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

$\mathbb{RP}\mathbb{1}\mathbb{P}\mathfrak{S}\mathbb{P} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ $\mathbb{PP}$ $\mathrm{d}x$

$$\alpha(x) = \begin{cases} x \\ \frac{1}{1+e^{-kx}} \\ \frac{e^x - e^{-x}}{e^x + e^{-x}} \end{cases}$$

$\langle x \rangle$

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

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

$$\int_a^b \mathbb{R}^2 g(u,v)\,\mathrm{d}P_{XY}\,(u,v) = \iint g(u,v) f_{XY}(u,v) \mathrm{d}\lambda(u) \mathrm{d}\lambda(v)$$

$$\lim_{x \to \infty} f(x)$$

$$\iiiint_V \mu(t,u,v,w)\,dt\,du\,dv\,dw$$

$$\sum_{n=1}^{\infty} 2^{-n} = 1$$

Définition 1. Si X et Y sont 2 v.a. ou definit la COVARIANCE entre X et Y comme $\mathrm{Cov}(X,Y) \overset{\mathrm{def}}{=} \mathbb{E}\left[(X - \mathbb{E}(X))(Y - \mathbb{E}(Y))\right] = \mathbb{E}(XY) - \mathbb{E}(X)\mathbb{E}(Y)$.

Chapitre 1

GENERALITES

1.1 Definitions de base

1.1.1 Groupe et Sous-Groupe

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

Définition 2. On dit que G est un GROUPE si :

1. $\forall a, b, c \in G: \ a(bc) = (ab)c$ (associative)
2. $\exists e \in G: \ \forall g \in G: \ ge = eg = g$ (élimant 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 sons-ensemble de G.

Définition 3. H est un SOUS-GROUPE de G si :

1. $H \neq \varnothing$
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 $\mathrm{ord}(G)$, $|G|$ 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 $\mathrm{ord}(x)$. Order x est $\mathrm{ord}(x) \overset{\text{def}}{=} |\langle x \rangle|$

Exemple 1.1.1. S_3.

1.1.2 La classe d'équivalence

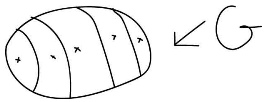
Définition 4. Soints G un groupe et H – un sous-groupe de G. On définit sur G la Relation d'Équivalence dite à gauche modulo H. Pour $x,\ y \in G$:

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

Si $x \in G$ la classe d'équivalence de x pour cette relation dite Classe à Gauche Modulo H est :

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

???



Remarque. *Les class d'équivalence constituée une partition de G.*
L'ensembe 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 $f_x : \begin{array}{ccc} H & \to & xH \\ h & \mapsto & xh \end{array}$ 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. *Soint 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 :

$$\begin{array}{cccc} \pi : & G & \overset{\text{surjection}}{\to} & \dfrac{|G|}{|H|}_g \ \text{– est surjet} \\ & x & \mapsto & \underbrace{xH}_{\bar{x}} \end{array}$$

$xH,\ yH \in \left({}^{G}\!/\!{}_{H}\right)_g$. Alors

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

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 5. Un sous groupe $H < G$ de G est dit DISTINGUE dans G ou NORMAL dans G, s'il est table 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 : $H \lhd G$.

Remarque.

— *Si G est un groupe abélien alors tout sous-groupede G est distingué dans G.*

— *Si $H \lhd G$, on n'd paas niassaiement : $xh = hx \ \forall x \in G, \ \forall h \in H$.*

— *Si $[G : H] = 2$ alors $H \lhd G$.*

Exemple 1.1.2.

1. $\langle \sigma_1 \rangle = \{e, \sigma_1, \sigma_2\}$ — sous-gropupe engendée pour σ_1 dans $\mathfrak{S}_3$. $[G : H] = 2 \Rightarrow \langle x \rangle \lhd \mathfrak{S}_3$.
2. $\langle \tau_1 \rangle = \{e, \tau_1\} \ntriangleleft \mathfrak{S}_3$. Car $\langle \tau_1 \rangle$ n'est pas stable par conjugaison. En effet : l'element $\tau_2\tau_1\tau_2^{-1} = \tau_2\tau_1\tau_2 = (12) = \tau_3 \notin H$.
3. Le *Noyau* du morphisme de grouped $f : G \to G'$ est l'ensemble $\ker f \coloneqq \{x \in G | f(x) = e'\}$, où e' est l'element neutre de G'. C'est un sous-groupe distingué de G.

Définition 6. Un groupeest dit SIMPLE s'il n'admet pas de sous-groupes distingués autre que lui-même et $\{e\}$.

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

— Alors G est un groupesimple. En effet, si H est un sous-groupede G alors, par de le Théoréme de Lagrange son ordre divise p, donc vant 1 ou p puisque p est premiere. Donc $H = \{e\}$ ou $H = G$. De plus, si $x \in G$
$\{e\}$ alors, pour le Th. de Lagrange son ordre divise p, donc vant 1 ou p poisque p est premiere donc vant p poisque $x \neq e$.

Donc $\langle x \rangle = G$. Donc G est cyclique (i.e engender par un élement et fini). Donc G est isomorphe à $\mathbb{Z}/_{p\mathbb{Z}}$.

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

En effet :

* $n\mathbb{Z} = \varnothing$ 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 certan $n \geq 0$.

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

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

$$\bar{x} + \bar{y} = \overline{x+y} \tag{1.1}$$

$$\bar{x}\bar{y} = \overline{xy} \tag{1.2}$$

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 sons 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 applé les facteurs invariantes de G.

Remarque. d_r *=exponent de* G = *ppcm des ordres des élements de* G.

Exemple 1.2.1. 1. Montrer qu'on groupe, dont tous les élémentes non neutres sont d'ordre 2, est abelien.

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

2. Déterminer à isomporphisme prés tous les groupe.

Solution

— Si G est d'ordre 1, alors G est réduit à $\{e\}$ où e est l'élementes neutre du 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 adment élément d'ordre 4 alors G est cyclique et donc $G \simeq \mathbb{Z}/_{4\mathbb{Z}}$, abélien. Sinon, d'appelés le Théoréme 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'aprés le Th. de Classification des groupes abéliens fi-

nis, G est, soit isomprphe à $G \simeq \mathbb{Z}/_{4\mathbb{Z}}$: imposible car G n'adment pas d'élément d'ordre 4. Soit isomorphe à : $G = \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$. Il est isomprphe au groupe de Klein. Il y a donc deux groupes s'ordre 4 à isomorphe prés : $\mathbb{Z}/_{4\mathbb{Z}}$ et $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ (et ils sont tous les deux abélien).
— 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 7. On dit un groupe G agit sur un ensemble X, si :

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

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

$$a = b + c \tag{1.3}$$
$$\pi : G \to S_X \tag{1.4}$$
$$g \mapsto \begin{pmatrix} \pi_g : X \to X & \\ & x \mapsto \pi_g(x) = g \cdot x \end{pmatrix} \tag{1.5}$$

Définition 8. Si un groupe G agit sur un ensemble X, la relation sur X : $x, y \in X$, $x \; y$ ssi $\exists g \in G, y = g \cdot x$ est une relation d'équivalence. La classe de x per cette relation s'applelle ORBITE de x, notée $\mathrm{orb}(x)$ ou $G \cdot x$: $\mathrm{orb}(x) = \{y \in X, y \sim x\} = \{g \cdot x, g \in G\}$ l'ensemble des orbits constitute une partition de X.

