Algèbre et Géométrie
L3, X6M0030

Hossein Abbaspour
Université de Nantes 2017

Table des matières

1.1. Groupe : Définition, notations et exemples

Soit G un ensemble. Une *loi de composition* est une application

$$m : G \times G \to G.$$

Parfois on utilise les termes *opération binaire* ou *multiplication* à la place de la loi de composition. Pour simplifier l'écriture, on utilise $x.y$ ou $x + y$ à la place de $m(x, y)$.

DÉFINITION 1.1.1. *Un groupe est un ensemble G. muni d'une loi de composition . possédant les propriétés suivantes :*

(1) Associativité : $(x.y).z = x.(y.z)$

(2) Élément neutre : il existe un élément $e \in G$ t.q. pour $x \in G$

$$e.x = x.e = x$$

(3) Tout $x \in G$ admet un symétrique (ou inverse) y, c'est-à-dire

$$xy = yx = e$$

REMARQUE 1.1.2. *Dans un groupe G, l'élément neutre est unique : Soient e_1 et e_2 deux éléments neutres.*

On a $e_1e_2 = e_2$ car e_1 est neutre et $e_1e_2 = e_1$ est neutre. Donc $e_1 = e_1e_2 = e_2$

REMARQUE 1.1.3. *Dans une groupe G l'inverse de $x \in G$ est unique car si y_1 et y_2 sont les inverses de x, on a : $(y_1x)y_2 = ey_2 = y_2$ et $(y_1x)y_2 = y_1(xy_2) = y_1e = y_1$ donc $y_1 = y_2$.*

NOTATION 1.1.4. *Quand on utilise la notation additive $+$ pour la loi de composition, l'inverse de x est noté $-x$ et l'élément neutre est noté 0.*

$$x + (-x) = (-x) + x = 0$$

Quand on utilise la notation multiplicative . pour la loi de composition, l'inverse de x est noté par x^{-1} et l'élément neutre est noté par 1 :

$$xx^{-1} = x^{-1}x = 1$$

EXEMPLE 1.1.5. *L'ensemble des entiers $\mathbb{Z}$ muni de l'addition $+$ est un groupe. L'élément neutre est 0. D'autres exemples sont les ensembles des nombres rationnels $\mathbb{Q}$ et réel. $\mathbb{R}$ muni de l'addition.*

EXEMPLE 1.1.6. *Soient $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$ et $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$. Alors $(\mathbb{R}^*, \times)$ et $(\mathbb{Q}^*, \times)$ sont des groupes. Dans tous les deux cas l'élément neutre est 1. Le point essentiel ici est que si $x \in \mathbb{Q}$ et $x \neq 0$ alors $\frac{1}{x} \in \mathbb{Q}$.*

EXEMPLE 1.1.7. *Les matrices :*
Soit

$$M_2(\mathbb{R}) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}\}$$

L'opération binaire sur $M_2(\mathbb{R})$ est définie par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} a+x & b+y \\ c+z & d+w \end{pmatrix}$$

L'élément neutre est la matrice $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

EXEMPLE 1.1.8. *Le cercle unité, est la partie de $\mathbb{C}^*$ définie par*
$S^1 := \{z \in \mathbb{C} \mid z = 1\} = \{e^{i\theta} \mid \theta \in \mathbb{R}\}$.

Le cercle unité S^1 muni de la multiplication habituelle (celle dans $\mathbb{C}$) est un groupe. L'associativité est claire et l'élément neutre $1 \in \mathbb{C}$ est également dans S^1.

On observe que l'inverse de $z \in S^1$ est également dans dans S^1, car

$$\mid z^{-1} \mid = \frac{1}{\mid z \mid} = 1.$$

Donc chaque élément $z \in S^1$ a un inverse dans S^1.

On peut voir ce dernier autrement : si $z = e^{i\theta}$

$$z^{-1} = \frac{1}{z} = \frac{1}{e^{i\theta}} = e^{-i\theta} \in S^1$$

Le résultat suivant montre comment on peut construire un nouveau groupe à partir de deux groupes.

PROPOSITION 1.1.9. *Soient (G_1, m_1) et (G_2, m_2) deux groupes. Alors le produit cartésien de G_1 and G_2 muni de la loi de composition*

$$m((x_1, x_2), (y_1, y_2)) := (m_1(x_1, y_1), m_2(x_2, y_2))$$

$x_1, y_1 \in G_1$ et $x_2, y_2 \in G_2$, est un groupe.

