Permuter

Alain Wazner. Pour Hélène, Léo et Corentin

Où les permutations forment un groupe

Soit E un ensemble fini, on appelle permutation de E, une bijection de E vers lui-même, on note $\mathcal{S}_E$ l'ensemble des permutations de E.
Comme la composée $f \circ g$ de f et g bijections de E vers E est une bijection de E vers E, l'inverse f^{-1} d'une bijection de E vers E est une bijection de E vers E, et Id_E (l'idendité sur E) : $\begin{cases} E \to E \\ x \mapsto x \end{cases}$ est une permutation de E, $(\mathcal{S}_E, \circ)$ est un groupe.
Si $E = \{1, 2, ..., n\}$ on appelle $(\mathcal{S}_n, \circ)$, le groupe des permutations de E.

Comment le groupe des permutations de tout ensemble fini s'identifie au groupe $(\mathcal{S}_n, \circ)$

Se donner un ensemble E à n élément c'est se donner une bijection e de $\{1, 2, ..., n\}$ vers E, ceci revient à dire que pour tout élément x de E il existe un seul entier i avec $1 \leq i \leq n$ tel que $x = e(i)$.
Soit σ une permutation de E alors, comme e est une bijection de $\{1, 2, ..., n\}$ vers E, pour tout $x \in E$, il n'existe qu'un seul $i \in \{1, 2, ..., n\}$ tel que $x = e(i)$. On appelle alors $\Phi_e(\sigma)(i)$ l'unique entier $j \in \{1, 2, ..., n\}$ - σ et e sont des bijections de $\{1, 2, ..., n\}$ vers lui-même et de $\{1, 2, ..., n\}$ vers E- tel que $\sigma(x) = e(j)$.
$\Phi_e(\sigma)$ **est donc une application de**

$\{1, 2, ..., n\}$ **vers lui-même. Cette application est bijective,** $\Phi_e(\sigma)$ **est donc une permutation de** $\{1, 2, \dots n\}$.
En effet on a la relation $\forall i \in \{1, 2, ..., n\}$,

$$\sigma(e(i)) = \sigma(x) = e(j) = e\left(\Phi_e(\sigma)(i)\right)$$

$\sigma(e(i)) = e\left(\Phi_e(\sigma)(i)\right)$ étant vraie pour tout $i \in \{1, 2, ..., n\}$ on en déduit que $\sigma \circ e = e \circ \Phi_e(\sigma)$, soit après composition par e^{-1} la réciproque de e : $\Phi_e(\sigma) = e^{-1} \circ \sigma \circ e$ est bijective comme composée de bijections.
Par la donnée de e **on a donc définit une application** Φ_e $\begin{cases} \mathcal{S}_E \to \mathcal{S}_n \\ \sigma \mapsto \Phi_e(\sigma) = e^{-1} \circ \sigma \circ e \end{cases}$
cette application est bijective car de

$$\Phi_e(\sigma) = e^{-1} \circ \sigma \circ e \Leftrightarrow \sigma = e \circ \Phi_e(\sigma) \circ e^{-1}$$

on déduit que $e \circ \tau \circ e^{-1}$ est l'unique antécédent de τ par Φ_e.
De plus si Id_E est la permutation identité de E alors $\Phi_e(Id_E)(i)$ est l'entier $j \in \{1, 2, ..., n\}$ tel que si $Id_e(x) = x = e(i)$ alors $Id_E(x) = x = e(j)$, on a $e(i) = e(j)$ soit $i = j$ et donc $\Phi_e(Id_E)(i) = i$, $\forall i$ et donc $\Phi_e(Id_E) = Id_{\{1,,..,n\}}$.
Si τ et σ sont des permutations de E alors

$$\begin{aligned} \Phi_e(\tau) \circ \Phi_e(\sigma) &= e^{-1} \circ \tau \circ e \circ e^{-1} \circ \sigma \circ e \\ &= e^{-1} \circ \tau \circ \sigma \circ e = \Phi_e(\tau \circ \sigma) \end{aligned}$$

Une application f d'un groupe $(G_1, .)$ vers un groupe $(G_2, \times)$ telle que l'image du neutre de G_1 soit celui de G_2 et telle que

$$f(g.h) = f(g) \times f(h),\ \forall g, h$$

s'appelle un morphisme de groupe, si elle est de plus bijective on l'appelle un isomorphisme de groupe.
Ainsi Φ_e est un isomorphisme du groupe $(\mathcal{S}_E, \circ)$ vers le groupe $(\mathcal{S}_n, \circ)$.
Un isomorphisme de groupe permet un transport de structure : Si f est un **isomorphisme du groupe** $(G_1, .)$ **vers le groupe** $(G_2, \times)$ alors

- **Pour tout sous-groupe H_1 de G_1, $f(H_1)$ est un sous groupe de G_2 équipotent à H_1.**
- **Pour tout sous-groupe H_2 de G_2 il existe un sous-groupe H_1 équipotent à H_2 de G_1 tel que $f(H_1) = H_2$.**

