dit si elles sont isomorphes, le lemme de Schur nous dit que le morphisme de représentation est une homothétie. Ainsi $Hom_{\mathbb{C}G}(V,V') = Vect(id)$. Donc finalement, $\langle\chi,\chi'\rangle = \dim(Hom_{\mathbb{C}G}(V,V')) = 1$.

□

Ce théorème nous montre donc que l'ensemble formé par les caractères irréductibles, c'est-à-dire l'ensemble des caractères de représentations irréductibles, forme une famille orthonormée dans l'espace FC des fonctions centrales pour le produit hermitien précédemment défini.

**iv) Isomorphes**

Dans cette partie, nous allons discuter des caractères des représentations irréductibles et des représentations isomorphes.

**Théorème.** *Soit $V$ une représentation linéaire de $G$, de caractère $\omega$. Supposons que $V$ se décompose en somme directe de représentations irréductibles : $V = \bigoplus_{i=1}^{k} W_i$.*

*Alors, si $W$ est une représentation irréductible de $G$ de caractère $\chi$, le nombre des $W_i$ isomorphes à $W$ est égal au produit scalaire hermitien : $\langle\omega,\chi\rangle$*

*Démonstration* : Notons $\chi_i$ le caractère de $W_i$. On sait que le caractère d'une somme directe est la somme des caractères. Ainsi : $\omega = \chi_1 + \cdots + \chi_k$.

Alors, $\langle \omega, \chi \rangle = \langle \chi_1, \chi \rangle + \cdots + \langle \chi_k, \chi \rangle$ par bilinéarité du produit hermitien. Or, d'après le théorème d'orthogonalité précédent, on a que $\langle \chi_i, \chi \rangle$ est égal à 1 ou à 0 si $W_i$ est isomorphe ou non à $W$. Ainsi si $\langle \omega, \chi \rangle = m$ alors $\langle \omega, \chi \rangle = m = 1 + 1 + \cdots + 1$ ($m$ fois), qui représente bien le nombre de représentations isomorphes à $W$. D'où le résultat espéré.

□

**Corollaire.** *Avec les notations précédentes, le nombre des $W_i$ isomorphes à $W$ ne dépend pas de la décomposition choisie.*

*Démonstration* : En effet, $\langle \omega, \chi \rangle$ ne dépend pas de la décomposition choisie.

□

Nous arrivons là au théorème de cette sous-partie :

**Théorème.** *Deux représentations sont isomorphes si et seulement si elles ont le même caractère.*

*Démonstration* : Soit $\rho : G \longrightarrow \mathbf{GL}_n(V)$ et $\rho : G \longrightarrow \mathbf{GL}_n(V')$ deux représentations.

$\Longrightarrow$ Supposons $\rho$ et $\rho'$ isomorphes, alors il existe un morphisme de représentation : $\varphi : V \longrightarrow V'$ tel que :

$$\forall g \in G,\ \rho'_g \circ \varphi = \varphi \circ \rho_g \iff \rho'_g = \varphi \circ \rho_g \circ \varphi^{-1}$$

Ainsi à partir de cette égalité, on en tire que :

$$\chi_{\rho'}(g) = \chi_{\varphi \circ \rho \circ \varphi^{-1}}(g) = \chi_\rho(g),\ \forall g \in G$$

On a donc bien $\chi_\rho = \chi_{\rho'}$.

$\Longleftarrow$ Supposons que $\rho$ et $\rho'$ ont le même caractère $\chi = \chi'$. Il existe alors $\alpha_,...,\alpha_h, \beta_1, ...; \beta_h$ et deux isomorphisme tels que : $V \simeq W_1^{\alpha_1} \oplus \cdots \oplus W_h^{\alpha_h}$ et $V' \simeq W_1^{\beta_1} \oplus \cdots \oplus W_h^{\beta_h}$ où les $W_i$ sont des représentations irréductibles. On a alors : $\chi = \alpha_1\chi_1 + \cdots + \alpha_h\chi_h$ et $\chi' = \beta_1\chi_1 + \cdots + \beta_h\chi_h$ où les $\chi_i$ sont les caractères des $W_i$. Or on sait que $\chi' = \chi$ , d'où $\beta_1\chi_1 + \cdots + \beta_h\chi_h = \alpha_1\chi_1 + \cdots + \alpha_h\chi_h$

Ainsi, on a alors $\forall j \in [\![1, n]\!]$

$$\begin{aligned}
&\langle \chi_j, \chi \rangle = \langle \chi_j, \chi' \rangle \\
\iff &\langle \chi_j, \sum_i \alpha_i \chi \rangle = \langle \chi_j, \sum_i \beta_i \chi_i \rangle \\
\iff &\sum_i \alpha_i \langle \chi_j, \chi_i \rangle = \sum_i \beta_i \langle \chi_j, \chi_i \rangle \\
\iff &\sum_i \alpha_i \delta_{ij} = \sum_i \beta_i \delta_{ij} \quad \text{par orthogonalité des caractères} \\
\iff &\alpha_j = \beta_j
\end{aligned}$$

où $\delta_{ij}$ est le symbole de Kronecker.

Ainsi on a finalement, $V \simeq V'$.

□

Ainsi, dans cette sous-partie, nous avons montré que l'étude des représentations se restreignait finalement à l'étude de leurs caractères puisque on peut ainsi déterminer toutes les représentations, à isomorphismes près bien sûr.

**v) Nombre de représentations**

Nous arrivons à la sous-partie finale qui va nous permettre de mettre en place notre théorème majeur pour le démonstration d'Hurwitz.

**Lemme.** *Soit $f \in FC(G)$ et soit $\rho : G \longrightarrow \boldsymbol{GL}_n(V)$ une représentation. On pose :*

$$\rho^f = \frac{1}{|G|} \sum_{g \in G} f(g)\rho_g$$

*Alors :*

1. *$\rho^f$ est un morphisme de représentations.*
2. *Si $V$ est irréductible de caractère $\chi$, alors $\rho^f$ est une homothétie et son rapport est : $\dfrac{\langle \overline{\chi}, f \rangle}{\chi(e)}$, où $e$ est l'élément neutre de $G$.*

<u>*Démonstration*</u> :

1. Pour se faire, montrons que $\rho^f$ commute avec tous les $\rho_h$, $h \in G$. En effet, à l'aide du changement de variable $g = hkh^{-1}$, on obtient :

$$\begin{aligned} \rho^f \rho_h &= \frac{1}{|G|} \sum_{g \in G} f(g)\rho_{gh} \\ &= \frac{1}{|G|} \sum_{k \in G} f(hkh^{-1})\rho_{hk} \\ &= \frac{1}{|G|} \sum_{k \in G} f(k)\rho_h\rho_k \\ &= \rho_h \rho^f \end{aligned}$$

2. Supposons que $V$ est irréductible, alors par le lemme de Schur, $\rho^f$ est une homothétie de rapport $\lambda$. Plus précisément, on a $Tr(\rho^f) = Tr(\lambda id) = \lambda \dim(V)$. Mais encore, on a aussi $Tr(\rho^f) = \sum_{t \in G} f(t) Tr(\rho_t) = \sum_{t \in G} f(t)\chi_\rho(t)$.