DÉMONSTRATION. Pour la simplicité on utilise . pour la loi de composition, donc le produit sur $G_1 \times G_2$ est donné par

$$(x_1, x_2)(y_1, y_2) := (x_1 y_1, x_2 y_2).$$

L'élénement neutre de $G_1 \times G_2$ est (e_1, e_2) où e_i est l'élément neutre de G_i : Pour tout $(x_1, x_2) \in G_1 \times G_2$ on a

$$(x_1, x_2)(e_1, e_2) = (x_1 e_1, x_2 e_2) = (x_1, x_2).$$

Associativité :

(1.1) $[(x_1, x_2)(y_1, y_2)](z_1, z_2) = (x_1 y_1, x_2 y_2)(z_1, z_2) = ((x_1 y_1)z_1, (x_2 y_2)z_2)$

(1.2) $(x_1, x_2)[(y_1, y_2)(z_1, z_2)] = (x_1, x_2)(y_1 z_1, y_2 z_2) = (x_1(y_1 z_1), x_2(y_2 z_2)),$

en utilisant l'associativité des produits de G_1 et G_2, on voit que $(x_1 y_1)z_1 = x_1(y_1 z_1)$ et $(x_2 y_2)z_2 = x_2(y_2 z_2)$, et donc

$$[(x_1, x_2)(y_1, y_2)](z_1, z_2) = (x_1, x_2)[(y_1, y_2)(z_1, z_2)]$$

Inverse : Tout $(x_1, x_2) \in G_1 \times G_2$ a (x_1^{-1}, x_2^{-1}) a pour l'inverse car

$$(x_1, x_2)(x_1^{-1}, x_2^{-1}) = (x_1 x_1^{-1}, x_2 x_2^{-1}) = (e_1, e_2).$$

Ici x_i^{-1} est l'inverse de x_i dans G_i.

□

DÉFINITION 1.1.10. *Un groupe $(G, .)$ est dit commutatif (ou abélien) si pour x et $y \in G$,*

$$x.y = y.x$$

EXEMPLE 1.1.11. *Les groupes $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ et $(S^1, \times)$, $(M_2(\mathbb{R}), +)$ sont abéliens mais*

Règles de calcul : Soit $(G, .)$ un groupe.

(1) Pour $x \in G$ et $n \in N$, la n-ième puissance de x est définie par récurrence
   - $x^0 = 1$
   - $x^n = x.x^{n-1}$
   - on définit $x^{-n} := (x^n)^{-1}$.

   En conséquence, pour tout k et l, $x^k.x^l = x^l.x^k$, et $(x^k)^l = x^{kl}$.

(2) $(xy)^n = x^n y^n$ si G est abélien.

(3) $(xy)^{-1} = y^{-1}x^{-1}$:

Démonstration :

$$(y^{-1}x^{-1})(x.y) \overset{\text{associativité}}{=} y^{-1}(x^{-1}.(x.y)) = y^{-1}((x^{-1}.x).y)) = y^{-1}(e.y) = y^{-1}y = e$$

Alors par l'unicité de l'inverse $(y^{-1}x^{-1}) = (xy)^{-1}$.

(4) Soient x, y et $a \in G$. Si $ax = ay$ alors $x = y$ car

$$x = e.x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = e.y = y$$

(5) Si $ax = y$ alors, $x = e.x = (a^{-1}a)x = a^{-1}(a.x) = a^{-1}y$, donc

$$x = a^{-1}y$$

1.2. Translations à gauche et à droite

On fixe un élément $a \in G$. On définit les applications $R_a : G \to G$ et $L_a : G \to G$ par

$$R_a(g) := ga \tag{1.1}$$

$$L_a(g) := ag \tag{1.2}$$

Proposition 1.2.1. *Soit G un groupe.*

(i) Pour tout $a \in G$, R_a et L_a sont bijectives

(ii) Pour a, b, $L_a \circ L_b = L_{ab}$ et $R_a \circ R_b = R_{ba}$.

(i) On traite la translation à gauche, pour la translation à droite les démonstrations sont très similaires. Si $L_a(x) = L_a(y)$ alors $ax = ay$ donc $a^{-1}(ax) = a^{-1}(ay)$ et $x = y$. Donc L_a est injective. Pour tout $g \in G$, $g = L_a(a^{-1}g)$ donc $g \in \text{Image}(L_a)$ et donc L_a est surjective.

(ii) $(L_a \circ L_b)(x) = L_a(L_b(x)) = a(bx) = (ab)x = L_{ab}(x)$.

