Compléments d'algèbre

J.J.T

Mai 2026

Kajikazawa in Kai Province, Katsushika Hokusai, 1816

Contents

Préliminaires

On suppose que le lecteur est familier avec les bases de l'algèbre, à savoir les définitions de groupes, anneaux et corps, ainsi que toute la terminologie et propriétés de bases associées aux morphismes entre ces espaces.

Quand il s'agit de parler d'anneaux, le contexte permettra d'identifier de quelles lois de composition internes qu'il s'agit; on se passera, par exemple, d'écrire $(A, +_A, \times_A)$ et on écrira à la place $(A, +, \times)$. On notera toujours $\hom(A, B)$ l'ensemble des morphismes entre deux structures algébriques; s'il s'agit d'anneaux, ce sera des morphismes d'anneaux, des groupes, des morphismes de groupes, etc.

$\overline{x}$ désignera toujours la classe d'équivalence de x, spécifié par le contexte du passage. On s'en passe de spécifier les lois quand elles sont évidentes (Pour GL_n c'est $\times$, $\mathfrak{S}_n$ c'est $\circ$, $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ c'est $\overline{\times}$ également noté $\times$, etc). Si G, F sont deux groupes, on note $\hom(G, F)$ l'ensemble des morphismes de G dans F. L'élément neutre d'un groupe G sera toujours noté e_G. $\mathbb{K}$ désignera toujours les corps $\mathbb{R}$ ou bien $\mathbb{C}$.

Introduction: Pourquoi les groupes?

La théorie des groupes semble être quelque chose de très abstrait dans un premier temps. Mais en réalité, les applications peuvent être très appliquées, riches et diverses. En arithmétique, leur utilité est riche est diverse, d'abord par l'utilisation de groupes quotients pour gérer tout ce qui est en lien avec les congruences,puis par la notion de primalité et divisibilité, mais également pour montrer des théorèmes puissants comme celui des progressions arithmétiques. De plus, la théorie des groupes a été conçue pour montrer que les équations de degré plus de 5 n'ont pas de solution par radicaux (théorie de Galois), et les applications de cette théorie touchent énormément de domaines, de la cryptographie et l'informatique à même la chimie moléculaire.

Bref, la théorie des groupes n'est pas si abstraite que ça. L'idée principale est de conférer une structure minimaliste a un ensemble qui lui donne des propriétés riches.

1 Rappels: Groupes Quotient et premier théorème d'isomorphisme

On se permet d'aller assez vite sur cette partie, supposée acquise par la majorité. A la fin, on corrige de manière expéditive quelques exercices classiques.

1.1 Groupes quotients, sous-groupes distingués et théorème de Lagrange

On attaque dans un premier temps les groupes quotients. L'idée majeure derrière cette construction est d'étendre la notion de congruence dans $\mathbb{Z}$ dans des groupes quelconques.

Proposition 1.1.1 : Soit G un groupe, $H < G$. La relation binaire $\mathcal{G}_H$, appelée relation de congruence à gauche de H et définie sur G est une relation d'équivalence:

$$\forall (x, y) \in G,\ x\mathcal{G}_H y \iff x^{-1}y \in H \iff \exists h \in H, y = xh$$

Remarque: En prenant $n \in \mathbb{N}^*$, $G = \mathbb{Z}$, $H = n\mathbb{Z}$, on obtient $x\mathcal{G}_H y \iff x \equiv y[n]$, d'où l'idée de généraliser les congruences que vous connaissez déjà bien. Puisque G n'est pas forcément abélien, on peut également définir la relation de congruence a a droite de H $\mathcal{D}_H$ de la manière suivante:

$$\forall (x, y) \in G,\ x\mathcal{D}_H y \iff xy^{-1} \in H \iff \exists h \in H, y = hx$$

On justifiera cette appellation bientôt.

Preuve: $\mathcal{G}_H$ est clairement réflexive ($e_G = e_H \in H$) et symétrique (si $h \in H$ alors $h^{-1} \in H$) car H est un groupe. Pour la transitivité, il faut un peu plus de travail. Soit $(x, y, z) \in G$ tel que $x\mathcal{G}_h y$ et $y\mathcal{G}_H z$. Alors:

$$x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$$

Car H est un groupe. □

① **Exercice 1 :** Montrer que $\mathcal{D}_H$ définit une relation d'équivalence sur G.

Qui parle de relation d'équivalences parle de partitions (classes d'équivalence) et de systèmes de représentants. En notant alors les classes d'équivalence induites par $\mathcal{G}_H$ ${}^G/_H$. Déterminons alors la forme des classes d'équivalence sous cette relation d'équivalence:

Proposition 1.1.2 : Soit Ω un système de représentants de ${}^G/_H$, et on note $\overline{g}$ la classe de g pour tout $g \in G$. Alors:

$$ {}^G/_H = \{gH,\ g \in \Omega\}$$

Avec pour tout $g \in G$, $gH = \{gh, h \in H\}$

Preuve: Soit $g \in \Omega$. Alors $x\mathcal{G}_H g$ si et seulement si $xg^{-1} \in H$, c'est a dire que $x \in gH$. Donc $\overline{g} \subset gH$ Réciproquement, si $x \in gH$ alors il existe $h \in H$ tel que $x = gh$, donc $gH \subset \overline{H}$, d'où le résultat. □

① **Exercice 2 :** Qu'en est-il pour $\mathcal{G}_H$?

On peut ainsi en déduire le théorème de Lagrange, fondamental en arithmétique et en théorie des groupes d'une manière générale.

Théorème 1.1.1 : Soit G un groupe fini et $H < G$. Alors $\#H|\#G$.

Preuve: On reprend les notations précédentes, et on pose Ω un système de représentants de ${}^G/_H$. Pour tout $g \in G$, on note $\overline{g}$ la classe d'équivalence à gauche modulo H. Puisque $\mathcal{G}_H$ est une relation d'équivalence, l'union de l'égalité en dessous est disjointe:

$$G = \bigcup_{g\in\Omega} \overline{g} = \bigcup_{g\in\Omega} gH$$

En prenant le cardinal, on en tire que:

$$\#G = \sum_{g\in\Omega} \#(gH)$$

Or, $h \mapsto gh$ est une bijection de H sur gH car g est inversible et les deux ensembles sont finis (il suffit de considérer h^{-1}). Donc $\#H = \#(gH)$ pour tout $g \in G$ et donc pour tout $g \in \Omega$. De ce fait, $\#G = \#H\#\Omega$, d'où le résultat. □

Remarque: Cette démonstration est exactement la même si on utilise $\mathcal{G}_H$ au lieu de $\mathcal{D}_H$. Par ailleurs, dire que H est distingué dans G est équivalent a dire que les relations d'équivalence $\mathcal{D}_H$ et $\mathcal{G}_H$ sont les mêmes.

L'intérêt des groupes quotients est souvent de regrouper dans le sous-groupe une propriété qui ne nous intéresse pas pour notre étude, par exemple $n\mathbb{Z}$ pour $\mathbb{Z}/n\mathbb{Z}$ pour étudier les congruences. Cependant, il est souvent nécessaire de garder les mêmes propriétés et lois induites par le groupe de départ, pour conserver la même structure de groupe. Ainsi, on veut qu'en prenant deux éléments de G/H, disons gH et $g'H$, on ait $gHg'H = gg'H$ afin de retrouver une structure habituelle de groupe. Autrement dit, $\Pi : g \to gH$ est un morphisme de groupes de G dans G/H. Cela n'est pas toujours vrai si G n'est pas abélien.

On rappelle qu'un sous-groupe distingué H dans G vérifie la propriété suivante : $\forall g \in G, gHg^{-1} \subset H$. Les définitions suivantes sont équivalentes :

Proposition 1.1.3 : Soit H distingué dans G, les trois propositions suivantes sont équivalentes :

1. $\forall g \in G, gHg^{-1} \subset H$
2. $\forall g \in G, gHg^{-1} = H$
3. $\forall g \in G, gH = Hg$

Preuve: La seule implication surprenante est $1 \Rightarrow 2$. Montrons la : Soit $g \in G$. $gHg^{-1} \subset H$ et $g^{-1}H(g^{-1})^{-1} = g^{-1}Hg \subset H \Rightarrow H \subset gHg^{-1}$, d'où l'égalité. □

Il existe d'autres propriétés plus générales sur ces groupes distingués que l'on va énumérer ici sans les démontrer :

Proposition 1.1.4 : Soit H sous-groupe de G, f un morphisme de G dans L. On a :

1. Si G abélien, H est distingué dans G.
2. 1 et G sont distingués dans G.
3. $\ker(f)$ est distingué dans G
4. Plus généralement, si K est distingué dans L, alors $f^{-1}(K)$ est distingué dans G
5. Si H est distingué dans G, alors $f(H)$ est distingué dans $f(G)$ (et donc dans L ssi f surjectif)

② **Exercice 3 :** Les démontrer.

Maintenant, revenons à la proposition de départ :

Proposition 1.1.5 : Il existe une loi de groupe tel que Π est un morphisme si et seulement si H est distingué dans G. Cette loi est forcément unique (définie par le morphisme s'il existe).

Preuve: Si une telle loi de groupe existe, alors $ker(\Pi) = \Pi^{-1}(\Pi(1)) = \Pi^{-1}(H) = H$, et donc H est distingué par la propriété du dessus. (Autre manière de le voir : $\forall g \in G, \Pi(gHg^{-1}) = \Pi(g)\Pi(g)^{-1} = \Pi(1) = H \Rightarrow gHg^{-1} \subset H$). Si H est distingué dans G, on vérifie bien que $\Pi(g)\Pi(g') = gHg'H = gg'HH = gg'H = \Pi(gg')$, et donc Π est bien un morphisme de groupes. □

On ne traitera ainsi que de quotients d'un groupe distingué dans l'autre, car ils conservent la structure du groupe. Notons que l'on peut dans tous les cas mener G/H d'une structure de groupe même si H n'est pas distingué, mais elle ne correspondra pas à la structure de groupe induite de G comme vu précédemment.

② **Exercice 4 :** Soit G un groupe fini d'ordre $n \in \mathbb{N}$. Montrer que pour tout $g \in G$, $g^n = e_G$. En déduire le petit théorème de Fermat. (On peut également en déduire le grand, mais la preuve ne rentrera pas dans la marge)

On tombe alors droit dans le vif du sujet en arithmétique, a savoir que $\mathbb{Z}/n\mathbb{Z}$ est un groupe pour l'addition.

② **Exercice 5 :** Montrer que tout groupe d'ordre p premier est isomorphe a $\mathbb{Z}/p\mathbb{Z}$.

③ **Exercice 6 :** Pour $n \in \mathbb{N}^*$, on note $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$ pour $\times$, a savoir les éléments $a \in \mathbb{Z}/n\mathbb{Z}$ tel qu'il existe $y \in \mathbb{Z}/n\mathbb{Z}$ vérifiant $ay = 1$.

1. Montrer que $\left(\left(\mathbb{Z}/n\mathbb{Z}\right)^\times, \times\right)$ est un groupe. On note son ordre $\varphi(n)$.
2. En déduire que pour tout $a \wedge n = 1$, $a^{\varphi(n)} \equiv 1[n]$ (C'est le théorème d'Euler)

Le théorème de Lagrange a pourtant des applications plus générale que ces derniers. En effet, un énoncé équivalent est le suivant:

Théorème 1.1.2 : Soit G un groupe fini et H un sous groupe (pas forcément distingué !) de G. Alors:

$$\#G/H = \frac{\#G}{\#H} \triangleq [G : H]$$

Cet énoncé va être particulièrement utile a plusieurs reprises.

② **Exercice 7 :** Soit G un groupe fini non commutatif. On note $\mathcal{Z}(G) = \{g \in G, \forall x \in G,\ xg = gx\}$. Montrer que $\mathcal{Z}(G) < G$ puis que $[G : \mathcal{Z}(G)] \leq 1/4$.

④ **Exercice 8 :** Soit G un groupe fini non commutatif. On note X, Y deux variables aléatoires indépendantes suivant une loi uniforme sur G. Montrer que $P(XY = YX) \leq 5/8$.

