Typesetting test.

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

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

$\langle x \rangle$

This is a long test Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Table des matières

Chapitre 1

GENERALITES

1.1 Grenailles sur les groupes

1.1.1 Groupe et Sous-Groupe

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

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

1. associative
2. élimant neutre
3. symétrique

Si commutative – abelian. Groupes : $(R, +)$, $(S_n, \circ)$, etc.
Soit H un sons-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 $\operatorname{ord}(G)$, $|G|$ 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 $\operatorname{ord}(x)$. Order x est $ord(x) \stackrel{def}{=} |\langle x \rangle|$. En particulier, $\operatorname{ord}(x) = |\,\langle x \rangle\,|$.

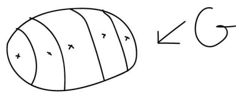
> **Exemple 1.1.1.** S_3.

1.1.2 La classe d'équivalence

> **Définition 3.** Soint 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'aplication 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 povoir $|H|$ (Le même pour le classe à droite).

Comme G est la reunion disjointe des xH, pour x dècrivant un systeme 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 :

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

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

1.2 Normal dans G

Définition 4. 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-group de 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 1.2.1.
1. $\langle\sigma_1\rangle = \{e, \sigma_1, \sigma_2\}$—sous-gropupe engendée pour σ_1 ans $\mathfrak{S}_3$. $[G : H] = 2 \Rightarrow \langle x\rangle \lhd \mathfrak{S}_3$.
2. $\langle\tau_1\rangle = \{e, \tau_1\} \not\lhd \mathfrak{S}_3$. 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 $Kerf := \{x \in G | f(x) = e'\}$, où e' est l'element neutre de G'. C'est un sous-groupe distingué de G.

$$\emptyset,\ \{\emptyset\},\ \{\emptyset,\ \{\emptyset\}\},\ \{\emptyset,\ \{\emptyset,\ \{\emptyset\}\}\},\ \ldots$$

$\mathbb{Z} : \mathbb{N} \times \mathbb{N} : (a,\ b)R(a',\ b')$ psi $a + b' = a' + b$.

$$\mathbb{Z} = {}^{\mathbb{N} \times \mathbb{N}}\!/\!_{R}$$

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

Exemple 1.2.2.
— Soit G un group d'ordre premier p, alors G est groupe simple.
— Alors G est un group simple. En effet, si H est un sous-group de 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 : $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

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

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

Theorem 2. *Tout groupe abélien de type fini G s'écrit de sons la forme :*

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

avec $d_1|d_2|...|d_r$ ($d_r \geq 2$) 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 1.2.3. 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 finis, 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 $|G| = 5$m puisque 5 est premier, G est cyclique et donc $\simeq \mathbb{Z}/_{5\mathbb{Z}}$–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. $\forall x \in X \; e \cdot x = x$
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 :

$$a = b + c \tag{1.2}$$

$$\pi : G \to S_X \tag{1.3}$$

$$g \mapsto \begin{pmatrix} \pi_g : X \to X & \\ & x \mapsto \pi_g(x) = g \cdot x \end{pmatrix} \tag{1.4}$$

Définition 7. 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 :

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

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 group des rotation de $\mathbb{R}^3$ de centre l'origine o agit sur $\mathbb{R}^3$. $G \times \mathbb{R}^3 \to R^3$ et $(r, x) \mapsto r.x = r(x)$. 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 : $\sigma_x \times X \mapsto X$, $(\sigma, x) \mapsto \sigma.x = \sigma(x)$.
   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 $G \times G \to G;\ (g, x) \mapsto g.x = gx$ (loi de composition dons G).
   Soient $x, y \in G$;
   ?$g \in G :\ y = gx \therefore g = yx^{-1}$. 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 :
   $$G \times G \mapsto G;\ (g, x) \mapsto g.x = gxg^{-1}$$
   En effet : (i) Si $x \in G$; on a : $e.x = exe^{-1} = x$.
   (ii) soint $g, g' \in G$ et $x \in G$ ou a :
   $$g.(g'.x) = g(.g'xg'^{-1}) = g(g'xg'^{-1})g^{-1} = (gg')x(g'^{-1}g^{-1}) = (gg')x(gg')^{-1} = (gg').x$$