   D'où, on trouve finalement : $\lambda \dim(V) = \displaystyle\sum_{t \in G} f(t)\chi_\rho(t) \iff \lambda = \frac{1}{\dim(V)} \sum_{t \in G} f(t)\chi_\rho(t) \iff$

   $\lambda = \dfrac{\langle \overline{\chi}, f \rangle}{\chi(e)}$

□

**Théorème.** *L'ensemble des caractères irréductibles de $G$ forme une base orthonormée de l'espace $FC$ des fonctions centrales.*

<u>*Démonstration*</u> : On a déjà vu que l'ensemble des caractères irréductibles est une famille orthonormée de l'espace des fonctions centrales. Pour montrer que cette famille est génératrice, il suffit de montrer que toute fonction centrale $f : G \longrightarrow \mathbb{C}$ qui est orthogonale à tous les caractères irréductible est nulle.

Soit $f$ une telle fonction. Pour toute représentation $\rho$, on définit $\rho^f$ comme dans le lemme précédent. Si $\rho$ est irréductible, alors par le lemme précédent, $\rho^f$ est une homothétie de rapport $\dfrac{\langle \overline{\chi_\rho}, f \rangle}{\chi_\rho(e)}$. Or $\langle \overline{\chi_\rho}, f \rangle = 0$ puisque $\chi_\rho$ est le caractère de $\rho$ qui est irréductible. Ainsi $\rho^f$ est nul (car

homothétie de rapport nul). Mais encore, si $\rho$ est somme directe de représentations irréductibles, alors en appliquant le lemme précédent à la restriction $\rho_i := \rho_{|V_i}$ de $\rho$ à une composante irréductible $V_i$ de $V$ alors, $\rho_i^f$ est nulle sur chaque composante irréductible de $V$, donc par somme, $\rho^f$ est nulle. Or, par le théorème de Maschke, toute représentation est somme directe de représentations irréductibles. Ainsi $\rho^f$ est toujours nulle.

Ainsi, en particulier, prenons $\rho$ la représentation régulière et calculons $\rho^f(\delta_e)$ :

$$0 = \rho^f(\delta_e) = \frac{1}{|G|}\sum_{g\in G} f(g)\rho_g(\delta_e) = \frac{1}{|G|}\sum_{g\in G} f_g\delta_g$$

Or par indépendance linéaire de $(\delta_g)_{g\in G}$, on a : $f(g) = 0$ pour tout $g$. Donc $f$ est nulle.

□

Voici, finalement, LE théorème tant attendu, qui nous permettra de conclure notre démonstration du théorème d'Hurwitz :

**Théorème.** *Le nombre de représentations irréductibles de $G$, à isomorphisme près, est égal au nombre de classes de conjugaison de $G$.*

*Démonstration* : Soient $C_1, ..., C_k$ les différentes classes de conjugaison de $G$. Dire qu'une fonction est centrale, revient à dire qu'elle est constante sur chacune des $C_1, ..., C_k$. Elle est donc déterminé par ses valeurs $\lambda_i$ sur les $C_i$, lesquelles peuvent être alors choisies arbitrairement. Il en vient donc que la dimension de l'espace FC des fonctions centrales est égale à $k$. Mais d'après le théorème précédent, on a que les caractères irréductibles forment une base de FC. Ainsi la dimension de FC est égale au nombre de caractères irréductibles, c'est-à-dire, au nombre de représentations irréductibles. Donc, pour remettre les choses en bon et due forme, le nombre de classe de conjugaison est égal au nombre de représentations irréductibles.

□

**vi) Somme et dimensions**

Nous allons ici donner juste un petite proposition mais qui est assez puissante :

**Proposition.** *Soit $G$ un groupe fini.*
*Si $n_1, ..., n_k$ sont les degrés des représentations irréductibles $\rho_1, .., \rho_k$ de $G$, on a :*

$$\sum_{i=1}^{k} n_i^2 = |G|$$

*Démontration* : On pose $R$ la représentation régulière de $G$. Alors $\chi_R(1) = |G|$. Plus précisément, si $\rho$ est une représentation irréductible de caractère $\alpha$, on a $\alpha(1) = \deg(\rho)$.

Puis, on sait que une représentation irréductible de caractère $\rho$ est contenue $\deg(\rho)$ fois dans la représentation régulière. En effet, on a vu que le nombre de fois qu'une représentation irréductible de caractère $\chi$ est contenu dans une représentation de caractère $\beta$ est : $\langle\beta, \chi\rangle$. Pour notre cas on a :

$$\langle\chi_R, \chi\rangle = \frac{1}{|G|}\sum_{s\in G}\chi_R(s^{-1})\chi(s) = \chi(1) = \deg(\rho)$$

Ainsi on peut écrire que $R = \bigoplus_{i=1}^{k} n_i\rho_i$ d'où $\chi_R = \sum_{i=1}^{k} n_i\chi_i$ puis finalement en évaluant en 1, on a : $\chi_R(1) = \sum_i n_i\chi_i(1) \iff |G| = \sum_i n_i n_i = \sum_i n_i^2$. □

### 1.2.3 Groupes abéliens

On va donner ici deux petites propositions :

**Proposition.** *Soit $G$ un groupe abélien fini.*
*Le nombre de représentation de degré 1 de $G$ est égal au cardinal de $G$.*

<u>*Démonstration*</u> : En effet, les matrices représentant un groupe abélien fini sont diagonalisables (Lagrange) et commutent entre elles. Elles sont donc diagonalisables simultanément. Ainsi, l'espace de représentation se décompose en somme directe de droite stables pour $G$. Puis par irréductibilité, la dimension et de 1.

Enfin le nombre de représentations irréductibles est égal au nombre de classes de conjugaison, ie au cardinal de $G$, puisque $G$ est abélien. □

**Proposition.** *Soit $G$ un groupe. On a une bijection entre l'ensemble des représentations de degré 1 de $G$ et l'ensemble des représentations de degré 1 de $G/[G,G]$.*

<u>*Démonstration*</u> : On pose $R'$ l'ensemble des représentations irréductibles (donc de degré 1) de $G/[G,G]$ et $R_1$ l'ensemble des représentations de degré 1 de $G$.

Soit $r : G \longleftarrow \mathbb{C}$ un représentation de degré 1 de $G$, alors, $[G,G]$ est trivial pour $r$ et on a un passage au quotient en posant $r' : G/[G,G] \longrightarrow \mathbb{C}$.

Posons $\varphi : R_1 \longleftarrow R',\ r \longmapsto r'$.

Soit maintenant $r''$ une représentation irréductible de $G/[G,G]$, alors, on la prolonge en une application $r : G \longrightarrow \mathbb{C}$ par la surjection canonique. Puis, soit $\psi$ l'applique de qui a $r''$ associe $r$. On vérifie qu'elle va bien de $R'$ dans $R_1$ et que $\varphi$ et $\psi$ sont bien des bijections réciproques l'une de l'autre. □

# Chapitre 2

# Matrices d'Hurwitz

Avant de commencer explicitement la démonstration du théorème d'Hurwitz, donnons à nouveau son énoncé :

**Théorème** (Hurwitz, 1898)**.** *Soit* $\mathbb{K}$ *un corps de caractéristique différente de* 2*. Si*

$$(x_1^2 + x_2^2 + ... + x_n^2)(y_1^2 + y_2^2 + ... + y_n^2) = z_1^2 + z_2^2 + ... + z_n^2 \tag{2.1}$$

*pour tout* $x_1, x_2, ..., x_n, y_1, y_2, ..., y_n$ *dans* $\mathbb{K}$ *et où les* $z_1, z_2, ..., z_n$ *sont des formes bilinéaires sur* $\mathbb{K}$ *dépendant des* $x_i$ *et des* $y_i$ *pour* $i \in [\![1, n]\!]$*, alors* $n = 1, 2, 4$ *ou* 8*.*

Partons de la relation donnée dans le théorème. Il est dit que les $z_k$ sont des formes bilinéaires sur $\mathbb{K}$ qui dépendent de $x$ et $y$. On peut donc écrire :

$$z_k = \sum_{i,j=1}^{n} = a_{ijk} x_i y_j$$

où $a_{ijk}$ est un scalaire.