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

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

$\pi : \; G \to \sigma_X$
$G \mapsto \pi_G$

i.e l'ensemble :

$$\ker \pi \{g \in G | \pi(g) = e_{\sigma_X}\} = \{g \in G | \pi_g = id_x\} = \{g \in G | \forall x \in X, \pi_g(x) = x\} = \{g \in G | \forall x \in X, g$$

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

Exemples.

1. Le groupedes rotation de $\mathbb{R}^3$ de centre l'origine o agit sur $\mathbb{R}^3$. $G \times \mathbb{R}^3 \to R^3$ et $(r, x) \mapsto r \cdot x = r(x)$. Les orbite sont les pphere centres en l'origine. L'action n'est donc pas transitive. Regarde rotation quelle fixe tout le monde. Évidemment l'action le fidèle. Rotation fixant tout point de $\mathbb{R}^3$ est l'idantite.
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 $G \times G \to G$; $(g, x) \mapsto g \cdot x = gx$ (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) soint $g, g' \in G$ 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 conjuration de x.
   — Le mogan de l'action est :
   $$\{g \in G | \forall x \in X, gxg^{-1} = x\} = \{g \in G | \forall x \in X,\ gx = xg\} \overset{\text{def}}{=} \text{"centre de } G\text{"} \overset{\text{def}}{=} Z(G)$$
   est réduit â $\{e\}$.

Définition 9. 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 $G \to X$, $g \mapsto g.x$ 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 stab(x) dans G.

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

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

1. $\#X = \sum_x [G : \mathrm{stab}(x)]$ *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* $\exists!$
$n = \prod_n p_i^{\alpha_i}$, $p_i - premire$

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 $r \geq$). 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'sidu : $2^3 = 8$.

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 :* $n_p = 1 \mod p$ *et* $n_p | q$.

> **Définition 10.** Si H est un sous-groupe d'un groupe G, les conjugues dans G sont les gHg^{-1}, pour $g \in G$ ($\{ghg^{-1}, h \in H\}$).

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

Theorem 5 (2^ème^ Théorème de Sylow)**.** *Soit* G *une groupe fini. Le conjugue 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 puse.. 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 niasse 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 :

$$n_5 \equiv \quad \mod 5$$
$$n_5 | 3$$

$\Rightarrow$ $n_5 = 1$. Tous les sous-groupe d'un groupe abeille sont distende.
Mais un groupe d'ordre 13 n'admet que deux sons-groupe (th de cagage) lui-meme et $\{e\}$. Donc G est simple.

2. Montre qu'un grou d'ordre 15 n'est pas simple. 5|15 donc existe sylow sous-groupe. Soit G un groupe d'ordre 15=3x5. G admet un 5-Sylow H. De plus le nombre n_5 de 5-Sylow de G vérifie : $n_5 = 1 mod 5$ et $n_5 | 3$ donc $n_5 = 1$.
Les conjugales de H sont encore des 5-Sylow. Or, il n'y a s'un seul 5-Sylow dans G. conclusion. G n'est pas simple.

1.5 Les Groupes symetrique

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

Remarque. Deux permutations à s'appontes disjoint commutent. Exemple : $\tau = (1, 2) \in \sigma_9$ et $\sigma = (345) \in \sigma_9$. Le support de τ est $\{1, 2\}$.

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

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

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 example : $\mathrm{ord}(\sigma) = \mathrm{ppcm}(\mathrm{ord}(136), \mathrm{ord}(24), \mathrm{ord}(598)) = \mathrm{ppcm}(3, 2, 3) = 6$

Autument dit, on a : $\sigma^6 = id$ et 6 est la lus petite puissance non mille verifment cela.

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

Ou deeoupre σ en podint de cycles : $\sigma = c_1 c_2 \ldots c_l$, c_i cycles. D'oui : $\tau\sigma\tau^{-1} = \tau(C_1 \ldots c_r)\tau^{-1} = (\tau c_1 \tau^{-1})(\tau c_2 \tau^{-1}) \ldots (\tau c_r \tau^{-1})$

Oi, on a : $\tau(i_1 \ldots i_m)\tau^{-1} = (\tau(i_1) \ldots \tau(i_m))$ usur conjugue dum-cycle $(i_1, i_2, \ldots, i_m)$

On effet, l'image par la permutation de gaushe et la permutation de droite de tout de $\tau(i_j)$, pour $j \in \{1, \ldots, i_n\}$ et des antesentius coincide.

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

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

Donc $f = g$.

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

Proposition 3. *On appele type d'une permutation $\sigma = c_1 \ldots c_r$. Ca suite $(l_1, \ldots, l_r)$ des lougneus des cycles c_i ordoners en order croissant $(l_1 \leq l_2 \leq \ldots \leq l_r)$. Deux permutations sont conjugues dans σ_n ssi elle ont meme type.*

Par exemple : les permutations

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

et

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

Dont conjuged dans σ_9 car elles dont touts deux de 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 pas les transpositions (2-cycles)*

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

3. σ_n est engendré pas les transpositions (dits elimentaires) de la forme $(i\ i+1)$

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

Démonstration. exercise □

Proposition : la signature $\varepsilon : \sigma_n \to \{\pm 1\}$ est un morphisme de groups. En particulier deux permutations conjugues on même signature. Transposition est impaire i de signature gele 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 lain de transpositions.

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

Le noyan $\mathfrak{A}_n$ du morphisme signature $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ est un sous-groupedistingué d'indice 2 ($n \geq 2$) de $\mathfrak{S}_n$, appelé la n=i ème groupealterné = c'est donc l'ensemble des permutations pairs de σ_n.

Proposition 4. *Si $n \geq 3$, le groupealteiné $\mathfrak{A}_n$ et engendre 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 groups finis

Thèorie introduite par Frobenius à la fin du XIX siècle.