1.2 Premier théorème d'isomorphisme et conséquences

Le premier théorème d'isomorphisme est hors programme, mais pourtant très facile a montrer, très intuitif et surtout très utile. Il s'énonce de la manière suivante:

Proposition 1.2.1 : Soit G, F deux groupes et $\varphi : G \to F$ un morphisme. Alors:

$$G/_{\ker \varphi} \cong \mathrm{Im}(\varphi)$$

Preuve: On pose $\overline{\varphi} : G/_{\ker \varphi} \to \mathrm{Im}(\varphi)$ l'application qui a $\overline{g} \mapsto \varphi(g)$. Alors $\overline{\varphi}$ est un isomorphisme de $G/_{\ker \varphi}$ sur $\mathrm{Im}(\varphi)$. En effet, $\overline{\varphi}$ est un morphisme de groupes car φ l'est, $\ker \varphi$ est un sous groupe distingué de G, et on vérifie rapidement que $\varphi(x * ker(\varphi)) = \varphi(x)$, d'où $\overline{\varphi}$ bien défini. Puisque φ réalise une surjection de G sur $\mathrm{Im}(\varphi)$ on en tire la surjectivité de $\overline{\varphi}$. De plus, $\ker(\overline{\varphi}) = \{\overline{g} \in G/_{\ker \varphi},\ \overline{\varphi}(\overline{g}) = e_F\} = \{\overline{g} = g\ker(\varphi), g \in G, \varphi(g) = e_F\} = \{\overline{g} = \ker\varphi\} = \{\ker(\varphi)\}$, donc $\overline{\varphi}$ est injectif car l'élément neutre de $G/_{\ker \varphi}$ est $\ker(\varphi)$, d'où le résultat. □

$$\begin{array}{ccccccccc}
\{0\} & \longrightarrow & \ker\varphi & \longrightarrow & G & \longrightarrow & G/\ker\varphi & \longrightarrow & \{0\} \\
 & & \downarrow\cong & & \downarrow\cong & & \vdots\exists!\cong & & \\
\{0\} & \longrightarrow & \ker\varphi & \longrightarrow & G & \longrightarrow & \mathrm{Im}\varphi & \longrightarrow & \{0\}
\end{array}$$

(Le graphique au dessus est pour la culture générale!) On remarque que l'on a en quelque sorte forcé l'injectivité de φ en modifiant l'ensemble de départ : si on prend g et g' tel que $\varphi(g) = \varphi(g')$, alors $gg'^{-1} \in \ker(\varphi) \Rightarrow g = g'k, k \in \ker(\varphi) \Rightarrow g\ker(\varphi) = g'\ker(\varphi)$, ainsi il suffit de considérer une congruence par $ker(\varphi)$ pour faire en sorte que dans un nouveau groupe quotient ces deux éléments soient les mêmes. C'est ce que l'on fait à chaque fois que l'on quotiente, et nous allons l'omettre à partir de maintenant.

L'interprétation que l'on doit avoir en tête de ce théorème est que nous pouvons ranger les éléments de G en fonction de leurs images respectives, et surtout que dans le cadre fini, nous avons le même nombre d'éléments qui est renvoyé sur chaque élément de l'image, comme le montre la proposition suivante (cf démo de Lagrange):

Corollaire 1: Soit G un groupe fini, F un groupe et $\varphi \in \hom(G, F)$. Alors pour tout $(y, y') \in \mathrm{Im}(\varphi)^2$, $\#\varphi^{-1}(\{y\}) = \#\varphi^{-1}(\{y'\})$.

Preuve: Pour tout $y \in \mathrm{Im}(\varphi)$, $\varphi^{-1}(\{y\}) = \overline{\varphi}^{-1}(y) \in G/_{\ker \varphi}$, donc est de cardinal égale a celui de $\ker(\varphi)$. □

Corollaire 2: Soit G un groupe fini, F un groupe et $\varphi \in \hom(G, F)$. Alors $\#G = \#\ker\varphi \times \mathrm{Im}\varphi$

Preuve: Il suffit d'appliquer le théorème de Lagrange : on a simultanément :

$$\#\mathrm{Im}\varphi = \#G/_{\ker \varphi} = \frac{\#G}{\#\ker\varphi}$$

□

Ces propriétés sont très générales et nous permettent de montrer des résultats assez surprenants.

② **Exercice 9 :** Soit G, F deux groupes finis. Montrer que s'il existe un morphisme surjectif de G dans F alors $\#F|\#G$. Montrer que s'il existe un morphisme injectif de G dans F alors $\#G|\#F$.

② **Exercice 10 :** Soit G un groupe fini et $\varphi \in \hom(G, G)$. Montrer que $\ker\varphi = \ker\varphi^2$ si et seulement si $\mathrm{Im}\varphi = \mathrm{Im}\varphi^2$.

On va énoncer un lemme crucial pour résoudre des problèmes plus poussés en théorie des groupes finis, le lemme de Cauchy. Il existe beaucoup de démonstrations, mais la suivante qui mobilise le premier théorème d'isomorphisme reste la plus élégante :

Lemme de Cauchy: Soit G un groupe abélien fini d'ordre $n \in \mathbb{N}^*$. Si p est un nombre premier divisant n, alors il existe $g \in G$ d'ordre p.

Preuve: Pour tout $g \in G$, on note $\omega(g)$ son ordre. Soit $X \subset G$ une partie génératrice de G ($X = G$ par exemple). Alors l'application:

$$\phi : \begin{cases} \bigoplus_{x\in X} {}^{\mathbb{Z}}/_{\omega(x)\mathbb{Z}} \to G \\ (n_x)_{x\in X} \mapsto \prod_{x\in X} x^{n_x} \end{cases}$$

Définit un morphisme de groupes surjectif car G est abélien et X le génère. Ainsi, n divise le produit des ordres des éléments de X d'après l'exercice 9. Donc pour tout nombre premier p qui divise n, il y a un élément $x \in X$ tel que $p|\omega(x)$. De ce fait, l'élément $x^{\omega(x)/p}$ est d'ordre p. □

Ce théorème peut en fait être généralisé à n'importe quel groupe même non abélien, mais il faudra attendre l'introduction des actions de groupe pour le prouver.

On utilisera plusieurs fois ce lemme dans le document pour justifier certaines démonstrations, notamment les théorèmes de Sylow, qui sont une sorte de généralisation de ce lemme. On pourra remarquer que ce résultat est une sorte de réciproque faible du théorème de Lagrange.

② **Exercice 11 :** Soit G un groupe abélien d'ordre pq avec p, q deux nombres premiers distincts. Montrer que G est cyclique.

1.3 Groupe dérivé

Il est tentant de se demander comment "abélianiser" un groupe fini quelconque. En effet, on sait bien que les groupes sont beaucoup plus simples quand ils sont abéliens, comme on va le montrer plus tard avec le théorème de structure. Fixons donc un groupe fini G; deux de ses éléments commutent x, y commutent lorsque $xy = yx$ ce qui est équivalent à dire que $xyx^{-1}y^{-1} = e$. On va donc définir une opération sur G qui va mesurer à quelle point G est abélien: pour tout $(x, y) \in G^2$, on note $[x, y] = xyx^{-1}y^{-1}$, appelé commutateur de (x, y). On définit alors le groupe dérivé de G de la façon suivante:

Définition 1.3.1 : Soit G un groupe fini. On note $D(G) = \langle [x, y],\ (x, y) \in G^2 \rangle$. $D(G)$ est alors un sous groupe de G invariant par automorphisme; on dit qu'il est un sous groupe caractéristique de G. En particulier, $D(G) \lhd G$.

② **Exercice 12 :** Montrer ce qui est annoncé dans la définition.

Plus $D(G)$ est petit, plus G est abélien. cette quantification peut être rendu rigoureuse avec la proposition suivante:

Proposition 1.3.1 : Soit G un groupe fini et $H < G$. Alors on a équivalence entre:

1. H contient $D(G)$
2. $H \lhd G$ et ${}^{G}/_{H}$ est abélien.

Preuve: On procède par double implication. Supposons que H contient $D(G)$. Soit $h \in H$. Alors on sait que quelque soit $x \in G$, $xhx^{-1}h^{-1} \in D(G) \subset H$ donc il existe $h' \in H$ tel que $xh = h'hx$. On en tire que $xH \subset Hx$ et donc par argument de cardinal $xHx^{-1} \subset H$ quelque soit $x \in G$, donc $H \lhd G$. Pour montrer que le quotient est abélien, on prend $\overline{x}, \overline{y}$ deux éléments du quotient et on remarque que, puisque $xyx^{-1}y^{-1} \in H$ on a $\overline{xyx^{-1}y^{-1}} = \overline{e}_G$, donc le quotient est bien abélien.

Réciproquement, supposons que $H \lhd G$ et ${}^{G}/_{H}$ est abélien. Alors pour tout $(x, y) \in G^2$ on a bien $\overline{xyx^{-1}y^{-1}} = \overline{e}_G$ dans le quotient donc $D(G) \subset H$. □

On vient donc de montrer que ${}^{G}/_{D(G)}$ est le plus grand quotient abélien de G. L'introduction du groupe dérivé vient en réalité de la question suivante: Si G est un groupe fini, et A un groupe abélien fini, quelles sont les morphismes $\varphi : G \to A$? Soit $\varphi : G \to A$ un tel morphisme. Alors pour tout x, y dans G on a nécessairement $\varphi(xy) = \varphi(yx)$, c'est à dire que $[x, y] \in \ker \varphi$. On en déduit que nécessairement $D(G) \subset \ker \varphi$, à savoir que φ tue au moins $D(G)$.

③ **Exercice 13 :** Soit G un groupe fini et A un groupe abélien fini. Montrer qu'on a une correspondance:

$$\mathrm{Hom}(G, A) \cong \mathrm{Hom}\left({}^{G}/_{D(G)}, A\right)$$

1.4 Des exercices classiques

On traite ici d'une manière générale des exercices qui sont souvent tombé aux oraux X/ENS en algèbre.

Proposition 1.4.1 : On note $\mathbb{F}_p$ le corps $\left({}^{\mathbb{Z}}/_{p\mathbb{Z}}, +, \times\right)$. Soit $n \in \mathbb{N}^*$. Alors:

$$\#\mathrm{GL}_n(\mathbb{F}_p) = \prod_{i=0}^{n-1}(p^n - p^i)$$

Preuve: Il suffit de faire du dénombrement colonne par colonne. Soit $M \in \mathrm{GL}_n(\mathbb{F}_p)$. Alors la première colonne C_1 peut être composé de n'importe quelle manière tant qu'elle n'est pas nulle; on a alors $p^n - 1$ choix. Pour la deuxième, il faut qu'on se place dans $\mathbb{F}_p \backslash \mathrm{vect}_{\mathbb{F}_p}(C_1)$: on a $p^n - p$ choix. En continuant de cette manière pour toute les $n-2$ colonnes restantes, on obtient le résultat souhaité.

Avec le premier théorème d'isomorphisme, on peut même déterminer le cardinal de $\mathrm{SL}_n(\mathbb{F}_p) = \{M \in \mathrm{GL}_n(\mathbb{F}_p),\ \det(M) = 1\}$. En effet, $\det : \mathrm{GL}_n(\mathbb{F}_p) \to \mathbb{F}_p^*$ est un morphisme surjectif de groupes, de noyaux $\mathrm{SL}_n(\mathbb{F}_p)$ (il suffit de considérer les matrices avec un élément x dans le coin en haut a gauche, puis que des 1 sur le reste de la diagonale et des 0 a tout les autres endroits). De ce fait:

$$\mathrm{GL}_n(\mathbb{F}_p)/_{\mathrm{SL}_n(\mathbb{F}_p)} \cong \mathbb{F}_p^*$$

Avec le théoreme de Lagrange on en tire que $\#\mathrm{SL}_n(\mathbb{F}_p) = \dfrac{1}{p-1}\displaystyle\prod_{i=0}^{n-1}(p^n - p^i)$.

② **Exercice 14 :** Je remplie une matrice de taille $n \geq 1$ avec des 1 et des zéros de façon a suivre une loi de probabilité uniforme. Quelle est la probabilité que ma matrice soit inversible?

On peut également parler des résidus quadratiques, un grand classique d'arithmétique des nombres premiers. On pose $\varphi : \mathbb{F}_p^* \to \mathbb{F}_p^*$ le morphisme $x \mapsto x^2$. $\mathbb{F}_p^*$ étant intègre, $\ker\varphi = \{-1, 1\}$ et donc:

$$\mathbb{F}_p^*/_{\{-1,1\}} \cong \{y \in \mathbb{F}_p,\ \exists x \in \mathbb{F}_p^*, y = x^2\}$$

On en tire qu'exactement la moitié des éléments de $\mathbb{F}_p^*$ sont des carrés dans $\mathbb{F}_p^*$. Mais on peut aller plus loin! Introduisons le symbole de Legendre:

$$\forall a \in \mathbb{F}_p^*,\ \left(\frac{a}{p}\right) = \begin{cases} 1 \text{ si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 \text{ sinon} \end{cases}$$

Alors on a le résultat suivant:

Proposition 1.4.2 : On a la formule:

$$\forall a \in \mathbb{F}_p^*,\ a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)[p]$$

Preuve: Quelque soit $a \in \mathbb{F}_p^*$, $a^{(p-1/2)} \in \ker(\varphi)$ définit précédemment, donc $a^{(p-1)/2} \equiv \pm 1[p]$. Si a est un carré, alors $a = x^2$ et donc $a^{(p-1)/2} = x^{p-1} \equiv 1[p]$ par le théorème d'Euler de l'exercice 6. D'autre part, par intégrité de $\mathbb{F}_p^*$, le polynôme $X^{(p-1)/2} - 1$ admet au plus $(p-1)/2$ racines. Or, il y a exactement $(p-1)/2$ racines carrés dans $\mathbb{F}_p^*$, d'où le résultat.

Ce résultat se nomme le critère d'Euler, et on le retrouve souvent aux écrits et oraux des concours.

Terminons ce chapitre avec un dernier type d'exercices classiques, qui donne des stratégies d'étude d'inversibilité dans $\mathcal{M}_n(\mathbb{Z})$.