Nous allons maintenant transformer cette équation sous forme d'équation matricielle. On a alors, pour tout $k \in [\![1, n]\!]$ :

$$\begin{aligned}
\begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_k \end{pmatrix} &= \begin{pmatrix} \sum_{i,j=1}^{n} = a_{ij1} x_i y_j \\ \sum_{i,j=1}^{n} = a_{ij2} x_i y_j \\ \vdots \\ \sum_{i,j=1}^{n} = a_{ijn} x_i y_j \end{pmatrix} \\
&= \begin{pmatrix} \sum_{j=1}^{n} (\sum_{i=1}^{n} a_{ij1} x_i) y_j \\ \sum_{j=1}^{n} (\sum_{i=1}^{n} a_{ij2} x_i) y_j \\ \vdots \\ \sum_{j=1}^{n} (\sum_{i=1}^{n} a_{ijn} x_i) y_j \end{pmatrix} \\
&= \begin{pmatrix} \sum_{i=1}^{n} a_{i11} x_i & \sum_{i=1}^{n} a_{i21} x_i & \cdots & \sum_{i=1}^{n} a_{in1} x_i \\ \sum_{i=1}^{n} a_{i12} x_i & \sum_{i=1}^{n} a_{i22} x_i & \cdots & \sum_{i=1}^{n} a_{in2} x_i \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^{n} a_{i1n} x_i & \sum_{i=1}^{n} a_{i2n} x_i & \cdots & \sum_{i=1}^{n} a_{inn} x_i \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}
\end{aligned}$$

Pratiquons maintenant, une deuxième transformation matricielle. Éudions la matrice de taille $n \times n$ précédemment créée $S$. On va pouvoir l'exprimer comme somme. En effet, on obtient :

$$S = x_1 \begin{pmatrix} a_{111} & a_{121} & \cdots & a_{1n1} \\ a_{112} & a_{122} & \cdots & a_{1n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{11n} & a_{12n} & \cdots & a_{1nn} \end{pmatrix} + x_2 \begin{pmatrix} a_{211} & a_{221} & \cdots & a_{2n1} \\ a_{212} & a_{222} & \cdots & a_{2n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{21n} & a_{22n} & \cdots & a_{2nn} \end{pmatrix} + \cdots + x_n \begin{pmatrix} a_{n11} & a_{n21} & \cdots & a_{nn1} \\ a_{n12} & a_{n22} & \cdots & a_{nn2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1n} & a_{n2n} & \cdots & a_{nnn} \end{pmatrix}$$

Maintenant, il nous est possible de réécrire cette somme sous la forme $S = x_1A_1 + x_2 + \cdots + x_nA_n$, où les matrices $A_p$ sont les matrices définies par : $A_p = (a_{pkj})_{j,k \in [\![1,n]\!]}$. Attention ici au changement d'indices qui provient de la multiplication matricielle.

On a donc finalement, en version matricielle :

$$Z = (x_1A_1 + x_2A_2 + \cdots + x_nA_n)Y = A_xY$$

où $Z = \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix}, Y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$ et $A_x = x_1A_1 + x_2A_2 + \cdots + x_nA_n$ .

Avec ces notations-ci, nous pouvons alors écrire :

$$\begin{aligned} z_1^2 + z_2^2 + ... + z_n^2 &= {}^tZ \cdot Z \\ &= {}^t(A_xY) \cdot A_xY \\ &= {}^tY\ {}^tA_xA_xY \\ &= ({}^tY\ {}^tA_xA_x)Y \end{aligned}$$

Mais encore, le membre de gauche de (2.1) peut aussi s'exprimer de la manière suivante :

$$(x_1^2 + x_2^2 + ... + x_n^2)(y_1^2 + y_2^2 + ... + y_n^2) = \left( \sum_i x_i^2 \right) \cdot {}^tYY$$

Ainsi, en égalisant les deux membres du théorème d'Hurwitz, on obtient :

$$({}^tY\ {}^tA_xA_x) \cdot Y = \left( \left( \sum_i x_i^2 \right) \cdot {}^tY \right) Y$$

Avant de continuer, donnons un petit lemme :

**Lemme.** *Soient $A, B \in \mathcal{M}_n(\mathbb{K})$ deux matrices symétriques. On suppose que pour tout $y$ dans $\mathbb{K}^n$, ${}^t(Ay) \cdot y = {}^t(By) \cdot y$. Alors $A = B$.*

*Démonstration :* Cette démonstration revient à montre que si $\forall y \in \mathbb{K}^n$, ${}^t(Ay)y = 0$ $(*)$ alors $A = 0$. En effet, ${}^t(Ay) \cdot y = {}^t(By) \cdot y \implies {}^t(Ay) \cdot y - {}^t(By) \cdot y = 0 \implies {}^t((A-B)y) \cdot y = 0 \implies A - B = 0 \implies A = B$. Supposons donc que $\forall y \in \mathbb{K}^n$, ${}^t(Ay)y = 0$

On pose $(e_1, ..., e_n)$ la base canonique de $\mathbb{K}^n$. On applique $(*)$ à $y = e_i + e_j$ $\forall i \neq j$. On obtient donc :

$$\begin{aligned} {}^t(A(e_i + e_j)) \cdot (e_i + e_j) &= {}^t(Ae_i + Ae_j)(e_i + e_j) \\ &= {}^t(Ae_i)e_i + {}^t(Ae_i)e_j + {}^t(Ae_j)e_i + {}^t(Ae_j)e_i \\ &= {}^t(Ae_i)e_j + {}^t(Ae_j)e_i \quad \text{par hypothèse} \\ &= a_{ij} + a_{ji} \end{aligned}$$

Ainsi ceci implique que : $\forall i, j,\ a_{ij} + a_{ji} = 0$. Mais comme $A$ est symétrique, on a $a_{ij} = a_{ji}$. Donc $2a_{ij} = 0 \implies a_{ij} = 0\ \forall i, j$. Donc la matrice $A$ est nulle.

En remarquant que les matrices ${}^tA_xA_x$ et $\sum_i x_i^2 Id_n$ sont symétriques, on peut appliquer le lemme précédent à la relation (2.2) et on obtient :

$$ {}^tA_xA_x = \left(\sum_i x_i^2\right) Id_n \tag{2.2}$$

Puis, en développant la partie de gauche de cette relation à l'aide du fait que $A_x = x_1A_1 + ... + x_nA_n$, nous obtenons :

$$ {}^tA_xA_x = \sum_{i=1}^{n} ({}^tA_iA_i)x_i^2 + \sum_{1 \leqslant i < j \leqslant n} ({}^tA_iA_j + {}^tA_jA_i)x_ix_j $$

Ainsi l'équation (2.3) est équivalente au système d'équations suivant :

$$ \begin{cases} {}^tA_iA_i = I_n & \forall i \\ {}^tA_iA_j + {}^tA_jA_i = O & \forall i < j \end{cases} $$

Nous obtenons alors les **équations des matrices d'Hurwitz**. Prouver le théorème d'Hurwitz revient donc à montrer que ces équations de matrices de taille $n \times n$ ne peuvent exister que si $n = 1, 2, 4, 8$. Nous supposerons donc $n > 2$.

Avec le système des équations des matrices d'Hurwitz, on peut remarquer que les matrices $A_i$ sont inversibles d'inverse ${}^tA_i$.

Dorénavant, nous posons : $B_i = A_i\ {}^tA_n$.