2.1 Premieres definitions, représentations, yep isomorphisms et représentation iuductis)

Définition 11. Une Représentation Linéaire d'une groupe G est la donnée d'une $\mathbb{C}$-espace vectoriel V muni d'une action (à gauche) de G agissant de manière linéaire

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

telle que :

1. $\forall x \in V,\ e \cdot x = x$ où x est l'element neutre de G
2. $\forall g, g' \in G,\ \forall x \in V :\ g \cdot (g' \cdot x) = (gg^{-1}) \cdot x$
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 12. Une représentation linéaire d'un groupe G est donc le donnée d'un $\mathbb{C}$-espace vectoriel V et d'un morphisme de groupes :

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

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 equivalents.

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

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

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 effect 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 groups. 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 $\begin{array}{ccc} \rho : G & \to & GL(V), \\ g & \mapsto & \rho_g \end{array}$ est un morphisme de groups, alors considérons :

$$G \times V \to V$$
$$(g, x) \mapsto g \cdot x := \rho_g(x)$$

Cela definit bien un action linear de G sur V car :

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

□

Définition 13 (Vocabulaire)**.**

- L'espace vectoriel V est `l'espace de la représentation`.
- La dimension de V est le `dégrée` (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 $GL(V)$. $G \simeq Im(ro) < GL(V) = C^n ro : G \to C^* g \mapsto ro_g \simeq GL_n(\mathbb{C})$
- Lorsque V est dimension finite (ce qui cela toujours le cas par la suite). Le choix d'une base fournit alors une représentation encore plus concrete 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 $\rho : G \to GL(V)$ une représentation (linéaire) de G. Si $g \in G$ est d'ordre n alors, on a :*

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

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'unite dans $\mathbb{C}$, que sont : $e^{\frac{2h\pi}{n}}$, $h \in \{0, .., m\}$).

Rappel. $f \in \mathrm{End}(V)$, $I_f = \{P(x) \in \mathbb{C}[x] \mid P(f) = 0\}$ *ideal 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 touts ses valeurs propre sont donc simples).*

Exemple 2.1.1.

1. La représentation `triviale` (on représentation unité).

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

2. Les représentation de degré 1 : ce sont les `homomorphisms` $\rho : G \to \mathbb{C}^*$ puisque si $\dim V = 1$ alors $GL(V) \simeq \mathbb{C}^*$. En effet les endomorphisms de V sont les `homothétis` : $f_\lambda : V \to V x \to \lambda x (\lambda \in \mathbb{C}^*)$. Et $GL(V) \to G^*$ est un isomorphisme $f_\lambda \to \lambda$.
   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 complexs de mondle 1. $|\rho_g| = 1$.
3. Soient $\mathfrak{S}_m$ considéré le groupesymétrique et $(e_1, \ldots, e_n)$ la base canonique de $\mathbb{C}^n$. On définit une représentation de degré n de $\mathfrak{S}_n$ en posant :

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

4. La `représentation de permutation` c'est un généralisation l'exemple précédent. Soit $G \times X \to X$ une action $(g, x) \mapsto g \cdot x$ d'un groupeG sur un ensemble fini x. Soit V un 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 : $V = \oplus_{x \in x} \langle \varepsilon_x \rangle = \oplus_{x \in X} \mathbb{C}_{\varepsilon_x}$. On définit une re linéaire

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

   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 $\mathbb{C}$, le fonction ε_x étant l'indicatrice de $x \in X$: $e_x(y) = 1six = y0six \neq y,\ y \in X$*

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

$$\begin{aligned} \rho : G &\to GL(V) \\ g &\mapsto \begin{pmatrix} \rho_g : V & \to & V \\ \varepsilon_x & \mapsto & \varepsilon_{g \cdot x} \end{pmatrix} \end{aligned}.$$

Définition 14. Deux représentation linier $\rho \to GL(V)$ et $\rho' : G \to GL(V')$ d'un groupe G. Sont dites Isomorphes ou Équivalents s'il existe un isomorphisme d'espace vectoriels $f : V \overset{\simeq}{\to} V'$ tel que l'on ont : $\forall g \in G, \rho'_g \circ f = f \circ \rho_g$.

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "\rho_g"'] \arrow[dr, phantom, "\circlearrowright"] & V' \arrow[d, "\rho'_g"] \\ V \arrow[r, "f"'] & V' \end{tikzcd}$$

On peut exprimer cette condition par la commutativité diagramme :

$$\begin{tikzcd} G \arrow[r, "\rho"] \arrow[d, "\rho'"'] & GL(V) \arrow[dl, "\tilde{f}"] \\ GL(V') & \end{tikzcd}$$

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

$$\begin{tikzcd} V \arrow[r, "\varphi"] \arrow[d, "f"'] \arrow[dr, phantom, "\circlearrowright"] & V' \arrow[d, "f"] \\ V \arrow[r, "\tilde{f}(\varphi)"'] & V' \end{tikzcd}$$

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 :

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

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

Si $\rho : G \to GL(V)$ 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 :

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

Remarque. $\forall w \in W, \ \rho_g|_W(w) = \rho_g(w) \overset{?}{\in} W$

Cela produit à le notion de représentation irréductible :

> **Définition 15.** Une représentation $\rho : G \to GL(V)$ 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 16.** On définit le SOMME DIRECTE de représentation de groupe fini G. Soient $\rho : g \to GL(V)$ et $\rho' : G \to GL(V')$ deux représentations de G. On définit la somme directe $\rho \oplus \rho'$ comme étant : La représentation d'espace vectoriel $V \oplus V'$ definit par :
>
> $$\begin{array}{rcl} \rho \oplus \rho' : G & \to & GL(V \oplus V') \\ g & \mapsto & (\rho \oplus \rho')_g \end{array}$$
>
> 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 groupefini 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 effect, 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 :

$$x \text{ orthogonal à } W \iff \rho_g(x) \text{ orthogonal } \rho_g(W) = W$$

□

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 17. On appelle Caractère de la Représentation $\rho : g \mapsto GL(V)$ l'application :

$$\begin{array}{rcl} \chi_\rho : G & \to & \mathbb{C} \\ g & \mapsto & \chi_\rho(g) = \mathrm{Tr}(\rho_g) \end{array}$$