1.3. Groupes symétriques

On considère l'ensemble fini $E = \{1, \cdots n\}$ de n éléments. On pose $S_n = \{f : E \to E \mid f \text{ est bijective } \}$ qui est naturellement muni de la loi de décomposition des applications : Pour tout $\tau, \sigma \in S_n$ et pour tout $y \in E$

$$(\tau \circ \sigma)(x) = \tau(\sigma(x))$$

Ceci nous fournit un groupe $(S_n, \circ)$ qui joue un rôle important dans l'étude des groupes.

L'élément neutre est l'application d'identité $id : E \to E$, $id(x) = x$, $\forall x \in E$. l'inverse de $\tau \in S_n$ est l'application réciproque $\tau^{-1} : E \to E$ qui existe car τ est bijective, en particulier τ^{-1} est bijective.

On remarque que la cardinalité de $S_n = n!$. On appelle les éléments de S_n les permutations de E et S_n le groupe symétrique de l'ensemble E.

On représent une permutation $\sigma : E \to E$ par une matrice $2 \times n$,

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Par exemple, pour $n = 3$, si $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, on a

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

et

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

On conclut que $\tau\sigma \neq \tau\sigma$ et S_3 et donc S_3 n'est pas abélien. En fait, le groupe S_n n'est pas abélien si $n \geq 3$.

1.4. Calcul mod n et $\mathbb{Z}_n$

On fixe $n \in \mathbb{Z}$. On dit que les entiers a et b sont congrus modulo n si n divise $a - b$ et on écrit

$$a \equiv b \mod (n)$$

Grâce à la division euclidienne on sait que tout entier a est congru avec une élément de $\mathbb{Z}_n := \{0, 1, \cdots, n-1\}$. On se restreint donc à $\mathbb{Z}_n$. Pour ne pas confondre avec $\mathbb{Z}$ on note désormais $i \in \mathbb{Z}_n$ par $\bar{i}$.

Structure additive. La somme $\bar{i} + \bar{j}$ est par définition le reste de la division de $i + j$ par n. Autrement dit $\bar{i} + \bar{j}$ est l'unique élément de $\mathbb{Z}_n$ tel que

$$i + j \equiv \bar{i} + \bar{j} \mod (n)$$

Il est clair que l'addition $+$ est associative et que $\bar{0}$ est l'élément neutre. L'inverse de $\bar{i}$ est $\overline{n - i} \in \mathbb{Z}_n$ quand $i \neq 0$. L'inverse de $\bar{0}$ est évidemment lui-mà[a]me.

Exemple 1.4.1. *Groupe linéaire*
Soit V un espace vectoriel. L'ensemble $\mathrm{End}(V)$ *des endomorphismes contient la partie*

$$\mathrm{GL}(V) : \{f : V \to V, \ \textit{linéaire} \mid f \ \textit{est bijective}\}$$

La loi de composition est, comme pour S_n, donnée par la composition des applications. Le point clé est ici est que l'inverse d'une bijection linéaire est linéaire. L'associativité : Pour tout x , on a

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$$

et

$$((f \circ (g \circ h))(x) = f \circ (g((h(x)) = f(g(h(x))),$$

donc $(f \circ g) \circ h = f \circ (g \circ h)$.

Structure multiplicative. On se demande naturellement si la multiplication dans $\mathbb{Z}$ induit une structure de groupe sur $\mathbb{Z}_n$. La réponse est oui si on se restreint à une partie de $\mathbb{Z}_n$. Il est clair que s'il y a une structure de groupe alors l'élément neutre est $\bar{1}$ et puisque $\bar{i}.\bar{0} = \bar{0}$ donc $\bar{O}$ n'a pas d'inverse. Donc il est nécessaire d'enlever $\bar{0}$ de $\mathbb{Z}_n$. Mais cela ne suffit pas non plus. Par exemple, dans $\mathbb{Z}_6$ et $\bar{2}\bar{3} = \bar{0}$ qu'on vient d'exclure. Cet exemple nous mène à la définition suivante. On pose

$$\mathbb{Z}_n^* := \{\bar{i} \mid (i, n) = 1\} \tag{1.1}$$

On munit $\mathbb{Z}_n^*$ de l'opération définie comme suit : Pour $\bar{i}$ et $\bar{j}$ on définit $\bar{i}.\bar{j}$ le reste de la division de ij par n Autrement dit c'est l'unique élément, noté $\overline{ij}$, dans $\mathbb{Z}_n$ tel que

$$ij \equiv \overline{ij} \mod (n)$$

On observe que si $(i, n) = (j, n) = 1$ alors $(ij, n) = 1$ [si pour un entier premier p, $p \mid ij$ et $p \mid n$ alors $p \mid i$ ou $p \mid j$ donc $(i, n) \neq 1$ ou $(j, n) \neq 1$]. Par conséquent ij (et le reste de la divisition de ij par n) et n sont aussi premiers entre eux. Donc $\overline{ij} \in \mathbb{Z}_n^*$. Donc l'opération binaire . est définie sur $\mathbb{Z}_n^*$ à valeurs dans $\mathbb{Z}_n^*$. Par la suite on explique l'existence de l'inverse : si $(i, n) = 1$, par le théorème de Bézout, il existe deux entirers r et s tels que $ri + sn = 1$.