Maintenant, on peut montrer que le système des équations des matrices d'Hurwitz est équivalents à :

$$ \begin{cases} B_n = Id_n \\ {}^tB_iB_i = Id_n \\ {}^tB_iB_j + {}^tB_jB_i = O & \forall i < j \end{cases} $$

En prenant $j = n$ dans la troisième équation, on a que ${}^tB_i = -B_i$ pour $i \neq n$. Ainsi les $n-1$ matrices $B_1, ..., B_{n-1}$ satisfont :

$$ {}^tB_i = -B_i \qquad B_i^2 = -Id_n \qquad B_iB_j = -B_jB_i\ \forall i \neq j $$

Ainsi, ce petit lemme final nous lancera sur nos deux démonstrations du-dit théorème ;

**Lemme.** *Soit $E$ un $\mathbb{K}$-espace vectoriel de dimension finie, avec $\mathbb{K}$ de caractéristique différente de 2. S'il existe une paire d'applications inversibles et anti-commutatifs sur $E$, alors la dimension de $E$ est paire.*

*Démonstration* : Supposons qu'il existe $\varphi, \varphi' : E \longrightarrow E$, inversibles et telles que $\varphi\varphi' = -\varphi'\varphi$. Prenons ensuite le déterminant de cette dernière relation : $\det(\varphi)\det(\varphi') = (-1)^{\dim E}\det(\varphi')\det(\varphi)$. Puisque $\varphi$ et $\varphi'$ n'ont pas de determinant nul, étant inversibles, on obtient : $1 = (-1)^{\det E}$.

Puisque la caractéristique de $\mathbb{K}$ est différente de 2, on a que $\dim(E)$ est forcément paire.

□

Ainsi en remarquant que les $B_i$ sont anti-commutatives et inversibles, alors en appliquant le lemme précédent, on voit que $n$ est forcément pair.

Il ne nous reste donc plus qu'à montrer que $n = 2, 4$ ou $8$.

# Chapitre 3

# Démonstration via l'algèbre linéaire

Pour démontrer le théorème d'Hurwitz via l'algèbre linéaire, nous allons avoir besoin d'un certain lemme que nous allons démontrer de suite.

Considérons un entier positif $m$ pair et des matrices $C_1, ..., C_m \in \mathcal{M}_d(\mathbb{K})$. Ces matrices sont 2 à 2 anti-commutatives et pour tout $i$, $C_i^2$ est une matrice diagonale non nulle.

À partir de ces $m$ matrices, nous pouvons construire $2^m$ différents produit de matrices. En particulier, si nous prenons un $m$-uplet $\delta = (\delta_1, \delta_2, ..., \delta_m) \in \{0,1\}^m$, on pose alors :

$$C^\delta = C_1^{\delta_1} ... C_m^{\delta_m}$$

On remarque plus particulièrement qu'il a $2^m$ uplets $\delta$ différents.

**Lemme.** *Avec les notations précédentes, les $2^m$ matrices $C^\delta$ sont linéairement indépendantes dans $\mathcal{M}_d(\mathbb{K})$. En particulier, $2^m \leqslant d^2$ lorsque $m$ est pair.*

*Démonstration* :

Supposons qu'il existe une relation linéaire :

$$\sum_\delta b_\delta C^\delta = O \tag{3.1}$$

où les $b_\delta$ sont dans $\mathbb{K}$ et ne sont pas tous nuls. Considérons cette relation avec le moins possible de $b_\delta$ différents de zéro.

Premièrement, montrons que nous avons $b_{\mathbf{0}} \neq 0$, où $b_{\mathbf{0}} = (0, 0, ..., 0)$. Puisque les $C_i$ anti-commutent et, lorsqu'on élève les $C_i$ au carré on obtient une matrice non nulle, on a que $C^{\delta'} C^{\delta'}$ est une matrice non-nulle pour n'importe quel $\delta$.

Mais encore, si l'on fixe $\delta'$ et que $\delta$ varie, on a :

$$\{C^\delta C^{\delta'} \mid \delta \in \{0,1\}^m\} = \{\lambda C^\delta \mid \delta \in \{0,1\}^m \ et \ \lambda \neq 0\}$$

Puis, prenons un $\delta'$ tel que $b_{\delta'} \neq 0$, multiplions alors (3.1) à droite par $C^{\delta'}$ donne une relation linéaire avec le même nombre de coefficients non-nuls que dans (3.1) mais maintenant, le coefficient de $C^0 = Id$ est non nul.

Ensuite, on montre facilement, grâce à l'anti-commutativité que :

$$C_i C_j C_i^{-1} = \begin{cases} C_j & = & si \ i = j \\ -C_j & = & si \ i \neq j \end{cases}$$

Ainsi par une récurrence, en utilisant la propriété précédente, on a :

$$C_i C^\delta C_i^{-1} = \pm C^\delta \tag{3.2}$$

Maintenant, il faudrait que l'on puisse déterminer le fameux signe $\pm$ ! On peut remarquer que cela dépend du nombre de 1 dans le m-uplet $\delta$. Soit un $\delta \in \{0,1\}^m$, posons alors son *poids* $w(\delta)$ comme étant le nombre de $\delta_i$ valant 1 dans le m-uplet $\delta$. Par exemple, $w(0) = 0$. On obtient alors une version plus précise de l'équation (3.2) :

$$C_i C^\delta C_i^{-1} = \varepsilon_{\delta,i} C^\delta \tag{3.3}$$

avec

$$\varepsilon_{\delta,i} = \begin{cases} (-1)^{w(\delta)} & = \quad si\ \delta_i = 0 \\ (-1)^{w(\delta)-1} & = \quad si\ \delta_i = 1 \end{cases}$$

Ainsi, on peut remarque que $\varepsilon_{0,i} = 1$ pour tout $i$.

Maintenant, choisissons un $i$ entre 1 et $n$ conjuguons (3.1) par $C_i$. A l'aide de (3.3), on a :

$$\sum_\delta \varepsilon_{\delta,i} b_\delta C^\delta = O \tag{3.4}$$

Et comme $\varepsilon_{0,i} = 1$, en soustrayant (3.4) à (3.1), on obtient la relation linéaire suivante :

$$\sum_\delta (1 - \varepsilon_{\delta,i}) b_\delta C^\delta = O \tag{3.5}$$

Dans (3.5) le coefficient du terme pour $\delta = 0$ est 0, alors que nous nous étions arrangé pour qu'il soit non-nul dans (3.1). Par conséquent, (3.5) est une relation linéaire avec moins de termes non-nuls que dans la toute première relation créée. Ainsi, tous les termes dans (3.5) disparaissent et il vient :

$$\delta \neq 0,\ b_\delta \neq 0 \implies \varepsilon_{\delta,i} = 1$$

Et ceci est valable pour tous les $i$ allant de 1 à $n$. Ainsi, chaque $\delta \neq 0$ ayant un coefficient non nul dans (3.1) a un $\varepsilon_{\delta,i}$ indépendant de $i$. Donc $\delta_i$ est indépendant de $i$ par (3.4) et alors $\delta = (1,1,...,1)$. Puis $w(\delta) = m$ donc $\varepsilon_{\delta,i} = (-1)^{m-1} = -1$ puisque$m$ est pair. Mais cela est contradictoire puisque $-1 \neq 1$ dans $\mathbb{K}$. On a donc montré que $b_\delta = 0$ pour tout $\delta \neq 0$, mais la relation linaire (3.1) a juste un terme non nul ce qui est impossible. Donc tous les $b_\delta$ sont nuls et les matrices $C^\delta$ sont libres. □

Retournons à la preuve de notre théorème. En appliquant ce lemme aux matrices $B_1, ..., B_{n-2}$ de $\mathcal{M}_n(\mathbb{K})$, et sachant que $n$ est pair, on utilise l'inégalité obtenue qui nous donne $2^{n-2} \leq n^2$. On vois clairement que pour $n > 2$, l'inégalité est vérifiée pour $n = 4, 6, 8$.