Soit $(m,n) \in (\mathbb{N}^*)^2$. On note $\pi_m : \mathbb{Z} \to {}^{\mathbb{Z}}/_{m\mathbb{Z}}$ la projection canonique, c'est a dire $\pi_m(a) = \overline{a}$ la classe d'équivalence de a modulo m. On peut alors définir:

$$\Pi_m : \begin{cases} \mathcal{M}_n(\mathbb{Z}) \to \mathcal{M}_n\left({}^{\mathbb{Z}}/_{m\mathbb{Z}}\right) \\ (a_{i,j})_{1\leq i,j\leq n} \mapsto (\pi_m(a_{i,j}))_{1\leq i,j\leq n} \end{cases}$$

Puisque $\left({}^{\mathbb{Z}}/_{m\mathbb{Z}}, +, \times\right)$ est un anneau, il va s'ensuivre que le déterminant est "cohérent" avec cette projection dans une manière bien précise qui est la suivante:

Proposition 1.4.3 : Soit $(m,n) \in (\mathbb{N}^*)^2$. On note $\pi_m : \mathbb{Z} \to {}^{\mathbb{Z}}/_{m\mathbb{Z}}$ la projection canonique. Alors π_m est compatible avec le déterminant sur $\mathcal{M}_n(\mathbb{Z})$, c'est a dire que $\pi_m \circ \det = \det \circ \Pi_m$.

Preuve: π_m est absolument multiplicative et linéaire. Soit donc $A = (a_{i,j})_{1\leq i,j\leq n} \in \mathcal{M}_n(\mathbb{Z})$ On fait alors référence au déterminant:

$$\pi_m(\det(A)) = \pi_m\left(\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma)\prod_{i=1}^{n} a_{i,\sigma(i)}\right) = \sum_{\sigma\in\mathfrak{S}_n} \pi_m(\varepsilon(\sigma))\prod_{i=1}^{n}\pi_m(a_{i,j}) = \det(\Pi_m(A))$$

□

On en tire des façons de montrer que certaines matrices de $\mathcal{M}_n(\mathbb{Z})$ sont des éléments de $\mathrm{GL}_n(\mathbb{R})$. En effet, Soit $A \in \mathcal{M}_{2n}(\mathbb{Z})$ ayant des 0 sur la diagonale et des ± 1 autre part. Alors A est inversible. Il suffit de remarquer que, modulo 2, on a:

$$\Pi_2(A) = \begin{pmatrix} \overline{0} & \overline{1} & \dots & \overline{1} \\ \overline{1} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ \overline{1} & \dots & \dots & \overline{1} \end{pmatrix}$$

Calculons le déterminant de $\Pi_2(A)$. En sommant toutes les colonnes: $C_1 \leftarrow C_1 + C_2 + ... + C_{2n}$, puis pour $i > 1$, $L_i \leftarrow L_i - L_1$:

$$\det(\Pi_2(A)) = \begin{vmatrix} \overline{2n-1} & \overline{1} & \dots & \dots & 1 \\ \overline{2n-1} & \overline{0} & \overline{1} & \ddots & \overline{1} \\ \overline{2n-1} & \overline{1} & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \overline{2n-1} & \overline{1} & \dots & \overline{1} & \overline{0} \end{vmatrix} = \begin{vmatrix} \overline{2n-1} & \overline{1} & \dots & \dots & \overline{1} \\ \overline{0} & \overline{-1} & \overline{0} & \dots & \overline{0} \\ \vdots & \ddots & \ddots & \vdots & \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \overline{0} & \overline{0} & \dots & \overline{0} & \overline{-1} \end{vmatrix} = \overline{(-1)^{2n-1}}\overline{2n-1} = \overline{1}$$

On en déduit que $\det(A) \equiv 1[2]$, donc notamment est non nul.
② **Exercice 15 :** Montrer qu'une matrice de $\mathcal{M}_n(\mathbb{Z})$ ayant que des entiers impaire sur la diagonale et des paires sur la diagonale supérieur ou inférieur est inversible dans $\mathcal{M}_n(\mathbb{R})$.

2 Actions de Groupes

2.1 Que sont les actions de groupes?

En prépa, on étudie les groupes de manière assez isolée comme des ensembles dont les éléments interagissent bien entre eux. Mais en réalité, les groupes ont été conçus dans le but d'intéragir avec d'autres ensembles. Le groupe symétrique $\mathfrak{S}_n$ par exemple découle directement de $[\![1,n]\!]$, et il serait dommage d'étudier $\mathfrak{S}_n$ d'une manière détachée de $[\![1,n]\!]$, car ce groupe intéragit sur les éléments de ce dernier d'une manière très intéressante. Caractérisons cette relation : on peut naturellement définir une application, nommée **action**, de la manière suivante:

$$\Phi : \begin{cases} \mathfrak{S}_n \times [\![1,n]\!] \to [\![1,n]\!] \\ (\sigma, k) \mapsto \sigma(k) \end{cases}$$

Cette application peut être vue comme une opération externe $\cdot$, et donc on peut noter $\Phi(\sigma, k) = \sigma \cdot k$. On remarque alors que $\cdot$ vérifie deux propriétés intéressantes:

i) $e_{\mathfrak{S}_n} \cdot k = k$ pour tout $k \in [\![1, n]\!]$

ii) $\forall (\sigma_1, \sigma_2) \in \mathfrak{S}_n^2$ et $1 \leq k \leq n$, $\sigma_1 \cdot (\sigma_2 \cdot k) = (\sigma_1 \circ \sigma_2) \cdot k$

On va donc essayer de caractériser les groupes G avec qui on peut mettre en lien un tel ensemble X avec une opération externe qui vérifie les mêmes propriétés qu'ici. Il s'avère que cette construction est extrêmement riche.

Définition 2.1.1 : Soit G un groupe et X un ensemble. On dit que G *agit* sur X s'il existe une opération binaire $\cdot : G \times X \to X$ qui satisfait:

1. *i)* $\forall x \in X$, $e_G \cdot x = x$
2. $\forall (g_1, g_2) \in G^2$, $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$

Remarque: Ceci est équivalent a la donnée d'un morphisme $\Phi : G \to \mathfrak{S}_X$. En effet, si G agit sur X alors:

$$\Phi : \begin{cases} G \to \mathfrak{S}_X \\ g \mapsto (x \mapsto g \cdot x) \end{cases}$$

Définit bien un morphisme injectif (il suffit de l'écrire). Cette réécriture s'avère souvent très utile.

Exercice 13: Soit G un groupe fini. Montrer que G agit toujours sur lui même par:

- **Translation**: pour tout $x \in G$ et $q \in G$, $g \cdot x = gx$
- **Conjugaison**: pour tout $x \in G$ et $G \in G$, $g \cdot x = gxg^{-1}$

On en tire le lemme suivant qui nous sera particulièrement utile dans le chapitre suivant:

Proposition 2.1.1 : Soit G un groupe fini d'ordre $n \geq 1$. Alors il existe un morphisme injectif $\phi : G \to \mathrm{GL}_n\left(\mathbb{Z}/2\mathbb{Z}\right)$.

Preuve: Notons $G = \{g_1, g_2, ..., g_n\}$ avec $g_1 = e_G$ et pour $(i, j) \in [\![1, n]\!]$, $i \neq j \Rightarrow g_i \neq g_j$. G agit sur lui même par translations, et on a alors:

$$\phi_1 : \begin{cases} G \to \mathfrak{S}_G \\ g \mapsto (x \mapsto gx) \end{cases}$$

ϕ_1 est un morphisme injectif. Or, on peut naturellement voir que $\mathfrak{S}_G \cong \mathfrak{S}_n$ par le morphisme:

$$\phi_2 : \begin{cases} \mathfrak{S}_n \to \mathfrak{S}_G \\ \sigma \mapsto \tilde{\sigma} \end{cases}$$

Avec $\tilde{\sigma} : G \to G$ définit comme $\tilde{\sigma}(g_i) = g_{\sigma(i)}$ pour tout $i \in [\![1, n]\!]$. ϕ_1, ϕ_2 étant deux morphismes injectifs et ϕ_2 étant de plus un isomorphisme, la composée $\phi_2^{-1} \circ \phi_1 : G \to \mathfrak{S}_n$. On termine la preuve en écrivant:

$$\phi_3 : \begin{cases} \mathfrak{S}_\mathfrak{n} \to \mathrm{GL}_n\left(\mathbb{Z}/2\mathbb{Z}\right) \\ \sigma \mapsto P_\sigma \triangleq (\overline{\delta_{i,\sigma(i)}}) \end{cases}$$

avec $\delta_{i,k} = 1$ si $i = k$ et 0 sinon. ϕ_3 est un morphisme injectif de groupes. On pose alors $\phi = \phi_3 \circ \phi_2^{-1} \circ \phi_1$. □

② **Exercice 16 :** Montrer que ϕ_3 est bien un morphisme de groupes.

Mais cela ne s'arrête pas là ! On peut en déduire des propriétés importantes sur nos groupes en étudiant les ensembles sur lesquels ils agissent naturellement.

2.2 Équation aux classes et applications

Soit G un groupe qui agit sur un ensemble $X \neq \emptyset$. Étant donné un $x \in X$, on notera $\mathcal{O}_x$ son **orbite**, c'est-à-dire son image sous G tout en entier: $\mathcal{O}_x = G \cdot x = \{g \cdot x, g \in G\}$. Il y a des éléments qui "stabilisent" x, c'est-à-dire des éléments $g \in G$ qui vérifient $g \cdot x = x$; ces éléments sont intéressants car ils forment un groupe : en effet, e stabilise tout élément donc stabilise x, et donc cet ensemble est non vide pour tout $x \in X$. De plus, pour tout g_1, g_2 qui stabilisent x, il est évident que $g_1 g_2^{-1}$ stabilise également x. Ainsi, l'ensemble des stabilisateurs de x forme un sous groupe de G; on le note $\mathcal{S}_x$, le **stabilisateur** de x.

La question se pose alors: a x fixé, quand est-ce que $g_1 \cdot x = g_2 \cdot x$? D'après les axiomes, cela serait équivalent a écrire $g_2^{-1} g_1 \in \mathcal{S}_x$; On va donc être amené a regarder les groupes quotients comme on les a introduites a la partie précédente. En effet, posons:

$$\phi : \begin{cases} G \to \mathcal{O}_x \\ g \mapsto g \cdot x \end{cases}$$

Alors $\phi \in \hom(G, \mathcal{O}_x)$ de noyaux $\ker \phi = \mathcal{S}_x$. On aimerait utiliser le premier théorème des isomorphismes, toutefois $\mathcal{O}_x$ n'est pas un groupe ! On peut en fait refaire la même démonstration en remarquant que

$$\overline{\phi} : \begin{cases} {}^{G}/_{\mathcal{S}_x} \to \mathcal{O}_x \\ \overline{g} = (g\mathcal{S}_x) \mapsto g \cdot x \end{cases}$$

est bien définie car les éléments de $\mathcal{S}_x$ ne changent pas la valeur de ϕ, surjective pour la même raison et injective par le fait que comme dans le premier théorème des isomorphismes nous forçons l'injectivité.

Ainsi $\overline{\phi}$ est une bijection, et on a :

$${}^{G}/_{\mathcal{S}_x} \cong \mathcal{O}_x$$

Il faut cependant remarquer que $\mathcal{S}_x$ n'est pas nécessairement distingué, et donc parler de ${}^{G}/_{\mathcal{S}_x}$ comme un groupe n'a pas vraiment de sens.

Ceci va nous être d'une grande utilité dans le chapitre suivant en particulier. Ce résultat est d'une profondeur exceptionnelle et admet des conséquences riches.

Définissions maintenant la relation R telle que pour tout $(x, y) \in X^2$, xRy si leurs orbites sont égales. Il est alors facile de vérifier que ceci est une relation d'équivalence sur G, et donc on peut lui accorder un système de représentants Ω. On a alors:

$$X = \coprod_{x \in \Omega} \overline{x}$$

Or, si $(x, y) \in X^2$ et $y \in \overline{x}$ cela est équivalent a dire que $y \in \mathcal{O}_x$. En effet, Si $y \in \overline{x}$ cela veut dire que $\mathcal{O}_x = \mathcal{O}_y$. En particulier, puisque $e \cdot y = y$, $y \in \mathcal{O}_x$. Réciproquement, si $y \in \mathcal{O}_x$ alors il existe un $\beta \in G$ tel que $\beta \cdot x = y$. Or, $g \mapsto g\beta$ est une bijection de $G \to G$, donc $\mathcal{O}_x = \{(g\beta) \cdot x, g \in G\} = \{g \cdot y, g \in G\}$. Ainsi:

$$X = \coprod_{x \in \Omega} \mathcal{O}_x \Longrightarrow \#X = \sum_{x \in \Omega} \#\mathcal{O}_x$$

Or, d'après le résultat de bijection ci-dessus et le théorème de Lagrange, on en tire que:

Proposition 2.2.1 :

$$\#X = \sum_{x \in \Omega} \frac{\#G}{\#\mathcal{S}_x}$$

C'est un résultat de dénombrement qui est fondamental par la suite qu'on va utiliser librement.

③ **Exercice 17 :** Soit G un groupe non abélien fini. On note $\mathcal{Z}(G) = \{z \in G, \forall g \in G, gz = zg\}$ son centre. Montrer l'existence de $\Theta \subset G$ et $(H_\theta)_{\theta \in \Theta}$ une collection de sous groupes stricts de G telle que:

$$\#G = \#\mathcal{Z}(G) + \sum_{\theta \in \Theta} \frac{\#G}{\#H_\theta}$$

⑤ **Exercice 18 :** Soit p un nombre premier. Montrer que tout groupe d'ordre p^2 est abélien.