On peut supposer que $1 \leq r \leq n-1$ sinon à l'aide de la division euclidienne on peut écrire $r = kn + r'$ où $r' \in \mathbb{Z}_n$ et nous avons alors $r'i + (k+s)n = 1$ où $r' \in \mathbb{Z}_n$ et s est remplacé par $s + k$.

A partir de l'identité $ri + sn = 1$ on obtient que $ri \equiv 1 \mod (n)$ et $\bar{r}\bar{i} = 1$. Donc $\bar{r}$ est l'inverse de $\bar{i}$.

1.5. Ordre d'un groupe et d'un élément

L'ordre d'un groupe G est par définition le cardinal de son ensemble sous-jacent de G et il est noté par $|G|$.

Définition 1.5.1. — *Si pour tout $n \in \mathbb{Z}$, $g^n \neq e$, on pose* $\mathrm{Ord}(g) = +\infty$
— *S'il exist $k \in \mathbb{Z}$ tel que $g^k = e$, on définit* $\mathrm{Ord}(g) = min\{k \in \mathbb{N} \mid g^k = e\}$. *On remarque que s'il existe un $k \in \mathbb{Z}$ tel que $g^k = e$, on a également $g^{-k} = e$, donc il existe $k \in \mathbb{N}$ tel que $g^k = e$, donc notre définition a un sens.*

Proposition 1.5.2. *(1) Si g d'ordre fini n alors $\{g^k \mid k \in \mathbb{Z}\} = \{e, \cdots, g^{n-1}\}$*
(2) Si $\mathrm{Ord}(g) = n$ *et $g^k = e$ alors $n \mid k$.*
(3) Si $\mathrm{Ord}(g) = +\infty$ *alors l'application $k \mapsto g^k$ est injective.*

Démonstration. (1) Soit $k \in \mathbb{Z}$. En divisant par n , on peut écrire $k = sn + r$ où $0 \leq r \leq n-1$ et

$$g^k = g^{sn+r} = g^{sn}g^r = (g^n)^s g^r = e^k g^r = g^r.$$

Donc $g^k \in \{e, \cdots, g^{n-1}\}$.

(2) On divise k par n ; on obtient $k = sn + r$ où $0 \leq r \leq n-1$ et

$$e = g^k = g^{sn+r} = g^{sn}g^r = (g^n)^s g^r = e^s g^r = g^r.$$

donc $g^r = e$ et $r < n$. Comme n est l'ordre de g, $r = 0$.

(3) Par l'absurde. Supposons que $g^k = g^l$; alors $g^{k-l} = e$: cela contredit $\mathrm{Ord}(g) = \infty$.

□

1.6. Sous-groupe

Définition 1.6.1. *Soit $(G, .)$ un groupe et $H \subset$ une partie de G. On dit que $H \neq \emptyset$ est un sous-groupe de G si H muni de la loi de composition . est un groupe.*

L'associativité de . dans H sera automatique car $H \subset$. Les conditions non triviales sont

(1) Si g_1 et g_2 sont dans H alors $g_1 g_2 \in H$. Autrement H est stable par la multiplication de G.
(2) Si $g \in H$ alors $g^{-1} \in H$.

Les conditions (1) et (2) impliquent que $e \in H$: comme $H \neq \emptyset$ alors il existe $x \in H$. Par (2) , $x^{-1} \in H$. Par (1) , $e = x.x^{-1} \in H$.

Exemple 1.6.2. *$(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ sont deux sous-groupes de $(\mathbb{R}, +)$.*

Exemple 1.6.3. *Pour tout $n \in \mathbb{Z}$,*

$$n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\},$$

est un sous-groupe de $(\mathbb{Z}, +)$.

Exemple 1.6.4. *Le cercle unité S^1 est un sous-groupe de $(\mathbb{C}^*, \times)$.*

Proposition 1.6.5. *Soit H un partie non-vide d'un groupe G. Alors H est un sous-groupe si seulement si pour tout $x, y \in H$, $xy^{-1} \in H$.*

DÉMONSTRATION. La partie ($\Rightarrow$) est claire.

