

Typesetting test

$$\sum_i^n \neq 60 \pm \infty \pi \Delta \neg \approx \sqrt{j} \int h \leq \geq$$

$$\textcolor{red}{\mathbb{R}\mathbb{P}} \textcolor{blue}{\mathbb{1}\mathbb{P}\mathfrak{G}\mathbb{P}} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mathbb{P}\mathbb{P} \, \mathrm{d} x$$

$$\alpha(x)=\left\{\begin{array}{l}x\\[1ex]\frac{1}{1+e^{-kx}}\\[1ex]\frac{e^x-e^{-x}}{e^x+e^{-x}}\end{array}\right.$$

$$\langle x \rangle$$

$$\chi_\rho(ghg^{-1})=\mathrm{Tr}(\rho_{ghg^{-1}})=\mathrm{Tr}(\rho_g\circ\rho_h\circ\rho_g^{-1})=\mathrm{Tr}(\rho_h)^{\mathrm{Tr}(AB)=\mathrm{Tr}(BA)}\chi_\rho(h)\oplus_{x\in X}$$

$$\mathrm{Mat}(\rho_g)=(a_{ij}(g))_{\substack{1\leq i\leq d\\1\leq j\leq d}}\text{ et }\mathrm{Mat}(\rho'_g)=(a'_{ij}(g))_{\substack{1\leq i'\leq d'\\1\leq j'\leq d'}}$$

Chapitre 1

GENERALITES

1.1 Définitions de base

1.1.1 Groupe et Sous-Groupe

Soit G un ensemble non vide ($G \neq \emptyset$).

Définition 1. On dit que G est un GROUPE si :

1. $\forall a, b, c \in G : a(bc) = (ab)c$ (associative)
2. $\exists e \in G : \forall g \in G : ge = eg = g$ (élément neutre)
3. $\forall g \in G \exists g^{-1} \in G : g^{-1}g = gg^{-1} = e$ (symétrique)

Si commutative – abelian. Groupes : $(R, +)$, (S_n, \circ) , etc.

Soit H un sous-ensemble de G .

Définition 2. H est un SOUS-GROUPE de G si :

1. $H \neq \emptyset$
2. $\forall x, y \in H : xy^{-1} \in H$

On notera $H < G$.

Si $x \in G$, alors le sous-groupe *engendré* par x est le plus petit sous-groupe de G contenant x . Notée $\langle x \rangle$. Si G est *fini* (\Leftrightarrow cardinal G est fini $\Leftrightarrow \#G < \infty$). Sont ORDRE de G est tout montant éléments. L'ordre d'un groupe G se note $\text{ord}(G)$, $|G|$ ou $\#G$.

Si $x \in G$, l'ordre de x est G plus petit entier $n \geq 1$ que $x^n = e$. On le note $\text{ord}(x)$.
Order x est $\text{ord}(x) \stackrel{\text{def}}{=} |\langle x \rangle|$

Exemple 1.1.1. S_3 .

1.1.2 La classe d'équivalence

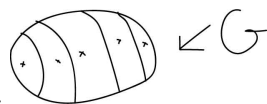
Définition 3. Soient G un groupe et H – un sous-groupe de G . On définit sur G la RELATION D'ÉQUIVALENCE dite à gauche modulo H . Pour $x, y \in G$:

$$x \equiv_g y \text{ mod } H \text{ ssi } x^{-1}y \in H$$

Si $x \in G$ la classe d'équivalence de x pour cette relation dite CLASSE À GAUCHE MODULO H est :

$$\begin{aligned} \bar{x} &= \{y \in G \mid y \equiv_g x \text{ mod } H\} = \{y \in G \mid y^{-1}x \in H\} = \{xh \mid \exists h \in H\} \\ &= xH \end{aligned}$$

???



Remarque. Les class d'équivalence constituée une *partition* de G . L'ensemble les classes d'équivalence est appelé ENSEMBLE QUOTIENT, et est noté :

$$\left(G/H \right)_g$$

On definit unne autre **relation d'equivalence** sur G , dite à droite modulo H le pour $x, y \in G$, $x \equiv_d y$ ssi $xy^{-1} \in H$. Pour $x \in G$ la classe de x pour cette relation est : $Hx = \{hx, h \in h\}$ – appelé **classe à droite de x modulo H** .

Si G est un groupe fini et si H est sous-groupe de G alors l'application pour $x \in G$ fixé $f_x : \begin{array}{ccc} H & \rightarrow & xH \\ h & \mapsto & xh \end{array}$ est une bijection.

On en déduit que toutes les classes à gauches xH ont même cardinal, à pouvoir $|H|$ (Le même pour le classe à droite).

Comme G est la reunion disjointe des xH , pour x décrivant un système de représentants des classes, on en déduit :

Theorem 1. Soient G un groupe fini et H un sous-groupe de G . Alors : $|H|$ divise $|G|$. Et on a : $\# \left(G/H \right) = \frac{|G|}{|H|}$.

L'entier $[G : H] = \# \left(G/H \right)$ s'appelé l'indice de H dans G . En particulier, l'ordre d'un élément divise l'ordre du groupe.

Application canonique :

$$\begin{array}{ccc} \pi : G & \xrightarrow{\text{surjection}} & \frac{|G|}{|H|}_g \text{ – est surjet} \\ x & \mapsto & \underbrace{xH}_{\bar{x}} \end{array}$$

$xH, yH \in \left(G/H \right)_g$. Alors

$$\begin{aligned}
xH \cdot yH &= (xy)H \\
\pi(xy) &= \pi(x)\pi(y) \\
\bar{x}\bar{y} &= \overline{xy}.
\end{aligned}$$

On souhaite même l'ensemble quotient de la structure de groupe qui fasse de la surjection canonique π un morphisme de groupe.

1.1.3 Normal dans G

Définition 4. Un sous groupe $H < G$ de G est dit DISTINGUE dans G ou NORMAL dans G , s'il est stable pour conjugaison :

- i.e. $\forall x \in G, \forall h \in H : xhx^{-1} \in H$
- i.e. $xHx^{-1} \subset H$
- i.e. $\forall x \in G, xH = Hx$

On note alors : $H \triangleleft G$.

Remarque.

- Si G est un groupe abélien alors tout sous-groupe de G est distingué dans G .
- Si $H \triangleleft G$, on n'a pas nécessairement : $xh = hx \forall x \in G, \forall h \in H$.
- Si $[G : H] = 2$ alors $H \triangleleft G$.

Exemple 1.1.2.

1. $\langle \sigma_1 \rangle = \{e, \sigma_1, \sigma_2\}$ — sous-groupe engendré pour σ_1 dans \mathfrak{S}_3 . $[G : H] = 2 \Rightarrow \langle x \rangle \triangleleft \mathfrak{S}_3$.
2. $\langle \tau_1 \rangle = \{e, \tau_1\} \not\triangleleft \mathfrak{S}_3$. Car $\langle \tau_1 \rangle$ n'est pas stable par conjugaison. En effet : l'élément $\tau_2 \tau_1 \tau_2^{-1} = \tau_2 \tau_1 \tau_2 = (12) = \tau_3 \notin H$.
3. Le Noyau du morphisme de groupe $f : G \rightarrow G'$ est l'ensemble $\text{Ker } f := \{x \in G \mid f(x) = e'\}$, où e' est l'élément neutre de G' . C'est un sous-groupe distingué de G .

Définition 5. Un groupe est dit SIMPLE s'il n'admet pas de sous-groupes distingués autres que lui-même et $\{e\}$.

Exemple 1.1.3. — Soit G un groupe d'ordre premier p , alors G est groupe simple.

- Alors G est un groupe simple. En effet, si H est un sous-groupe de G alors, par le Théorème de Lagrange son ordre divise p , donc vaut 1 ou p puisque p est premier. Donc $H = \{e\}$ ou $H = G$. De plus, si $x \in G \setminus \{e\}$ alors, pour le Th. de Lagrange son ordre divise p , donc vaut 1 ou p puisque p est premier donc vaut p puisque $x \neq e$. Donc $\langle x \rangle = G$.

Donc G est cyclique (i.e engender par un élément et fini). Donc G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Considéons le groupe abélien $(\mathbb{Z}, +)$. Si l'on note $n\mathbb{Z} = \{nk, k \in \mathbb{Z}\}$ l'ensemble des multiples de n dans \mathbb{Z} (pour $n \geq 0$) alors : $(n\mathbb{Z}, +)$ est un sous-groupe de \mathbb{Z} .

En effet :

* $n\mathbb{Z} = \emptyset$ car $0 = n \cdot 0 \in \mathbb{Z}$.

* soient $a, b \in n\mathbb{Z}$ qui $a - b \in n\mathbb{Z}$.

Réciproquement, tout sous-groupe de \mathbb{Z} est de la forme $n\mathbb{Z}$ pour un certain $n \geq 0$.

$n\mathbb{Z}$ est un sous-groupe distingué de \mathbb{Z} (car \mathbb{Z} est abélien). On considère l'anneau quotient : $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

$$\bar{x} + \bar{y} = \overline{x + y} \quad (1.1)$$

$$\bar{x}\bar{y} = \overline{xy} \quad (1.2)$$

1.2 Groupes abéliens finis

Theorem 2 (de Kronecker, ou Théorème de classification des Groupes Abéliens de type fini). *Tout groupe abélien de type fini G s'écrit de sous la forme :*

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z} \times \mathbb{Z}^s,$$

avec $d_1|d_2|\dots|d_r$ ($d_r \geq 2$) et $s > 0$. Ces de sont appelé les facteurs invariantes de G .