Preuve : Si H_1 est un sous-groupe de G_1 et si e_1 et e_2 sont les neutres respectifs des groupes de G_1 et G_2, de $e_1 \in G_1$ alors $e_2 = f(e_1) \in f(H_1)$, si $y_1, y_2 \in f(H_1)$ alors $\exists x_1, x_2 \in H_1$ tels que

$y_1 = f(x_1)$ et $y_2 = f(x_2)$ et $f(x_1) \times f(x_2) = f(x_1.x_2) \in f(H_1)$ car $x_1.x_2 \in H_1$.
Si H_2 est un sous-groupe de G_2 alors soit $I = f^{-1}(H_1) = \{x \in G_1/f(x) \in H_2\}$. $e_1 \in I$ car $f(e_1) = e_2 \in H_2$.
Si $x_1, x_2 \in I$ alors $f(x_1.x_2) = f(x_1) \times f(x_2) \in H_2$ car $f(x_1) \in H_2$ et $f(x_2) \in H_2$, donc $x_1.x_2 \in I$, I est un groupe tel que $f(I) = H_1$.
En se donnant e l'isomorphisme Φ_e identifie le groupe $(\mathcal{S}_n, \circ)$ et tous ses sous-groupes à $(\mathcal{S}_E, \circ)$ et tous ses sous-groupes.
Caractériser $(\mathcal{S}_E, \circ)$ et tous ses sous-groupes c'est donc caractériser $(\mathcal{S}_n, \circ)$ et tous ses sous-groupes. L'isomorphisme par lequel cette identication est possible dépend à priori du choix de e, on emploie le terme d'isomorphisme non canonique pour Φ_e. A partir de ce qui suit pour étudier $(\mathcal{S}_E, \circ)$, on se donnera une bijection e de $\{1, 2, ..., n\}$ vers E et on étudiera $(\mathcal{S}_n, \circ)$.

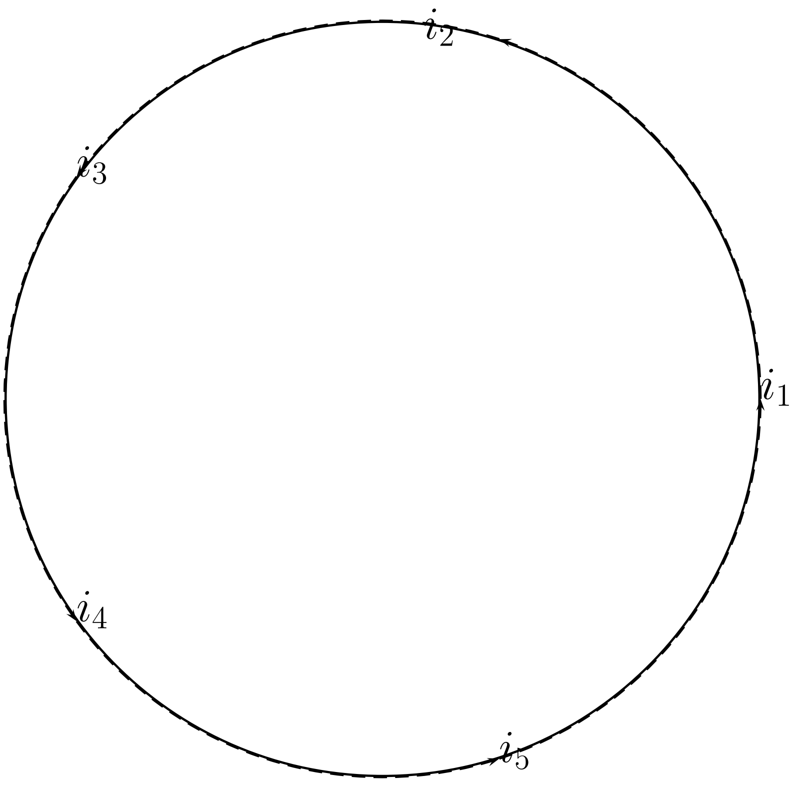
cycles

Soit $\sigma \in \mathcal{S}_n$ alors on écrit $\sigma = (\sigma(1), ..., \sigma(n))$.
Exemple : $\sigma = (4, 2, 1, 3)$ est la permutation de

$$\mathcal{S}_4 \text{ telle que } \begin{cases} \sigma(1) = 4 \\ \sigma(2) = 2 \\ \sigma(3) = 1 \\ \sigma(4) = 3 \end{cases}$$

Cycles

S'il existe $I = \{i_1, ..., i_r\} \subset \{1, ..., n\}$ tel que $\sigma(j) = j$ si $j \notin I$ et tel que $\sigma(i_k) = i_{k+1}$ si $k \neq r$ et $i_r = 1$ alors on dit que σ est un cycle d'ordre r.