($\Leftarrow$) : On va montrer que les conditions (1) et (2) sont satisfaites. Tout d'abord, on choisit un élément $x \in H \neq \emptyset$; pour $y = x$ on obtient que $e = xx^{-1} \in H$ donc $e \in H$. Condition (2) : Pour $g \in H$, on a $g^{-1} = eg^{-1} \in H$ (on applique l'hypothèse à $x = e$ et $y = g$). Donc H est stable par l'inversion.

Condition (1) : Soient g_1, $g_2 \in H$. Par la partie précédente, on sait que $g_2^{-1} \in H$ Donc en appliquant l'hypothèse à $x = g_1$ et $y = g_2^{-1}$, on a $g_1 g_2 = xy^{-1} \in H$.

□

EXEMPLE 1.6.6. *On fixe $n_1, \cdots, n_p \in \mathbb{Z}$ et définit*

$$\langle n_1, \cdots, n_p \rangle := \{a_1 n_1 + \cdots + a_p n_p \mid a_i \in \mathbb{Z}\}.$$

A l'aide de la proposition 1.6.5 on peut aisément vérifier que $\langle n_1, \cdots, n_p \rangle$ est un sous-groupe de $\mathbb{Z}$.

Soit $q = pgcd(n_1, n_2, \cdots, n_k)$, par le théorème de Bézout il existe des entiers $r_1, \cdots, r_k$ tels que

$$q = r_1 n_1 + \cdots + r_k n_k \in \langle n_1, \cdots, n_p$$

et donc pour $s \in \mathbb{Z}$, $sq \in \langle n_1, \cdots, n_p \rangle$ autrement dit

$$\{sq \mid s \in \mathbb{Z}\} \subset \langle n_1, \cdots, n_p \rangle.$$

Réciproquement, si a_i sont des enteirs, $a_1 n_1 + \cdots + a_p n_p \rangle \in \{sq \mid s \in \mathbb{Z}\}$ car il existe des entiers α_i's tels que $n_i = \alpha_i q$ et donc

$$a_1 n_1 + \cdots + a_p n_p = a_1 \alpha_1 q + \cdots + a_p \alpha_p q \in \{sq \mid s \in \mathbb{Z}\}.$$

Ceci montre que $\langle n_1, \cdots, n_p \rangle \subset \{sq \mid s \in \mathbb{Z}\}$ et

$$\{sq \mid s \in \mathbb{Z}\} = \langle n_1, \cdots, n_p \rangle$$

EXEMPLE 1.6.7. *Soit $G = \mathrm{GL}(\mathbb{R}^n)$ et $q = \sum q_{ij} x_i x_j$ une forme quadratique. L'ensemble des applications linéaires qui conservent q*

$$O(\mathbb{R}^n, q) := \{A \in \mathrm{GL}(V) \mid q(Ax) = q(x)$$

est un sous-groupe de $GL(\mathbb{R}^n)$. On l'appele le groupe orthogonal de la forme q.

DÉFINITION 1.6.8. *Pour un élément $g \in G$, on se demande naturellement quel est le plus petit sous-groupe de G qui contient g. Tel sous-groupe doit contenir toutes les puissances g^n $n \in \mathbb{Z}$ car il contient g. Il s'avère que*

$$\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\} \tag{1.1}$$

est en fait un sous-groupe de G qu'on appelle le sous-groupe engendré par g.

Mà[a]me si un groupe G n'est pas abélien, il contient un sous-groupe abélien, appelé le centre du groupe G

$$Z(G) := \{g \in G \mid \forall x \in G \quad gx = xg\}$$

Lorsque $Z(G)$ n'est pas le sous-groupe trivial $\{e\}$, il fournit des informations intéressantes sur G.

PROPOSITION 1.6.9. *Si $H_1, H_2 \leq G$, alors $H_1 \cap H_2 \leq G$*

DÉMONSTRATION. Si x et $y \in H_1 \cap H_2$, alors x et $y \in H_i$, $i = 1, 2$, comme H_i est un sous-groupe, alors $xy^{-1} \in H_i$, $i = 1, 2$.

□

1.7. Morphisme de groupes

Une méthode pour étudier un groupe consiste à le comparer avec les groupes . Pour ce faire on a besoin de parler de morphisme de groupes.

Définition 1.7.1. *Une application $f : G \to H$ entre deux groupes est un morphisme de groupes si pour tout $x, y \in G$,*

$$f(x.y) = f(x).f(y)$$

Exemple 1.7.2. *(1) Pour tout groupe abélien G et tout $n \in \mathbb{Z}$, $f : G \to G$ définie par $f(x) := x^n$ est un morphisme de groupes. C'est une conséquence de l'identité $x^n y^n = (xy)^n$ qu'on a vue en "Règles de Calcul".*

(2) $tr : (M_2(\mathbb{R}), +) \to (\mathbb{R}, +)$ et $\det : (\mathrm{GL}(V), \circ) \to (\mathbb{R}^*, \times)$ sont deux morphismes de groupes.