Remarque. $d_r =$ exponent de $G =$ ppcm des ordres des éléments de G .

Exemple 1.2.1. 1. Montrer qu'un groupe, dont tous les éléments non neutres sont d'ordre 2, est abélien.

Solution $(ab)(ab) = 2 \Rightarrow a(abab)b = aeb = ab, a^2bab^2 = ebae = ba$

2. Déterminer à isomorphisme près tous les groupes.

Solution

— Si G est d'ordre 1, alors G est réduit à $\{e\}$ où e est l'élément neutre de G .

— Si $|G| = 2$ alors, puisque 2 est premier, G est cyclique et donc : $G \simeq \mathbb{Z}/2\mathbb{Z}$ i.e. $G \simeq (\mathbb{Z}/2\mathbb{Z}, +)$ (abélien)

— Si $|G| = 3$ alors la même, $G \simeq \mathbb{Z}/3\mathbb{Z}$.

— Si $|G| = 4$, si G admet élément d'ordre 4 alors G est cyclique et donc $G \simeq \mathbb{Z}/4\mathbb{Z}$, abélien. Sinon, d'appelés le Théorème de Lagrange tous les éléments, non neutres de G sont d'ordre 2. s'appelle exercice precedent on en déduit que G est abélien.

D'après le Th. de Classification des groupes abéliens finis, G est, soit isomorphe à $G \simeq \mathbb{Z}/4\mathbb{Z}$: impossible car G n'admet pas d'élément d'ordre 4. Soit isomorphe à : $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Il est

isomorphe au groupe de Klein. Il y a donc deux groupes d'ordre 4 à isomorphisme près : $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (et ils sont tous les deux abéliens).

- Si $|G| = 5$ puisque 5 est premier, G est cyclique et donc $G \simeq \mathbb{Z}/5\mathbb{Z}$ — il est abélien.

1.3 Groupes agissant sur un ensemble

Soient G est un groupe et X un ensemble.

Définition 6. On dit un groupe G agit sur un ensemble X , si :

1. $\forall x \in X \quad e \cdot x = x$
2. $\forall x \in X, \forall g \in G \quad g \cdot (g' \cdot x) = (gg') \cdot x$

On peut aussi voir une action de G sur X comme un morphisme de G dans le groupe S_X des permutations de X :

$$a = b + c \quad (1.3)$$

$$\pi : G \rightarrow S_X \quad (1.4)$$

$$g \mapsto \left(\begin{array}{l} \pi_g : X \rightarrow X \\ x \mapsto \pi_g(x) = g \cdot x \end{array} \right) \quad (1.5)$$

Définition 7. Si un groupe G agit sur un ensemble X , la relation sur X : $x, y \in X, x \sim y$ ssi $\exists g \in G, y = g \cdot x$ est une relation d'équivalence. La classe de x par cette relation s'appelle ORBITE de x , notée $\text{orb}(x)$ ou $G \cdot x$: $\text{orb}(x) = \{y \in X, y \sim x\} = \{g \cdot x, g \in G\}$ l'ensemble des orbites constitue une partition de X .

On dit que l'action est *Transitive* en que G agit transitivement s'il n'y a qu'une seule orbite, i.e. $\forall x, y \in X, \exists g \in G, y = g \cdot x$.

Le *Noyau* de l'action est le noyau du morphisme

$$\begin{aligned} \pi : G &\rightarrow S_X \\ G &\mapsto \pi_G \end{aligned}$$

i.e l'ensemble :

$$\text{Ker} \pi = \{g \in G | \pi(g) = e_{S_X}\} = \{g \in G | \pi_g = \text{id}_X\} = \{g \in G | \forall x \in X, \pi_g(x) = x\} = \{g \in G | \forall x \in X, g \cdot x = x\}$$

On dit que l'action est FIDÈLE si son noyau est réduit à $\{e\}$ i.e. le morphisme π associé est injectif.

Exemples.

1. Le groupe des rotations de \mathbb{R}^3 de centre l'origine agit sur \mathbb{R}^3 . $G \times \mathbb{R}^3 \rightarrow \mathbb{R}^3$ et $(r, x) \mapsto r \cdot x = r(x)$. Les orbites sont les sphères centrées en l'origine. L'action n'est donc pas transitive. Regarde rotation qui fixe tout le monde. Évidemment l'action est fidèle. Rotation fixant tout point de \mathbb{R}^3 est l'identité.

2. Si X est un ensemble, le groupe σ_X agit sur X par permutation : $\sigma_x \times X \mapsto X$, $(\sigma, x) \mapsto \sigma \cdot x = \sigma(x)$.

L'action est évidemment transitive. σ est dans le mogan du morphisme associe a cette action ssi : $\forall x \in X, \sigma(x) = x$: donc $\sigma = id_x$ et donc l'action est fidèle.

3. Tout groupe G agit sur même par multiplication a gauche se qua $G \times G \rightarrow G$; $(g, x) \mapsto g \cdot x = gx$ (loi de composition dons G).

Soient $x, y \in G$; on a $y = gx$, avec $g = yx^{-1}$. L'action est donc transitive. Soit g dans le moyen de l'action ou a alors :

$$\forall x \in G, gx = x; \text{ d'oi } g = e$$

Donc l'action est fidèle.

4. Tout groupe G agit sur lui-meme par conjugaison :

$$G \times G \mapsto G; (g, x) \mapsto g \cdot x = gxg^{-1}$$

En effet : (i) Si $x \in G$; on a : $e \cdot x = exe^{-1} = x$.

(ii) soient $g, g' \in G$ et $x \in G$ ou a :

$$g \cdot (g' \cdot x) = g \cdot (g' x g'^{-1}) = g(g' x g'^{-1}) g^{-1} = (gg') x (g'^{-1} g^{-1}) = (gg') x (gg')^{-1} = (gg') \cdot x$$

Utilise $(ab)^{-1} = b^{-1} a^{-1}$.

— $\text{orb}(e) = \{geg^{-1}, g \in G\} = \{e\}$ Donc l'action n'est pas transitive si $G \neq \{e\}$

— Si $x \in G$ alors $\text{orb}(x) = \{gxg^{-1}, g \in G\}$ donc de conjugation de x .

— Le mogan de l'action est :

$$\{g \in G | \forall x \in X, gxg^{-1} = x\} = \{g \in G | \forall x \in X, gx = xg\} \stackrel{\text{def}}{=} \text{"centre de } G" \stackrel{\text{def}}{=} Z(G)$$

est réduit â $\{e\}$.

Définition 8. Si un groupe G agit sur un ensemble X et si $x \in X$, on définit le stabilisateur (ou groupe s'isotropie) de X pour cette action par : $\text{stab}(x) = \{g \in G | g \cdot x = x\}$. (noté aussi G_X)

Proposition 1. C'est un sous groupe de G .

Proposition 2. Pour X l'application $G \rightarrow X, g \mapsto g.x$ définit une bijection de l'ensemble $X / \text{stab } x$ des classe a gauche monade $\text{stab}(x)$ sont l'orbite de x .

Aussi, le cardinal de l'orbite $\text{orb}(X)$ est égal a l'indice de $\text{stab}(x)$ dans G .

$$\# \text{orb}(x) = [G : \text{stab}(x)]$$

Theorem 3. Formule des classe Soit G un groupe fini agsdant aensembl fini x mois :

1. $\#X = \sum_x [G : \text{stab}(x)]$ où

2. Le moite u d'orbites est donné par la formule (théorème de Burnside) :

$$m = \frac{1}{|G|} \sum_{g \in G} \#X_g$$

où $X_g = \{x \in X | g.x = x\}$. Bernside.

Remarque. $|G| = n$, $d|n$: $\exists H < G$ t.q. $|H| = d$? Cyclique, oui $\exists!$

$n = \prod_n p_i^{\alpha_i}$, p_i - première

1.4 Les Théorèmes de Sylow

Soit G un groupe fini et point p un nombre premier tel que p^r divise l'ordre de G mais p^{r+1} ne le divise pas (avec $r \geq 0$). Alors tout sous-groupe de G s'appelle un p -sous-groupe de Sylow ou p -Sylow de G .

Par exemple, G est un groupe d'ordre de $n = 2^3 \times 3^5 \times 5^2 \times 7$ alors une 3-Sylow de G est un Sylow de G d'ordre : $2^3 = 8$.

Theorem 4 (1^{er} théorème de Sylow). Soit G une groupe d'ordre $p^\alpha q$ avec p premier et $(p, q) = 1$ (et $\alpha \geq 1$)

Pour tout entier β tel que : $1 \leq \beta \leq \alpha$, il existe un sous-groupe de G d'ordre p^β . En particulier, il existe un p -Sylow de G .

De plus, le nombre n_p de p -Sylow de vérifie : $n_p \equiv 1 \pmod p$ et $n_p | q$.

Définition 9. Si H est un sous-groupe d'un groupe G , les conjugués dans G sont les gHg^{-1} , pour $g \in G$ ($\{ghg^{-1}, h \in H\}$).

En particulier H est distingué dans G ssi il est égal à tous des conjugués.

Theorem 5 (2^{ème} Théorème de Sylow). Soit G une groupe fini. Le conjugué d'un p -Sylow de G est encore un p -Sylow de G .