On peut maintenant élargir l'énoncé de Cauchy à des groupes finis non abéliens :

Lemme de Cauchy (fort) Soit G un groupe quelconque fini d'ordre $n \in \mathbb{N}^*$. Si p est un nombre premier divisant n, alors il existe $g \in G$ d'ordre p.

Preuve : Cette preuve, très élégante, est un "tour de magie" et cache un peu l'intuition.

Considérons l'ensemble $X = \{(g_1, ..., g_p) \in G^p, g_1 g_2 ... g_p = e_G\}$ et la fonction f permutant les éléments d'un x de X :

$$f : \begin{cases} X \to X \\ (g_1, g_2, ..., g_p) \mapsto (g_p, g_1, ..., g_{p-1}) \end{cases}$$

Cette fonction est bien définie car si $g_1 ... g_p = e_G$, une manipulation algébrique simple donne $g_p g_1 ... g_{p-1} = e_G$. On définit maintenant une action de $\mathbb{Z}$ sur X de la forme :

$$\begin{cases} \mathbb{Z} \times X \to X \\ (n, x) \mapsto f^n(x) \end{cases}$$

On vérifie que cela forme bien une action. On remarque maintenant que les points fixes de f sont les $(g, g, ..., g) \in X$, d'où $g^p = e_G$. Ainsi les orbites de taille 1 sont au nombre de $n_p + 1$, où n_p est ne nombre d'éléments de G d'ordre p, et le 1 représente l'élément neutre.

Soit $x \in X$. On va montrer que si $f^d(x) = x, d \leq p$ minimal, alors $d = 1$ ou $d = p$. En effet, si $f^d(x) = x$ pour $d < p$, alors $1 = kd + k'p$ par Bézout et donc $f(x) = x$ et x est à orbite de taille 1, ce qui prouve le lemme.

Les orbites forment une partition :

$$\#X = n_p + 1 + \sum_{x \in \mathcal{R}} \#\mathcal{O}_x \equiv n_p + 1 \pmod{p}$$

avec $\mathcal{R}$ un ensemble de représentants des orbites de taille p.

De plus, $\#X = (\#G)^{p-1}$ car chaque p-uplet $x \in X$ est parfaitement caractérisé par ses $p-1$ premiers éléments, le dernier doit être l'inverse du produit des $p-1$ premiers. On a enfin

$$(\#G)^{p-1} \equiv 0 \equiv n_p + 1 \pmod{p} \Longrightarrow n_p \geq p - 1$$

ce qui conclut la preuve. □

⑤ **Exercice 19 :** Généraliser l'énoncé du lemme de Cauchy: si G est un groupe d'ordre fini, p un nombre premier et $\alpha \in \mathbb{N}$, montrer que si p^α divise l'ordre de G alors G admet un sous groupe d'ordre p^α. *On pourra raisonner par récurrence sur la taille de G.*

③ **Exercice 20 :** Soit $n \in \mathbb{N}^*$. Montrer que l'on peut définir un action de groupe pour que $\mathbb{Z}/n\mathbb{Z}$ agisse sur $\mathbb{U}_n$. En déduire l'identité de Gauss:

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

Avec φ l'indicatrice d'Euler.

2.3 Formule de Burnside

La formule de Burnside (ou lemme de Burnside suivant les textes) est un résultat puissant de dénombrement. Posons pour tout $g \in G$ $\mathrm{Fix}(g) = \{x \in X, g \cdot x = x\}$ les **fixateurs** de g. Pour dénombrer les fixateurs, on peut considérer:

$$\sum_{g\in G}\mathrm{Fix}(g)=\sum_{g\in G}\sum_{x\in X}[g\cdot x=x]$$

Avec $[g\cdot x=x]$ valant 1 si $g\cdot x=x$ et 0 sinon (c'est la notation d'Iverson). En supposant X et G finis, on peut intervertir les sommes :

$$\sum_{x\in X}\sum_{g\in G}[g\cdot x=x]=\sum_{x\in X}\#\mathcal{S}_x=\#G\sum_{x\in X}\frac{1}{\#\mathcal{O}_x}=\#G\sum_{O\in {}^{X}/_{G}}\sum_{x\in O}\frac{1}{\#O}=\#G\#{}^{X}/_{G}$$

Avec ${}^{X}/_{G}$ l'ensemble des classes d'équivalence pour la relation $x\mathcal{R}y\iff\exists g\in G, g\cdot x=y$, représentant ainsi le nombre d'orbites de X pour cette action. On a donc obtenu une formule pour dénombrer les orbites de l'action :

$$\#{}^{X}/_{G}=\frac{1}{\#G}\sum_{g\in G}\mathrm{Fix}(g)=\#\{orbites\}$$

Concrètement, cette formule nous est utile dans des questions de dénombrement ou il est question de symétrie. Un grand classique est le problème des colliers de Polya : étant donné 6 perles blanches, 3 perles grises et 2 perles noires, combien de colliers différents peut-on faire ? La question est plus difficile que prévu car les colliers sont considérés à rotation et symétrie axiale près, et il faut donc utiliser un groupe particulier représentant les transformations du collier dans le plan, appelé groupe diédral, D_{2n}.

Etude rapide du groupe diédral et application à des problèmes de dénombrement :

D_{2n} correspond au groupe de permutations qui conservent un collier de n éléments dans le plan. Sans rentrer dans les détails complètement hors programme, on peut décrire les $2n$ éléments de ce groupe comme ceci :

1. l'élément neutre e qui correspond à l'identité
2. l'élément c d'ordre n qui correspond à une rotation "élémentaire" du collier
3. les éléments de la forme c^k, qui correspondent à n rotations composées pour $k<n$
4. un élément s d'ordre 2 qui correspond à un "retournement" du collier
5. les éléments de la forme sc^k pour $k<n$

On peut vérifier qu'on a l'identité géométrique suivante : $scs=c^{-1}$, d'où on peut en tirer $sc^ks=c^{-k}$. Remarquons que nous n'avons pas proprement défini le groupe diédral, qui s'écrit comme des éléments de $\mathfrak{S}_n$, mais que nous avons seulement défini la manière dont ces éléments agissent avec le collier, cela suffit.

On peut maintenant définir l'ensemble des colliers X : on peut les définir comme une liste ordonnée de couleurs dans blanc, gris, noir avec nécessairement 6 termes "blanc", 3 "gris" et 2 "noir". (Proprement, on peut les définir comme l'ensemble des fonctions de $[1,12]$ dans {blanc, gris, noir} respectant cette propriété). Un simple exercice de dénombrement donne que $\#X=\binom{11}{2}\binom{9}{3}=4620$, mais on compte beaucoup trop de colliers car un grand nombre d'entre eux ainsi comptés sont les mêmes, par rotation ou "retournement". Ce qu'on souhaite dénombrer est en réalité le **nombre d'orbites de l'action de D_{2n} sur X**. On va donc utiliser la formule de Burnside.

On veut compter le nombre de fixateurs de σ pour chaque σ de D_{2n}. On les énumère :

1. Pour l'élément neutre, chaque élément est un fixateur : $\mathrm{Fix}(g)=4620$
2. Pour les c^k, il faut d'abord observer que c est d'ordre 11, premier : nécessairement par théorème de Lagrange le cardinal du groupe engendré par c^k, sous-groupe de c, divise 11 : c'est donc soit 1 soit 11, et pour $k<n$ c^k est différent de e, donc nécessairement c^k est lui aussi d'ordre 11. On a donc 10 éléments d'ordre 11 de la forme c^k. Un tel collier qui fixerait l'élément c^k fixerait ainsi toutes les rotations sans "retournement", et donc aurait toutes ses couleurs égales. Il n'y a donc pas d'éléments fixant c^k, et son fixateur est vide.

3. Pour les 11 éléments sc^k pour k compris entre 0 et $n-1$, la propriété algébrique $sc^k s = c^{-k}$ nous indique que ces éléments sont tous d'ordre 2. On remarque d'abord que le choix de k est arbitraire, car l'on pouvait définir s comme sc^k qui est bien d'ordre 2 et bien un "retournement" du collier, seulement sur un autre axe. Concentrons-nous donc sur le cas $k = 0$. Le nombre de perles étant impair, une perle est nécessairement fixée : cela doit être la perle grise, car cela est la seule couleur avec un nombre impair de perles (si on fixait une perle d'une couleur paire, alors les perles non fixées de cette couleur seraient de cardinal impair, et on n'aurait pas de symétrie par rapport à l'axe de rotation du collier). Ainsi, toutes les autres perles viennent par paires monochromes préservées par s. Parmi ces 5 paires, une est noire, une est grise, les trois autres sont blanches. Il y a donc $5 * 4 = 20$ colliers différents fixant s : $\forall k, \mathrm{Fix}(sc^k) = 20$

On a donc par la formule de Burnside :

$$\#\{\text{colliers}\} = \frac{1}{\#D_n}(1 * \#X + 10 * 0 + 11 * 20) = 220$$

et il y a donc 220 colliers possibles avec cette configuration de perles.

2.4 p-groupes

Les théorèmes de Sylow sont d'importants théorèmes traitant des groupes finis : ils nous garantissent l'existence de plus grands sous-groupes possibles pour n'importe quel groupe fini. Mêlés à d'autres théorèmes de réduction de groupes (Cauchy, Hall, Schur-Zassenhaus par ordre de difficulté), ils permettent de simplifier l'écriture d'un groupe en plus petits sous groupes et donc simplifier l'étude de groupes.

On considérera dans toute cette section p un nombre premier.

Définition 2.4.1 : Un **p-groupe** est un groupe contenant p^α éléments, avec p premier et α entier naturel.

Ainsi, ${}^{\mathbb{Z}}/_{p^n\mathbb{Z}}$ est un p-groupe.

④ **Exercice 21 :** Montrer que $U_n({}^{\mathbb{Z}}/_{p\mathbb{Z}})$, les matrices triangulaires supérieures de ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$ à coefficients diagonaux égaux à 1 est un p-groupe. (Après avoir lu la partie suivante, en déduire une autre manière de démontrer le premier théorème de Sylow.)

On va maintenant considérer un ensemble X fini sur lequel un p-groupe G agit. On note $\mathrm{Fix}(X) = \{x \in X, \forall g \in G, gx = x\}$ l'ensemble des points fixes de X, c'est-à-dire l'ensemble des éléments de X à orbite réduite à un élément.

Proposition 2.4.1 : $\#X \equiv \#\mathrm{Fix}(X) \pmod p$

Preuve: On rappelle que l'on a $\#\mathcal{S}_x = {}^{\#G}/_{\#\mathcal{O}_x}$ pour tout x de X. De plus, $\#\mathcal{S}_x$ divise $\#G$ par le théorème de Lagrange. Ainsi :

- si $\#\mathcal{S}_x = \#G$, alors $\#\mathcal{O}_x = 1$ et donc $x \in \mathrm{Fix}(X)$. C'est d'ailleurs une équivalence.
- sinon, $\#\mathcal{O}_x \equiv 0 \pmod p$

Donc par les partitions des orbites, $\#X = \#\mathrm{Fix}(X) + \sum_{x\in\mathcal{R}} \#\mathcal{O}_x \equiv \#\mathrm{Fix}(X) \pmod p$ où $\mathcal{R}$ est un système de représentants des orbites non réduites à un élément, donc de cardinal multiple de p.

Cette proposition nous sera utile pour montrer les théorèmes de Sylow.

2.5 Le premier théorème de Sylow

Un p-groupe possède plusieurs propriétés intéressantes que je ne vais pas énoncer car trop loin du programme, mais elles sont utiles pour démontrer les théorèmes de Sylow non prouvés à la fin de ce poly. Il est apparu nécessaire d'étudier les plus grands p-groupes contenus dans un groupe fini, appelés **p-Sylows** .

Définition 2.5.1 : On dit qu'un sous groupe P d'un groupe fini G est un p-Sylow si $\#G = p^\alpha m$ où $p \wedge m = 1$ et $\#P = p^\alpha$.

Remarquons que cette définition correspond bien à l'intuition qu'on peut se faire d'un plus grand p-sous groupe : on ne peut pas créer un p-groupe d'ordre $p^{\alpha+1}$ par théorème de Lagrange. De plus, nous n'avons pas encore prouvé l'existence de ces groupes, il se trouve que non seulement il en existe forcément un, mais de plus il y en a souvent beaucoup.

Théorème 2.5.1 : (Sylow) Il existe un p-Sylow pour tout groupe fini G.

Preuve : Il faut d'abord montrer un lemme qui va nous être bien utile:

Lemme: Soit G un groupe admettant un p-Sylow S. Alors tout sous groupe H de G admet également un p-Sylow de la forme $H \cap gSg^{-1}$ pour un certain $g \in G$.