Proposition 1.7.3. *Pour tout morphisme de groupes $f : G \to H$, nous avons*

(1) $f(e_G) = e_H$

(2) Pour tout $g \in G$,

$$f(g)^{-1} = f(g^{-1})$$

Démonstration. (1) On choisit un élément $x \in G$ et on considère $h = f(x)$. Nous avons

$$f(e_G)h = f(e_G)f(x) = f(e_G x) = f(x) = h,$$

alors par l'unicité de l'élément neutre de H on conclut que $f(e_G) = e_H$.

(2) On voit que $f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$, alors par l'unicité de l'inverse $f(g)^{-1}$ dans H, on en déduit que

$$f(g^{-1}) = f(g)^{-1}.$$

□

Définition 1.7.4. *Un automorphisme de G est un morphisme de groupes $f : G \to G$ qui est bijectif.*

La conjugaison nous fournit une classe importante d'automorphisme de groupes : Pour $g \in G$, on définit $i_g : G \to G$ par

$$i_g(x) = gxg^{-1}.$$

— i est injective : si $gxg^{-1} = gyg^{-1}$, donc $g^{-1}gxg^{-1}g = g^{-1}gyg^{-1}g$ alors $x = y$.
— Pour $x \in G$, $x = gg^{-1}xgg^{-1} = i_g(g^{-1}xg)$, donc $x \in \mathrm{Image}(i_g)$.
— $i_g(x)i_g(y) = gxg^{-1}gyg^{-1} = gxyg^{-1} = i_g(xy)$, cela montre i_g est un morphisme de groupes.

Proposition 1.7.5. *L'ensemble $\mathrm{Aut}(G) = \{f : G \to G \mid f$ est automorphisme$\}$ muni de la composition des applications est un groupe.*

Démonstration. Nous savons que la décomposition des applications est associative. et l'application de l'identité est l'élément neutre. L'inverse d'un morphisme bijectif f est l'application réciproque f^{-1} mais il faut montrer que f^{-1} est un morphisme de groupes. Comme f est un morphisme de groupes, on a

$$f(f^{-1}(x)f^{-1}(y)) = f(f^{-1}(x))f(f^{-1}(y)) = xy,$$

alors par la définition de l'application réciproque

$$f^{-1}(xy) = f^{-1}(x)f^{-1}(y).$$

□

PROPOSITION 1.7.6. *L'application $i : G \to \mathrm{Aut}(G)$ donnée par $g \mapsto i_g$ est un morphisme de groupes.*

DÉMONSTRATION. Pour tout g_1 et g_2 on a

$$(i_{g_2} \circ i_{g_1})(x) = i_{g_2}(g_1 x g_1^{-1}) = g_2(g_1 x g_1^{-1})g_2^{-1} = (g_2 g_1)x(g_1^{-2}g_2^{-1}) = (g_2 g_1)x(g_2 g_1)^{-1} = i_{g_2 g_1}(x)$$

d'où

$$i_{g_2} \circ i_{g_1} = i_{g_2 g_1}$$

qui montre que i est un morphisme de groupes.

□

DÉFINITION 1.7.7. *Un sous-groupe H de G est dit distingué, et on écrit $H \trianglelefteq G$ s'il est stable par tous les automorphismes intérieurs, i.e. pour tout $g \in G$*

$$gHg^{-1} \subset H,$$

PROPOSITION 1.7.8. *Si $H \trianglelefteq G$ alors pour tout $g \in G$*

$$gHg^{-1} = H$$

DÉMONSTRATION. Nous savons déjà que $gHg^{-1} \subset H$, montrons l'autre inclusion. En appliquant l'hypothèse pour g^{-1}, nous avons également $g^{-1}Hg \subset H$, qui après la conjugaison par g donne

$$g(g^{-1}Hg)g^{-1} \subset gHg^{-1}$$

d'où $H \subset gHg^{-1}$. Nous avons donc l'égalité $H = gHg^{-1}$. □

PROPOSITION 1.7.9. *Soit $f : G \to H$ un morphisme de groupes.*

(1) L'image de f ,

$$\mathrm{Image}(f) := \{f(g) \mid g \in G\}$$

est un sous-groupe de H.