Reciproquement, tous les p -Sylow de G sont conjugués dans G .

En fin, tout sous-groupe de G (i.e d'ordre une puissance de p) est contenu dans un p -Sylow.

Exercice

1. Soit G un groupe d'ordre 13. Est-il nécessairement abélien ? combien admet-il d'élément d'ordre 13 ? Puisque 13 est premier, G est nécessairement cyclique, donc isomorphe à $(\mathbb{Z}/13\mathbb{Z}, +)$, donc il est abélien. Il admet $\varphi(13) = 12$ éléments d'ordre 13.

De plus, le nombre n_p de p -Sylow de G vérifie :

$$\begin{aligned} n_5 &\equiv 1 \pmod 5 \\ n_5 &| 3 \end{aligned}$$

$\Rightarrow n_5 = 1$. Tous les sous-groupe d'un groupe abélien sont distingués.

Mais un groupe d'ordre 13 n'admet que deux sous-groupes (th de Lagrange) lui-même et $\{e\}$. Donc G est simple.

2. Montre qu'un grou d'ordre 15 n'est pas simple. $5 \mid 15$ donc existe sylow sous-groupe.
 Soit G un groupe d'ordre $15=3 \times 5$. G admet un 5-Sylow H . De plus le nombre n_5 de 5-Sylow de G vérifie : $n_5 = 1 \bmod 5$ et $n_5 \mid 3$ donc $n_5 = 1$.
 Les conjugués de H sont encore des 5-Sylow. Or, il n'y a qu'un seul 5-Sylow dans G . conclusion. G n'est pas simple.

1.5 Les Groupes symétriques

On note σ_n les groupes des permutations sur l'ensemble $\{1, \dots, n\}$.

Remarque. Deux permutations à supports disjoints commutent. Exemple : $\tau = (1, 2) \in \sigma_9$ et $\sigma = (3, 4, 5) \in \sigma_9$. Le support de τ est $\{1, 2\}$.

$$\tau\sigma = \sigma\tau$$

Theorem 6. *Tout permutation s'écrit comme produit de cycles à supports disjoints - une telle décomposition est unique à l'ordre près.*

Exemple : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 6 & 2 & 9 & 1 & 7 & 5 & 8 \end{pmatrix} \in \sigma_9$ $\sigma = (136)(24)(598)$

Par exemple : $\text{ord}(\sigma) = \text{ppcm}(\text{ord}(136), \text{ord}(24), \text{ord}(598)) = \text{ppcm}(3, 2, 3) = 6$

Autrement dit, on a : $\sigma^6 = \text{id}$ et 6 est la plus petite puissance non nulle vérifiant cela.

Calcul pratique du conjugué d'une permutation σ dans σ_n . Si $\tau \in \sigma_n$, $\tau\sigma\tau^{-1}$ est un conjugué de σ .

On décompose σ en produit de cycles : $\sigma = c_1 c_2 \dots c_l$, c_i cycles. D'où : $\tau\sigma\tau^{-1} = \tau(c_1 \dots c_r)\tau^{-1} = (\tau c_1 \tau^{-1})(\tau c_2 \tau^{-1}) \dots (\tau c_r \tau^{-1})$

Où, on a : $\tau(i_1 \dots i_m)\tau^{-1} = (\tau(i_1) \dots \tau(i_m))$ usur conjugué d'un cycle (i_1, i_2, \dots, i_m)

On effectue, l'image par la permutation de gauche et la permutation de droite de tout de $\tau(i_j)$, pour $j \in \{1, \dots, i_n\}$ et des antécédents coïncide.

On a $\forall i \in \{1, \dots, m\}$, $g(\tau(i_j)) = \tau(i_{j+1})$ et $f(\tau(i_j)) = (\tau(i_1 \dots i_m))(i_j) = \tau(i_{j+1})$ et $\forall x \in \{1, \dots, n\}$

$\{\tau(i_j), j \in \{1, \dots, n\}\}$, on a :

$$g(x) = x = f(x)$$

Donc $f = g$.

Exemple : Soit $\sigma = (1528) \in \sigma_9$, et soit $\tau = (127)$. $\tau\sigma\tau^{-1} = ? = (\tau(1)\tau(5)\tau(2)\tau(8)) = (2578)$

Proposition 3. *On appelle type d'une permutation $\sigma = c_1 \dots c_r$. La suite (l_1, \dots, l_r) des longueurs des cycles c_i ordonnés en ordre croissant $(l_1 \leq l_2 \leq \dots \leq l_r)$. Deux permutations sont conjuguées dans σ_n ssi elles ont même type.*

Par exemple : les permutations

$$G_1 = (28)(35)(196)$$

et

$$G_2 = (14)(79)(263)$$

Dont conjuguées dans σ_9 car elles ont tous deux le type $(2, 2, 3)$

La proposition précédente montre que le groupe σ_n est engendré par les cycles. On a également :

Theorem 7. 1. σ_n est engendré par les transpositions (2-cycles)

2. σ_n est engendré par les transpositions de la forme (1i)

3. σ_n est engendré par les transpositions (dits élémentaires) de la forme (i i + 1)

4. σ_n est engendré par les deux permutations (12) et (12...n)

Démonstration. exercice □

Proposition : la signature $\varepsilon : \sigma_n \rightarrow \{\pm 1\}$ est un morphisme de groupes. En particulier deux permutations conjuguées ont même signature. Transposition est impaire i de signature égale à -1 . Ainsi ε est un morphisme surjectif (de que $n \geq 2$), et une permutation est paire (i.e. de signature 1) ssi elle est produit d'un nombre pair de transpositions.

Une cycle de longueur paire est une permutation impaire et impaire paire.

Le noyau \mathfrak{A}_n du morphisme signature $\varepsilon : \mathfrak{S}_n \rightarrow \{-1, 1\}$ est un sous-groupe distingué d'indice 2 ($n \geq 2$) de \mathfrak{S}_n , appelé le n-ième groupe alterné = c'est donc l'ensemble des permutations paires de σ_n .

Proposition 4. Si $n \geq 3$, le groupe alterné \mathfrak{A}_n est engendré par les 3-cycles.

Démonstration. Hint (1b)(1a)=(1ab) □

Theorem 8 (Galois). \mathfrak{A}_n est un groupe simple ssi $n \neq 4$.

Chapitre 2

Représentations linéaires des groupes finis

Théorie introduite par Frobenius à la fin du XIX siècle.

2.1 Premières définitions, représentations, yep isomorphismes et rep. iuctis)

Définition 10. Une REPRÉSENTATION LINÉAIRE d'un groupe G est la donnée d'un \mathbb{C} -espace vectoriel V muni d'une action (à gauche) de G agissant de manière linéaire

$$\begin{aligned} G \times V &\rightarrow V \\ (g, v) &\mapsto g \cdot v, \end{aligned}$$

telle que :

1. $\forall x \in V, e \cdot x = x$ où x est l'élément neutre de G
2. $\forall g, g' \in G, \forall x \in V : g \cdot (g' \cdot x) = (gg') \cdot x$
3. $\forall g \in G, \forall x, x' \in V, \forall \lambda, \lambda' \in \mathbb{C} : g \cdot (\lambda x + \lambda' x') = \lambda g \cdot x + \lambda' g \cdot x'$

Définition 11. Une représentation linéaire d'un groupe G est donc la donnée d'un \mathbb{C} -espace vectoriel V et d'un morphisme de groupes :

$$\begin{aligned} \rho : G &\rightarrow GL(V) \\ g &\mapsto \rho(g) = \rho_g : V \rightarrow V. \end{aligned}$$

où $GL(V)$ est le groupe des automorphismes du \mathbb{C} -espace vectoriel V .

On a donc : $\forall g, g' \in G, \rho_{gg'} = \rho_g \circ \rho_{g'}$. Et aussi : $\rho_e = id_V$ et $\rho_{g^{-1}} =$

$$(\rho_g)^{-1} \forall g \in G$$

Ces deux définitions sont bien équivalents.

Démonstration. En effet, si G opère sur V de la manière linéaire a lois considérons l'application :

$$\rho : G \rightarrow ?$$

$$g \mapsto \left(\begin{array}{ccc} \rho_g : & V & \rightarrow V \\ & x & \mapsto \rho_g(x) = g \cdot x \end{array} \right)$$

ρ_g est un endomorphisme du \mathbb{C} -espace vectoriel V , car si $x, x' \in V$ et si $\lambda, \lambda' \in \mathbb{C}$ on a : $\rho_g(\lambda x + \lambda' x') = g(\lambda x + \lambda' x') = \lambda g \cdot x + \lambda' g \cdot x' = \lambda \rho_g(x) + \lambda' \rho_g(x')$

De plus, ρ_g est bijectif car $\ker \rho_g = \{0\}$; en effet soit $x \in V$ on a : $\rho_g(x) = 0 \Rightarrow g \cdot x = 0$ d'où $g^{-1}g \cdot x = \rho^{-1}0 = \rho_{g^{-1}}(0) = 0$, d'où $(g^{-1}g) \cdot x = 0$ d'où $e \cdot x = 0 \Rightarrow x = 0$

Si l'on suppose V de dimension fini alors ρ_g est bijectif et ρ est à valeurs dans $GL(V)$.

De plus, l'application ρ est un morphisme de groupes. En effet, si $g, g' \in G$ et si $x \in V$, on a : $f_{gg'} = (gg') \cdot x = g \cdot (g' \cdot x) = \rho_g(\rho_{g'}(x))$.