Preuve du lemme: On note X l'ensemble des classes a gauche de G modulo S. G (respectivement H) agit sur X par translations a gauche; en effet, en posant Ω_G (respecivement Ω_H) un système de représentants de $\mathcal{G}_S$, on a $X = \{\omega S\}_{\omega\in\Omega}$, et:

$$\cdot : \begin{cases} G \times X \to X \\ (g, \omega S) \mapsto ((g\omega)S) \end{cases}$$

définie bien une action de groupes (on définit de manière analogue l'action de H sur S). Soit $\omega S \in X = \overline{\omega}$. Alors le stabilisateur de $\overline{\omega}$ sous l'action de G noté $\mathcal{S}_{\overline{\omega},G}$ (resp. $\mathcal{S}_{\overline{\omega},H}$)est donné par:

$$\mathcal{S}_{\overline{\omega},G} = \{g \in G, (g\omega)S = \omega S\} = \{g \in G, (\omega^{-1}g\omega)S = S\} = \{g \in \omega S\omega^{-1}\} = \omega S\omega^{-1}$$

Et de la même manière, pour l'action de H on a $\mathcal{S}_{\overline{\omega},H} = \omega S\omega^{-1} \cap H$. Or:

$$\#X = \frac{\#G}{\#S} \not\equiv 0[p]$$

On en tire grâce a l'équation aux classes qu'une des orbites de X sous l'action de H est premier a p. On le note $\mathcal{O}$. Soit donc $x \in \mathcal{O}$ et H_x le stabilisateur de x dans H. Alors H_x est de la forme $H \cap gSg^{-1}$ pour un certain $g \in G$ et $[H : H_x] = \#\mathcal{O}$ qui est premier avec p. Donc H_x est un p-Sylow de H de la forme voulue. □

Le corollaire qui va nous être utile est surtout le suivant: Si G est un groupe admettant des p-Sylow alors tout groupe de G en a aussi. Cela va nous permettre de conclure.

Preuve du premier théorème de Sylow: On montre d'abord que $GL_n(\mathbb{Z}/p\mathbb{Z})$ admet un p-Sylow. En effet, on a déjà trouvé son cardinal:

$$\#\mathrm{GL}_n\left(\mathbb{Z}/p\mathbb{Z}\right) = \prod_{i=0}^{n-1}(p^n - p^i) = p^{\frac{n(n-1)}{2}}\prod_{i=0}^{n-1}(p^{n-i} - 1)$$

Ainsi, si $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ admettait un p-Sylow, il serait forcément de cardinal $p^{\frac{n(n-1)}{2}}$. Or:

$$T \triangleq \left\{ \begin{pmatrix} 1 & x_1 & \dots & x_{n-1} \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 \end{pmatrix},\ (x_1, ..., x_{\frac{n(n-1)}{2}}) \in (\mathbb{Z}/p\mathbb{Z})^{\frac{n(n-1)}{2}} \right\}$$

Est un tel p-Sylow. Soit alors G un groupe fini d'ordre $n \geq 1$. Alors on adapte de très peut la démonstration du lemme 1 pour montrer que G s'injecte dans $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$, c'est a dire que G est isomorphe a un certain G' sous groupe de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. Or, ce dernier admettant un p-Sylow on en tire avec le lemme de la démonstration du premier théorème de Sylow que G' admet un p-Sylow H. On considérant l'isomorphisme réciproque on conclut. □

2.6 Exercices

On vous propose ici quelques exercices appliquant tous les éléments de cette dernière partie.

② **Exercice 22 :** On appelle **exposant** d'un groupe G le plus petit entier $n \geq 1$ tel que $\forall g \in G, g^n = 1$. Montrer qu'un groupe d'exposant 2 est abélien.

③ **Exercice 23 :** On appelle **indice** d'un sous-groupe H de G la donnée $\#{}^{G}/_{H}$ si elle est non infinie. Montrer que H est distingué dans G si l'indice de H est égal à 2.

③ **Exercice 24 :** On dit qu'un groupe G est **cyclique** d'ordre n s'il existe un g tel que G est engendré par g, et que le plus petit entier k tel que $g^k = e_G$ est n.

1. Montrer que pour tout x de G, $\exists k \leq n, g^k = x$
2. Montrer que g^d est d'ordre $\frac{n}{n \wedge d}$.

③ **Exercice 25 :** Soit G un groupe cyclique d'ordre n. On appelle $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G. Montrer que $\mathrm{Aut}(G)$ est en bijection avec $({}^{\mathbb{Z}}/_{n\mathbb{Z}})^\times$

② **Exercice 26 :** Montrer que tout sous-groupe distingué H dans G est le noyau d'un morphisme de groupes.

② **Exercice 27 :**

1. Décrire les sous-groupes de $\mathbb{Z}$, puis les sous-groupes non denses de $\mathbb{R}$.
2. Décrire les morphismes surjectifs de $(\mathbb{Q}, +)$ dans $(\mathbb{Q}, \times)$

③ **Exercice 28 :** Quel est le cardinal minimal d'un groupe non abélien ?

⑤ **Exercice 29 :** On va déterminer les n tels que $({}^{\mathbb{Z}}/_{n\mathbb{Z}})^\times$ sont cycliques, et déterminer plein de résultats intéressants pendant.

1. D'abord, on montre que pour $\mathbb{K}$ corps, tout sous-groupe fini de $\mathbb{K}^\times$ est cyclique.
   (a) Montrer le cas $\mathbb{K} = \mathbb{C}$ avec le sous-groupe $\mathbb{U}_n$.
   (b) Montrer que si G groupe et $x, y \in G$ deux éléments qui commutent, d'ordres finis a et b avec $a \wedge b = 1$, alors xy est d'ordre ab.
   (c) Soit $G \subset \mathbb{K}^\times$ un sous-groupe fini, montrer l'égalité dans $\mathbb{K}[X]$:
   $$X^{\#G} - 1 = \prod_{g \in G} (X - g)$$
   (d) Pour $\#G = p_1^{n_1} p_2^{n_2} ... p_r^{n_r}$, montrer qu'il existe un élément d'ordre $p_i^{n_i}$. (Difficile, on utilisera la question précédente)
   (e) Conclure sur le fait que G est cyclique.
2. Puis on montre des propriétés arithmétiques sur les premiers :
   (a) Soit $k \geq 0$ un entier. Montrer que si p nombre premier impair, alors :
   $$(1+p)^{p^k} \equiv 1 + p^{k+1} [p^{k+2}]$$
   Montrer également
   $$(1+4)^{2^k} \equiv 1 + 2^{k+2} [2^{k+3}]$$
   (b) Soit p premier impair et $m \geq 1$. Montrer que le groupe $({}^{\mathbb{Z}}/_{p^m\mathbb{Z}})^\times$ est cyclique.
   (c) Soit $m \geq 2$. Montrer qu'on a $({}^{\mathbb{Z}}/_{2^m\mathbb{Z}})^\times \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{2^{m-2}\mathbb{Z}}$. On trouvera un isomorphisme adapté par la question a.
3. Conclure.

⑤ **Exercice 30 :** Soit $n \in \mathbb{N}^*$.

1. Montrer que pour out p premier et $(A, B) \in \mathcal{M}_n(\mathbb{Z})$, $\mathrm{Tr}((A+B)^p) \equiv \mathrm{Tr}(A^p) + \mathrm{Tr}(B^p)[p]$
2. En déduire que pour tout $A \in \mathcal{M}_n(\mathbb{Z})$ et p premier, $\mathrm{Tr}(A^p) \equiv \mathrm{Tr}(A)[p]$
3. On pose $u_0 = 3, u_1 = 0$ et $u_2 = 14$, et on pose pour tout $n \in \mathbb{N}$, $u_{n+3} = 7u_{n+1} - 6u_n$. Montrer que pour tout nombre premier p, $p|u_p$.

3 Initiation à la théorie des représentations

La théorie des représentations peut sembler, dans un premier temps, comme une théorie parachuté un peu de nul part. Cela est dommage, car en réalité il est assez facile à motiver une fois qu'on a bien saisi l'esprit des morphismes entre structures algébriques. Avant d'expliquer cette philosophie, montrons un théorème connu qui va venir illustrer notre propos.

3.1 Théorème de structure des groupes abéliens finis

On note G un groupe abélien fini (gaf) et $\widehat{G} = \hom(G, \mathbb{C}^*)$ son dual, dont on va appeler les éléments *caractères* de G. L'exercice suivant montre quelques propriétés élémentaires de $\widehat{G}$. La théorie des caractères est fondamentale, et nous donne une premier point de vue de la théorie des représentations des groupes finis. Cette théorie va nous permettre de montrer lé théorème de structure des groupes abéliens finis, qui effectivement conclut quant a leur nature. Elles sont par ailleurs essentiels pour démontrer le théorème de progression arithmétique de Dirichlet.

② **Exercice 31 :** Soit χ un caractère de G. Montrer que $\mathrm{Im}(\chi) = \mathbb{U}_d$ pour un certain $d \in \mathbb{N}^*$, et montrer que $(\widehat{G}, \times)$ est un groupe.

On va montrer que G est en réalité isomorphe à son dual. Pour le montrer, il faut d'abord traiter le cas où G est cyclique, qui est assez facile.

② **Exercice 32 :** Soit G un groupe cyclique d'ordre n, et g un générateur de G. Montrer successivement que:

1. Pour $\omega \in \mathbb{U}_n$, la formule $\chi_\omega(g^k) = \omega^k$ définit un caractère de G;
2. On a $\widehat{G} = \{\chi_\omega,\ \omega \in \mathbb{U}_n\}$;
3. $\omega \to \chi_\omega$ est un isomorphisme de $\mathbb{U}_n$ sur $\widehat{G}$.

Et en déduire que $G \cong \widehat{G}$.

Le lemme suivant montre que le passage au dual est "multiplicatif":

Proposition 3.1.1 : Soit G_1, G_2 deux gaf. Alors $\widehat{G_1 \times G_2} \cong \widehat{G_1} \times \widehat{G_2}$

Preuve: Pour tout $(\chi_1, \chi_2) \in \widehat{G}_1 \times \widehat{G}_2$, on note $\chi_1 \otimes \chi_2 : G_1 \times G_2 \to \mathbb{C}^*$ l'application:

$$(\chi_1 \otimes \chi_2)(g_1, g_2) = \chi_1(g_1)\chi_2(g_2)$$

Alors $\psi : \widehat{G}_1 \times \widehat{G}_2 \to \widehat{G_1 \times G_2}$, $(\chi_1, \chi_2) \mapsto \chi_1 \otimes \chi_2$ est un isomorphisme de groupes (regarder sur $G_1 \times \{e_2\}$ et $\{e_1\} \times G_2$) □

On va maintenant énoncer, puis démontrer, le théorème de structure des groupes abéliens finis, qui est un des grands piliers de la théorie des groupes. Il nous permet de complètement comprendre la structure générale des groupes abéliens finis, et ses applications vont êtres immédiates.

Théorème 3.1.1 : de structure des gaf Soit G un gaf. Alors il existe $r \in \mathbb{N}^*$ et $d_1, ..., d_r$ des entiers naturels tel que $d_1|d_2|...|d_r$ et:

$$G \cong {}^{\mathbb{Z}}/_{d_1\mathbb{Z}} \times ... \times {}^{\mathbb{Z}}/_{d_r\mathbb{Z}}$$

Preuve: Pour se faire, il va falloir montrer deux lemmes capitaux et classiques de la théorie des groupes.

Lemme 1: Soit G un gaf et $H < G$. Alors tout caractère de H se prolonge en un caractère de G.

Preuve: Soit χ un caractère de $H < G$. Si $H = G$ il n'y a rien à dire. Sinon, prenons $x \in G \backslash H$ et notons $K = \langle H, x\rangle = \{x^k h,\ h \in H\}$. On va prolonger χ en un caractère de K et en itérant le processus un nombre fini de fois, on finira par avoir prolongé χ sur G tout en entier.

Un caractère χ' prolongeant χ sur K est défini uniquement par $\chi'(x)$ car il coïncide avec χ sur H. La difficulté repose sur le fait que la définition de χ' doit absolument être cohérente avec celle de χ, ce qui nous conduit à considérer $\{k \in \mathbb{Z},\ x^k \in H\}$. C'est un sous groupe non trivial de $\mathbb{Z}$ car $x^{|G|} \in H$ d'après Lagrange et est donc de la forme $m\mathbb{Z}$ avec $m \geq 2$. Posons $\gamma = \chi(x^m)$ et on choisit un $\alpha \in \mathbb{U}$ tel que $\alpha^m = \gamma$. On définit alors χ' pour tout $h \in H$ et $k \in \mathbb{Z}$:

$$\chi'(x^k h) = \alpha^k \chi(h)$$

On vérifie que cela définit bien un caractère compatible avec la définition de χ. En faisant une descente finie sur le cardinal de G on a le résultat. □

On va vouloir montrer le théorème 4 par récurrence sur le cardinal du gaf. Pour ce faire, il faut commencer quelque part ; montrons donc le lemme suivant, qui est un classique de X/ENS:

Lemme 2: Soit G un gaf. Alors il existe $x \in G$ tel que l'ordre de x soit $\exp(G)$.

Preuve: Pour tout $G \in G$, on note $\omega(g)$ l'ordre de g. Montrons d'abord que si u, v sont deux éléments de G tels que $\omega(u) \wedge \omega(v) = 1$, alors $\omega(uv) = \omega(u)\omega(v)$. En effet, on considère $g \in \langle u\rangle \cap \langle v\rangle$. Alors $\langle g\rangle$ est un sous groupe de $\langle u\rangle$ et $\langle v\rangle$ donc l'ordre de g divise à la fois celui de u et v, et donc leur PGCD. On en tire que $g = e$, et donc pour tout $(k, p) \in \mathbb{Z}^2$, $u^k \neq v^p$ sauf si $u^k = v^p = e$.

On a alors $(uv)^k = u^k v^k = e$ si et seulement si $u^k = v^{-k}$, ce qui est possible si et seulement si $u^k = v^{-k} = e$, donc $\omega(u)|\omega(uv)$ et $\omega(v)|\omega(uv)$. Les deux étant premiers entre eux, on en tire que $\omega(u)\omega(v)|\omega(uv)$. Or, puisque $(uv)^{\omega(u)\omega(v)} = 1$ on a $\omega(uv)|\omega(u)\omega(v)$, d'où le résultat.