(2) Le noyau de f,

$$\mathrm{Ker}(f) := \{g \in G \mid f(g) = e_H\}$$

est un sous-groupe distingué de G

DÉMONSTRATION. (1) Soit $x = f(g_1)$ et $y = f(g_2) \in \mathrm{Image}(f)$, alors $xy^{-1} = f(g_1)f(g_2)^{-1} = f(g_1)f(g_2^{-1}) = f(g_1 g_2^{-1}) \in \mathrm{Image}(f)$.

(2) Si $g_1, g_2 \in \ker(f)$,

$$f(g_1 g_2^{-1}) = f(g_1)f(g_2^{-1}) = (g_1)f(g_2)^{-1} = e_H.e_H = e_H$$

donc $g_1 g_2^{-1} \in \ker(f)$ donc $\ker(f)$ est un sous-groupe. Soient $g \in G$ et $h \in \ker(f)$, on a

$$f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)e_H f(g)^{-1} = fg)f(g)^{-1} = e_H$$

alors $ghg^{-1} \in \ker(f)$ et $\ker(f)$ est distingué

□

PROPOSITION 1.7.10. *Soit $f : G \to H$ un morphisme de groupes.*

(1) L'image d'un sous-groupe $K \leq G$ par f, est un sous-groupe de H, i.e.

(2)

$$f(K) := \{f(g) \mid g \in K\} \leq G.$$

(3) L'image réciproque par f d'un sous-groupe P de H est un sous-groupe de G

$$f^{-1}(P) := \{g \in G \mid f(g) \in P\}$$

est un sous-groupe G. De plus, si P est distingué alors $f^{-1}(P)$ est distingué.

DÉMONSTRATION. (1) Soit $x = f(g_1)$ et $y = f(g_2) \in f(K)$, alors $xy^{-1} = f(g_1)f(g_2)^{-1} = f(g_1)f(g_2^{-1}) = f(g_1g_2^{-1}) \in f(K)$ car $g_1g_2^{-1} \in K$, K étant un sous-groupe.

(2) Si $g_1, g_2 \in f^{-1}(P)$,

$$f(g_1g_2^{-1}) = f(g_1)f(g_2^{-1}) = f(g_1)f(g_2)^{-1} \in P$$

car $f(g_1)$ et $f(g_2) \in P$ et P est un sous-groupe ; alors $g_1g_2^{-1} \in f^{-1}(P)$. Soient $g \in G$ et $h \in f^{-1}P)$, on

$$f(ghg^{-1}) = f(g)f(h)f(g)^{-1} \in P$$

car $f(h) \in P$ et P est distingué. alors $ghg^{-1} \in f^{-1}(P)$ et $f^{-1}(P)$ est distingué.

□

LEMME 1.7.11. *Un morphisme $f : G \to H$ est injectif si et seulement* $\ker(f) = \{e_G\}$.

EXEMPLE 1.7.12. *l'application $i_nS_n \to S_{n+1}$ donnée par*

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \to \begin{pmatrix} 1 & 2 & \cdots & n & n+1 \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) & n+1 \end{pmatrix}$$

Autrement $i_n(\sigma)$ est la permutation qui agit sur $n+1$ comme l'identité et sur $\{1, \cdots, n\}$ comme σ. On peut donc se permettre de traiter S_n comme un sous-groupe de S_{n+1}. En composant ces inclusions, on peut considérer S_n comme un sous-groupe de S_{n+2} autrement $i_{n+1}i_n : S_n \to S_{n+2}$ est une injection. Pour la simplicité, on se permettra d'identifier $\sigma \in S_n$ avec sont image $i_n(\sigma) \in S_{n+1}$ et on écrira σ à la place $i_n(\sigma)$.

EXEMPLE 1.7.13.
— *Le noyau de $i : G \to \mathrm{Aut}(G)$ est le centre $Z(G)$ car si pour $g \in G$, $i_g = id_G$, alors pour tout $x \in G$,*

$$gxg^{-1} = x$$

qui est équivalent à $gx = xg$ et donc $g \in Z(G)$. Et le réciproquement si $g \in Z(G)$ alors $i_g(x) = gxg^{-1} = xgg^{-1} = x$ et donc $i_g = id_G$.