Maintenant, pour éliminer le cas où $n = 6$, nous allons étudier les sous-espaces propres de $B_1$.

Considérons les $B_i$ comme des applications linéaires de $\mathbb{K}^n$. Puisque $B_j^2 = -Id$, les valeurs propres de $B_j$ est $\pm i$. Par suite on définit sur $\mathbb{K}^n$, le produit scalaire standard :

$$\forall x = (x_1, .., x_n), y = (y_1, ..., y_n) \in \mathbb{K}^n,\ \langle x, y \rangle = \sum_i^n x_i y_i$$

Comme ${}^t B_j = -B_j$, on peut dire que $B_j$ est (anti)symétrique donc l'opérateur représenté par $B_j$ est (anti)autoadjoint, ainsi :

$$\langle B_j v, w \rangle = -\langle v, B_j w \rangle \quad \forall v, w \in \mathbb{K}^n$$

Ensuite, si nous posons $E_i = \{v \in \mathbb{K}^n \mid B_1 v = iv\}$ et $E_{-i} = \{v \in \mathbb{K}^n \mid B_1 v = -iv\}$ les sous-espaces propres de $B_1$, on a la décomposition suivante : $\mathbb{K}^n = E_i \oplus E_{-i}$.

Comme $E_i$ et $E_{-i}$ sont des sous-espaces propres, ils sont stables par $B_1$. Puis comme $B_1$ est injective, on a $B_1(E_i) = E_i$ et $B_1(E_{-i}) = E_{-i}$.

Pour plus de généralité, on va montrer que, pour $j = 2, 3, ..., n-1$, $B_j(E_i) = E_{i-1}$ et $B_j(E_{i-1}) = E_i$. En effet, pour $v \in E_i$ :

$$B_1(B_j v) = -B_j(B_1 v) = -B_j(iv) = -iB_j v$$

Ce qui montre que $B_j v \in E_{-i}$ et par suite que $B_j(E_i) \subset E_{-i}$. On pourra montrer de manière similaire que $B_j(E_{-i}) \subset E_i$. Ainsi, par injectivité de $B_j$, on obtient $\dim(E_i) \leqslant \dim(E_{-i})$ et $\dim(E_{-i}) \leqslant \dim(E_i)$. d'où grâce à ces deux inégalités, on a $\dim(E_i) = \dim(E_{-i})$. Enfin grâce à la décomposition de $\mathbb{K}^n$ que nous avions avec les sous-espaces propres, on obtient que $\dim(E_i) = \dim(E_{-i}) = \frac{n}{2}$.

Ensuite pour $j = 2, 3, ..., n-1$, la composition $C_j = B_2 \circ B_j$ est une application linéaire inversible sur $U$. Puis par un rapide calcul, on pourrait montrer $C_3$ et $C_4$ anti-commutent. Ainsi, sur $U$, il existe une paire d'applications linéaires inversibles et anti-commutant, on peut alors appliquer le petit lemme final du chapitre sur les matrices d'Hurwitz qui nous donne que $\dim(E_i) = \frac{n}{2}$ est paire.

Ainsi $2|\frac{n}{2}$, d'où $4|n$. Ceci élimine le choix où $n = 6$. Ainsi $n = 2, 4, 8$. Ce qui prouve le théorème d'Hurwitz.

# Chapitre 4

# Démonstration via la théorie des groupes

Recommençons la démonstration d'une autre manière. Considérons $n > 2$, on va montrer que forcément $n = 4$ ou 8. Considérons le groupe de matrices engendré par les $B_i$ précédemment définies. Ce groupe est constitué des produits matriciels suivants : $\pm B_1^{\alpha_1}...B_{n-1}^{\alpha_{n-1}}$ où $\alpha_i = 0, 1$.

En effet, montrons l'égalité de ces deux ensembles $\pm B_1^{\alpha_1}...B_{n-1}^{\alpha_{n-1}} = \langle B_i \rangle$ par double inclusion :

$\subset$ Puisque $B_i \in \langle B_i \rangle$ alors par définition, $\Pi_i B_i^{\alpha_i}$. Puis on a aussi $-B_i = {}^tB_i = B_i^{-1} \in \langle B_i \rangle$. Ainsi, $B_i^{-1} \cdot -B_i \in \langle B_i \rangle \implies -Id \in \langle B_i \rangle$. On a donc bien, $\pm\Pi_i B_i^{\alpha_i} \in \langle B_i \rangle$.

$\supset$ On va montrer que $\pm B_1^{\alpha_1}...B_{n-1}^{\alpha_{n-1}}$ est un sous-groupe de $GL_n(\mathbb{K})$.

On a alors $(\pm B_1^{\alpha_1}...B_{n-1}^{\alpha_{n-1}})(\pm B_1^{\alpha'_1}...B_{n-1}^{\alpha'_{n-1}}) = \pm B_1^{\alpha_1+\alpha'_1}...B_{n-1}^{\alpha_{n-1}+\alpha'_{n-1}} = \pm B_1^{e_1}...B_{n-1}^{e_{n-1}}$. Or on a que $B_i^2 = -Id$, ainsi $e_i = 0$ ou 1.

Puis on vérifie aussi que $(\pm B_1^{\alpha_1}...B_{n-1}^{\alpha_{n-1}})^{-1} = \pm B_{n-1}^{\alpha_{n-1}}...B_1^{\alpha_1} = \pm B_1^{\alpha_1}...B_{n-1}^{\alpha_{n-1}}$ □

Considérons alors le groupe $G$ engendré par les éléments $g_1, ..., g_{n-1}$ vérifiant :

$$g_i^2 = \varepsilon \neq 1, \quad \varepsilon^2 = 1, \quad g_i g_j = \varepsilon g_j g_i \ \forall i \neq j$$

Tout élément du groupe $G$ est de la forme : $\varepsilon^{a_0} g_1^{a_1} \cdots g_{n-1}^{a_{n-1}}$ avec $a_i = 0, 1$.

On peut de suite remarquer que $\varepsilon$ commute avec tous les $g_i$. Ainsi $\varepsilon \in Z(G)$.

Attention, nous rentrons ici dans la partie clé de la démonstration via la théorie des groupe et des représentations de groupe. Il nous faut démontrer 4 points :

1. $\text{Card}(G) = 2^n$
2. $[G, G] = \{1, \varepsilon\}$
3. Si $g \notin Z(G)$ alors la classe de conjugaison de $g$ est $\{g, \varepsilon g\}$
4. La parité de $n$ implique que $Z(G) = \{1, \varepsilon, g_1...g_{n-1}, \varepsilon g_1...g_{n-1}\}$

Cela dit, le document de Keith CONRAD était dans l'erreur quant au premier. On peut constater que dans la démonstration du premier point faite par K. CONRAD, on voit qu'il a oublié de multiplier une égalité des deux côtés, ce qui faussait la démonstration. Ainsi, mon directeur de TIPE et moi avons modifié et clarifié ces deux points. Ainsi, il nous faut donc concrètement démontrer les 4 points suivants :

1. On a $|G| = 2^n$ si $n$ est impair et $2^n$ ou $2^{n-1}$ si $n$ est pair.
2. $[G, G] = \{1, \varepsilon\}$
3. Si $g \notin Z(G)$ alors la classe de conjugaison de $g$ est $\{g, \varepsilon g\}$

4. La parité de $n$ implique que $Z(G) = \{1, \varepsilon, g_1...g_{n-1}, \varepsilon g_1...g_{n-1}\}$

On va alors démontrer point par point les assertions précédentes.