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

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

1. $\chi_\rho(x) = \dim V =$ *« degré de ρ »* $=:$ *« degré de χ_ρ »*
2. $\forall g \in G,\ \chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$ *— conjugue 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. $\chi_\rho(e) = \mathrm{Tr}(\rho_e) = \mathrm{Tr}(\mathrm{Id}_V) = \dim V$
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 : $\chi_\rho(ghg^{-1}) = \mathrm{Tr}\big(\rho_{ghg^{-1}}\big) = \mathrm{Tr}\big(\rho_g \circ \rho_h \circ \rho_g^{-1}\big) = \mathrm{Tr}(\rho_h) \overset{\mathrm{Tr}(AB)=\mathrm{Tr}(BA)}{=} \chi_\rho(h)$. χ_ρ prend la méme valeur sur tous les éléments d'une classe de conjugaison.
4. Si $(e_1, \dots, e_n)$ est un base de V et $(e'_1, \dots, e'_m)$ est un bsde de V' alors :

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

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

□

Exemple 2.3.1. Exemples de calcules de caractères :

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

$$\begin{array}{rcl} \rho : G & \to & GL(V) \\ g & \mapsto & \left(\begin{array}{rcl} \rho_g : V & \to & V \\ e_x & \mapsto & e_{g \cdot x} \end{array} \right) \end{array}$$

où $V = \oplus_{x \in X} \langle e_x \rangle$.
On a : $\begin{array}{rcl} \chi_\rho : G & \to & \mathbb{C} \\ g & \mapsto & \mathrm{Tr}(\rho_g) \end{array}$.
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 est tous les autres coefficients sont nuls. De plus, si $\mathrm{Mat}_{(e_x)}(\rho_g) = (a_{ij})$ 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 : $\chi_\rho(g) = Tr(\rho_g) = \#\{x \in X \mid g \cdot x = x\}$
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 : $\chi_\rho(g) = Tr(\rho_g) = \#\{x \in G \mid gx = x\} = \begin{cases} |G| & \text{si } g = e, \\ 0 & \text{sinon} \end{cases}$.

Définition 18. Nous qualifier errons D'IRRÉDUCTIBLE tout caractère d'une représentation irréductible.

`Le tableau des caractères` (irréductible) d'une groupefini G est un tableau à c lignes et c colons, où c es 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 class 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'ou munit de la structure hermitien 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 $f = \sum_{g \in G} \lambda \operatorname{Ind}_g$ où $\begin{array}{rcl} \operatorname{Ind}_g : G & \mapsto & \mathbb{C} \\ x & \mapsto & \left\{ \begin{array}{ll} 1 & x = g \\ 0 & \text{sinon} \end{array} \right. \end{array}$ (avec $\lambda = f(g) \Rightarrow f = \sum_{g \in G} f(g) \operatorname{Ind}_g$)) donc $(\operatorname{Ind}_g)_{g \in G}$ 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 représentations de G alors* $\langle \chi, \chi' \rangle = \left\{ \begin{array}{ll} 1 & \textit{si } \chi = \chi' \\ 0 & \textit{sinon} \end{array} \right.$.

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

On a :

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

et

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

D'où :

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

...!? how do we compute this sum ?

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 $f : V \to V'$ un morphisme compatible avec les deux représentations (i.e. $\forall g \in G,\ f \circ \rho_g = \rho'_g \circ f$).*

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "\rho_g"'] \arrow[dr, phantom, "\circlearrowright"] & V' \arrow[d, "\rho'_g"] \\ V \arrow[r, "f"'] & V' \end{tikzcd}$$

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

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

$$\begin{array}{rcl} \rho : G & \to & \mathbb{C}^* \\ g & \mapsto & \rho_g \end{array}$$

le caractère χ associé à cette représentation ρ est

$$\begin{array}{rcl} \chi : G & \to & \mathbb{C} \\ g & \mapsto & \chi(g) = \mathrm{Tr}(\rho_g) = \rho_g \end{array}.$$

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

Exercice 1. On note $\hat{G}$ l'ensemble des caracteurs linéaires de G : $\hat{G} = \{\text{morphismes } \chi : G \mapsto \mathbb{C}^*\}$ ... !? where do those "caracteurs" come from ? Don't we have to define a representation before getting to "characteurs". 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 :

$$\begin{array}{rcl} \chi_0 : G & \to & \mathbb{C}^* \\ g & \mapsto & 1 \end{array}.$$

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

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

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

   !?

2.5 Théorème de Forbenius

Soit G un groupe. On note $\mathcal{F}(G)$ le $\mathbb{C}$-espace vectoriel des fonctions de G dans $\mathbb{C}$ et $\mathcal{F}_C(G)$ le sous-espace vectoriel de $\mathcal{F}(G)$ constitue des `fonctions centrales` sur G (i.e. constants sur les classes du conjugaison).

Une élément de $F_C(S)$ est donc une fonction $F : G \to \mathbb{C}$ vérifiant : $\forall g, h \in G\ f(ghg^{-1}) = f(g)$.

Remarque. *On a que les caractères X_ρ des représentations ρ du G sont des fonctions centrales sur G.*

On rappelle qu'un `caractère irréductible` de G est le caractère d'un représentation irréductible.

Theorem 10. *Les caractères irréductibles d'un groupe G forment une base orthonormée de l'espace $\mathcal{F}_C(G)$ des fonctions centrales sur G.*

Croquis de la preuve. On a un que les caractères irréductibles forment un système libre de fonctions de $\mathcal{F}_C(G)$. Notons F le sous-espace vectoriel de $\mathcal{F}(G)$ engendre par les caractères irréductibles de G. L'idée de la preuve est de vérifier que l'orthogonal $F^\perp$ de F dans $\mathcal{F}_C(G)$ est réduit à $\{0\}$, en utilisant le lemme de Schur. □

Corollaire 1. Le nombre de (classes d'isomorphisme de) représentations irréductibles de G est égal an nombre de classe de conjugaison de G.

Démonstration. D'après le théorème de Frobenius, le nombre de représentations irréductibles de G est égal a la dimension de l'espace $\mathcal{F}_C(G)$ des fonctions centrales sur G. Or, une fonction est centrale ssi elle est constante sur chaque classe de conjugaison ; une fonction centrale $\Phi : G \to \mathbb{C}$ peut donc s'écrire de manière unique sous la forme $\Phi : \sum_{C \in \mathrm{conj}(G)} \lambda_C \mathbb{1}_C$, où $\mathrm{conj}(G) =$ «classe de conjugaison de G» et $\mathbb{1}_C$ est la fonction indicatrice de C. $\lambda_c \in \mathbb{C}$ (on a : $\lambda_C = \Phi(g)$ où g est n'importe quel élément de C) Les $\mathbb{1}_C$, pour $C \in \mathrm{conj}(G)$ forment donc une base de $\mathcal{F}_C(G)$, qui de ce fait est de dimension égal $\#\,\mathrm{conj}(G)$. □