Réciproquement (\Rightarrow). i $\rho : G \rightarrow GL(V)$,
 $g \mapsto \rho_g$ est un morphisme de groupes, alors considérons :

$$G \times V \rightarrow V$$

$$(g, x) \mapsto g \cdot x := \rho_g(x)$$

Cela définit bien une action linéaire de G sur V car :

1. Si $x \in V$, $e \cdot x = \rho_e(x) \stackrel{*}{=} id_V(x) = x$ (* car l'image de l'élément neutre par morphisme de groupes est l'élément neutre)
2. Si $g, g' \in G$, $x \in V$: $g \cdot (g' \cdot x) = \rho_g(\rho_{g'}(x)) = (\rho_g \rho_{g'})(x) \stackrel{\rho - \text{morphisme}}{=} \rho_{gg'}(x) = (gg') \cdot x$
3. $g \cdot (\lambda x + \lambda' x') = \rho_g(\lambda x + \lambda' x') = \lambda \rho_g(x) + \lambda' \rho_g(x') = \lambda g \cdot x + \lambda' g \cdot x'$

□

Définition 12 (Vocabulaire).

- L'espace vectoriel V est l'**espace de la représentation**.
- La dimension de V est le **degree** (ou la **dimension**) de la représentation.
- Lorsque ρ est injectif, la représentation est dite **fidèle**. Le groupe G se représente alors de manière concrète comme un sous-groupe de $GL(V)$.
- Lorsque V est dimension finie (ce qui est toujours le cas par la suite). Le choix d'une base fournit alors une représentation encore plus concrète comme groupe de matrices (ou si $\dim_{\mathbb{C}} V = n$ alors $GL(V) \simeq GL_n(\mathbb{C})$).

Remarque. Soient G un groupe fini et $\rho : G \rightarrow GL(V)$ une représentation (linéaire) de G . Si $g \in G$ est d'ordre n alors, on a :

$$(\rho_g)^n = \rho_{g^n} = \rho_e = id_v = "1"$$

Donc l'endomorphisme ρ_g est racine du polynôme $x^n - 1$, que n'a que des racines simples (à savoir les racines n -ème de l'unité dans \mathbb{C} , que sont : $e^{\frac{2h\pi}{n}}$, $h \in \{0, \dots, n\}$).

Rappel. $f \in \text{End}(V)$, $I_f = \{P(x) \in \mathbb{C}[x] \mid P(f) = 0\}$ idéal de l'anneau principal $\mathbb{C}[x]$. (car \mathbb{C} est un corps) L'unique polynôme unitaire que engendre I_f est appelé la polynome minimal de f .

La polynôme minimal de ρ_g est donc un divisor de $x^n - 1$ et n'a donc lui aussi que de racines simples. Ce la pon que l'endomorphisme ρ_g est diagonalisable (car tous ses valeurs propre sont donc simples).

Exemple 2.1.1. 1. La représentation **triviale** (on représentation unité).

$$\begin{aligned}\rho : G &\rightarrow GL(\mathbb{C}) \simeq \mathbb{C}^* \\ g &\mapsto (\rho_g : id : \mathbb{C} \rightarrow \mathbb{C} \ x \mapsto x)\end{aligned}$$

2. Les représentation de degré 1 : ce sont les homomorphismes $\rho : G \rightarrow \mathbb{C}^*$ puisque si $\dim V = 1$ alors $GL(V) \simeq \mathbb{C}^*$. En effet les endomorphismes de V sont les homothétis : $f_\lambda : V \rightarrow V \ x \mapsto \lambda x (\lambda \in \mathbb{C}^*)$. Et $GL(V) \rightarrow G^*$ est un isomorphisme $f_\lambda \mapsto \lambda$.

Si G est fini, tout elements du G est d'ordre fini (par le th. de Lagrange) donc, pour tout $g \in G$, ρ_g est un racine de l'unité dans \mathbb{C} . (Car si $g^n = e$ alors $\rho_{g^n} = (\rho_g)^n$). En particulier, ce sont des numbers complexes de mondle 1. $|\rho_g| = 1$.

3. Soient \mathfrak{S}_n considéré le groupesymétrique et (e_1, \dots, e_n) la base canonique de \mathbb{C}^n . On définit une représentation de degré n de \mathfrak{S}_n en posant :

$$\begin{aligned}\rho : \mathfrak{S}_n &\rightarrow GL(\mathbb{C}^n) \\ \sigma &\mapsto \begin{pmatrix} \rho_\sigma : \mathbb{C}^n & \rightarrow & \mathbb{C}^n \\ e_i & \mapsto & \rho_\sigma(e_i) = e_{\sigma(i)} \end{pmatrix}\end{aligned}$$

4. La **représentation de permutation** c'est un généralisation l'exemple précédent. Soit $G \times X \rightarrow X$ une action $(g, x) \mapsto g \cdot x$ d'un groupe G sur un ensemble fini X . Soit V un \mathbb{C} espace vectoriel de dimension égale au cardinal de X , dune base indexée par les elements de X : $\{\varepsilon_x, x \in X\}$. On a donc : $V = \bigoplus_{x \in X} \langle \varepsilon_x \rangle = \bigoplus_{x \in X} \mathbb{R}_{\varepsilon_x}$. On définit une re linéaire

$$\rho : G \rightarrow GL(V) \ g \mapsto (\rho_g : V \rightarrow V \ \varepsilon_x \mapsto \rho_g(\varepsilon_x) = \varepsilon_{g \cdot x})$$

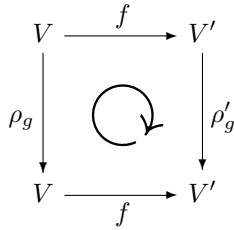
C'est la représentation de permutation associé à l'action de G sur X .

Remarque. On peut voir V comme l'espace vectoriel complexe des fonctions d'finies sur X et à valeurs dans \mathbb{R} , le fonction ε_x étant l'indicatrice de $x \in X$: $e_x(y) = 1 \text{ si } x = y, 0 \text{ si } x \neq y, y \in X$

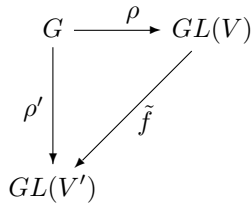
5. La représentation Régulière. C'est l'exemple precedent avec $X = G$ agissant sur lui-même translation à gauche :

$$\rho : G \rightarrow GL(V)g \mapsto (\rho_g : V \rightarrow V \varepsilon_x \mapsto \varepsilon_g \cdot x).$$

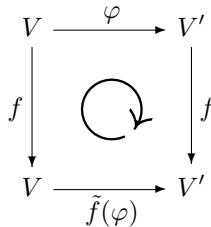
Définition 13. Deux représentation linier $\rho : G \rightarrow GL(V)$ et $\rho' : G \rightarrow GL(V')$ d'un groupe G . Sont dites ISOMORPHES ou ÉQUIVALENTS s'il existe un isomorphisme d'espace vectoriels $f : V \rightarrow V'$ tel que l'on ont : $\forall g \in G, \rho'_g \circ f = f \circ \rho_g$.



On peut exprimer cette condition par la commutativité diagramme :



où $\tilde{f} : GL(V) \rightarrow GL(V')$ designe l'isomorphisme suivant defini par : $\tilde{f}(\varphi) = f \circ \varphi \circ f^{-1}, \forall \varphi \in GL(V)$



En termes de matrices, cela signifie que les matrices associés à la premier represantion sont semblables à leurs homologués dans la seconde, via la même matrice de passage :

$$\forall g \in G, \text{Mat}(\rho'_g) = \text{Mat}(f) \times \text{Mat}(\rho_g) \times \text{Mat}(f)^{-1}$$

(A, B Semblables si $\exists P : B = PAP^{-1}$)

Si $\rho : G \rightarrow GL(V)$ est une représentation d'un groupe G . Si W est un sous-espace vectoriel de V STABLE par les différents automorphismes ρ_g pour $g \in G$ i.e $\rho_g(W) \subset W$

(i.e $\forall g \in G, \forall w \in W, \rho_g(w) \in W$)

Alors on peut considérer la sous-représentation :

$$\begin{aligned}\rho|_x : G &\rightarrow GL(W) \\ g &\mapsto \rho_g|_W\end{aligned}$$

Remarque. $\forall w \in W, \rho_g|_W(w) = \rho_g(w) \in W$

Cela produit à le notion de représentation inéducable :

Définition 14. Une représentation $\rho : G \rightarrow GL(V)$ est dite IRRÉDUCTIBLE si les seules sous-espaces *stables* de V sont $\{0\}$ et V .

Ainsi les reparamétrisation de *degré 1* constituent des représentations irréductibles particuliers.