Au dessus, un cycle d'ordre 5

Si σ est un cycle d'ordre r alors si $k < r$ alors $\sigma^k \neq Id$, $\sigma^r = Id$ où Id est la permutation de $\mathcal{S}_n$ telle $x \mapsto x$ et $\sigma = \underbrace{\sigma \circ \cdots \circ \sigma}_{r\ fois}$.

Preuve On représente les entiers i_k par des points A_k du cercle de rayon 1 rapporté à un repère orthonormé dont l'origine O est le centre du cercle et tels que l'angle $\left(\widehat{Ox, \overrightarrow{OA_k}}\right)$ soit de mesure $\dfrac{2(k-1) \times \pi}{r}$ (Sur la figure précédente $r = 5$). σ : si $k < r$ alors $i_k \mapsto i_{k+1}$ et $i_r \mapsto i_1$, la représentation sur le cercle donne si $k < r$ alors $A_k \mapsto A_{k+1}$ et $A_r \mapsto A_1$, quand σ agit sur $\{i_1, ..., i_r\}$ par $\sigma.i_k = \sigma(i_k)$, σ agit sur la représentation des i_k en A_k par **une rotation d'angle de mesure** $\dfrac{2 \times \pi}{r}$. Par composition σ^i agit sur la représentation des i_k en A_k par **une rotation d'angle de mesure** $\dfrac{2i \times \pi}{r}$. Cette rotation est l'identité si $i = r$ et différente de l'identité si $i < r$, d'où $\sigma^i \neq Id$ si $i < r$ et $\sigma^r = Id$.

Transposition : On appelle transposition un cycle d'ordre 2.

groupes stabilisateur, orbites, équations aux classes

Action de groupe E étant un ensemble et G une action du groupe G sur E est la donnée d'une

opération externe $\begin{cases} G \times E \to E \\ (g, x) \mapsto g.x \end{cases}$ telle que $\forall g_1, g_2 \in G, \forall x \in E,\ g_1.(g_2.X) = (g_1 g_2).x$ telle que si e est le neutre de G alors $\forall x \in E,\ e.x = x$.
Exemple : Sur l'ensemble des sommets d'un polygones régulier à n cotés, le groupe des isométries qui conservent le polygone définit une action de groupe par : si ρ est une telle isométrie et $\{A_1, ..., A_n\}$ l'ensemble de ces sommets par $\rho.A_i = \rho(A_i)$.

Stabilisateur, orbites Soient un ensemble E et $(G, \times)$ un groupe, $(g, x) \mapsto g.x$ une action de $(G, \times)$ sur E alors $\forall x \in E$ l'ensemble $G_x = \{g \in G / g.x = x\}$ est un sous-groupe de G appelé **stabilisateur** de x.
Orbites : Soient un ensemble E et $(G, \times)$ un groupe, $(g, x) \mapsto g.x$ une action de $(G, \times)$ sur E alors $\forall x \in E$ l'ensemble $\omega(x) = \{y \in E / \exists g \in G,\ y = g.x\}$ est appelé orbite de x sous l'action de G.
On a la propriété suivante : Si x et y sont deux éléments de E alors

- Soit $\omega(x) = \omega(y)$.
- Soit $\omega(x) \cap \omega(y) = \emptyset$.

Preuve : Si $\exists z \in \omega(x) \cap \omega(y)$ alors $\exists g_x, g_y \in G/z = g_x.x = g_y.y$, il suit que $\left\{ \begin{array}{l} x = \left(g_x^{-1} \times g_y\right).y \\ y = \left(g_y^{-1} \times g_x\right).x \end{array} \right.$.
Si $w \in \omega(x)$ alors $\exists g \in G$ tel que

$$\begin{aligned} w &= g.x = g.\left(\left(g_x^{-1} \times g_y\right).y\right) \\ &= \left(g \times g_x^{-1} \times g_y\right).y \in \omega(y) \end{aligned}$$

Si $w \in \omega(y)$ alors $\exists g \in G$ tel que

$$\begin{aligned} w &= g.y = g.\left(\left(g_y^{-1} \times g_x\right).x\right) \\ &= \left(g \times g_y^{-1} \times g_x\right).x \in \omega(x) \end{aligned}$$

Puisque $\forall x \in E/x \in \omega(x)$ (en effet $x = e.x$) E est l'union disjointe des orbites de tous ses points, ce qui s'écrit

$$\boxed{E = \bigsqcup_{x \in E} \omega(x)}$$

Quotients d'un groupe par ses stabilisateurs, formule des classes Si $(G, .)$ est un groupe dont H est un sous-groupe, on appelle G/H le quotient de G par H l'ensemble $\{x.H/x \in G\}$ où $x.H$ désigne l'ensemble de tous les produits $x.h$ avec $h \in H$.
Exemple : Si $\mathbb{Z}$ désigne l'ensemble des entiers relatifs, c'est un groupe quand on le munit de l'opération d'addition. En considérant que 0 est pair l'ensemble des entiers relatifs pairs est un sous-groupe de $\mathbb{Z}$: ce sous-groupe est noté **au risque de confusions $2\mathbb{Z}$ (en effet $2\mathbb{Z}$ fait référence**

au produit des entiers relatifs par 2 **est n'est pas plus que** $\mathbb{Z}$ **un groupe multiplicatif, par contre c'est bien un groupe additif)**. $\mathbb{Z}/2.\mathbb{Z}$ est donc l'ensemble des $n+2\mathbb{Z}$ avec $n \in \mathbb{Z}$. $n + 2\mathbb{Z}$ suivant que n est pair ou impair est l'ensemble des nombres pairs ou l'ensemble des nombres impairs, donc **l'ensemble d'ensembles** $\mathbb{Z}/2.\mathbb{Z}$ comprend deux éléments : l'ensemble des entiers relatifs pairs et l'ensemble des entiers relatifs impairs.