Corollaire 2 (Décomposition canonique d'une représentation)**.** Si $\rho : G \to GL(V)$ est une représentation linéaire de G et si $V = W_1 \oplus ... \oplus W_k$ est une décomposition de V ...!? and or of en somme directe de représentation irréductible $\rho = \rho_1 \oplus ... \oplus \rho_k : G \to GL(W_1 \oplus ... \oplus W_k)$ et si $W \in \mathrm{Irr}(G) := \{C \mid \text{class d'isomorphismes de représentation irréductible de } G\}$ alors le nombre m_W de W_i qui sont isomorphes à W est égal à $\langle \chi_W, \chi_V \rangle$. En particulier, il ne dépend pas de la décomposition et :

$$V \simeq \oplus_{W \in \mathrm{Irr}(G)} \langle \chi_W, \chi_V \rangle\, W.$$

i.e. $V \simeq \oplus_{W \in \mathrm{Irr}(G)} m_W W$ avec $m_w = \langle \chi_W, \chi_V \rangle$ où χ_W : caractère associe à W, χ_V : caractère associe à V .

Démonstration. On a : $\chi_V = \chi_{W_1} \oplus ... \oplus \chi_{W_k}$ et donc : $\langle \chi_W, \chi_V \rangle = \langle \chi_W, \chi_{W_1} \rangle + ... + \langle \chi_W, \chi_{W_k} \rangle$ Or $\langle \chi_W, \chi_{W_i} \rangle = 1$ si $W_i \simeq W$; 0 sinon. Donc $m_W = \langle \chi_W, \chi_V \rangle$. □

Corollaire 3. Deux représentations d'un même groupe fini sont isomorphes ssi elles ont même caractère.

Démonstration. D'après le corollaire 2 si $\rho : G \to GL(V)$ et $\rho' : G \to GL(V')$ sont deux représentations de G ayant même caractère χ alors : V et V' peut tous les deux isomorphes à :$\oplus_{W\in\mathrm{Irr}(G)} \langle \chi_W, \chi\rangle W$. Réciproquement, si ρ et ρ' sont isomorphes on a déjà vu que $\chi_\rho = \chi'_\rho$. □

Corollaire 4 (Critère d'irréductibilité)**.** Une représentation $\rho : G \to GL(V)$ de G est irréductible ssi $\langle \chi_V, \chi_V\rangle = 1$.

Démonstration. Si $V \simeq \oplus_{W\in\mathrm{Irr}(G)} m_W W$ alors $\langle \chi_V, \chi_V\rangle = \left\langle \sum_{W\in\mathrm{Irr}(G)} m_W \chi_W, \sum_{W\in\mathrm{Irr}(G)} m_W \right.$ $\sum_{W\in\mathrm{Irr}(G)} m_W^2$. comme les $m_W \in \mathbb{N}$, on en déduit : $\langle \chi_V, \chi_V\rangle = 1$ ssi tous les m_W sont égaux à 0 sauf un qui est égal à 1 ; ssi $V \simeq W$; ssi $V \in \mathrm{Irr}(G)$ i.e. V irréductible. □

Corollaire 5 (Formule de Bernside)**.** G est un groupe fini. On a $\sum_{W\in\mathrm{Irr}(G)} (\dim W)^2 = |G|$

Démonstration. Considérons la représentation régulière de G :

$$\begin{array}{rcl} \rho : G & \to & GL(V) \\ g & \mapsto & \left(\begin{array}{rcl} \rho_g : V & \to & V \\ \varepsilon_x & \mapsto & \varepsilon_{g\cdot x} \end{array} \right) \end{array}$$

$\dim V = |G|, V = \oplus_{x\in G} \mathbb{C}_{\varepsilon_x}$

Si W et une représentation irréductible de G alors W apparait dans la représentation régulière avec la multiplicité $\dim W$.

En effet, le caractère χ de la représentation régulière est donne par : $\chi(e) = |G|$ et $\chi(g) = 0$ si $g \neq e$ (car $\chi(g) = Tr(\rho_g) = \# x \in G | gx = x$). Qr, la multiplicité de W dans V es, d'après le corollaire 2, égale à : $\langle \chi_W, \chi\rangle = \frac{1}{|G|} \sum_{g\in G} \overline{\chi_W(g)} \chi(g) = \bar{\chi}_W(e) = \dim W$. On en déduit que : $\chi = \sum_{W\in\mathrm{Irr}(G)} (\dim W) \chi_W$

En appliquant cette identité à $g = e$, on trouve : $|G| = \chi(e) = \sum_{W\in\mathrm{Irr}(G)} (\dim W) \chi_W(e) = \sum_{W\in\mathrm{Irr}(G)(\dim W)^2}$ □

2.6 Le cas des groupes abéliens

Theorem 11. *Si G est abélien, toute représentations irréductibles de G est de dimension 1. Autrement dit, l'ensemble $\mathrm{Irr}(G)$ des classes d'isomorphismes de représentation irréductible de G coïncide avec l'ensemble $\hat{G}$ des caractères linéaires de G.*

Démonstration. Si G est abélien, le classes de conjugaison de G sont touts réduites à un élément ($h \in G$ $g \in Gghg^{-1} = hgg^{-1} = h\,\mathrm{conj}(h) = \{h\}$) et donc $\#\,\mathrm{conj}(G) = |G|$. Puisque $\#\,\mathrm{Irr}(G) = \#\,\mathrm{conj}(G)$ d'après le corollaire 1, puisque $\sum_{W\in\mathrm{Irr}(G)} (\dim W)^2 = |G|$, d'après le corollaire 5 et comme $\dim W \geq 1 \forall W \in \mathrm{Irr}(G)$, on en déduit que : $\forall W \in \mathrm{Irr}(G)$ on a $\dim W = 1$. □

Remarque. *Si $\rho : G \to GL(V)$ est une représentation de G de $\dim 1$ alors : $\dim_{\mathbb{C}} V = 1$ i.e. $V \simeq \mathbb{C}$, d'où : $GL(V) \simeq \mathbb{C}^*$. D'où $\rho : G \to \mathbb{C}^*$ morphisme. C'est donc un caractère linéaire de G. Et le caractère χ associe coïncide avec ρ.*

Corollaire 6. Si G est abélien, toute fonction de G dans $\mathbb{C}$ est combination linaire de caractères linéaires.

Démonstration. D'après le Théorème Frobenius, toute fonction centrale (et donc toute fonction puisque G est abélien) est combination linéaire de caractères irréductibles. □

Exercice 2. Déterminer les représentations et les caractères irréductibles du groupe $\mathbb{Z}/n\mathbb{Z}$ pour $n \geq 1$.