2.2 Théorème de Maschke

Définition 15. On définit le SOMME DIRECTE de représentation de groupe fini G . Soient $\rho : g \rightarrow GL(V)$ et $\rho' : G \rightarrow GL(V')$ deux représentations de G . On définit la somme directe $\rho \oplus \rho'$ comme étant : La représentation d'espace vectoriel $V \oplus V'$ défini par :

$$\begin{aligned}\rho \oplus \rho' : G &\rightarrow GL(V \oplus V') \\ g &\mapsto (\rho \oplus \rho')_g\end{aligned}$$

definit par $\forall v \in V, \forall v' \in V' : (\rho \oplus \rho')_g(v + v') = \rho_g(v) + \rho'_g(v')$

Theorem 9 (Théorème de Maschke). *Toute représentation linéaire complexe de degré fini d'un groupe fini est somme directe de représentation irréductibles.*

Lemme 1. *Tout sous-espace stable d'une représentation linéaire complexe de degré fini d'un groupe fini admet un sous-espace **Supplémentaire Stable**.*

Preuve du Lemma. Il existe un produit scalaire hermitien sur l'espace de la représentation stable sous l'action du groupe. En effet, si $\langle \cdot, \cdot \rangle$ désigne un produit scalaire quelconque sur V , le produit scalaire suivant est stable par ρ : Pour $x, y \in V$:

$$\langle x, y \rangle_\rho = \frac{1}{|G|} \sum_{g \in G} \langle \rho_g(x), \rho_g(y) \rangle$$

En effet, si $h \in G$, on a ;

$$\langle \rho_h(x), \rho_h(y) \rangle_\rho = \frac{1}{|G|} \sum_{g \in G} \langle \rho_g(\rho_h(x)), \rho_g(\rho_h(y)) \rangle = \frac{1}{|G|} \sum_{g \in G} \langle \rho_{gh}(x), \rho_{gh}(y) \rangle = \langle x, y \rangle_\rho$$

car $g \mapsto gh$ est une bijection de G sur lui-même. Si W est un sous-espace vectoriel de V stable sous l'action de G alors le supplémentaire orthogonal de W est lui aussi stable sous l'action puisque :

x orthogonal à $W \iff \rho_g(x)$ orthogonal $\rho_g(W) = W$

□

Démonstration du Théorème. On fait une récurrence sur la dimension de l'espace vectoriel de la représentation.

Si $\dim V = 1$ ou si V est irréductible : Ok.

Si $\dim V \geq 2$ et V est non irréductible alors V possède de un sous-représentation W . Distincte de $\{0\}$ et V .

Si $\langle \cdot, \cdot \rangle$ est un produit scalaire hermitien sur V invariant sous l'action de G , le supplémentaire orthogonal W^\perp de W est lui aussi stable sous l'action de G .

On a lors : $V = W \oplus W^\perp$ et W et W^\perp sont de dimensions $< \dim V$. L'hypothèse de récurrence permet de les décomposer comme des sommes directes de représentation irréductibles, ce que prouve qu'on peut en faire autant de V . □

2.3 Caractère d'une représentation

Définition 16. On appelle CARACTÈRE DE LA REPRÉSENTATION $\rho : g \mapsto GL(V)$ l'application :

$$\begin{aligned} \chi_\rho : G &\rightarrow \mathbb{C} \\ g &\mapsto \chi_\rho(g) = \text{Tr}(\rho_g) \end{aligned}$$

où $\text{Tr}(\rho_g)$ — désigne la **trace** de l'endomorphisme ρ_g .

Proposition 5. Soit $\rho : G \mapsto GL(V)$ une représentation d'un groupe fini G de caractère χ_ρ :

1. $\chi_\rho(x) = \dim V = \ll \text{degré de } \rho \gg =: \ll \text{degré de } \chi_\rho \gg$
2. $\forall g \in G, \chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$ — conjugué complexe
3. $\forall g, h \in G, \chi_\rho(ghg^{-1}) = \chi_\rho(h)$ i.e χ_ρ est ue fonction **centrale** sur G
4. $\chi_{\rho \oplus \rho'} = \chi_\rho + \chi_{\rho'}$ si $\rho' : g \mapsto GL(V')$ représentation
5. Si ρ et ρ' sont équivalents alors $\chi_\rho = \chi_{\rho'}$

Démonstration. 1. $\chi_\rho(e) = \text{Tr}(\rho_e) = \text{Tr}(\text{Id}_V) = \dim V$

2. Si G est fini et si $g \in G$, les *valeurs propres* de l'endomorphisme ρ_g sont des racines de l'unité. En particulier, elles sont de module 1 et donc $\lambda^{-1} = \bar{\lambda}$ si λ est un valeur pros de ρ_g .

Remarquons que les valeurs props de l'endomorphisme $\rho_{g^{-1}} = \rho_g^{-1}$ sont les inverses de celles de ρ_g (en effet si $f(x) = \lambda x$ — endomorphisme alors $x = f^{-1}(f(x)) = f^{-1}(\lambda x) = \lambda f^{-1}(x)$ donc $f^{-1}(x) = \frac{1}{\lambda}x$).

Puisque la trace d'endomorphisme diagonalisable est égale à la somme des valeurs propres comptés avec multiplicités, on en déduit que :

$$\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}, \forall g \in G.$$

3. Si $g, h \in G$, on a : $\chi_\rho(ghg^{-1}) = \text{Tr}(\rho_{ghg^{-1}}) = \text{Tr}(\rho_g \circ \rho_h \circ \rho_g^{-1}) = \text{Tr}(\rho_h) \stackrel{\text{Tr}(AB) = \text{Tr}(BA)}{=} \chi_\rho(h)$. χ_ρ prend la même valeur sur tous les éléments d'une classe de conjugaison.

4. Si (e_1, \dots, e_n) est une base de V et (e'_1, \dots, e'_m) est une base de V' alors :

$$(e_1, 0), (e_2, 0), \dots, (e_n, 0), (0, e'_1), (0, e'_2), \dots, (0, e'_m)$$

est une base de $V \oplus V'$ et la matrice de $(\rho \oplus \rho')_g$ est $\begin{pmatrix} \text{Mat}(\rho_g) & 0 \\ 0 & \text{Mat}(\rho'_g) \end{pmatrix}$ dont la trace est la somme des traces de $\text{Mat}(\rho_g)$ et $\text{Mat}(\rho'_g)$

5. Invariance de la trace par changement de base.

□

Exemple 2.3.1. Exemples de calculs de caractères :

1. Si G est un groupe opérant sur un ensemble fini X , considérons la représentation de permutations ρ associée :

$$\begin{aligned} \rho : G &\rightarrow GL(V) \\ g &\mapsto \begin{pmatrix} \rho_g : V \rightarrow V \\ e_x \mapsto e_{g \cdot x} \end{pmatrix} \end{aligned}$$

où $V = \bigoplus_{x \in X} \langle e_x \rangle$.

$$\text{On a : } \begin{aligned} \chi_\rho : G &\rightarrow \mathbb{C} \\ g &\mapsto \text{Tr}(\rho_g) \end{aligned}$$

Dans la base $(e_x)_{x \in X}$ de V , pour $g \in G$ fixe, la matrice du ρ_g est une matrice de permutation i.e. a exactement un 1 par ligne et par colonne et tous les autres coefficients sont nuls.

De plus, si $\text{Mat}_{(e_x)}(\rho_g) = (a_{ij})$ alors le terme diagonal : $a_{xx} = 1 \Leftrightarrow g \cdot x = x \Leftrightarrow x$ est un point fixe de g , sinon $a_{xx} = 0$.

On en déduit que : $\chi_\rho(g) = \text{Tr}(\rho_g) = \#\{x \in X \mid g \cdot x = x\}$

2. Caractère de la représentation régulière. Cas particulier de la rep de permutation avec G fini, $X = G$, l'action étant la multiplication : $g \cdot x = gx$ si $g, x \in G$. On a alors : $\chi_\rho(g) = \text{Tr}(\rho_g) = \#\{x \in G \mid gx = x\} = \begin{cases} |G| & \text{si } g = e, \\ 0 & \text{sinon} \end{cases}$.

Définition 17. Nous qualifierons d'irréductible tout caractère d'une représentation irréductible.

Le tableau des caractères (irréductible) d'un groupe fini G est un tableau à c lignes et c colonnes, où c est le nombre de classes de conjugaison de G , dont les entrées sont les valeurs de caractères irréductibles sur les classes de conjugaison de G . (nous venons qu'il y a autant de classes d'isomorphisme de caractère irréductible, que de classes de conjugaison.)

2.4 Orthogonalité des caractères.

Soit G un groupe fini. On considère le \mathbb{C} -espace vectoriel $\mathcal{F}(G)$ des fonctions complexes définies sur G ($f : G \mapsto \mathbb{C}$) que l'on munit de la structure hermitienne donnée par le produit scalaire. Pour $\varphi, \psi \in \mathcal{F}(G)$:

$$\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} \psi(g).$$

On a : $\dim_{\mathbb{C}} \mathcal{F}(G) = |G|$. En effet, si $f \in \mathcal{F}(G)$ alors $f = \sum_{g \in G} \lambda \text{Ind}_g$ où $\begin{matrix} \text{Ind}_g : G & \mapsto & \mathbb{C} \\ x & \mapsto & \begin{cases} 1 & x = g \\ 0 & \text{sinon} \end{cases} \end{matrix}$ (avec $\lambda = f(g) \Rightarrow f = \sum_{g \in G} f(g) \text{Ind}_g$) donc $(\text{Ind}_g)_{g \in G}$ base de $\mathcal{F}(G)$.

Proposition 6. Les caractères irréductibles d'un groupe G forment un système orthonormal de fonctions de l'espace vectoriel hermitien $\mathcal{F}(G)$. I.e. si χ et χ' sont les caractères une de G alors $\langle \chi, \chi' \rangle = \begin{cases} 1 & \text{si } \chi = \chi' \\ 0 & \text{sinon} \end{cases}$.