Montrons désormais le lemme. Soit $x \in G$ d'ordre maximal. Il faut montrer que l'ordre de tout $y \in G$ divise celui de x. Fixons $y \in G$ et notons $n = \omega(x)$ et $m = \omega(y)$. Il s'agit de montrer que pour tout nombre premier p, $v_p(m) \leq v_p(n)$. Ainsi, pour p fixé, on note $m = p^a r$ et $n = p^b s$ avec $p \wedge r = p \wedge s = 1$. Alors x^{p^b} est d'ordre s et y^r est d'ordre p^a. Avec ce qu'on vient de montrer, on a alors $\omega(x^{p^b} y^r) = p^a s \leq p^b s$ par hypothèse de la maximalité de l'ordre de x. Donc $a \leq b$, d'où le résultat. □

Nous sommes désormais armés pour montrer le 3.1.1.

On raisonne par récurrence sur la taille de G. Si $|G| = 1$ ou $|G| = 2$ c'est évident. Supposons alors que la propriété est vérifiée pour tout groupe de taille $1, 2, ..., n-1$ et prenons G un groupe de cardinal n, $n \geq 3$. Alors il existe $y \in G$ tel que son ordre soit l'exposant de G. On note $\omega(y) = m$ et H le groupe engendré par y. Soit $\tilde{\chi}$ un caractère bijectif de H sur $\mathbb{U}_m$ que l'on prolonge en un caractère χ de G. On va montrer que:

$$G \cong H \times \ker \chi$$

On pose donc $\phi : H \times \ker(\chi) \to G$ qui à (h, k) associe hk. Alors ϕ est injectif. En effet, si $hk = e$ alors $k \in H \cap \ker(\chi) = \{e\}$ car on a supposé $\chi_{|H}$ bijectif. Donc $h = k = e$. χ est injectif.

Pour montrer que χ est surjectif, on remarque que puisque l'ordre de tout élément de G divise m χ est à valeurs dans $\mathbb{U}_m$. Or, puisque $\chi_{|H}$ est un isomorphisme, on en tire que les $(h \ker \chi)_{h \in H}$ forment une partition de G par le premier théorème d'isomorphisme, d'où le résultat.

Donc $|\ker(\chi)| = |G|/|H| < n$, donc il existe $r \geq 2$ et $d_1|...|d_{r-1}$ tel que:

$$G \cong {}^{\mathbb{Z}}/_{d_1\mathbb{Z}} \times ... \times {}^{\mathbb{Z}}/_{d_{r-1}\mathbb{Z}} \times H \cong {}^{\mathbb{Z}}/_{d_1\mathbb{Z}} \times ... \times {}^{\mathbb{Z}}/_{d_{r-1}\mathbb{Z}} \times {}^{\mathbb{Z}}/_{m\mathbb{Z}}$$

Par cette isomorphisme, on peut exhiber un élément $g \in G$ pour lequel l'élément correspondant dans le produit ci-dessus soit $(0, ..., 1, 0)$ donc d'ordre d_{r-1}, donc $d_{r-1}|m$, d'où le résultat. □

Grâce à 3.1.1, on en tire que $G \cong \widehat{G}$. En effet:

Proposition 3.1.2 : Soit G un gaf. Alors $G \cong \widehat{G}$. En particulier, $|G| = |\widehat{G}|$.

Preuve: On applique la proposition 3.1.1 et le théorème 3.1.1:

$$\widehat{G} \cong \widehat{\mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_r\mathbb{Z}} \cong \widehat{\mathbb{Z}/d_1\mathbb{Z}} \times ... \times \widehat{\mathbb{Z}/d_r\mathbb{Z}} \cong \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_r\mathbb{Z} \cong G$$

D'où le résultat. □

La démonstration ci dessus devrai être médité dessus; c'est peut être le premier exemple que le lecteur voit, sans comprendre réellement, la profondeur et l'ampleur de la théorie des morphismes. L'intérêt des morphismes est de pourvoir transporter le structure d'un groupe, quelque chose de très générale, sur une autre structure algébrique avec une perte minimale d'information. Un isomorphisme est alors la même chose qu'un transfert de structure avec 0 perte d'information. Ici, on a essayé de limiter les dégâts en transportant la plus grande des roues dans la décomposition en produit cycliques de G sur $\mathbb{C}$ afin de mieux comprendre sa structure entière, car on maitrise parfaitement ce dernier. C'est la philosophie générale derrière la théorie des représentations: on va transporter le groupe sur un espace vectoriel afin de comprendre sa structure géométrique.

④ **Exercice 33 :**

1. Soit G un gaf et $m \geqslant 1$ un diviseur de $|G|$. Montrer que G admet un sous groupe d'ordre m.

2. Le résultat subsiste-t-il si l'on suppose G seulement fini?

④ **Exercice 34 :**

1. Soit p un nombre premier et $n \geqslant 1$. Montrer que $\mathrm{Aut}\left(\mathbb{Z}/p^n\mathbb{Z}\right) \cong \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$, et que ce dernier est cyclique d'ordre $p^{n-1}(p-1)$ lorsque p est impair, et isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$ lorsque $p = 2$.

2. En déduire le critère de cyclicité établit à l'exercice 29.

③ **Exercice 35 :**

1. Soit G un gaf. Montrer que G est cyclique si et seulement si pour tout $n \geqslant 1$, le nombre d'éléments de G d'ordre divisant n est d'au plus n.

2. En déduire que si $\mathbb{K}$ est un corps commutatif alors tout sous groupe fini de $\mathbb{K}^\times$ est cyclique.

3.2 Théorème de Maschke

Définition 3.2.1 : Soit G un groupe. On appelle représentation de G tout couple (V, ρ) avec V un $\mathbb{C}$-espace vectoriel et $\rho : G \to \mathrm{GL}(V)$ un morphisme de groupes. On appel alors la dimension de la représentation la dimension de V.

La théorie de représentations peut se faire sur un corps quelconque, mais dans nos énoncés il sera toujours sous entendu que les représentations se font sur le corps des complexes $\mathbb{C}$, qui présente l'avantage d'être algébriquement clos et de caractéristique nulle. On regardera néanmoins des exercices ou on regarde ce qui se passe lorsqu'on change cette hypothèse.

Cette définition est équivalente à la donné d'une action de groupe de G sur V qui agit linéairement par rapport à ce dernier. L'intérêt et de donner une intuition géométrique vis a vis du structure de groupe de G. Définissons de façon usuel toutes les notions fondamentales qui apparaissent si souvent dans l'algèbre de façon analogue pour les représentations.

Définition 3.2.2 : Soit G un groupe et (V, ρ) une représentation de G et $W \subset V$ un s.e.v. On suppose que $\rho(G)(W) \subset W$ (on dit que W est invariant par ρ). On dit alors que $(W, \rho_{|W})$ est une sous représentation de (V, ρ).

Définition 3.2.3 : Soit G un groupe et (V, ρ) une représentation. On dit que (V, ρ) est une représentation irréductible lorsque V n'admet aucun s.e.v invariant par ρ.

L'hypothèse de l'irréductibilité est une condition très forte qu'il faut savoir exploiter, comme le montre l'exercice suivant:

② **Exercice 36 :** Soit G un groupe fini et (V, ρ) une représentation irréductible de G. Montrer que $\dim(V) < +\infty$.

Il est alors assez naturel de se demander si toute représentation d'un groupe quelconque peut s'écrire comme une somme directe de représentations irréductibles. Ce fait n'est pas tout à fait triviale. En effet, on voudrait raisonner par récurrence mais pour se faire, étant donné une sous représentation de (V, ρ) il faudrait montrer qu'il admet un supplémentaire stable. C'est alors le théorème de Maschke qui va nous sauver.

Théorème 3.2.1 : Soit G un groupe fini et (V, ρ) une représentation de dimension finie de G. Supposons que (V, ρ) ne soit pas irréductible de telle sorte qu'il admet un sous espace non triviale invariant par ρ noté W. Alors W admet un supplémentaire W' invariant par ρ.

Preuve: Le problème revient à trouver un supplémentaire stable à un sous espace vectoriel qui est stable par tout les $(\rho(g))_{g\in G}$. En effet, si la représentation (V, ρ) est irréductible, il n'y a rien à démontrer. Sinon, S'il existe un sous espace vectoriel stricte de V noté W stable par tout les $(\rho(g))_{g\in G}$, rien ne garanti qu'un supplémentaire quelconque est également stable par tout les $(\rho(g))_{g\in G}$. On mobilise alors *l'astuce de la moyenne*,, introduite d'abord par Maschke. Soit $p : V \to W$ un projecteur dont l'image est W. On pose:

$$\pi = \frac{1}{|G|} \sum_{g\in G} \rho(g)^{-1} \circ p \circ \rho(g)$$

On vérifier facilement que $\pi_{|W} = \mathrm{Id}_W$ et que pour tout $g \in G$, $\pi \circ \rho(g) = \rho(g) \circ \pi$. On en déduit que π est un projecteur d'image W, et que $\ker(\pi)$ est un supplémentaire à W stable par tout les $(\rho(g))_{g\in G}$, d'où le résultat. □

Ainsi, si G est un groupe fini et (V, ρ) est une représentation réductible de dimension finie de G, la représentation matricielle de ρ_g pour $g \in G$ est diagonal par bloc, avec chaque bloc pour chaque ρ_g de la même taille. On en tire par récurrence forte le théorème suivant:

Théorème 3.2.2 : (Maschke) Toute représentation (V, ρ) de dimension fini d'un groupe fini se décompose en somme directe de représentations irréductibles. Plu précisément, si (V, ρ) est une représentation de groupes de G, il existe $p \geq 1$ et $W_1, ..., W_p$ des sous espaces vectoriels strictes de V vérifiant $\dim(W_i) \geqslant 1$ quelque soit $1 \leqslant i \leqslant p$, (W_i, ρ_i) des représentations irréductibles de G avec $\rho_i(g) = \rho(g)_{|W_i}$ quelque soit $1 \leqslant i \leqslant p$ et:

$$V = \bigoplus_{i=1}^{p} W_i, \text{ on écrit alors } (V, \rho) = \bigoplus_{i=1}^{p} (W_i, \rho_i)$$

④ **Exercice 37 :**

1. Soit $n \geqslant 1$. Montrer que tout sous groupe fini de $\mathrm{GL}_n(\mathbb{K})$ se conjugue à un sous groupe de $\mathcal{O}_n(\mathbb{K})$.

2. En déduire que tout sous groupe fini de $\mathrm{GL}_2(\mathbb{R})$ est soit cyclique, soit engendré par deux éléments.

② **Exercice 38 :** Montrer que le théorème de Maschke reste vrai si on considère une représentation de G sur un corps $\mathbb{K}$ vérifiant $\chi(\mathbb{K}) \nmid |G|$.

Pour concrétiser tout ceci, regardons quelques exemples précis.

1. Une des représentations les plus connues est celle de $(\mathbb{U}, \times)$. On introduit $V = \mathbb{R}^2$ et $\rho : \mathbb{U} \to \mathrm{GL}_2(\mathbb{R})$ le morphisme suivant pour $\theta \in [0, 2\pi[$:

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

Cette représentation est clairement irréductible et traduit géométriquement la manière dont $\mathbb{U}$ agit sur le plan complexe par rotations.

2. Soit G un groupe fini. Une représentation irréductible de dimension 1 sur le corps $\mathbb{K} = \mathbb{C}$ est simplement la donné d'un morphisme de groupes $\chi : G \to \mathbb{C}^*$. En notant $n = |G|$, puisque $g^n = e_G$ quelque soit $g \in G$, on en déduit que χ est à valeurs dans $\mathbb{U}_n$. On retrouve alors les caractères qu'on a introduit à la partie précédente qui nous a permis de montrer le théorème de structure des gafs.

3. Soit X un ensemble non vide et G un groupe qui agit sur les éléments de X de façon fidèle. Soit V le $\mathbb{K}$ espace vectoriel engendré par une base indexée par les éléments de X $(e_x)_{x\in X}$. Alors $\rho : G \to \mathrm{GL}(V)$ qui à g associé l'endomorphisme ρ_g qui vérifie $\rho_g(e_x) = e_{gx}$ quelque soit $x \in X$ est une représentation du groupe G.

Introduisons une représentation de groupes qui va nous être très utile et qui motivera bien la définition de la transformée de Fourier sur les groupes finis.

Définition 3.2.4 : Soit G un groupe fini. On note $\mathcal{F}(G)$ l'espace des fonctions définis sur G a valeurs dans $\mathbb{C}$. On note $\pi : G \to \mathrm{GL}(\mathcal{F}(G))$ le morphisme:

$$\forall g \in G,\ \forall f \in \mathcal{F}(G),\ \pi(g) \cdot f = [x \mapsto f(g^{-1}x)]$$

On obtient alors une représentation de G appelée la représentation régulière.

① **Exercice 39 :** Montrer qu'il s'agit bien d'une représentation de G.

Cette représentation va débloquer pas mal de choses, et va surtout nous faire introduire la transformée de Fourier de façon parfaitement naturelle. Avant tout ça par contre, continuons à adapter les notions classiques de l'algèbre linéaire aux représentations.