Si $(G, .)$ **est un groupe de sous-groupe** H **alors tous les ensembles** $x.H$ **sont équipotents** : En effet : $\begin{cases} x.H \to y.H \\ w \mapsto yx^{-1}w \end{cases}$ est une bijection de $x.H$ vers $y.H$.

Si $x, y \in G$ **et si** H **est un sous-groupe de** G **alors on a l'alternative :**

- $xH = yH$**.**
- $xH \cap yH = \emptyset$**.**

Si $xH \cap yH \neq \emptyset$ alors $\exists h_x, h_y \in H$ tels que $x.h_x = y.h_y$ il suit que

- $x = y.h_y.h_x^{-1}$
- $y = x.h_x.h_y^{-1}$

$\forall h \in H$ $x.h = y.h_y.h_x^{-1}.h \in y.H$ donc $x.H \subset y.H$ et $y.h = x.h_x.h_y^{-1}.h \in x.H$ donc $y.H \subset x.H$. On a prouvé que $xH \cap yH \neq \emptyset \Rightarrow xH = yH$ ce qui équivalent à l'alternative énoncée.

$\forall x \in G$ $x \in x.H$: En effet si e est le neutre alors

$e \in H$ et $x = x.e \in x.H$.
G est l'union disjointe des ensembles $x.H$ avec $x \in G$

$$\boxed{G = \bigsqcup_{x \in G} x.H}$$

Pour un ensemble E fini on note $|E|$ le nombre d'éléments de E (nombre appelé cardinal).
Si $(G, .)$ est un groupe fini : alors tout sous-groupe H de G est fini et tout ensemble $x.H$ est fini. Les ensembles $x.H$ étant équipotents ont même cardinal, ce cardinal est celui de H car $H = e.H$ avec e le neutre du groupe G. La formule $G = \bigsqcup_{x \in G} x.H$ entraîne que G est l'union disjointe d'ensembles de même cardinal $|H|$ donc G est un multiple de H et puisque G est union disjointe de **tous** les ensembles $x.H$ on a $|G| = |G/H| \times |H|$. Ce qui résume par :
Si $(G, .)$ est un groupe fini alors, pour tout sous-groupe H de G, $|H|$ divise $|G|$ et $|G/H| = \dfrac{|G|}{|H|}$.
Si $(G, \times)$ est un groupe qui agit sur un ensemble E par $(g, x) \in G \times E \mapsto g.x \in E$ alors pour tout $x \in E$ l'orbite $\omega(x)$ est équipotente au quotient G/G_x du groupe G par le stabilisateur G_x de x : Si $z = y \times g_x$ avec $y \in G,\ x \in E,\ g_x \in G_x$ alors

$z.x = (y \times g_x).x = y.(g_x.x) = y.x$ ne dépend pas de g_x et appartient à $\omega(x)$: on définit bien une application de G/G_x vers $\omega(x)$ en associant à tout élément $y \times g_x$ de $y.G_x$ la valeur (indépendante de g_x) $(y \times g_x).x = y.x$. Cette application est surjective : $y.x$ a pour antécédent $y \times G_x$, elle est aussi injective car si $y.x = z.x$ alors $y^{-1}.(y.x) = y^{-1}(z.x)$ soit $(y^{-1} \times y).x = (y^{-1} \times z).x$ ou $x = (y^{-1} \times z).x$ et donc $y^{-1} \times z \in G_x$ soit $z \in y \times G_x$ ce qui entraîne, d'après ce qui précède, $z \times G_x = y \times G_x$. **On en déduit que si $(G, \times)$ est un groupe fini qui agit sur E alors pour tout x de E $\omega(x)$ est fini, son cardinal divise le cardinal de G et vaut $\dfrac{|G|}{|G_x|}$.**