1. On étudie la relation suivante :

$$\varepsilon^{a_0} g_1^{a_1}...g_{n-1}^{a_{n-1}} = 1$$

On suppose qu'il existe $i \in [\![1, n-1]\!]$ tel que $a_i = 1$ fixé. On multiplie la relation précédente par $g_i$ à droite et on obtient :

$$\varepsilon^{a'_0} g_1^{a_1}...\widehat{g_i}...g_{n-1}^{a_{n-1}} = g_i$$

On sait ensuite que $g_i g_j = \varepsilon g_j g_i$ pour $i \neq j$, ou plus précisément, par récurrence on obtient que

$$(\prod_{k\neq i} g_k^{a_k}) g_i = \varepsilon^{\sum_{k\neq i} a_k} g_i (\prod_{k\neq i} g_k^{a_k})$$

On obtient donc finalement que

$$\varepsilon^{\sum_{k\neq i,j} a_k} = \varepsilon$$

Or $\varepsilon$ est d'ordre 2, ainsi on se place dans $\mathbb{Z}/2\mathbb{Z}$ et on a $\sum_{k\neq i,j} a_k = 1$. On obtient alors un système $(S)$ de $n-2$ équations à $n-2$ inconnues car $j \in [\![1, n-1]\!] \setminus \{i\}$. On suppose alors quitte à renuméroter que $i = n-1$ :

$$(S) \iff \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ 1 & 1 & \ddots & \cdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 1 \\ 1 & 1 & \cdots & 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ \vdots \\ a_{n-2} \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ \vdots \\ 1 \end{pmatrix}$$

On fait l'opération élémentaire sur ce système $L_1 - L_k$ avec $k \neq 1$. Ainsi la première ligne du système devient $10...010...0 = 0$ avec un 1 en première et $k$-ième position, ce qui s'écrit $a_1 + a_k = 0$ d'où $a_1 = a_k$ dans $\mathbb{Z}/2\mathbb{Z}$. Donc tous les $a_i$, $i \in [\![1, n-2]\!]$, sont égaux. Mais il ne sont pas égaux à 0 car sinon le système $(S)$ serait absurde.
On réécrit le système avec $a_k = 1,\ \forall k$ et on obtient la ligne suivante $0 + 1 + ... + 1 = 1$ avec $n-3$ itérations de 1, toujours dans $\mathbb{Z}/2\mathbb{Z}$.

$\longrightarrow$ 1er cas : Si $n$ est impair.
Alors $n-3$ est pair, ce qui est absurde puisque dans $\mathbb{Z}/2\mathbb{Z}$ un nombre de fois pair de 1 vaudrait 0, or $0 \neq 1$. Ainsi, il n'existe pas de $i$ tel que $a_i = 1$. D'où $\forall i,\ 1 \leqslant i \leqslant n-1$, $a_i = 0$ et finalement $\varepsilon^{a_0} = 1 \implies a_0 = 0$.

$\longrightarrow$ 2ème cas : si $n$ est pair.
Alors on peut avoir $a_i = 1$ par un raisonnement similaire que précédemment. On peut donc avoir une relation du type :

$$\varepsilon g_1 g_2...g_i...g_{n-1} = 1$$

avec $a_i = 1$ et $\forall k, a_k = 1$.
Dans ce cas $G = \langle g_1, ..., g_{n-2} \rangle$ puisque $g_{n-1} = \varepsilon g_{n-2}...g_2 g_1$. On se etrouve dans les mêmes conditions avec $n-1$ à l aplace de $n$ et $n-1$ impair.

On peut donc en tirer que tout élément $g$ de $G$ s'écrit $g = \varepsilon^{a_0} g_1^{a_1}...g_{n-1}^{a_{n-1}}$ avec $a_i = 0, 1$ :

— Si $n$ est impair, l'écriture est unique.
— Si $n$ est pair soit l'écriture est unique soit $g = \varepsilon^{a_0} g_1^{a_2} ... g_{n-2}^{a_{n-2}}$ est unique.
On en conclut donc que $\text{Card}(G) = 2^n$ si $n$ est impair et $\text{Card}(G) = 2^n$ ou $2^{n-1}$ si $n$ est pair. □

2. Puisque $n - 1 \geqslant 2$, les propriétés de $G$ nous donne $g_1 g_2 g_1^{-1} g_2^{-2} = g_1 g_2 \varepsilon g_2^{-1} g_1^{-1} = \varepsilon g_1 g_2 g_2^{-1} g_1^{-1} = \varepsilon$. Ainsi puisque $[G, G]$ est le groupe engendré par les commutateurs, on a $[G, G] = \{1, \varepsilon\}$. □

3. En effet, si $g \in Z(G)$ alors $C_g = \{hgh^{-1} \mid h \in G\} = \{ghh^{-1} \mid h \in G\} = \{g\}$
De même si $g \notin Z(G)$ alors on a $C_g = \{hgh \mid h \in G\} = \{hgh^{-1}g^{-1}g \mid h \in G\} = \{[h, g]g \mid h \in G\} = \{g, \varepsilon g\}$ □

4. Soit $g$ un élément du centre de $G$. Celui-ci vérifie alors $gg_i = g_i g$ pour tout $i$. On pose alors $g = \varepsilon^{a_0} g_1^{a_1} ... g_{n-1}^{a_{n-1}}$ avec $a_i = 0, 1$.
En utilisant le fait qu $g_i g_j g_i^{-1} = \varepsilon g_j$, on a :

$$\begin{aligned} gg_i = g_i g &\iff \varepsilon^{a_0} g_1^{a_1} ... g_{n-1}^{a_{n-1}} = g_i \varepsilon^{a_0} g_1^{a_1} ... g_{n-1}^{a_{n-1}} g_i^{-1} \\ &\iff \varepsilon^{a_0} g_1^{a_1} ... g_{n-1}^{a_{n-1}} = \varepsilon^{a_0 + \sum_{j \neq i}^{n-1} a_j} g_1^{a_1} ... g_{n-1}^{a_{n-1}} \end{aligned}$$

Mais puisque $\varepsilon$ est d'ordre 2, alors dans $\mathbb{Z}/2\mathbb{Z}$, on a :

$$g \in Z(G) \iff \sum_{j \neq i}^{n-1} a_j = 0 \ \forall i$$

Ensuite pour $i \neq k$, on a aussi dans $\mathbb{Z}/2\mathbb{Z}$,

$$\sum_{j \neq i}^{n-1} a_j = \sum_{j \neq k}^{n-1} a_j$$

Donc $a_i = a_k$. Et finalement $a_1 = ... = a_{n-1}$ donc $g = \varepsilon^{a_0}$ ou $g = \varepsilon^{a_0} g_1 ... g_{n-1}$. Et comme

$$g \in Z(G) \iff (n-2)a_1 = 0$$

alors le centre possède tous les éléments voulus puisque $n$ est pair. Or si $n$ fut impair, alors le centre de $G$ serait $\{1, \varepsilon\}$. □

Maintenant que nous avons démontré les points importants, nous allons passer dans la théorie des représentations de groupe via deux propositions qui concluront notre démonstration.

**Proposition.** *Soit $G \subset Gl_n$ un groupe tel que $|G| = 2^{n-1}$, $D(G) = \{\pm Id\}$ et $|Z(G)| = 2$ alors $n$ est pair et $n = 2, 4, 8$.*

<u>*Démonstration*</u> : On a vu que pour un tel groupe les classes de conjugaison sont de 2 types : soit $g$ si $g \in Z(G)$ soit $\{g, \varepsilon g\}$ si $g \notin Z(G)$.