Démonstration. Soient $\rho : G \mapsto GL(V)$ et $\rho' : G \mapsto GL(V')$ deux représentations irréductibles de G et soient $\chi : G \rightarrow \mathbb{C}$ et $\chi' : G \rightarrow \mathbb{C}$ leurs caractères associés ; et soit $\text{Mat}(\rho_g) = (a_{ij}(g))_{\substack{1 \leq i \leq d \\ 1 \leq j \leq d}}$ et $\text{Mat}(\rho'_g) = (a'_{ij}(g))_{\substack{1 \leq i' \leq d' \\ 1 \leq j' \leq d'}}$ (où $d = \deg(\rho) = \dim V$ et $d' = \deg(\rho') = \dim V'$).

On a :

$$\chi(g) = \text{Tr}(\rho_g) = \sum_{i=1}^d a_{ii}(g)$$

et

$$\chi'(g) = \text{Tr}(\rho'_g) = \sum_{i=1}^{d'} a'_{ii}(g).$$

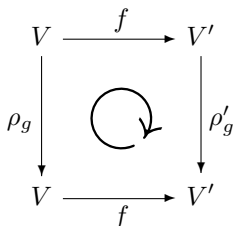
D'où :

$$\begin{aligned} \langle \chi, \chi' \rangle &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \chi'(g) = \frac{1}{|G|} \sum_{g \in G} \sum_{i,j} \overline{a_{ii}(g)} a'_{jj}(g) \\ &= \begin{cases} 0 & \text{si } \rho \text{ et } \rho' \text{ sont non-isomorphes} \\ 1 & \text{si } \rho \simeq \rho' \text{ (d'où : } \chi = \chi') \end{cases} \end{aligned}$$

par le lemme de Schur (traduit en relations algébriques)

□

Lemme 2 (Lemme de Schur). Soient $\rho : G \mapsto GL(V)$ et $\rho' : G \mapsto GL(V')$ deux représentations linéaire irréductibles d'un groupe fini G et $f : V \rightarrow V'$ un morphisme compatible avec les deux représentations (i.e. $\forall g \in G, f \circ \rho_g = \rho'_g \circ f$).



Si les deux représentations ne sont pas isomorphes alors $f = 0$. Sinon f est un isomorphisme et (en identifiant V et V') on a : $f = \lambda \text{Id}$, $\lambda \in \mathbb{C}$ (i.e. f est une homothétie).

Remarque. Cas particuliers des caractères (irréductible) de représentations (irréductibles) de degré 1 d'un groupe G :

$$\begin{aligned} \rho : G &\rightarrow \mathbb{C}^* \\ g &\mapsto \rho_g \end{aligned}$$

le caractère χ associé à cette représentation ρ est

$$\begin{aligned} \chi : G &\rightarrow \mathbb{C} \\ g &\mapsto \chi(g) = \text{Tr}(\rho_g) = \rho_g \end{aligned} .$$

Donc $\chi = \rho$; χ est appelé un caractère **linéaire**.

Exercice. On note \hat{G} l'ensemble des caractères linéaires de G : $\hat{G} = \{\text{morphisms } \chi : G \mapsto \mathbb{C}^*\}$. On définit le produit $\chi\chi'$ de deux caractères linéaires de G par : $\forall g \in G$: $(\chi\chi')(g) = \chi(g)\chi'(g)$.

1. Montrer que \hat{G} , muni ce produit, est un groupe abélien.
2. On rappelle que le caractère trivial est défini par :

$$\begin{aligned} \chi_0 : G &\rightarrow \mathbb{C}^* \\ g &\mapsto 1 \end{aligned} .$$

Montrer que, si G est fini, et si $\chi \in \hat{G}$ alors : $\frac{1}{|G|} \sum_{g \in G} \chi(g) = \begin{cases} 1 & \text{si } \chi = \chi_0 \\ 0 & \text{sinon} \end{cases}$.

3. En déduire les relations d'orthogonalité des caractères linéaires. Si $\chi, \chi' \in \hat{G}$ alors :

$$\langle \chi, \chi' \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \chi'(g) = \begin{cases} 1 & \text{si } \chi = \chi' \\ 0 & \text{sinon} \end{cases} .$$

Chapitre 3

Exercices

3.1 $\mathbb{Z}/91\mathbb{Z}$

Exercice Résoudre l'équation $x^2 - 1 = 0$ dans $\mathbb{Z}/91\mathbb{Z}$. L'anneau $\mathbb{Z}/91\mathbb{Z}$ est-il un corps ?

Remarque. Un polynôme dans un corps K ne peut avoir plus d'une racine.

Rappel :

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier. On a $91 = 7 \times 13$ donc $\mathbb{Z}/91\mathbb{Z}$ n'est pas un corps.

Si A est un anneau unitaire on note A^* l'ensemble des éléments inversibles de A . (i.e. qui admettent un symétrique pour la multiplication). Alors (A^*, \times) est un groupe. On a :

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$$

où $a \in \mathbb{Z}$ et $\bar{a} = a + n\mathbb{Z}$.

On définit la fonction indicatrice d'Euler φ pour : $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*| =$ le nombre d'entier $\leq n$ et premier avec n .

D'où $|(\mathbb{Z}/91\mathbb{Z})^*| = \varphi(91) = ?$. D'après le Théorème des restes chinois on a :

$$\text{rcl} \mathbb{Z}/91\mathbb{Z} \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \text{ car } (7, 13) = 1 \tag{3.1}$$

$$x + 91\mathbb{Z} \mapsto (x + 7\mathbb{Z}, x + 13\mathbb{Z}) \tag{3.2}$$

On en déduit un isomorphisme sur les groupes multiplicatifs : $(\mathbb{Z}/91\mathbb{Z})^* \simeq ((\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/13\mathbb{Z})^*)$.

D'où : $\varphi(91) = |(\mathbb{Z}/91\mathbb{Z})^*| = |(\mathbb{Z}/7\mathbb{Z})^*| \times |(\mathbb{Z}/13\mathbb{Z})^*| = \varphi(7)\varphi(13) = 6 \times 12 = 72$

(7 est premier $\Rightarrow (\mathbb{Z}/7\mathbb{Z})^*$ est un corps $\Rightarrow (\mathbb{Z}/7\mathbb{Z})^* = (\mathbb{Z}/7\mathbb{Z}) \setminus \{\bar{0}\}$ $\Rightarrow \varphi(7) = 6$.

p -premier $\Rightarrow \varphi(p) = p - 1$.

On a : $x^2 - \bar{1}$ dans $\mathbb{Z}/91\mathbb{Z}$ où $\bar{a} = a + 91\mathbb{Z}$. On a : $x^2 - \bar{1} = \bar{0} \Leftrightarrow x^2 = \bar{1}$. $\bar{1}$ est solution évidente $-\bar{1} = \bar{90}$ est aussi solution évidente. Déterminons le nombre de solution de cette équation.

Remarque. Soit G un groupe(multiplicatif) et x un élément de G . $x^n = e \Leftrightarrow \text{ord}(x) | n$.
 $x^2 = 1$ dans $(\mathbb{Z}/91\mathbb{Z})^*$ signifie que x est d'ordre divisant 2 i.e. d'ordre 1 ou 2.

On l'élément neutre $\bar{1}$ est le seul élément d'ordre 1 dans $(\mathbb{Z}/91\mathbb{Z})^*$. On cherche donc \bar{a} present éléments d'ordre 2 de $(\mathbb{Z}/91\mathbb{Z})^*$.

Rappel : Si $f : G \rightarrow G'$ est un isomprphisme de groupes alors : $\text{ord}(f(x)) | \text{ord}(x)$, $\forall x \in G$.

On cherche donc les éléments d'ordre 2 de $(\mathbb{Z}/91\mathbb{Z})^* \simeq (\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/13\mathbb{Z})^*$. Soit $(\bar{a}, \bar{b}) \in (\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/13\mathbb{Z})^*$ $\text{ord}((\bar{a}, \bar{b})) = \text{ppcm}(\text{ord}(\bar{a}), \text{ord}(\bar{b}))$. (plus petit common multiple).

$$\text{ord}(\bar{a}, \bar{b}) = 2 \Leftrightarrow \text{ppcm}(\text{ord}(\bar{a}), \text{ord}(\bar{b})) = 2$$

Par le Th. de Lagrange on a :

$$\text{ord}(\bar{a}) | (\mathbb{Z}/7\mathbb{Z})^* \quad \text{i.e.} \quad \text{ord}(\bar{a}) | 6$$

$$\text{ord}(\bar{b}) | (\mathbb{Z}/13\mathbb{Z})^* \quad \text{i.e.} \quad \text{ord}(\bar{b}) | 12$$

Rappel. — Si p est premier alors $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique.

— Si p est premier impair et si $m \geq 1$ alors $(\mathbb{Z}/p^m\mathbb{Z})^*$ est cyclique d'ordre $\varphi(p^m) = (p-1)p^{m-1}$

— $(\mathbb{Z}/2\mathbb{Z})^*$ et $(\mathbb{Z}/4\mathbb{Z})^*$ sont cyclique et si $m \geq 3$ alors $(\mathbb{Z}/2^m\mathbb{Z})^* \simeq (\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/2^{m-1}\mathbb{Z})^*$

Si G est un groupe cyclique d'ordre n et si d est un divisem de n alors G admet un sous-groupe d'ordre d et un seul et il est cyclique.