Solution 1. n classes de conjugaison. Le groupe additif étant abélien et d'ordre n, il admet n classes de conjugaison (touts réduits à un élément) et donc admet n (classes d'isomorphismes de) représentation irréductible, et touts de dimension 1.

car $\sum_{W \in \mathrm{Irr}(\mathbb{Z}/n\mathbb{Z})} (\dim W)^2 = |\mathbb{Z}/n\mathbb{Z}| = n$ ...!? what car ?

correspondant donc caractère linéaire de $\mathbb{Z}/n\mathbb{Z}$ i.e. aux morphismes de groupe $\chi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$

Or, $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique, engendre par $\bar{1}$ (où $\bar{a} = a + n\mathbb{Z}$) Donc : les morphismes $\chi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$sont entièrement détermines par l'image $\chi(\bar{1})$. (En effet : $\chi(\bar{a}) = \chi(\bar{1} + ... + \bar{1}) = \chi(\bar{1})^a$.

De plus : $\chi()^{\bar{n}} = \chi(\bar{1} + \ ... \ \bar{1}) = \chi(\bar{n}) = \chi(\bar{0}) = 1$.

Donc $\chi(\bar{1})$ est une racine n-ème de l'unité dans C. Or l'ensemble $\mu_n(\mathbb{C})$ des racines n-ème de l'unité dans C est $\mu_n(\mathbb{C}) = \{e^{2\pi \frac{k}{}} n, k = 0, 1, 2...\}$

Si $\chi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$ est un caractère linaire, il existe $k \in \{0, ..., n-1\}$ t.q. $\chi(\bar{1}) = e^{\frac{2ik\pi}{n}}$.

On trouve donc n caractère linéaire (on représentation irréductible) de $\mathbb{Z}/n\mathbb{Z}$, à savoir : $\chi_0, ..., \chi_{n-1}$ définis par : $\begin{array}{rcl} \chi_k : \mathbb{Z}/n\mathbb{Z} & \to & C^* \\ \bar{a} & \mapsto & \chi_h(\bar{a}) \end{array}$

Exemple 1. $n = 2$ $G = \mathbb{Z}/n\mathbb{Z}$ toute des caractères du $\mathbb{Z}/2\mathbb{Z}$? Le groupe $G/2G$ admet 2 caractères linéaires :

$$\begin{aligned} \chi_0 : \mathbb{Z}/2\mathbb{Z} &\to C^* \\ \bar{0} &\mapsto 1 \\ \bar{1} &\mapsto 1 \end{aligned}$$

$$\begin{aligned} \chi_1 : \mathbb{Z}/2\mathbb{Z} &\to C^* \\ \bar{0} &\mapsto 1 \\ \bar{1} &\mapsto -1 \end{aligned}$$

$\chi_1(\bar{a}) = e^{\frac{2i\pi a}{2}}$

	χ_0	χ_1
$\mathrm{conj}(0) = \{0\}$	1	1
$\mathrm{conj}(1) = \{1\}$	1	-1

Toute les caractères de $\mathbb{Z}/2\mathbb{Z}$

Exemple 2. $n = 3$ Exemple : le groupe $\mathbb{Z}/3\mathbb{Z}$ admet 3 caractères linéaires (au représentation irréductible) :

$$\begin{array}{rcl} \chi_0 : {}^{\mathbb{Z}}\!/\!_{3\mathbb{Z}} & \to & \mathbb{C}^* \\ a & \mapsto & 1 \end{array} \qquad \begin{array}{rcl} \chi_1 : {}^{\mathbb{Z}}\!/\!_{3\mathbb{Z}} & \to & \mathbb{C}^* \\ a & \mapsto & e^{\frac{2i\pi r}{3}} \end{array}$$

$$\begin{array}{rcl} \chi_2 : {}^{\mathbb{Z}}\!/\!_{3\mathbb{Z}} & \to & \mathbb{C}^* \\ a & \mapsto & e^{\frac{4i\pi r}{3}} \end{array}$$

	χ_0	χ_1	χ_2
conj(0)	1	1	1
conj(1)	1	j	j^2
conj(2)	1	j^2	j

Chapitre 3

Exercices

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

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

Remarque. *Un polynôme dans un corps K ne peut avon plus d ?racine.*

Rappel :

L'annequ $\mathbb{Z}/n\mathbb{Z}$ 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 elements *inversibles* de A. (i.e. qui admetten un symetrique pour le multiplication). Alors $(A*, \times)$ est un groupe. On a :

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

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

On définit la fonction indicatice d'éuler φ pour : $\varphi(n) := |\left(\mathbb{Z}/n\mathbb{Z}\right)^*| = \text{ le nombre d'entier } \leq$
D'où $|\left(\mathbb{Z}/91\mathbb{Z}\right)^*| = \varphi(91) = ?$. D'aprés le Théoréme des restes chinous ou a :

$$\begin{aligned} rcl\mathbb{Z}/91\mathbb{Z} \simeq & \quad \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \text{ car } (7, 13) = 1 & (3.1) \\ x + 91\mathbb{Z} \mapsto & \quad (x + 7\mathbb{Z}, x + 13\mathbb{Z}) & (3.2) \end{aligned}$$

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

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

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

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 $-\bar{1} = \overline{90}$ est aussi solution évidente. Determinons le nombre de solution de cette équation.

Remarque. *Soit G un groupe(multiplicatif) et x un élement de G. $x^n = e \Leftrightarrow \operatorname{ord}(x)|n$. $x^2 = 1$ dans $\left(\mathbb{Z}/_{91\mathbb{Z}}\right)^*$ 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 $\left(\mathbb{Z}/_{91\mathbb{Z}}\right)^*$. On cherche donc $\bar{a}$ present élements d'ordre 2 de $\left(\mathbb{Z}/_{91\mathbb{Z}}\right)$.