Décomposition d'une permutation en produit de cycles

Le groupe $(\mathcal{S}_n, \circ)$ agit sur l'ensemble $\{1, 2, .., n\}$ par : $\begin{cases} \mathcal{S} \times \{1, 2, .., n\} \to \{1, 2, .., n\} \\ (\sigma, i) \mapsto \sigma.i = \sigma(i) \end{cases}$. Soit $\sigma \in \mathcal{S}_n$ on pose $\sigma^0 = Id$ la permutation identité et si $n \geq 1$ on pose $\sigma^n \overset{déf}{=} \sigma \circ \sigma^{n-1}$ et on appelle σ^n la puissance n-ième de σ car on a la relation $\boxed{\sigma^m \circ \sigma^n = \sigma^{m+n}}$. L'ensemble $\{\sigma^n / n \in \mathbb{N}\}$ **est fini** comme sous-ensemble de $\mathcal{S}_n$, il suit que pour au moins deux entiers **distincts** m et n (supposons $m > n$), on a $\sigma^m = \sigma^n$, ceci s'écrit alors

$\sigma^n \circ \sigma^{m-n} = \sigma^n$ et en composant par la permutation inverse de σ^n, on obtient $\sigma^{m-n} = Id$. Pour toute permutation σ il existe une entier non nul o (dans ce qui précède $o = m - n$) tel que $\sigma^o = Id$, nous posons $o(\sigma)$ le plus petit entier o non nul o tel que $\sigma^o = Id$. $o(\sigma)$ est appelé l'ordre de σ et on a :

- (i) Si $1 \leq i < o(\sigma)$ alors $\sigma^i \neq Id$
- (ii) L'ensemble $\{\sigma^n / n \in \mathbb{N}\}$ est l'ensemble $\{Id, \sigma, ..., \sigma^{o(\sigma)-1}\}$, c'est un sous-groupe de $\mathcal{S}_n$ à $o(\sigma)$ éléments noté $< \sigma >$ et appelé **le groupe cyclique engendré par** σ.
- (iii) Pour tout $\tau \in < \sigma >$ on a $\tau^{o(\sigma)} = Id$.

Preuve : (i) : si pour $1 \leq i < o(\sigma)$ $\sigma^i = Id$ alors $o(\sigma) \leq i$ par définition, sachant que $i < o(\sigma)$ il vient $o(\sigma) < o(\sigma)$ ce qui est impossible.

(ii) Si i, j sont des entiers de $\{0, \ldots, o(\sigma) - 1\}$ **distincts** tels que $\sigma^i = \sigma^j$ alors

- si $i > j$ alors $\sigma^i = \sigma^j \Leftrightarrow \sigma^{i-j}\sigma^j = \sigma^j$: ceci entraîne après composition par $\left(\sigma^j\right)^{-1}$ que $\sigma^{i-j} = Id$ et comme $0 < i - j < o(\sigma)$ ceci est impossible.
- si $i < j$ alors $\sigma^i = \sigma^j \Leftrightarrow \sigma^i = \sigma^{j-i} \circ \sigma^i$: ceci entraîne après composition par $\left(\sigma^i\right)^{-1}$ que $Id = \sigma^{j-i}$ et comme $0 < j - i < o(\sigma)$ ceci est impossible.

$\{Id, ..., \sigma^{o(\sigma)} - 1)\}$ définit bien un ensemble à $o(\sigma)$ éléments inclus dans l'ensemble des puissances entières de σ mais une puissance entière de σ est un σ^r où $0 \leq r < o(\sigma)$, ces ensembles sont donc égaux, en effet on peut faire **la division euclidienne de tout entier n par $o(\sigma)$**; C'est à dire trouver $q, r \in \mathbb{N}$ avec $0 \leq r < o(\sigma)$ tels que $n = o(\sigma) \times q + r$ on a alors :

$$\begin{aligned} \sigma^n &= \sigma^{o(\sigma) \times q + r} = \left(\sigma^{o(\sigma)}\right)^q \circ \sigma^r \\ &= Id^q \circ \sigma^r = Id \circ \sigma^r = \sigma^r \end{aligned}$$

Remarque : Bien que toute permutation soit cyclique (elle engendre un groupe cyclique), toute permutation n'est pas un cycle comme le montre cet exemple sur $\mathcal{S}_4$: $\sigma = (2, 1, 4, 3)$ vérifie $\sigma \circ \sigma = Id$ et n'est pas un cycle. Si c'était le cas, suivant la définition des cycles, σ étant d'ordre 2 devrait avoir $4 - 2 = 2$ points fixes (des entiers i tels que $\sigma(i) = i$).

Quelques définition :

- **Soit σ une permutation de $\mathcal{S}_n$ on appelle point fixe de σ un entier i tel que $\sigma(i) = i$.**
- **Soit $\mathcal{C}$ un cycle de $\mathcal{S}_n$, on appelle support de $\mathcal{C}$, on le note $Supp(\mathcal{C})$ l'ensem-**

ble des entiers compris entre 1 et n qui ne sont pas des points fixes de $\mathcal{C}$.