3.3 Le lemme de Schur et ses corollaires

On va définir une relation d'équivalence entre les représentations irréductibles d'un groupe fini G. Pour se faire, on va s'inspirer de la relation d'équivalence qu'est la similitude entre deux endomorphismes dans l'algèbre linéaire classique.

Définition 3.3.1 : Soit G un groupe fini, $(V, \rho), (W, \tau)$ deux représentations de ce dernier. On note $\mathrm{Hom}_G(V, W)$ l'ensemble des opérateurs d'entrelacements entre V et W, c'est à dire les application linéaires $T : V \to W$ tels que pour tout $g \in G$, $T \circ \rho(g) = \tau(g) \circ T$. De façon équivalente, ce sont tout les applications linéaires T de V dans W tel que pour tout $g \in G$ le diagramme suivant commute:

$$\begin{array}{ccc} V & \xrightarrow{T} & W \\ {\scriptstyle \rho(g)}\downarrow & & \downarrow{\scriptstyle \tau(g)} \\ V & \xrightarrow{T} & W \end{array}$$

Il est peut être pas claire pourquoi on introduit cette notion d'opérateurs d'entrelacement, mais la définition suivante devrait éclaircir ce dernier.

Définition 3.3.2 : Soit G un groupe fini, $(V, \rho), (W, \tau)$ deux représentations de ce dernier. On dit que (V, ρ) et (W, τ) sont des représentations équivalentes s'il existe un $T \in \mathrm{Hom}_G(V, W)$ inversible. Moralement, cela veut dire qu'il existe un isomorphisme $T : V \to W$ tel que pour tout $g \in G$, $\tau(g) = T \circ \rho(g) \circ T^{-1}$, c'est à dire que tout les $(\rho(g))_{g\in G}$ sont semblables aux $(\tau(g))_{g\in G}$ dans une même base commune. On note alors $(V, \rho) \cong (W, \tau)$.

① **Exercice 40 :** Montrer qu'il s'agit bien d'une relation d'équivalence

Puisque tout représentation de dimension fini d'un groupe fini G est somme directe de sous représentations irréductibles, on est amené à étudier les conséquences de cette relation d'équivalence entre les représentations irréductibles. Plus précisément, on va déterminer la nature de $\mathrm{Hom}_G(V, W)$ dans le cas ou V, W sont deux représentations irréductibles, équivalentes ou non. Il s'avère qu'une version simplifié de ce problème est bien connu aux taupins. Avant tout, il faut introduire la notions d'irréductibilité d'une famille d'endomorphismes.

Définition 3.3.3 : Soit E un $\mathbb{K}$-espace vectoriel (pas forcément de dimension finie). Une partie $U \subset \mathcal{L}(E)$ est dit irréductible si pour tout $u \in U$ les seuls sous espaces vectoriels de E stable par u sont $\{0\}$ et E.

Ceci est clairement en accord avec notre définition d'une représentation irréductible (V, ρ) de G, car être une représentation irréductible est la même chose que de dire que la famille $(\rho(g))_{g\in G}$ est une famille irréductible. Attention! L'erreur classique serait de se dire que si $\mathbb{K}$ est un corps algébriquement clos $\mathcal{L}(E)$ ne pourrait pas avoir de partie irréductible. Or, cela est faux en général. La définition d'un partie irréductible est que les seuls sous espaces de E stabilisés par tout les éléments de U sont les sous espaces triviaux. Les éléments de U peuvent quand même admettre des sous espaces stables non triviales, mais si c'est le cas alors il doit forcément exister un autre élément de U qui ne stabilise pas ces mêmes espaces pour que U soit irréductible.

Si l'on croise un taupin aléatoire dans la rue et on lui demande d'énoncer le lemme de Schur, il va soit dire qu'il n'en a jamais entendu parler, soit énoncer la version des taupins, qu'on met sous forme d'exercice.

② **Exercice 41 :** Soient E et F deux $\mathbb{K}$-espaces vectoriels et $\phi \in \mathcal{L}(E, F)$ non nulle.

1. Montrer que s'il existe une partie irréductible $U \subset \mathcal{L}(E)$ tel que pour tout $u \in U$, il existe $v \in \mathcal{L}(F)$ tel que $\phi \circ u = v \circ \phi$, alors ϕ est injective.

2. Montrer que s'il existe une partie irréductible $V \subset \mathcal{L}(F)$ tel que pour tout $v \in V$, il existe $u \in \mathcal{L}(E)$ tel que $\phi \circ u = v \circ \phi$, alors ϕ est surjective.

③ **Exercice 42 :** Soit E un $\mathbb{K}$ espace vectoriel de dimension fini avec $\mathbb{K}$ algébriquement clos. Soit U une partie irréductible de $\mathcal{L}(E)$ non vide, et $\phi \in \mathcal{L}(E)$. Montrer, à l'aide du lemme de Schur de Taupin, que si ϕ commute avec tout les éléments de U alors ϕ est une homothétie.

Énonçons alors le lemme de Schur, qui, aussi simple qu'il soit, nous permettra d'en déduire des résultats profondes sur les représentations de groupes.

Proposition 3.3.1 : (Schur) Soit G un groupe fini, (V, ρ), (W, τ) deux représentations irréductibles de G. Alors:

1. Si $(V, \rho) \ncong (W, \tau)$, $\mathrm{Hom}_G(V, W) = \{0\}$.

2. Si $(V, \tau) \cong (W, \tau)$ alors $\mathrm{Hom}_G(V, W)$ est une droite vectorielle. En particulier, si $(V, \rho) = (W, \tau)$ on a $\mathrm{Hom}_G(V, V) = \{\lambda \mathrm{Id}_V,\ \lambda \in \mathbb{C}\}$.

Pour y parvenir, il faut d'abord montrer un petit résultat intermédiaire présenté sous forme d'exercice:

② **Exercice 43 :** Soit G un groupe, (V, ρ) et (W, τ) deux représentations. Soit $T \in \mathrm{Hom}_G(V, W)$. Montrer que quelque soit $g \in G$ $\ker(T)$ est stable par $\rho(g)$ et que $\mathrm{Im}(T)$ est stable par $\tau(g)$.

③ **Exercice 44 :** Soit G un gaf et (V, ρ) une représentation irréductible de G. Montrer que $\dim(V) = 1$.

Procédons: si les représentations ne sont pas équivalentes, soit $T \in \mathrm{Hom}_G(V, W)$. Alors $\ker(T)$ est est invariant par ρ. Par hypothèse d'irréductibilité, on en tire que $\ker(T) = \{0\}$ ou bien $\ker(T) = V$. Supposons alors qu'on peut exiger que T est non identiquement nulle. Alors $\ker(T) = \{0\}$ donc T est injectif. Or, l'image est invariant par τ, donc est forcément égale à W car on a supposé que T est non identiquement nulle. Or cela est impossible, car ça impliquera que les représentations sont équivalentes, d'où le résultat. □

Supposons que les représentations sont équivalentes. Il existe donc un opérateur d'entrelacement inversible entre les représentations (V,ρ) et (W,τ) qu'on va noter Φ. Soit donc $T \in \mathrm{Hom}_G(V,W)$. Quitte à considérer $\Phi^{-1}\circ T$ on peut supposer que $(V,\rho)=(W,\tau)$. Il est claire que $\Phi^{-1}\circ T$ est un opérateur d'entrelacement entre les représentations (V,ρ) et (V,ρ). Puisque $\mathbb{C}$ est algébriquement clos, $\mathrm{Sp}(\Phi^{-1}\circ T)$ est non vide et donc il existe un $\lambda\in\mathbb{C}$ tel que le sous espace caractéristique E_λ soit de dimension $\geqslant 1$. Or, puisque V est irréductible et que E_λ est invariant par ρ, on en tire que $E_\lambda = V$ tout entier. Ainsi, $\Phi^{-1}\circ T = \lambda \mathrm{Id}_V$ et donc $T=\lambda\Phi$, d'où le résultat. □

L'utilité de ce lemme ne semble pas être immédiat, mais le lecteur attentif remarquera que l'application introduite dans la démonstration du théorème de Maschke est un opérateur d'entrelacement. En s'inspirant de ce dernier, on est conduit à étudier les opérateurs de la même forme. On va en déduire des résultats remarquables sur les représentations grâce à cette remarque. Avant tout, introduisons une notation qu'on justifiera plus tard. Si f est une fonction qui est définie sur G et est à valeurs dans un espace muni d'une opération binaire $+$, on note:

$$\int_G f(g)\ d\mu_G(g) = \frac{1}{|G|}\sum_{g\in G} f(g)$$

C'est simplement un intégral discret. Cela simplifiera les notations considérablement. Donnons une application du lemme de Schur.

Proposition 3.3.2 : Soit G un groupe fini et (V,ρ), (W,τ) deux représentations irréductibles de ce dernier. Soit $A\in\mathcal{L}(V,W)$. On pose:

$$\tilde{A} = \int_G \tau(g)^{-1} A\rho(g)\ d\mu_G(g)$$

Alors si les représentations (W,τ) et (V,ρ) ne sont pas équivalentes, $\tilde{A}\equiv 0$. Si $(W,\tau)=(V,\rho)$ alors $\tilde{A} = \dfrac{\mathrm{Tr}(A)}{\dim(V)}\mathrm{Id}_V$.

Preuve: Il relève de calculs qui présentent aucune difficulté que $\tilde{A}\in\mathrm{Hom}_G(V,W)$. D'après le lemme de Schur, on a immédiatement le premier cas. Pour le second, on sait que $\tilde{A}=\lambda\mathrm{Id}_V$. Or, $\mathrm{Tr}(A)=\lambda\dim(V)$, d'où le résultat. □

③ **Exercice 45 :** Que devient la proposition ci-dessus si on suppose seulement que $(V,\rho)\cong(W,\tau)$ pour la deuxième condition?

C'est surtout ce corollaire du lemme de Schur qui va tout débloquer. Avec lui, on va pourvoir démontrer des résultats magnifiques concernant les représentations de G.

Définition 3.3.4 : Soit G un groupe fini et (V,ρ) une représentation de dimension finie de ce dernier. On appel la représentation contragédiente la représentation induite de V sur son dual V^* noté $(V,\tilde{\rho})$, définit par:

$$\forall(\lambda,v)\in V^*\times V,\ \forall g\in G,\quad \tilde{\rho}(g)(\lambda)(v) = \lambda(\rho(g)^{-1}v)$$

On vérifie facilement qu'il s'agit bien d'une représentation.

Pour le moment, on a tout fait sans parler de matrices. C'est maintenant que cela va devenir utile. Une première remarque est que, si (V,ρ) est une représentation de dimension fini de G, on peut munir V d'un produit Hermitien noté $\langle\cdot|\cdot\rangle$. De là, on peut définir un nouveau produit hermitien pour lequel tout les $(\rho(g))_{g\in G}$ sont unitaire. En effet, il suffit de considérer:

$$\forall(v_1,v_2)\in V^2,\ [v_1,v_2] = \sum_{g\in G}\langle\rho(g)v_1|\rho(g)v_2\rangle$$

On en déduit que dans la bonne base, quelque soit $g\in G$ on a $\rho(g)^* = \rho(g)^{-1}$ et donc on raisonnera toujours dans ce cas là. On peut alors déduire l'expression matricielle de la représentation contragédiente. En effet, si on note pour tout $g\in G$, $\rho(g)=(\rho(g)_{i,j})_{1\leqslant i,j\leqslant n}$ et $\tilde{\rho}(g)=(\tilde{\rho}(g)_{i,j})_{1\leqslant i,j\leqslant n}$ avec $n=\dim(V)$, en notant $(e_1,...,e_n)$ la base dans lequel les $(\rho(g))_{g\in G}$ sont unitaires et $(e_1^*,...,e_n^*)$ la base duale canonique, on obtient que:

$$\tilde{\rho}(g)_{i,j} = \tilde{\rho}(g)(e_j^*)(e_i) = e_j^*(\rho(g)^* e_i) = \rho(g)_{j,i}^* = \overline{\rho(g)_{i,j}}$$

On en tire que matriciellement, $\tilde{\rho}(g) = \overline{\rho(g)}$. De ce fait, on en déduit le résultat suivant:

Proposition 3.3.3 : Soit G un groupe fini et (V, ρ) une représentation de G de dimension fini. Alors (V, ρ) est une représentation irréductible si et seulement si la représentation contragédiente $(V^*, \tilde{\rho})$ l'est.

Cette étude de la nature des représentations en fonction des coefficients matriciels nous éclaire beaucoup sur le sujet, et nous mène naturellement à la théorie des caractères. Introduisons donc une famille de fonctions d'intérêt potentiel:

Définition 3.3.5 : Soit G un groupe fini et (V, ρ) une représentation de G. On appel coefficient matriciel toute application $\phi_{\lambda,v}^{\rho} \in \mathcal{F}(G)$ de la forme $\phi_{\lambda,v}^{\rho}(g) = \lambda(\pi(g)v)$. On note $\check{\phi}_{\lambda,v}^{\rho} : g \mapsto \lambda(\rho(g)^{-1}v)$

① **Exercice 46 :** On reprend les notations de la définition ci-dessus, et on suppose que la représentation est de dimension finie $n \geqslant 1$. Justifier cette appellation en montrant que l'application $\phi_{i,j} : g \mapsto \rho(g)_{i,j}$ définit pour $1 \leqslant i, j \leqslant n$ est en effet un coefficient matriciel.