On pose ensuite $|Z(G)| = 2^z$.

On va alors comptabiliser le nombre de classes de conjugaison. Il y en a $\frac{2^{n-1} - 2^z}{2}$ pour ceux qui ne sont pas dans le centre et $2^z$ pour ceux du centre. Ainsi on a :

$$\#\text{classes de conjugaison} = \frac{2^{n-1} - 2^z}{2} + 2^z$$

On sait qu'on a exactement $\mathrm{Ind}_G D(G)$ représentation de degré 1. Ainsi, il reste $2^{n-2} + 2^{z-1} - 2^{n-2} = 2^{z-1}$ représentation de degré strictement supérieur à 1.

$\longrightarrow$ Si $z = 1$, alors il reste une représentation de degré supérieur à 1. On pose alors $d$ son degré.

On sait qu'on a, par somme des degré des représentations : $2^{n-2} + d^2 = 2^{n-1} \implies d = 2^{\frac{n-2}{2}}$ avec $n$ par.

On regarde maintenant la représentation naturelle de $G$, notée $V \simeq \mathbb{K}^n$ avec $\mathbb{K}^n = \bigoplus_i V_i$ où les $V_i$ sont des représentations irréductibles de $G$.

Soit $V_i$ une sous-représentation de degré 1 et supposons par l'absurde que $0 \neq v_i \in V_i$. Alors, par hypothèse on a : $(-Id)(v_i) = -v_i$ mais puisque $-Id$ est engendré par $ghg^{-1}h^{-1}$, on a : $ghg^{-1}h^{-1}v_i = \lambda_g\lambda_h\lambda_{g^{-1}}\lambda_{h^{-1}}v_i$. Et comme on est en dimension 1, on est en présence de scalaire qui commutent, ainsi $\lambda_g\lambda_h\lambda_{g^{-1}}\lambda_{h^{-1}}v_i = v_i$. Finalement, $v_i = -v_i \implies v_i = 0$ ce qui est absurde.

Ainsi, $\mathbb{K}^n = kV_0$ avec $V_0$ la seule représentation irréductible de degré $d$. Et en passant à la dimension, on obtient : $n = kd \implies d|n$.

Et finalement, Si $2^{\frac{n-2}{2}}|n$ alors $n = 2, 4, 8$. En effet, si on pose $n = 2^s r$ avec $r \geqslant 1$ impair. Alors,

$$\begin{aligned} 2^{\frac{n-2}{2}}|2^s r &\implies \frac{n-2}{2} \leqslant s \\ &\implies \frac{2^s r - 2}{2} \leqslant s \\ &\implies 2^{s-1} r \leqslant s + 1 \end{aligned}$$

Si $s = 0$ impossible.
Si $s = 1$ alors $r = 1$ et finalement $n = 2^s r = 2$.
Si $s = 2$ alors $r = 1$ et finalement $n = 2^s r = 4$.
Si $s = 3$ alors $r = 1$ et finalement $n = 2^s r = 8$.
Si $s = 4$ impossible.
On a donc bien les cas désirés et cela conclut notre théorème. □

**Proposition.** *Soit $G$ un sous-groupe de $Gl_n$.*
*On suppose que $|G| = 2^n$, $D(G) = \{\pm Id\}$ et $|Z(G)| = 4$ . Alors $n = 2, 4, 8$.*

<u>*Démonstration*</u> : Par un raisonnement similaire que précédemment, on sait qu'il reste $2^{z-1}$ représentations irréductibles de degré supérieur strictement à 1, avec $z = |Z(G)|$.

$\longrightarrow$ Si $z = 2$, on a 2 représentations irréductibles de degré supérieur à 1. Posons $d_1$ et $d_2$ leur degré. On a donc $2^{n-1} + d_1 r + d_2^2 = 2^n \implies d_1^2 + d_2^2 = 2^{n-1}$.

La conclusion de cette démonstration va reposer sur le lemme suivant :

**Lemme.** *Pour $x, y_i n\mathbb{N}$, tel que $x^2 + y^2 = 2^m$ alors :*
— *Si $m$ est pair, alors l'ensemble solution des couples $(x, y)$ est le suivant : $\{\ (2^{\frac{m}{2}}, 0), (0, 2^{\frac{m}{2}})\ \}$*
— *Si $m$ est impair, alors l'ensemble solution des couples $(x, y)$ est : $\{\ (2^{\frac{m-1}{2}}, 2^{\frac{m-1}{2}})\ \}$*

<u>*Démonstration du lemme*</u> : On va le démontrer par récurrence sur $m \in \mathbb{N}$.

Pour $m = 0$, $x^2 + y^2 = 1$ est bien vérifié par $(1, 0)$ et $(0, 1)$.

Pour $m = 1$, $x^2 + y^2 = 2$. On a $x^2 \leqslant 2 \implies 0 \leqslant x \leqslant 1$ et aussi $y^2 \leqslant 2 \implies 0 \leqslant y \leqslant 1$. Donc finalement $x = y = 1$.

On suppose maintenant $m \geqslant 1$. On se place dans $\mathbb{Z}/2\mathbb{Z}$. D'où

$$\begin{aligned} \overline{x}^2 + \overline{y}^2 = \overline{2^m} &\implies \overline{x^2} + \overline{y^2} = 0 \\ &\implies \overline{x} + \overline{y} = 0 \\ &\implies (\overline{x}, \overline{y}) = \{\ (\overline{0}, \overline{0}), (\overline{1}, \overline{1})\ \} \end{aligned}$$

Supposons alors par l'absurde que $(\overline{x}, \overline{y}) = (\overline{1}, \overline{1})$, alors $x$ et $y$ sont impairs.

On regarde l'équation modulo 4. On a $\overline{x}^2 + \overline{y}^2 = \overline{0}$ puisque $m \geqslant 2$. Mais ensuite,comme $x$ et $y$ sont impairs, on a rapidement que $\overline{x}^2 = \overline{y}^2 = \overline{1}$ [4].

Or $\overline{2} = \overline{1} + \overline{1} = \overline{0}$ ce qui est absurde modulo 4.

Finalement, $x$ et $y$ sont pairs et on note $x = 2x'$ et $y = 2y'$. Et donc : $x'^2 + y'^2 = 2^{m-2}$ et donc $x' = y'$. □

Ainsi on a $2^{n-1} + d_1^2 + d_2^2 = 2^n \implies d_1^2 + d_2^2 = 2^{n-1} \implies d_1 = d_2 = 2^{\frac{n-2}{2}}$ par le lemme précédent car $n-1$ est impair.

On peut alors écrire $\mathbb{K}^n = m_1 V_1 \bigoplus m_2 V_2$. Donc si on passe au dimension, on a :

$$n = \dim \mathbb{K}^n = \dim(m_1 V_1) + \dim(m_2 V_2) = (m_1 + m_2) 2^{\frac{n-2}{2}}$$

Ainsi, $2^{\frac{n-2}{2}} | n$. Et on a vu précédemment que $n = 2, 4, 8$. □

On a donc tous les cas possible pour conclure sur la démonstration du théorème d'Hurwitz.

# Chapitre 5

# Ouvertures et questionnements

Après avoir démontrer ce théorème, on peut essayer de l'interpréter de manière plus algébrique et parler plus précisément de corps et groupes.

Partons de l'ensemble des rotations : $\mathcal{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a^2 + b^2 = 1, a, b \in \mathbb{R} \right\}$.