En particulier, de plus, les gènèrators du groupd (aditif) $(\mathbb{Z}/n\mathbb{Z})$ sont les \bar{a} avec $a \in \{1, \dots, n\}$ et $(a, n) = 1$. Il y en a donc : $\varphi(n)$.

En particulier, le groupe cyclique G admet $\varphi(d)$ éléments d'ordrde d (d étant un divisem de l'ordre de G).

D'où $(\text{ord}(\bar{a}), \text{ord}(\bar{b})) \in \{(1, 2), (2, 1), (2, 2)\}$. Conclusion. Il y a donc trois elementes d'ordre 2 dans $(\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/13\mathbb{Z})^*$, i.e. aussi $(\mathbb{Z}/91\mathbb{Z})^*$. L'equation $x^2 = 1$ admet donc 4 solutions dans $(\mathbb{Z}/91\mathbb{Z})^*$.

Rappel. Si G est un groupecyclique d'ordre n engendré par g alors :

$$\text{ord}(g^m) = \frac{n}{(n, m)}.$$

Remarque. $G = (\mathbb{Z}/7\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ $\text{ord}(\bar{2}) = 3$, $\text{ord}(\bar{3}) = 6$ (just check). $\bar{3}$ — generator.

$$D'o\grave{u} \langle \tilde{3} \rangle = \left(\mathbb{Z}/7\mathbb{Z} \right)^* . \text{ ord}(\tilde{3}^m) = 2 \Leftrightarrow \frac{6}{(6,m)} = 2 \Leftrightarrow (6,m) = \frac{6}{2} = 3 \Leftrightarrow m = 3 .$$

Conclusion $\tilde{3}^3 = \tilde{6}$ est d'ordre 2 dans $\left(\mathbb{Z}/7\mathbb{Z} \right)^*$.

Donc, les éléments d'ordre 2 de $\left(\mathbb{Z}/7\mathbb{Z} \right)^* \times \left(\mathbb{Z}/13\mathbb{Z} \right)^*$ sont : $(\tilde{1}, -\tilde{1}), (-\tilde{1}, \tilde{1}), (-\tilde{1}, -\tilde{1})$.
 $\left(\mathbb{Z}/91\mathbb{Z} \right) \rightarrow \left(\mathbb{Z}/7\mathbb{Z} \right)^* \times \left(\mathbb{Z}/13\mathbb{Z} \right)^*$

$$\overline{64} \stackrel{?}{\mapsto} (\tilde{1}, -\tilde{1})$$

$$\overline{27} \stackrel{?}{\mapsto} (-\tilde{1}, \tilde{1})$$

$$\overline{90} \stackrel{?}{\mapsto} (-\tilde{1}, -\tilde{1})$$

$$-\overline{13} \mapsto (\tilde{1}, \tilde{0}) (!)$$

$$\overline{14} \mapsto (\tilde{0}, \tilde{1}) (!)$$

$$(\tilde{1}, -\tilde{1}) = (\tilde{1}, \tilde{0}) + (\tilde{0}, \tilde{1}) = \varphi(-\overline{13}) - \varphi(\overline{14}) = \varphi(-\overline{13} - \overline{14}) = \varphi(-\overline{27}) = \varphi(\overline{64}) .$$

Déterminons une identité de Bezout entrée les entier premiers entre eux 7 et 13, au moyen de l'algorithme d'Euclide étendre :

$$\begin{array}{rcl} 13 & = & 7 \times 1 + 6 \\ 7 & = & 6 \times 1 + 1 \\ 1 & = & 7 - 6 \times 1 = 7 - (13 - 7 \times 1) \times 1 = 13 \times (-1) + 7 \times 2 = 1 \end{array}$$

remember -13 and 14.

Remarque. On a : $\left(\mathbb{Z}/91\mathbb{Z} \right)^* \stackrel{\text{Th. de rests chinois car } (7, 13) = 1}{\simeq} \left(\mathbb{Z}/7\mathbb{Z} \right)^* \times \left(\mathbb{Z}/13\mathbb{Z} \right)^* \simeq \left(\mathbb{Z}/6\mathbb{Z} \right)^* \times \left(\mathbb{Z}/12\mathbb{Z} \right)^* \not\simeq \left(\mathbb{Z}/72\mathbb{Z} \right)^*$ car $(6, 12) \neq 1$. Conclusion : le groupe $\left(\mathbb{Z}/91\mathbb{Z} \right)^*$ n'est pas cyclique.

3.2 Sylow

Exemple 3.2.1. 1. Soit G un groupe d'ordre 33.

- Détermine le nombre de 3-Sylow de G . Le groupe G peut'il être simple ?
- Déterminer le nombre de 11-Sylow de G . En déduire que G nécessairement abélien. Est-il nécessairement cyclique ?

Solution :

- D'après le 1^{er} Th. de Sylow, le nombre n_3 de 3-Sylow de G vérifie :

$$\begin{cases} n_3 = 1 \pmod{3} \\ n_3 | 11 \end{cases}$$

D'où : $n_3 = 1$. G admet donc un unique 3-Sylow H . Or, d'après 2^{ème} Th de Sylow, les conjugués d'un 3-Sylow sont encore un 3-Sylow.

Donc les conjugués de H sont égaux à H . Donc $H \triangleleft G$. Le groupe G admet donc un sous-groupe distingué n'est pas simple.

2. De même, le nombre n_{11} de 11-Sylow de G vérifie :

$$\begin{cases} n_{11} \equiv 1 \pmod{11} \\ n_{11} \mid 3 \end{cases}$$

D'où : $n_{11} = 1$. G admet donc un unique 11-Sylow K et, de même, il est distingué dans G . On a :

- (a) $H < G$, $K < G$
 (b) $H \cap K = \{e\}$ car H et K sont d'ordres premiers entre eux (si $g \in H \cap K$ alors d'après le th de Lagrange, on a :

$$\begin{cases} \text{ord}(g) \mid |H| \\ \text{ord}(g) \mid |K| \end{cases}$$

- (c) $G = HK$ car $\#HK = \frac{|H| \times |K|}{|H \cap K|} = \frac{3 \times 11}{1} = 33 = |G|$.

D'où : $G \simeq H \times K$ (G est isomorphe au produit direct interne de H par K).

Or H est d'ordre 3, et 3 est premier, donc H est cyclique et donc $H \simeq \mathbb{Z}/3\mathbb{Z}$. De même : K est d'ordre 11 et 11 est premier, donc K est cyclique et donc $K \simeq \mathbb{Z}/11\mathbb{Z}$. Donc : $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ donc G est abélien. Par le Théorème des restes Chinois puisque $(3, 11) = 1$, on a :

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \simeq \mathbb{Z}/33\mathbb{Z}.$$

Donc $G \simeq \mathbb{Z}/33\mathbb{Z}$. G est cyclique.

Exemple 3.2.2. On considère le groupe des inversibles $(\mathbb{Z}/33)^*$ de l'anneau $\mathbb{Z}/33$.

1. Quel est l'ordre de $(\mathbb{Z}/33)^*$?
2. Le groupe $(\mathbb{Z}/33)^*$ est-il cyclique ?
3. Admet-il un élément d'ordre 4 ?
1. On a : $|(\mathbb{Z}/33)^*| = \varphi(33) = \varphi(3 \times 11) = |\text{car}(3, 11)| = \varphi(3) \times \varphi(11) = 2 \times 10 = 20$, car $\varphi(p^k) = (p-1)p^{k-1}$.

Remarque. A-t-on $\bar{12} \in (\mathbb{Z}/33)^*$? (où $\bar{a} = a + 33\mathbb{Z}$). Non car $(12, 33) \neq 1$.

$|(\mathbb{Z}/33)^*| = \text{nombre d'éléments} \leq 33$ et premiers avec 33.

2. D'après le Th. des Restes Chinois, puisque $(3, 11) = 1$, on a un iso-

morphisme d'anneaux

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \simeq \mathbb{Z}/33\mathbb{Z}$$

qui induit un isomorphisme de groupes sur les groupes des inversibles :

$$\left(\mathbb{Z}/3\mathbb{Z}\right)^* \times \left(\mathbb{Z}/11\mathbb{Z}\right)^* \simeq \left(\mathbb{Z}/33\mathbb{Z}\right)^*$$

Rappel. Si p est un premier impair et si $m \geq 1$ alors :

$$\left(\mathbb{Z}/p^m\mathbb{Z}\right)^* \simeq \mathbb{Z}/(p-1)p^{m-1}\mathbb{Z}$$

$$\left(\mathbb{Z}/2^m\mathbb{Z}\right)^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-1}\mathbb{Z}$$

Alors $\left(\mathbb{Z}/33\mathbb{Z}\right)^* \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/10\mathbb{Z}) \not\simeq \mathbb{Z}/20\mathbb{Z}$ car $(2, 10) \neq 1$. Donc $\left(\mathbb{Z}/33\mathbb{Z}\right)^*$ n'est pas cyclique.

3. Soit $(a, b) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$. $\text{ord}((a, b)) = \text{ppcm}(\text{ord}(a), \text{ord}(b))$.
Où : $\text{ord}(a, b) = 4 \leftrightarrow \text{ppcm}(\text{ord}(a), \text{ord}(b)) = 4$, avec $\text{ord}(a)|2$
et $\text{ord}(b)|10$ — impossible. Donc le groupe $\left(\mathbb{Z}/33\mathbb{Z}\right)^*$ n'admet pas d'élément d'ordre 4.