Utilise $(ab)^{-1} = b^{-1}a^{-1}$.
* $Orb(e) = \{geg^{-1}, g \in G\} = \{e\}$ Donc l'action n'est pas transitive si $G \neq \{e\}$
Si $x \in G$ alors $Orb(x) = \{gxg^{-1}, g \in G$ donc de conjuration de x.
* Le mogan de l'action est :

$$\{g \in G | \forall x \in X, gxg^{-1} = x\} = \{g \in G | \forall x \in X,\ gx = xg\} = centredeG = Z(G)$$

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 : $Stab(x) = \{g \in G | g.x = x\}$. (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 ${}^{X}\!/_{Stabx}$ des classe a gauche monade $Stab(x)$ sont l'orbite de x.*

Aussi, le cardinal de l'orbite $Orb(X)$ est égal a l'indice de stab(x) dans G.

$$\#Orb(x) = [G : Stab(x)]$$

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

1. $\#X = \sum_x [G : Stab(x)]$ *où*
2. *Le moite u d'orbites est donné par la formule (théorème de Burnside) :*

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

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

Remarque. $|G| = n$, $d|n$: $\exists H < G$ *t.q.* $|H| = d$ *? Cyclique, oui* $\exists!$
$n = \prod_n p_i^{\alpha_i},\ p_i - premire$

4) Les Théorèmes de Sylov

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-Sylov de G est un Sylov de G d'sidu : $2^3 = 8$.

1er theoreme de Sylov : 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-Sylov de G.

De plus, le nombre n_p de p-Sylow de vérifie : $n_p = 1 mod p$ et $n_p | q$.

Définition 9. 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.

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 :

   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.

1.3.1 Les Groupes symetrique

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

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 4. *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 : $Ord(\sigma) = ppcm(ord(136), ord(24), ord(598)) = ppcm(3, 2, 3) = 6$

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 : $\sigma = c_1 c_2 ... c_l$, c_i cycles. D'oui : $\tau\sigma\tau^{-1} = \tau(C_1...c_r)\tau^{-1} = (\tau c_1 \tau^{-1})(\tau c_2 \tau^{-1})...(\tau c_r \tau^{-1})$

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

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

On a $\forall \in \{1, ..., m\}$, $g(\tau(i_j)) = \tau(i_{j+1})$ et $f(\tau(i_j)) = (\tau(i_1 \ ... \ i_m))(i_j) = \tau(i_{j+1})$ et $\forall x \in \{1, ..., n\}$
$\{\tau(i_j), j \in \{1, ..., n\}$, 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 $\sigma = c_1...c_r$. Ca suite $(l_1, ..., l_r)$ des lougneus des cycles c_i ordoners en order croissant ($l_1 \leq l_2 \leq ... \leq l_r$). 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 $(2, 2, 3)$

Proposition 4. *Montre que le groupe σ_n est engendré lar les cycles. On a également :*

Theorem 5.
1. *σ_n est engendré pas les transpositions*
2. *...... de la forme (1 i)*
3. *.... (dits elimentaires) de la forme (i i+1)*
4. *les deux permutations (12) et (12...n)*

Démonstration. exercise. □

Proposition : la signature $\epsilon : \sigma_n \to \{\pm 1\}$ 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 transpositons.

Une cycle de longuent laire est une permutation singuie et simasfasfasafasdfasdfasdfasdfasdfasdfasdfasdfasdf ; ;lj ;lj ;lkj ;lkj ;lkj ;lkja ;lsdkjfa ;lsdjfa ;lsdjf

Le nogan $\mathfrak{A}$ du morphisme signature $\varepsilon : \sigma_n \to \{-1, 1\}$ est un sous-group distange d'indice 2 (n>= 2) de σ_n, appelé la m=iem group alteinee = cest donc l'ensemble des permutations pains de σ_n.

Proposition 5. *Si $n \geq 3$, le group alteiné $\mathfrak{A}_n$ et engendre par les 3-cycles.*

Démonstration. exercise. Hint (1b)(1a)=(1ab) □

Theorem 6. *Galois $\mathfrak{A}_n$ est un groupe simple ssi $n \neq 4$.*

Exemple 1.3.1. 1. Soit G un groupe d'ordre 33.