- **Deux cycles $\mathcal{C}_1, \mathcal{C}_2 \in \mathcal{S}_n$ sont dits à supports disjoints si l'intersection de leurs supports est vide.**

Décomposition d'une permutation en produit de cycles **Toute permutation est un produit commutatif de cycles disjoints.**

Une preuve : Un sous-groupe H de $< \sigma >$ est $< \sigma^r >$ où r est un diviseur de $o(\sigma)$: Comme sous-ensemble de $< \sigma >$ un sous groupe est un ensemble $\{\sigma^n / n \in E \subset \mathbb{N}\}$, s'il se réduit à $\{Id\}$ alors c'est $< \sigma^{o(\sigma)} >$, sinon il existe un plus petit entier non nul r tel que $\sigma^r \in H$, si $n \in E$ la division euclidienne de n par r s'écrit $n = qr + s$ où $0 \leq s < r$ et $H \ni \sigma^n = (\sigma^r)^q \circ \sigma^s$. Comme $\sigma^r \in H$, on en déduit que $\sigma^s \in H$, comme r est le plus petit entier non nul de E c'est que $s = 0$ et donc n est multiple de r. E est un ensemble de multiples de r, c'est **l'**ensemble des multiples de r, puisque H contenant σ^r il contient -par composition- pour tous les $k \in \mathbb{N}$ les permutations $(\sigma^r)^k = \sigma^{kr}$, par ce qui précède $H =< \sigma^r >$ qui est un groupe à r éléments. On en déduit de plus que r est un diviseur de $o(\sigma)$ cardinal du groupe $< \sigma >$.

Les sous-groupes de $< \sigma >$ sont les $< \sigma^r >$

avec r diviseur de $o(\sigma)$.

Quand le groupe $(<\sigma>, \circ)$ agit sur $\{1, ..., n\}$ par $\sigma^n.i = \sigma^n(i)\ \forall n \in \mathbb{N}, i \in \{1, ..., n\}$ le stabilisateur G_i est un groupe $<\sigma_i^r>$, avec r_i diviseur de $o(\sigma)$, le cardidal de G/G_i est $\dfrac{o(\sigma)}{r_i}$, celui de $\omega(i)$ est alors r_i.

Pour toutes les valeurs de i l'ensemble $<\sigma>/G_i = <\sigma>/<\sigma^{r_i}>$ est un groupe. Voici une preuve :

Un élément de $<\sigma>/G_i = <\sigma>/<\sigma^{r_i}>$ est une classe d'équivalence, soit l'ensemble $\sigma^r <\sigma^{r_i}> = \{\sigma^r \circ (\sigma^{r_i})^q / r, q \in \mathbb{N}\}$. On définit alors sur $<\sigma>/G_i$ le produit des deux classes $\sigma^r <\sigma^{r_i}> \times \sigma^{r'} <\sigma^{r_i}>$ comme l'ensemble des produits de composition $\tau \circ \epsilon$ avec $\begin{cases} \tau \in \sigma^r <\sigma^{r_i}> \\ \epsilon \in \sigma^{r'} <\sigma^{r_i}> \end{cases}$

Les produits $\tau \circ \epsilon$ s'écrivent $\sigma^r \circ \sigma^{kr_i} \circ \sigma^{r'} \circ \sigma^{lr_i}$ avec $k, l \in \mathbb{N}$ soit encore $\sigma^{r+r'} \circ \sigma^{(k+l)r_i}$. Quand k et l varient dans $\mathbb{N}$, leur somme $k+l$ varie aussi dans $\mathbb{N}$ donc :

$$(E)\boxed{\sigma^r <\sigma^{r_i}> \times \sigma^{r'} <\sigma^{r_i}> = \sigma^{r+r'} <\sigma^{r_i}>}$$

Le produit de deux classes de G/G_i est une classe de G/G_i et l'expression précédente montre que ce produit est commutatif. Les calculs successifs de

$$\left(\sigma^r <\sigma^{r_i}> \times \sigma^{r'} <\sigma^{r_i}>\right) \times \sigma^{r''} <\sigma^{r_i}>$$

et de

$$\sigma^r < \sigma^{r_i} > \times \left(\sigma^{r'} < \sigma^{r_i} > \times \sigma^{r''} < \sigma^{r_i} >\right)$$