On a le résultat suivant, corollaire du lemme de Schur, qui va tout débloquer.

Proposition 3.3.4 : Soit G un groupe fini, (V, ρ) et (W, τ) deux représentations irréductibles de ce dernier. Soient $(\lambda, v) \in V^* \times V$ et $(\mu, w) \in W^* \times W$ et $\phi_{\lambda,v}^{\rho}$, $\phi_{\mu,w}^{\tau}$ les coefficients matriciels associés. Alors:

$$\int_G \phi_{\lambda,v}^{\rho}(g)\check{\phi}_{\mu,w}^{\tau}(g)\ d\mu_G(g) = \begin{cases} 0 \text{ si } (V,\rho) \ncong (W,\tau) \\ \dfrac{\lambda(w)\mu(v)}{\dim(V)} \text{ si } (V,\rho) = (W,\tau) \end{cases}$$

Preuve: Il faut habilement mobiliser Schur! On commence par réecrire l'intégrale:

$$\int_G \phi_{\lambda,v}^{\rho}(g)\check{\phi}_{\mu,w}^{\tau}(g)\ d\mu_G(g) = \lambda\left(\int_G \rho(g)\mu(\tau(g)^{-1}w)v\ d\mu_G(g)\right)$$

On est donc amené à introduire l'application linéaire $f : W \to V$ qui à $\omega \mapsto \mu(\omega)v$. On a alors:

$$\int_G \phi_{\lambda,v}^{\rho}(g)\check{\phi}_{\mu,w}^{\tau}(g)\ d\mu_G(g) = \lambda\left(\int_G \rho(g) f \tau(g)^{-1} d\mu_G(g) w\right)$$

On mobilise alors Schur. on en déduit immédiatement la première condition. Pour le second, on a alors:

$$\int_G \phi_{\lambda,v}^{\rho}(g)\check{\phi}_{\mu,w}^{\tau}(g)\ d\mu_G(g) = \lambda\left(\frac{\mathrm{Tr}(f)}{\dim(V)}w\right) = \frac{\lambda(w)\tau(v)}{\dim(V)}$$

D'où le résultat. □

On va en déduire un premier résultat sur le nombre de représentations irréductibles à isomorphisme près grâce à cette proposition.

Définition 3.3.6 : Soit G un groupe fini. On note $\widehat{G}$ l'ensemble des classes d'équivalences des représentations irréductibles pour la relation d'équivalence $\cong$. On appel cet espace le dual de G.

Proposition 3.3.5 : Soit G un groupe fini. Alors $|\widehat{G}| \leqslant |G|$.

Preuve: Supposons que $|\widehat{G}| > |G|$. Soit $(\delta_1, ..., \delta_{|G|+1}) \in \widehat{G}\ |G|+1$ classes distincts et quelque soit $1 \leqslant i \leqslant |G|+1$ prenons $(V_i, \rho_i) \in \delta_i$, $(\lambda_i, v_i) \in V_i^* \times V_i$ tel que $\phi_{\lambda_i,v_i}^{\rho_i}$ est non identiquement nulle et

vérifie $\lambda_i(v_i) \neq 0$. Alors la famille $(\phi^{\rho_i}_{\lambda_i,v_i})_{1\leqslant i\leqslant |G|+1}$ est une famille libre de $\mathcal{F}(G)$. En effet, supposons qu'il existe $(\mu_1,...,\mu_{|G|+1}) \in \mathbb{C}^{|G|+1}$ tel que:

$$\sum_{i=1}^{|G|+1} \mu_i \phi^{\rho_i}_{\lambda_i,v_i} \equiv 0$$

Alors en utilisant la proposition précédente, quelque soit $1 \leqslant j \leqslant |G|+1$:

$$\int_G \left(\sum_{i=1}^{|G|+1} \mu_i \phi^{\rho_i}_{\lambda_i,v_i}(g) \right) \check{\phi}^{\rho_j}_{\lambda_j,v_j}(g)\ d\mu_G(g) = \mu_j \frac{\lambda_j(v_j)^2}{\dim(V_j)} = 0$$

Or, cela contredit le fait que $\dim(\mathcal{F}(G)) = |G|$, d'où le résultat. □

3.4 Caractères et théorème de Burnside

Dans cette partie, notre but va être de raffiner la proposition précédente. Pour ce faire, il va être nécessaire de passer par la théorie de caractères. Les caractères sont une famille de fonctions qui caractérisent à eu seuls les représentations d'un groupe fini G. Si on connais les caractères sur G, on peut connaitre tout les représentations de ce dernier.

Définition 3.4.1 : Soit G un groupe fini et (V,ρ) une représentation. On appel caractère associé à la représentation (V,ρ) l'application $\chi_V \in \mathcal{F}(G)$ qui est définit par $\chi_V(g) = \mathrm{Tr}(\rho(g))$ quelque soit $g \in G$.

Voici deux propriétés immédiates des caractères qu'on met sous forme d'exercice:

② **Exercice 47 :** Soit G un groupe fini.

1. Montrer que si (V,ρ) et (W,τ) sont deux représentations de dimensions finis équivalentes de G alors $\chi_V = \chi_W$.

2. Montrer que si $(V,\rho) = \bigoplus_{i=1}^{p} (W_i,\rho_i)$ alors $\chi_V = \sum_{i=1}^{p} \chi_{W_i}$

3. Montrer que si (V,ρ) est une représentation de dimension finie de G alors $\chi_V(e_G) = \dim(V)$.

Avant de procéder, on rappel qu'on peut munir $\mathcal{F}(G)$ d'un produit Hermitien classique noté $\langle\cdot|\cdot\rangle$ de la façon suivante:

$$\forall (f,h) \in \mathcal{F}(G),\ \langle f|h\rangle = \frac{1}{|G|}\sum_{g\in G} \overline{f(g)}h(g) = \int_G \overline{f(g)}h(g)\ d\mu_G(g)$$

Proposition 3.4.1 : Soit G un groupe fini. Quelque soit $\delta \in \widehat{G}$ notons (V_δ,ρ_δ) un représentant de δ, et notons χ_δ le caractère associé. Alors pour tout $(\delta,\mu) \in \widehat{G}^2$, on a:

$$\langle \chi_\delta | \chi_\mu \rangle = \begin{cases} 1 \text{ si } \mu = \delta \\ 0 \text{ sinon.} \end{cases}$$

Preuve: On commence par montrer le lemme suivant:

Lemme: Soit G un groupe fini et (V,ρ) une représentation irréductible de G de dimension $n \geqslant 1$. Alors pour tout $1 \leqslant i,j,k,\ell \leqslant n$

$$\langle \rho(g)_{i,k} | \rho(g)_{j,\ell} \rangle = \frac{\delta_{i,j}\delta_{\ell,k}}{\dim(V)}$$

Pour le montrer, on considère la base canonique de $\mathcal{L}(V)$ sous forme matricielle $(E_{k,\ell})_{1\leqslant k,\ell\leqslant n}$. Soit donc $(k,\ell) \in [\![1,n]\!]^2$. On va appliquer le lemme de Schur:

$$\left(\int_G \rho(g)^{-1} E_{k,\ell}\rho(g)\ d\mu_G(g)\right)_{i,j} = \frac{\delta_{k,l}\delta_{i,j}}{\dim(V)} = \int_G \overline{\rho(g)}_{i,k}\rho(g)_{j,\ell}\ d\mu_G(g)$$

D'où le résultat. D'après le lemme de Schur, il est évident que si $\delta \neq \mu$ alors $\langle \chi_\delta | \chi_\mu \rangle = 0$. Sinon, en notant $n = \dim(V_\delta)$:

$$\langle \chi_\delta | \chi_\delta \rangle = \sum_{i=1}^{n}\sum_{j=1}^{n} \langle \rho(g)_{i,i} | \rho(g)_{j,j} \rangle = \frac{1}{\dim(V_\delta)} \sum_{i=1}^{n} 1 = 1$$

D'où le résultat. □

On est désormais dans la mesure de raffiner la proposition concernant la finitude de $\widehat{G}$.

② **Exercice 48 :**

1. Soit G un groupe fini, (V, ρ) et (W, τ) deux représentations de dimension fini de G. Montrer que $(V, \rho) \cong (W, \tau)$ si et seulement si $\chi_W = \chi_V$.

2. Peut ont avoir $(V, \rho) \cong (V^*, \tilde{\rho})$?

   Montrer que (V, ρ) est irréductible si et seulement si $\langle \chi_V, \chi_V \rangle = 1$.

Théorème 3.4.1 : Burnside Soit G un groupe fini. Alors:

$$|G| = \sum_{\delta \in \widehat{G}} \dim(V_\delta)^2$$

Avec quelque soit $\delta \in \widehat{G}$, (V_δ, ρ_δ) un représentant de la classe d'équivalence δ.

Preuve: La représentation régulière $(\mathcal{F}(G), \pi)$ est de dimension fini valant le cardinal de G. D'après le théorème de Maschke, il existe $p \geqslant 1$ représentations de G notés (V_1, ρ_1),...,(V_p, ρ_p) tels que:

$$(\mathcal{F}(G), \pi) = \bigoplus_{i=1}^{p} (V_i, \rho_i)$$

Notons χ le caractère de $(\mathcal{F}(G), \pi)$ et χ_i le caractère de chaque (V_i, ρ_i). Alors:

$$\chi = \sum_{i=1}^{p} \chi_i = \sum_{\delta \in \widehat{G}} m_\delta \chi_\delta$$

Dans la dernière somme on a simplement regroupé les termes en fonction de leur classe d'équivalence car les caractères sont les mêmes dans ce cas là. Reste à déterminer $(m_\delta)_{\delta \in \widehat{G}}$. Or, d'après la proposition précédente:

$$m_\delta = \langle \chi | \chi_\delta \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\chi_\delta(g)$$

Or, $\chi(g) = \mathrm{Tr}(\pi(g))$. En se plaçant dans la base canonique de $\mathcal{F}(G)$, c'est à dire la famille des $(\delta_g)_{g \in G}$, les fonctions qui vérifient:

$$\forall g \in G,\ \forall h \in G,\ \delta_g(h) = \begin{cases} |G| \text{ si } g = h \\ 0 \text{ sinon} \end{cases}$$

Alors étant donné $(g, h) \in G^2$, $\pi(g)(\delta_h) = \delta_{gh}$ et donc pour $g \neq e_G$, $\chi(g) = 0$, tandis que pour $g = e_G$, $\chi(g) = \dim(\mathcal{F}(G)) = |G|$. On en tire que:

$$m_\delta = \frac{1}{|G|}(|G|\chi_\delta(e_G)) = \dim(V_\delta)$$

Ainsi:

$$\chi(e_G) = |G| = \sum_{\delta \in \widehat{G}} \dim(V_\delta)\chi_\delta(e_G) = \sum_{\delta \in \widehat{G}} \dim(V_\delta)^2$$

D'où le résultat. □

Par argument de dimension on sait donc que $\mathcal{F}(G)$ est isomorphe à $\prod_{\delta \in \widehat{G}} \mathcal{L}(V_\delta)$ en tant qu'espace vectoriel, mais aurait-on une équivalence de représentations? Essayons de faire une analyse synthèse. Supposons qu'on souhait exprimer un élément $f \in \mathcal{F}(G)$ sous la forme:

$$f(g) = \sum_{\delta \in \widehat{G}} \sum_{1 \leqslant i,j \leqslant d_\delta} c_\delta(i,j)\pi_\delta(g)_{i,j}$$

Avec $d_\delta = \dim(V_\delta)$ quelque soit $\delta \in \widehat{G}$ et $\pi_\delta(g)_{i,j}$ le coefficient matricielle de la représentation régulière. Alors

$$c_\delta(i,j) \int_G \pi_\delta(g)_{i,j}\overline{\pi_\delta(g)_{i,j}}\, d\mu_G(g) = \int_G f(g)\overline{\pi_\delta(g)_{i,j}}\, d\mu_G(g) = \frac{c_\delta(i,j)}{d_\delta}$$

Ainsi, notre analyse nous amène à essayer de montrer que quelque soit $g \in G$:

$$f(g) = \sum_{\delta \in \widehat{G}} d_\delta \sum_{1 \leqslant i,j \leqslant d_\delta} \int_G f(s)\overline{\pi_\delta(s)_{i,j}}\, d\mu_G(s)\pi_\delta(g)_{i,j}$$

C'est infecte, donc introduisons la notation suivante:

Définition 3.4.2 : Soit G un groupe fini, $(\mathcal{F}(G), \pi)$ la représentation régulière. Pour tout $f \in \mathcal{F}(G)$, on note $\mathcal{F}f \in \prod_{\delta \in \widehat{G}} \mathcal{L}(V_\delta)$ qui s'écrit $\mathcal{F}f = (F(\delta))_{\delta \in \widehat{G}}$ avec quelque soit $\delta \in \widehat{G}$:

$$F(\delta) = \int_G f(g)\pi_\delta(g)\, d\mu_G(g)$$

On note δ^* la classe d'équivalence de la représentation contragédiente de (V_δ, ρ). $\mathcal{F}f$ est appelée la transformée de Fourier de f

Avec ces notations, on obtient, en reprenant la somme ci-dessus, que dans un monde idéal, quelque soit $g \in G$:

$$f(g) = \sum_{\delta \in \widehat{G}} d_\delta \mathrm{Tr}(F(\delta^*)\pi_\delta(g)^T)$$