3.3 \mathfrak{S}_4 et \mathfrak{A}_4

$\mathfrak{A}_4 < \mathfrak{S}_4$ — permutations paires de \mathfrak{S}_4 .

On fait agir \mathfrak{S}_4 sur lui-même par conjugaison :

$$\begin{aligned} \mathfrak{S}_4 \times \mathfrak{S}_4 &\rightarrow \mathfrak{S}_4 \\ (g, h) &\mapsto g \cdot h = ghg^{-1} \end{aligned}$$

Exercice 1. 1. Montrer que cette définit bien une action. Soit $h \in \mathfrak{S}_4$. A quoi correspond l'orbite de h et le stabilisateur de h ?

$$\begin{aligned} \text{orb}(h) &= \{g \cdot h, g \in \mathfrak{S}_4\} \\ &= \{ghg^{-1}, g \in \mathfrak{S}_4\} \\ &= \text{classe de conjugaison on de } h \text{ dans } \mathfrak{S}_4, \end{aligned}$$

$$\begin{aligned} \text{stab}(h) &= \{g \in \mathfrak{S}_4, gh = h\} \\ &= \{g \in \mathfrak{S}_4, ghg^{-1} = h\} \\ &= \{g \in \mathfrak{S}_4, gh = hg\} \\ &= \text{"centre de } h" \neq Z(G). \end{aligned}$$

2. Déterminer les **classes de conjugaison** de \mathfrak{S}_4 . $x, y \in \mathfrak{S}_4$: $x \sim y$ ssi $\exists g \in \mathfrak{S}_4$ t.q. $y = g \cdot x = gxg^{-1}$.

$$\text{class}(x) = \{y \in \mathfrak{S}_4 \mid \exists g \in \mathfrak{S}_4, y = gxg^{-1}\} = \{y = gxg^{-1} \mid g \in \mathfrak{S}_4\} = \text{orb}(x)$$

Rappel. Deux éléments de \mathfrak{S}_n sont conjugués dans \mathfrak{S}_n ssi ils ont le même type.

$$\begin{aligned} \mathfrak{S}_4 = \{e\} \cup \{\text{type } 2 : (12), (13) \dots (34)\} \cup \{\text{type } 3 : (123), (124) \dots (243)\} \\ \cup \{\text{type } 4 : (1234), (1243) \dots (1432)\} \cup \{\text{type } 2, 2 : (12)(34), (13)(24), (14)(23)\} \end{aligned}$$

$$\mathfrak{S}_4 = \text{conj}(e) \cup \text{conj}((12)) \cup \text{conj}((123)) \cup \text{conj}(1234) \cup \text{conj}((12)(34))$$

Remarque.

- deux éléments g et g' de \mathfrak{S}_n sont conjugués dans \mathfrak{S}_n , s'il existe $\sigma \in \mathfrak{S}_n$ tel que $g' = \sigma g \sigma^{-1}$,
- deux éléments g et g' de \mathfrak{A}_n sont conjugués dans \mathfrak{A}_n , s'il existe $\sigma \in \mathfrak{A}_n$ tel que $g' = \sigma g \sigma^{-1}$.

3. Montrer que si $\sigma \in \mathfrak{S}_4$, les conjugués de σ dans \mathfrak{S}_4 forment deux classes de conjugaison dans \mathfrak{A}_3 s'il n'existe pas permutation impaire commutant avec σ

Remarque. Le groupe \mathfrak{S}_4 agit sur l'ensemble \mathfrak{S}_4 par conjugaison. Le groupe \mathfrak{A}_4 agit sur l'ensemble \mathfrak{A}_4 par conjugaison. Si σ appartient à l'ensemble \mathfrak{S}_4 , alors : $\text{Stab}_{\mathfrak{S}_4}(\sigma) = \{g \in \mathfrak{S}_4 \mid g\sigma = \sigma g\}$ et $\text{Stab}_{\mathfrak{A}_4}(\sigma) = \{g \in \mathfrak{A}_4 \mid g\sigma = \sigma g\}$. S'il n'existe pas de permutation impaire commutant avec σ alors :

$$\text{stab}_{\mathfrak{S}_4}(\sigma) = \text{stab}_{\mathfrak{A}_4}(\sigma)$$

Or : $\# \text{orb}_{\mathfrak{S}_4}(\sigma) = [\mathfrak{S}_4 : \text{stab}_{\mathfrak{S}_4}(\sigma)] = [\mathfrak{S}_4 : \text{stab}_{\mathfrak{A}_4}(\sigma)] = [\mathfrak{S}_4 : \mathfrak{A}_4] \times [\mathfrak{A}_4 : \text{stab}_{\mathfrak{A}_4}(\sigma)] = 2 \cdot \# \text{orb}_{\mathfrak{A}_4}(\sigma)$. Donc les conjugués de σ dans \mathfrak{S}_4 constituent deux classes de conjugaison dans \mathfrak{A}_4 .

Exercice 2. On considère le 3-cycle $\sigma = (123) \in \mathfrak{S}_4$

1. Quel est l'ordre du stabilisateur de σ dans \mathfrak{S}_4 ?
2. En déduire qu'il n'existe pas de permutation impaire qui commute avec σ
3. En déduire les classes de conjugaison de \mathfrak{A}_4 .

Solution :

1. L'orbite de σ dans \mathfrak{S}_4 pour l'action de est précisément la classe de conjugaison de G (dans \mathfrak{S}_4) il s'agit de l'ensemble des 3-cycles de \mathfrak{S}_4 . Il y en a 8. Ou : $[\mathfrak{S}_4 : \text{stab}_{\mathfrak{S}_4}(\sigma)] = \# \text{orb}(\sigma) = 8$. D'où : $|\text{stab}_{\mathfrak{S}_4}| = \frac{|\mathfrak{S}_4|}{8} = \frac{24}{8} = 3$.
2. Il n'y a que trois permutations de \mathfrak{S}_4 qui commutent avec σ : Donc $\text{stab}_{\mathfrak{S}_4}(\sigma) = \{e, \sigma, \sigma^2\}$, $\sigma^2 = (132)$ — permutation pairs. Il n'existe donc pas de permutation impaire qui commute avec σ .
3. $\mathfrak{A}_4 = \{e\} \cup \{3\text{-cycles type}\} \cup \{(2,2)\text{-cycles type}\}$. $|\mathfrak{A}_4| = \frac{|\mathfrak{S}_4|}{2} = 12$. D'après les questions précédents la classe de conjugaison $\text{conj}_{\mathfrak{S}_4}(\sigma)$ de σ dans \mathfrak{S}_4 , qui est égale à l'ensemble de 3-cycles de σ dans se décompose en deux classes de conjugaisons dans \mathfrak{A}_4 :

$$\text{conj}_{\mathfrak{A}_4}((123)) = \{(123), (142), (134), (243)\} \text{ et}$$

$$\text{conj}_{\mathfrak{A}_4}((132)) = \{(132), (124), (143), (234)\}$$

Remarque. Si σ est un 3-cycle (123) alors σ et σ^2 ne sont pas conjugués dans \mathfrak{A}_4 car sinon il existerait un cycle τ tel que :

$$(132) = \sigma^2 = \tau\sigma\tau^{-1} = (\tau(1)\tau(2)\tau(3)) \Rightarrow \tau = (23) \text{ mais } (23) \notin \mathfrak{A}_4.$$

En revanche, les types (2, 2) constituent encore une classe de conjugaison dans \mathfrak{A}_2 car il existe une permutation impaire qui commute avec (12)(34), à savoir (12).
Conclusion

$$\mathfrak{A}_4 = \text{conj}_{\mathfrak{A}_4}(e) \cup \text{conj}_{\mathfrak{A}_4}((123)) \cup \text{conj}_{\mathfrak{A}_4}((132)) \cup \text{conj}_{\mathfrak{A}_4}((12)(34)).$$

Remarque. Considérons l'ensemble $K = \{e, (12)(23), (13)(24), (14)(23)\}$. K est un sous-groupe de \mathfrak{A}_4 , il est stable par conjugaison, donc il est distingué dans \mathfrak{A}_4 . Donc : \mathfrak{A}_4 n'est pas simple ! $K \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (groupe de Klein).

Exercice 3. Si G est un groupe, on rappelle que le sous-groupe $D(G)$ de G engendre par les commutateurs i.e. par les éléments : $xyx^{-1}y^{-1}$ pour $x, y \in G$

1. Montrer que $D(G) \triangleleft G$.
2. Montrer que $H \triangleleft G$ et G/H est abélien, alors $H \supset D(G)$.

Solution :

1. $D(G)$ est stable par tout automorphisme (car l'image d'un commutateur par un automorphisme de G est encore un commutateur ; en effet, on a : $f(xyx^{-1}y^{-1}) = f(x)f(y)f(x)^{-1}f(y)^{-1}$) donc f envoie par tout automorphisme intérieur $f_h : G \rightarrow G$; $g \mapsto ghg^{-1}$. Donc $D(G)$ est un sous-groupe "caractéristique" de G a fortiori est un sous-groupe distingué de G .
2. Si $H \triangleleft G$ et H abélien alors soient $x, y \in G$ Puisque G est abélien, on a :

$$xHyH = yHxH$$

$$\bar{x}\bar{y} = \bar{y}\bar{x}$$

$$xyH = yxH$$

Donc $x^{-1}y^{-1}xy \in H$ D'où : H contient tous les commutateurs donc H contient $D(G)$