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

On cherche donc les élements d'ordre 2 de $\left(\mathbb{Z}/_{91\mathbb{Z}}\right)^* \simeq \left(\mathbb{Z}/_{7\mathbb{Z}}\right)^* \times \left(\mathbb{Z}/_{13\mathbb{Z}}\right)*$. Soit $(\tilde{a}, \dot{b}) \in \left(\mathbb{Z}/_{7\mathbb{Z}}\right)^* \times \left(\mathbb{Z}/_{13\mathbb{Z}}\right)^*$ $\operatorname{ord}((\tilde{a}, \dot{b})) = \operatorname{ppcm}(\operatorname{ord}(\tilde{a}), \operatorname{ord}(\dot{b}))$. (plus petit common multiple).

$$\operatorname{ord}(\tilde{a}, \dot{b}) = 2 \Leftrightarrow \operatorname{ppcm}(\operatorname{ord}(\tilde{a}), \operatorname{ord}(\dot{b})) = 2$$

Par le Th. de Lagrange on a :

$$\operatorname{ord}(\tilde{a})| \left(\mathbb{Z}/_{7\mathbb{Z}}\right)^* \text{ i.e. } \operatorname{ord}(\tilde{a})|6$$

$$\operatorname{ord}(\dot{b})| \left(\mathbb{Z}/_{13\mathbb{Z}}\right)^* \text{ i.e. } \operatorname{ord}(\dot{b})|12$$

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

- *Si p est premier impair et si $m \geq 1$ alors $\left(\mathbb{Z}/_{p^m\mathbb{Z}}\right)^*$ est cyclique d'ordre $\varphi(p^m) = (p-1)p^{m-1}$*
- *$\left(\mathbb{Z}/_{2\mathbb{Z}}\right)^*$ et $\left(\mathbb{Z}/_{4\mathbb{Z}}\right)^*$ sont cyclique et si $m \geq 3$ alors $\left(\mathbb{Z}/_{2^m\mathbb{Z}}\right)^* \simeq \left(\mathbb{Z}/_{2\mathbb{Z}}\right) \times \left(\mathbb{Z}/_{2^{m-1}\mathbb{Z}}\right)^*$*

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 cyclicue.

En particulier, de plus, les gènèrators du groupd (aditif) $\left(\mathbb{Z}/_{n\mathbb{Z}}\right)$ 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 $\varphi(d)$ élements d'ordrde d (d etant un divisem de l'ordre de G).

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

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

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

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

D'où $\langle\tilde{3}\rangle = \left(\mathbb{Z}/7\mathbb{Z}\right)^*$. $\mathrm{ord}(\tilde{3}^m) = 2 \Leftrightarrow \frac{6}{(6,m)} = 2 \Leftrightarrow (6,m) = \frac{6}{2} = 3 \Leftrightarrow m = 3$.
Conclusion $\tilde{3}^3 = \tilde{6}$ *est d'ordre 2 dans* $\left(\mathbb{Z}/7\mathbb{Z}\right)^*$.

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

$$\begin{aligned}
\overline{64} &\overset{?}{\mapsto} (\tilde{1}, -\dot{1}) \\
\overline{27} &\overset{?}{\mapsto} (-\tilde{1}, \dot{1}) \\
\overline{90} &\overset{?}{\mapsto} (-\tilde{1}, -\dot{1}) \\
-\overline{13} &\mapsto (\tilde{1}, \dot{0})\ (!) \\
\overline{14} &\mapsto (\tilde{0}, \dot{1})\ (!)
\end{aligned}$$

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

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

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

remember -13 and 14.

Remarque. *On a :* $\left(\mathbb{Z}/91\mathbb{Z}\right) \overbrace{\simeq}^{\text{Th. de rests chinois car } (7,13)=1} \left(\mathbb{Z}/7\mathbb{Z}\right)^* \times \left(\mathbb{Z}/13\mathbb{Z}\right)^* \simeq \left(\mathbb{Z}/6\mathbb{Z}\right) \times \left(\mathbb{Z}/12\mathbb{Z}\right)^* \not\simeq \left(\mathbb{Z}/72\mathbb{Z}\right)^*$ *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.

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

Solution :

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

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

D'où : $n_3 = 1$. G admet donc un unique 3-Sylow H. Or, d'apis 2$^{\text{ème}}$ Th de Sylow, les conjugues d'un 3-Sylow sont encore un 3-Sylow. Donc les conjugues de H sont égaux à H. Donc

$H \lhd G$. Le groupe G admet donc un sous-groupedistingué n'est pas simple.

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

$$\begin{cases} n_{11} = 1 \mod 11 \\ n_{11} | 3 \end{cases}$$

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

(a) $H < G, \ K < G$

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

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

(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 an 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 abelian. Par le Théorème des reste 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 inversibes $\left(\mathbb{Z}/_{33}\right)^*$ de l'anneau $\mathbb{Z}/_{33}$.

1. Ones est l'order de $(\mathbb{Z}/_{33})^*$?
2. Le groupe $(\mathbb{Z}/_{33})^*$ st-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* $\overline{12} \in \left(\mathbb{Z}/_{33}\right)^*$ *? (où* $\bar{a} = a + 33\mathbb{Z}$*). Non car* $(12, 33) \neq 1$.

   $|\left(\mathbb{Z}/_{33}\right)^*| =$ *nombre d'éléments* ≤ 33 *et premiers avec* 33.

2. D'après le Th. des Rests Chinois, puisque $(3, 11) = 1$, on a un isomorphisme d'anneaux

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

qui induit un isomorphisme de groups sur les groups 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 $(a, b) \in \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{10\mathbb{Z}}$. $\mathrm{ord}((a, b)) = \mathrm{ppcm}(\mathrm{ord}(a), \mathrm{ord}(b))$. O'où : $\mathrm{ord}(a, b) = 4 \leftrightarrow \mathrm{ppcm}(\mathrm{ord}(a), \mathrm{ord}(b)) = 4$, avec $\mathrm{ord}(a)|2$ et $\mathrm{ord}(b)|10$ — impossible. Donc le groupe $(\mathbb{Z}/_{33\mathbb{Z}})^*$ n'admet pas d'élément d'ordre 4.

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

$\mathfrak{A}_4 < \mathfrak{S}_4$ — permutations paris de $\mathfrak{S}_4$.
On fait agir $\mathfrak{S}_4$ sur lui-même par conjugaison :

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

Exercice 3. 1. Montrer que cette définit bien une action. Soit $h \in \mathfrak{S}_4$. A quoi correspond l'orbites de h et le stabilisateur de h ?

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

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

2. Determiner 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.*

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

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

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 conjugasion 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 : $Stab_{\mathfrak{S}_4}(\sigma) = \{g \in \mathfrak{S}_4 | g\sigma = \sigma g\}$ et $Stab_{\mathfrak{A}_4}(\sigma) = \{g \in \mathfrak{A}_4 | g\sigma = \sigma g\}$. 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 : $\#\,\text{orb}_{\mathfrak{S}_4}(\sigma) = [\mathfrak{S}_4 : \text{stab}_{\mathfrak{S}_4}(\sigma)] = [\mathfrak{S}_4 : \text{stab}_{\mathfrak{A}_4}(\sigma)] = [\mathfrak{S}_4 : \mathfrak{A}_4] \times [\mathfrak{A}_4 : \text{stab}_{\mathfrak{S}_4}(\sigma)] = 2 \cdot \#\,\text{orb}_{\mathfrak{A}_4}(\sigma)$. Donc les conjugués de σ dans $\mathfrak{S}_4$ constituent deux class de conjugaison dans $\mathfrak{A}_4$.