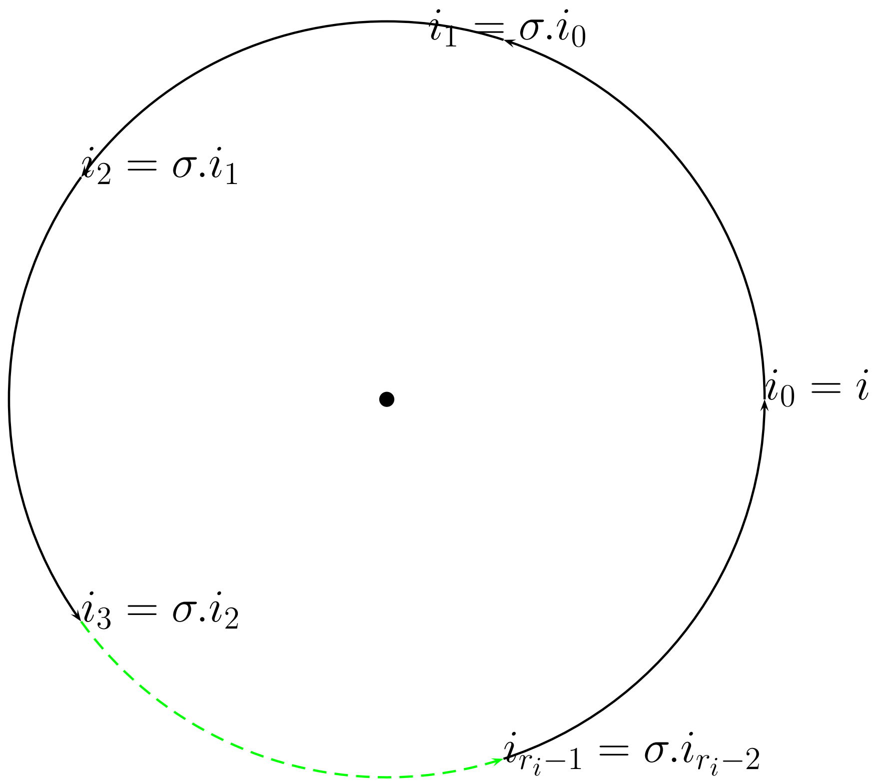
montrent, par utilisation de (E), que ces deux classes sont égales à la classe $\sigma^{r+r'+r''} < \sigma^{r_i} >$: le produit $\times$ est associatif. Comme $\sigma^{o(\sigma)} = Id$, $< \sigma^{r_i} >$ est une classe élément de G/G_i neutre pour l'opération $\times$ sur cet ensemble par utilisation de (E). Pour $r \in \mathbb{N}$ on se donne $k \in \mathbb{N}$ tel que $ko(\sigma) > r$ alors $ko(\sigma) - r \in \mathbb{N}$ et

$$\sigma^r < \sigma^{r_i} > \times \sigma^{ko(\sigma)-r} < \sigma^{r_i} >= \sigma^{ko(\sigma)} < \sigma^{r_i} >=< \sigma^{r_i} >$$

$(G/G_i, \times)$ **est un groupe.**
Comme $\forall r \in \mathbb{N}$

$$\sigma^r < \sigma^{r_i} >= \sigma < \sigma^{r_i} > \times \cdots \times \sigma < \sigma^{r_i} >$$

G/G_i est le groupe cyclique à $\dfrac{o(\sigma)}{r_i}$ éléments $< \sigma^{r_i} >$ et la bijection $G/G_i \to \omega(i)$ associe à $\sigma^r < \sigma^{r_i} >$ l'entier $\sigma^r.i = \sigma^r(i)$ avec la relation $\left(\sigma^r < \sigma^{r_i} > \times \sigma^{r'} < \sigma^{r_i} >\right).i = \left(\sigma^r \circ \sigma^{r'}\right).i$, on a alors le shéma :



Si on appelle $\mathcal{C}(i)$ le cycle $(i, \sigma(i), \sigma^2(i), ..., \sigma^{r_i-1}(i))$ alors

(i) $\mathcal{C}(i)$ **a pour support** $\omega(i)$
(ii) $\forall i, j \in \{1, \ldots, n\}$
– $\omega(i) = \omega(j) \;\Leftrightarrow\; \mathcal{C}(i) = \mathcal{C}(j)$
– $\mathcal{C}(i)|_{\omega(i)} = \sigma|_{\omega(i)}$
– $\mathcal{C}(i) \circ \mathcal{C}(j) = \mathcal{C}(j) \circ \mathcal{C}(i)$

Preuve : (i) le support de $\mathcal{C}(i)$ est $\{\sigma(i), \sigma^2(i), ..., \sigma^{r_i-1}(i)\}$ sous-ensemble de