2. Détermine le nombre de 3-Sylow de G. Le group G peut'il être simple ?
3. Déterminer le nombre de 11-Sylow de G. En déduire que G nécessairement abélien. Est-il nécessairement cyclique ?
   D'a pas le 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 adment donc un unique 3-Sylow H. Od, d'apé 2nd Th de Sylow, les conjuges d'un 3-Sylow sont encore un 3-Sylow. Donc les conjuges de H sont égaux à H. Donc $H < G$. Le groupe g admet donc un sous-group distangé prpe : il n'est donc pas simple.
2. De même, le nombre $n_1 1$ de 11-Sylow de G vérifie :

$$\begin{cases} n_1 1 = 1 \ mod 11 \\ n_1 1 | 3 \end{cases}$$

   D'où : $n_1 1 = 1$ G adment donc un unique 11-Sylow K ed, 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 isomprphe an produit direct interne de H par K). Ou : H est d'ordre 3, et 3 est premier, donc H est syclique et donc $H \simeq \mathbb{Z}/_{3\mathbb{Z}}$. De même : K — 11, 11 —,

— K — $K \simeq \mathbb{Z}/_{11\mathbb{Z}}$ Donc : $G \simeq \mathbb{Z}/_{3\mathbb{Z}}\mathbb{Z}/_{11\mathbb{Z}}$ donc G est abélian. Par le Théoréme des reste Chinisis prisque (3,11)=1, on a

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

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

Exemple 1.3.2. 2

On considére le groupe des inveisides $\mathbb{Z}/_{33}{}^*$ 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 : $|(\mathbb{Z}/_{33})^*| = \phi(33) = \phi(3\times 11) = |\text{car } (3,11)| = \phi(3) \times \phi(11) = 2 \times 10 = 20$

   Remarque. *A-t-on* $\bar{12} \in (\mathbb{Z}/_{33})^*$ *? (où* $\bar{a} = a + 33\mathbb{Z}$*).Non car* $(12, 33) \neq 1$*.* $|(\mathbb{Z}/_{33})^*|$ *= nombre d'enties <= 33 et premiers avec 33.*

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

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

   qui indrit un isomporphime de groups sur les groups des inversides :

   $$(\mathbb{Z}/_{11\mathbb{Z}})^*(\mathbb{Z}/_{11\mathbb{Z}})^* \simeq (\mathbb{Z}/_{33\mathbb{Z}})^*$$

   Rappel : Si p est un premier imat et si $m \geq 1$ alors : $(\mathbb{Z}/_{p^m\mathbb{Z}})^* \simeq \mathbb{Z}/_{(p-1)p^{m-1}\mathbb{Z}}$ D'où : $(\mathbb{Z}/_{33\mathbb{Z}})^* \simeq \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{10\mathbb{Z}} \not\simeq \mathbb{Z}/_{20\mathbb{Z}}$ car $(2, 10) \neq 1$. Donc $(\mathbb{Z}/_{33\mathbb{Z}})^*$ n'est pas cyclique. Soit $(a, b) \in \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{10\mathbb{Z}}$. $\text{ord}((a, b)) = ppcm(\text{ord}(a), \text{ord}(b))$. O'où : $\text{ord}(a, b) = 4 \leftrightarrow ppcm(\text{ord}(a), \text{ord}(b)) = 4$. avec $\text{ord}(a)|2$ et $\text{ord}(b)|10$ imposible. Donc le groupe $(\mathbb{Z}/_{33\mathbb{Z}})^*$ n'admet pas d'élt d'ordre 4.

Probléme : $gA_4 < gS_4$ permutations pains de $\mathfrak{S}_4$.

1. On fait agir gS_4 sur lui-même par conjugasion : $\mathfrak{S}_4 \times \mathfrak{S}_4 \to \mathfrak{S}_4$, $(g, h) \mapsto$

$g \cdot h = ghg^{-1}$

(a) Montrer que cete définit bie-une action. Soit $h \in \mathfrak{S}_4$. A quoi conspand l'oi dite de h et le stabilisateur de h ?

$$\mathrm{orb}(h) = \{gh, g \in \mathfrak{S}_4\} \quad = \{ghg^{-1}, g \in \mathfrak{S}_4\} = \text{ classe de conjugation on de } h \text{ dans } \mathfrak{S}_4 \ . \tag{1.5}$$

$$\mathrm{Stab}(h) = \{g \in \mathfrak{S}_4, gh = h\} \quad = \{g \in \mathfrak{S}_4, ghg^{-1} = h\} = \{g \in \mathfrak{S}_4, gh = hg\} \quad = \text{centralisement de } \tag{1.6}$$

(b) Déterminu les class de conjugaison de $\mathfrak{S}_4$. $x, y \in \mathfrak{S}_4$: $x \sim y$ ssi $\exists g \in \mathfrak{S}_4$ t.q. $y = g \cdot x \ y = gxg^{-1}$.