Exercice 4. On considére 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 pércisément la classe de conjugaison de G (dans $\mathfrak{S}_4$) il'sagit de l'ensemble des 3-cylces de $\mathfrak{S}_4$. Il y en a 8. Ou : $[\mathfrak{S}_4 : \text{stab}_{\mathfrak{S}_4}(\sigma)] = \#orb(\sigma) = 8$. D'où : $|\,\text{stab}_{\mathfrak{S}_4}| = \frac{|\mathfrak{S}_4|}{8} = \frac{24}{8} = 3$.
2. Il u'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. $\mathfrak{A}_4 = \{e\} \cup \{\text{3-cycles type}\} \cup \{(2,2)\text{-cycles type}\}$. $|\mathfrak{A}_4| = \frac{|\mathfrak{S}_4|}{2} = 12$. D'apre 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 decompose eu deux classed de conjugaisons dans $\mathfrak{A}_4$:
   $\text{conj}_{\mathfrak{A}_4}((123)) = \{(123), (142), (134), (243)\}$ 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 conjugate 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

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

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 5. 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. Muter que $D(G) \lhd G$.
2. Montier que $H \lhd G$ et G/H est abélien, alors $H \supset D(G)$.

Solution :

1. $D(G)$ est stable par tout automorphisme (car l'image d'un commutant 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 a fonction par tout automorphisme intérieur $f_h : G \to G;\ g \mapsto ghg^{-1}$. Donc $D(G)$ est un sous-groupe "caractéristique" de G a fortiori est un sous-groupe distingué de G.
2. Si $H \lhd G$ et H abelien alors poient $x, y \in G$ Prisque 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 commutaients donc H contient $D(G)$

Exercice 6. $|G| = 112 = 2^7 \times 7$ On suppose G simple.

1. $\mathcal{H} =$ 2-sylow de G Par le 1er Théorème de Sylow si n est le nombre de 2-Sylow de G : $n = 1 \mod 2$ et $n_2 | 7$ et $n_2 | 7 => n_2 \in \{1, 7\}$ Si $n_2 = 1$ alois let donc distingue dans G. Or, G est suppose simple, il n'admet donc pas de sous-groupe distingue propre. Donc $n_2 = 7$ i.e. $\#\mathcal{H} = 7$.

2.

2.1) i) Soit $H \in \mathcal{H}$, on a : $e \cdot H$ ii) Soient $g, g' \in G, h \in \mathcal{H}$; on a $g \cdot (g' \cdot H) = g \cdot (g'Hg'^{-1}) = g(g'Hg')g^{-1} = gg'Hgg'^{-1}g' = (gg')H(gg')^{-1} = (gg')H$. 2.2)D'après le 2ème Théorème de Sylow, si H et H' sont deux 2-Sylow de G, alors ils sont conjugues dans G. $\exists g \in G$ tel que $H' = gHg^{-1}$ i.e. tel que $H' = g \cdot H$; donc H et H' sont dans le même orbite. Il ñ'y a donc qu'une seule orbite : l'action est donc `transitive`.

2.3) Fidèle ? Considérons le morphisme π associe à cette action : $\begin{array}{rcl} \pi : G & \to & \mathfrak{S}_{\mathcal{H}} \\ g & \mapsto & \begin{array}{rcl} \pi_g : \mathcal{H} & \to & \mathcal{H} \\ H & \mapsto & g \end{array} \end{array}$

Le noyau $\ker\pi$ et tant que noyau d'un morphisme de groupe, est une sous-groupe distingué de G. Or G est suppose simple. Donc $\ker\pi = \{e\}$.

Mais $\ker\pi = G$ signifie que $\forall g \in G$, $\forall H \in \mathcal{H}$ on a : $gHg^{-1} = H$. Donc, tout les orbites sont réduites à une élément. Or l'action est transitive, il ñ'y a qu'une seule orbite. (et non pas 7). Donc $\ker\pi \neq g$. conclusion : $\ker\pi = e$ i.e. π est injectif i.e. l'action est fidèle.

2.4) D'après le 1ère Théorème d'isomorphisme on a : ${}^{G}\!/_{\ker\pi} \simeq Im(\pi)$ Mais $\ker\pi = e$ donc ${}^{G}\!/_{\ker\pi} \simeq G$. Donc $G \simeq Im(\pi) < \mathfrak{S}_{\mathcal{H}} \simeq \mathfrak{S}_7$. Donc G est isomorphe à une sous groupe de $\mathfrak{S}_7$.

3) $G \to (\pi)\mathfrak{S}_7 \to (\varepsilon)\{1,-1\}$ — $\varepsilon\pi$ 3.1) Si $\varepsilon\pi$ est surjective alors $Im(\varepsilon\pi) = \{1,-1\} \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ Le noyau $\ker(\varepsilon\pi)$ de $\varepsilon\pi$ est une sous-groupe de G et, d'après le 1 Th d'isomorphisme, on a : ${}^{G}\!/_{\ker(\varepsilon\pi)} \simeq Im(\varepsilon\pi) = \{1,-1\}$ d'où : $[G : \ker(\varepsilon\pi)] = |{}^{G}\!/_{\ker(\varepsilon\pi)}| = |Im(\varepsilon\pi)| = 2$

Donc $\ker(\varepsilon\pi)$ est un sous-groupe de G d'indice 2.

3.2) Puisque G est supposé simple, il ne peut admette de sous-groupe d'indice 2 car un tel sous groupe serait un sous-groupe distingue propre de G. Donc $\varepsilon\pi$ n'est pas surjective or $\varepsilon\pi(e) = 1$ donc $1 \in Im(\varepsilon\pi)$. Donc : $Im(\varepsilon\pi) = \{1\}$. On en déduit que $Im(\pi) \subset \mathfrak{A}_7$ (permutations pairs de $\mathfrak{S}_7$). or : $G \simeq Im(\pi)$ car π est injectif. Donc G est isomorphisme à un sous-groupe de $\mathfrak{A}_7$.

3.3) Par le Théorème de Lagrange, ou doit avoir que l'ordre de G doit divise l'ordre de $\mathfrak{A}_7$ or : $|G| = 2^4 7$ et $|\mathfrak{A}_7| = 2^3 7 3^2 5$ et $2^4 7 \not| 2^3 7 3^2 5.$ on obtient donc une contradiction. Conclusion : G n'est pas simple.