$\{\sigma^n(i)/n \in \mathbb{N}\} = \omega(i)$. Comme ces ensembles ont même cardinal r_i ils sont égaux.
(ii) Soit $j \in \omega(i)$ alors $j = \sigma^k(i)$ avec $k < r_i$. Si $k = 0$ alors $j = i = \mathcal{C}(i)\left(\sigma^{r_i-1}(i)\right) = \sigma\left(\sigma^{r_i-1}(i)\right)$, si $k > 0$ alors $j = \sigma^k(i) = \mathcal{C}(i)\left(\sigma^{k-1}(i)\right) = \sigma\left(\sigma^{k-1}(i)\right)$: les images j de $i,\ \sigma(i),\ \ldots,\ \sigma^{r_i-1}(i)$ par σ et $\mathcal{C}(i)$ sont égales donc $\mathcal{C}(i)|_{\omega(i)} = \sigma|_{\omega(i)}$.
(iii) : Si $i = j$ alors $\mathcal{C}(i) \circ \mathcal{C}(j) = \mathcal{C}(j) \circ \mathcal{C}(i)$ car $\mathcal{C}(i) = \mathcal{C}(j)$.
Si $i \neq j$ alors si $j \in \omega(i)$ alors $\omega(i) = \omega(j)$ puis $\mathcal{C}(i) = \mathcal{C}(j)$ et donc $\mathcal{C}(i) \circ \mathcal{C}(j) = \mathcal{C}(j) \circ \mathcal{C}(i)$. Si $j \notin \omega(i)$ alors $\omega(i)$ et $\omega(j)$ sont des orbites disjointes, $\mathcal{C}(i)$ et $\mathcal{C}(j)$ sont à supports disjoints. $\mathcal{C}(i)$ et $\mathcal{C}(j)$ sont égales à l'identité sur $\{1, ..., n\}\backslash\omega(i)$ et $\{1, ..., n\}\backslash\omega(j)$ comme $\omega(i)$ et $\omega(j)$ sont disjoints. Restreintes à l'ensemble $\{1, ..., n\}\backslash\omega(i)\cup\omega(j)$ les permutations $\mathcal{C}(i)$ et $\mathcal{C}(j)$ sont égales à l'identité et commutent. Restreinte à l'ensemble $\{1, ..., n\}\backslash\omega(j)$ (resp $\{1, ..., n\}\backslash\omega(i)$) la permutation $\mathcal{C}(i)$ (resp $\mathcal{C}(j)$) est l'identité : $\mathcal{C}(i)$ et $\mathcal{C}(j)$ commutent sur $\omega(i)$ et $\omega(j)$ et donc $\boxed{\mathcal{C}(i) \circ \mathcal{C}(j) = \mathcal{C}(j) \circ \mathcal{C}(i)}$.
(iv) Si $\mathcal{C}(i) = \mathcal{C}(j)$ alors $\mathcal{C}(i)$ et $\mathcal{C}(j)$ ont même support et $\omega(i) = \omega(j)$.
Si $\omega(i) = \omega(j)$ alors $\mathcal{C}(i)$ et $\mathcal{C}(j)$ ont même support et il suit que pour $0 \leq r < |\omega(i)|$ on a $j = \sigma^r(i)$, il suit $\forall n \in \mathbb{Z},\ \sigma^n(i) = \sigma^m(j)$ avec $m = n + r$ on

en déduit que $\{\sigma^n(i)/n \in \mathbb{Z}\} = \{\sigma^m(j)/m \in \mathbb{Z}\}$ **Soit** $\mathcal{C}(i) = \mathcal{C}(j)$.

σ **est le composé, nécessairement commutatif, des cycles** $\mathcal{C}(i)$ **où chaque** i **est un seul élément choisi arbitrairement -c'est à dire « par un hasard »- dans le support de chaque** $\mathcal{C}(i)$ **:** En faisant agir le groupe $G = \{\sigma^n/n \in \mathbb{Z}\}$ sur l'ensemble $\{1, \ldots, n\}$ par $\sigma^n.i = \sigma^n(i)$ la formule

$$\boxed{\{1, \ldots, n\} = \bigsqcup_{i \in \{1,\ldots,n\}} \omega(i)}$$

devient

$$\boxed{\{1, \ldots, n\} = \bigsqcup_{i \in \{1,\ldots,n\}} Supp\,(\mathcal{C}(i))}$$

Les supports des $\mathcal{C}(i)$ étant disjoints, si $1 \leq i \leq n$ et $j \in \omega(i) = Supp\,(\mathcal{C}(i))$ le composé de tous les $\mathcal{C}(i)$ a pour image $\mathcal{C}(i)(j)$; Par définition de $\mathcal{C}(i)$ on peut trouver $k \in \{1, \ldots, n\}$ tel que $j = \sigma(k)$ et $\sigma(j) = \sigma^2(k)$ soit $\sigma(j) = \mathcal{C}(i)(j)$ **autrement dit l'image** j **par** σ **est l'image de** j **par le composé de tous les** $\mathcal{C}(i)$. Ceci étant vrai pour tout $1 \leq i \leq n$ et $j \in \omega(i) = Supp\,(\mathcal{C}(i))$ **on a égalité entre** σ **et le composé de tous les** $\mathcal{C}(i)$.

Propriété : A permutation des cycles près, la décomposition d'une permutation en produit de cycle est unique.

Preuve : suivant ce qui précède :

- L'ensemble des supports dont le produit est une permutation σ donnée est uniquement déterminé comme l'ensemble des orbites de l'action du groupe $< \sigma >$.
- Se donnant un élément de cet ensemble (un support S_i) il n'y a qu'un seul cycle ayant ce support et qui est un terme du produit. En ettet : dire que cette orbite est le support d'un sous-groupe cyclique de $< \sigma >$ d'ordre le cardinal de S_i détermine que $< \sigma >$ est stable sur S_i et que restreinte à S_i c'est **le cycle** $(j, \sigma(j), \ldots, \sigma^{card(S_i)-1}(j))$ où j est n'importe quel élément de S_i puisque tout groupe cyclique est généré de cette manière par n'importe lequel de ses éléments.
- Comme les cycles du produit égal à σ sonr deux à deux commutants cette décomposition est unique à permutation de ses cycles distincts près.