Maintenant on s'intéresse à l'ensemble $\mathbb{C} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ On peut dire que $\mathbb{C}$ est munie d'une addition (celle des matrices) et d'une multiplication celle des matrices. Mais plus encore ...

**Théorème.** $\mathbb{C}$ *est un corps.*

*Démonstration* : On va le montrer un peu grossièrement.

— $\mathbb{C}$ est stable par addition. Plutôt clair par la stabilité des matrices.

— On constate l'écriture suivante :

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \sqrt{a^2+b^2} \frac{1}{\sqrt{a^2+b^2}} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \tag{5.1}$$

Et on pose $R_{a,b} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$

L'écriture (5.1) se décompose en un produit d'un élément de $\mathbb{R}_+$, ie $\sqrt{a^2+b^2}$ que l'on note aussi $||(a,b)||$ et d'un élément de $\mathcal{SO}_2(\mathbb{R})$, ie $\frac{1}{\sqrt{a^2+b^2}} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ ; on reconnait là l'écriture module et argument d'un nombre complexe.

Ainsi, on a, avec la nouvelle écriture : $R_{a,b} \times R_{a',b'} = ||(a,b)|| \cdot ||(a',b')|| R_{\frac{(a,b)}{||(a,b)||}} R_{\frac{(a',b')}{||(a',b')||}}$.

On a donc la stabilité de $\mathbb{C}$ par multiplication puisque $||(a,b)|| \cdot ||(a',b')|| \in \mathbb{R}^+$ et $R_{\frac{(a,b)}{||(a,b)||}} R_{\frac{(a',b')}{||(a',b')||}} \in \mathcal{SO}_2(\mathbb{R})$.

— Puis on a aussi : $R^{-1}_{(a,b)} = ||(a,b)||^{-1} R^{-1}_{\frac{(a',b')}{||(a',b')||}}$ toujours avec un élément de $\mathbb{R}^+$ et $\mathcal{SO}_2(\mathbb{R})$.

Donc $\mathbb{C}$ est aussi stable par inverse. □

Maintenant nous allons suivre les traces de Sir Hamilton sur la création des *Quaternions*.

Prenons le groupe suivant des matrices de rotations complexes :

$$\mathcal{SU}_2(\mathbb{C}) = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \mid |a|^2 + |b|^2 = 1, a, b \in \mathbb{C} \right\}$$

Il faut maintenant noter un différence majeur entre $\mathcal{SO}_2$ et $\mathcal{SU}_2$ :

— $\mathcal{SO}_2 \simeq (a,b) \in \mathbb{R}^2, a^2+b^2=1$. On voit qu'on est sur un cercle et qu'on fait comme une addition d'angle. C'est donc *commutatif.*

— $\mathcal{SU}_2 \simeq a_1^2+a_2^2+b_1^2+b_2^2=1$ Et cette relation N'est PAS *commutative.*

On va alors construire l'ensemble $\mathbb{H} = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \mid a,b \in \mathbb{C} \right\}$

**Théorème.** $\mathbb{H}$ *est un corps non-commutatif.*

<u>*Démonstration*</u> : Comme on a vu précédemment, les éléments de $\mathbb{H}$ ne commutent pas. En effet, si on note les éléments de $\mathbb{H}$ ainsi : $\begin{pmatrix} a_1+ia_2 & -b_1+ib_2 \\ b_1+ib_2 & a_1-ia_2 \end{pmatrix}$ où $a_1,a_2,b_1,b_2 \in \mathbb{R}$.

On peut voir que $\mathbb{H}$ est un $\mathbb{R}$-espace vectoriel de dimension 4 avec pour base les éléments suivants :

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

Et on observe que $i^2=j^2=k^2=-1$ et que $ij=-ji$. D'où la non-commutativité.

— Regardons la multiplication de deux éléments de $\mathbb{H}$ :

$(x+yi+zj+lk)(x'+iy'+z'j+l'k) = (xx'+yy'+zz'+ll')+(xy'+yx'+zl'-tz')i+(...)j+(...)k$

Ce qui donne toujours un élément de $\mathbb{H}$.

— Recherchons un inverse dans $\mathbb{H}$. On rappelle que dans $\mathbb{C}$ : $z^{-1} = \dfrac{\overline{z}}{|z|^2}$ et on peut faire le rapprochement suivant :

$$\overline{z} \leftrightsquigarrow \text{conjugaison}$$
$$|z|^2 \leftrightsquigarrow \text{determinant}$$

Ainsi on pose l'application suivante :

$$N : \mathbb{H} \longrightarrow \mathbb{R}^+$$
$$H_{a,b} = \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \longmapsto \det(H_{a,b}) = |a|^2+|b|^2$$

On remarque que $H_{a,b}H_{a,b}^* = N(H_{a,b})\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = N(H_{a,b})$. Puis, si $H_{a,b} \neq 0$ alors $N(H_{a,b}) \neq 0$ On a finalement

$$H^{-1} = \frac{H_{a,b}^*}{N(H_{a,b})}$$

Autrement dit,

$$(x+yi+zj+lk)^{-1} = \frac{x-yi-zj-lk}{x^2+y^2+z^2+l^2}$$

□

Donc l'important est de remarquer les faits suivants :

1. Dans $\mathbb{C}$, $N(zz') = N(z)N(z')$ d'où

$$(x^2+y^2)(x'^2+y'^2) = (xx'-yy')^2+(xy'+x'y')^2$$

2. Dans $\mathbb{H}$, on a aussi $N(hh') = N(h)N(h')$ d'où

$$(x^2 + y^2 + z^2 + l^2)(x'^2 + y'^2 + z'^2 + l'^2) = (xx' - yy' - zz' - ll')^2 + ...$$

D'où le lien avec le théorème d'Hurwitz.

On peut aussi citer la dernière identité connue sous le nom *d'identité de Degen* :

$$\begin{aligned}(a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 + a_6^2 + a_7^2 + a_8^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2 + b_5^2 + b_6^2 + b_7^2 + b_8^2) = \\ (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 - a_5b_5 - a_6b_6 - a_7b_7 - a_8b_8)^2 + \\ (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3 + a_5b_6 - a_6b_5 - a_7b_8 + a_8b_7)^2 + \\ (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2 + a_5b_7 + a_6b_8 - a_7b_5 - a_8b_6)^2 + \\ (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1 + a_5b_8 - a_6b_7 + a_7b_6 - a_8b_5)^2 + \\ (a_1b_5 - a_2b_6 - a_3b_7 - a_4b_8 + a_5b_1 + a_6b_2 + a_7b_3 + a_8b_4)^2 + \\ (a_1b_6 + a_2b_5 - a_3b_8 + a_4b_7 - a_5b_2 + a_6b_1 - a_7b_4 + a_8b_3)^2 + \\ (a_1b_7 + a_2b_8 + a_3b_5 - a_4b_6 - a_5b_3 + a_6b_4 + a_7b_1 - a_8b_2)^2 + \\ (a_1b_8 - a_2b_7 + a_3b_6 + a_4b_5 - a_5b_4 - a_6b_3 + a_7b_2 + a_8b_1)^2\end{aligned}$$

Je pense qu'il est possible d'ouvrir sur le fait que les cas possibles sont pour $n = 1, 2, 4, 8$. Tout bons mathématiciens voit là le début des puissances de 2. De plus,les cas de ces égalité d'Hurwitz correspondent aux normes des corps des réel (dimension 1), des complexes (dimension 2), des quaternions (dimension 4) et des octonions (dimension 8). Ainsi, je me demande s'il n'y est vraiment pas possible de créer un corps de dimension 16 ou 32 et possédant un norme ainsi...