$cl(x) = \{y \in \mathfrak{S}_4 | \exists g \in \mathfrak{S}_4, y = gxg^{-1}\} = \{y = gxg^{-1} | g \in \mathfrak{S}_4\} = \mathrm{orb}(x)$

Rappel : Deux eles de $\mathfrak{S}_n$ sont conjuges dans $\mathfrak{S}_n$ ssi ils ont même type.

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

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

Remarque. *Deux élements g et g' de $\mathfrak{S}_n$ sont coujugués dans $\mathfrak{S}_n$ s'il existe $\sigma \in \mathfrak{S}_n$ tel que $g' = \sigma g \sigma^{-1}$. * deux élets g et g' de $\mathfrak{A}_n$ sont conjugùs dans $\mathfrak{A}_n$. S'il existe $\sigma \in \mathfrak{A}_n$ tel que : $g' = \sigma g \sigma^{-1}$.*

(c) 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. — $\mathfrak{A}_4$ — Si σ appantient 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 impaine commutant avec σ alors :*

$$Stab_{\mathfrak{S}_4}(\sigma) = Stab_{\mathfrak{A}_4}(\sigma)$$

Ov : $\#orb_{\mathfrak{S}_4}(\sigma) = [\mathfrak{S}_4 : Stab_{\mathfrak{S}_4}(\sigma)] = [\mathfrak{S}_4 : Stab_{\mathfrak{A}_4}(\sigma)] = [\mathfrak{S}_4 : \mathfrak{A}_4] \times [\mathfrak{A}_4 : Stab_{\mathfrak{S}_4}(\sigma)] = 2 \cdot \# \mathrm{ord}_{\mathfrak{A}_4}(\sigma)$. Donc les coujugús de σ dans $\mathfrak{S}_4$ constituent deux class de conjugassion dans $\mathfrak{A}_4$.

(d) On considre le 3-cycle $\sigma = (123) \in \mathfrak{S}_4$

i. Quel est l'ordre du stabilisateur de σ dans $\mathfrak{S}_4$?

ii. En d*drire qu'il n'existe pas de permutation impline qui commute avec σ

iii. En e*dies les calss de conjugasion de $\mathfrak{A}_4$.

i. 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 : $[\mathfrak{S}_4 : \mathrm{Stab}_{\mathfrak{S}_4}(\sigma)] = \#orb(\sigma) = 8$. D'où : $|\mathrm{Stab}_{\mathfrak{S}_4}| = \frac{|\mathfrak{S}_4|}{8} = \frac{24}{8} = 3$.

ii. Il u'y a que trois permutations de $\mathfrak{S}_4$ qui commutent avec σ : Donc $Stab_{\mathfrak{S}_4}(\sigma) = \{e, \sigma, \sigma^2\}$.

iii. $\mathfrak{A}_4 = \{e\} \cup \{3-\text{cycles}\} \cup \{type(2,2)\}$. $|\mathfrak{A}_4| = \frac{|\mathfrak{S}_4|}{2} = 12$. Dapre les qustions précédents la classe de conjugatsion $Conj_{\mathfrak{S}_4}(\sigma)$ de σ dans $\mathfrak{S}_4$ne de. compose eu deux classed se conjugaisons dans $\mathfrak{A}_4$ $Con_{\mathfrak{A}_4}((123)) = \{(123),(142),(134),(243)\}$. $Conj_{\mathfrak{A}_4} = \{(132),(124),(143),(234)\}$

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 :*

$$(123) = \sigma^2 = \tau\sigma\tau^{-1} = (\tau(1)\tau(2)\tau(3)) \Rightarrow \tau = (23) \text{ mais } (23) \notin \mathfrak{A}_4.$$

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

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

Remarque. *Considerons l'ensemble $K = \{e,(12)(23),(13)(24),(14)(23)\}$. K est un sous-groupe de $\mathfrak{A}_4$, il est stobe par conjugasion, 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).*

2. Si G est un groupe, on rappelle que le sous-groupe de G engendre par les commutateurs i.e. par les éléments : $xyx^{-1}y^{-1}$ pour $x, y \in G$
   (a) Muter que $D(G) \lhd G$.
   (b) Montier que $H \lhd G$ et G/H est abélien alors $H \supset D(G)$.
   (a) $D(G)$ est stadle par tout automorphisme (car l'image d'un commutatm 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 fortiri est un sous-groupe distingué de g.
   (b) 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 comentatens donc H contient D(G)