— $\det : GL(\mathbb{R}^) \to \mathbb{R}$ *est un morphisme de groupes et son noyau est le sous-groupe distingué*

$$\mathrm{SL}(n, \mathbb{R}) := \{M \in \mathrm{GL}(\mathbb{R}^n) \mid \det(M) = 1\}.$$

— $tr : M_n(\mathbb{R}) = \mathrm{End}(\mathbb{R}^n) \to \mathbb{R}$ *est un morphisme de groupes dont le noyau est*

$$\mathrm{sl}(n, \mathbb{R}) = \{M \in M_n(\mathbb{R}) \mid tr(M) = 0\}.$$

Soit G un groupe. Pour toutes parties $H, K \subset G$, on définit

$$HK := \{hk \mid h \in H \& k \in K\}$$

PROPOSITION 1.7.14. *(i) Si $H \trianglelefteq G$ et $K \leq G$ alors $HK \leq G$*
(ii) Si $H \trianglelefteq G$ et $K \trianglelefteq G$ alors $HK \trianglelefteq G$

DÉMONSTRATION. (i) Soit $x = h_1k_1$ et $y = h_2k_2 \in HK$. O n considère $xy^{-1} = h_1k_1k_2^{-1}h_2^{-1}$. Comme H est distingué alors $k_1k_2^{-1}H = Hk_1k_2^{-1}$, et donc il existe $h \in H$ tel que $k_1k_2^{-1}h_1 = hk_1k_2^{-1}$ d'où

$$xy^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1hk_1k_2^{-1} \in HK$$

et donc HK est un sous-groupe.

(ii) Soit $g \in G$ et $hk \in HK$. Alors $ghkg^{-1} = (ghg^{-1})(gkg^{-1}) \in HK$.

□

1.8. Sous-groupe engendré

On fixe un groupe G. Par la proposition 1.6.9, l'intersection de deux sous-groupes de G est un sous-groupe de G. De la même manière, l'intersection d'une famille (éventuellement infinie) de sous-groupes, est un sous-groupe de G.

DÉFINITION 1.8.1. *Soit E une partie de G. L'intersection de tous les sous-groupes de G contenant de E est noté $\langle E\rangle$, dit engendré par E.*

PROPOSITION 1.8.2. *Pour toute partie E, Le sous-groupe $\langle E\rangle$ est le plus petit sous-groupe contenant E.*

DÉMONSTRATION. Soit $H \leq G$ un sous-groupe contenant E, par la définition de $\langle E\rangle$, $\langle E\rangle \subset H$. □

PROPOSITION 1.8.3. *Pour toute partie $E \subset G$,*

$$\langle E\rangle = \{x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} |, x_i \in E \quad \epsilon_i = \pm 1\}.$$

DÉMONSTRATION. Tout d'abord $\{x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} \mid x_i \in E \quad \epsilon_i = \pm 1\}$ est un sous groupe car

$$(x_1^{\epsilon_1} \cdots x_n^{\epsilon_n})(x_{n+1}^{\epsilon_{n+1}} \cdots x_m^{\epsilon_m})^{-1} = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} x_m^{-\epsilon_m}) \cdots x_{n+1}^{-\epsilon_{n+1}} \in \{x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} \mid x_i \in E \quad \epsilon_i = \pm 1\}$$

Deuxièmement, $E \subset \{x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} \mid x_i \in E \quad \epsilon_i = \pm 1\}$, et si H est un sous-groupe de G contant E , alors contient toutes les expressions de la forme $x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ où $x_i \in E \subset H$, car H est un sous-groupe. On conclut que $\langle E\rangle = \{x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} \mid x_i \in E \quad \epsilon_i = \pm 1\}$. □

COROLLAIRE 1.8.4. *Si $E' \subset E$ alors $\langle E'\rangle \leq \langle E\rangle$.*

DÉFINITION 1.8.5. *Un groupe G est dit cyclique sir il est engendré par un élément, i.e. il existe $g \in G$ tel que*

$$G = \langle g\rangle$$

Par exemple $G = \mathbb{Z}$ est un groupe cyclique et $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$.

Le sous-groupe dérivé $D(G)$ d'un groupe est le sous-groupe engendré par les commutateurs i.e

$$D(G) := \langle [g, h] \mid g, h \in G\rangle$$

où $[g, h] := ghg^{-1}h^{-1}$.

PROPOSITION 1.8.6. *Le sous-groupe dérivé $D(G)$ est distingué.*

DÉMONSTRATION. Soit $g \in G$. D'abord on montre que $gD(G)g^{-1} = \langle g[h, k]g^{-1} \mid h, k \in G\}$. Soit E l'ensemble des commutateurs.

$$D(G) = \bigcap_{E\subset H, H\text{sous-groupe de G}} H,$$

alors

$$gD(G)g^{-1} = \bigcap_{E\subset H, H\text{sous-groupe de G}} gHg^{-1} = \bigcap_{gEg^{-1}\subset gHg^{-1}, H\text{sous-groupe de G}} gHg^{-1}$$
$$= \bigcap_{gEg^{-1}\subset H', H'\text{sous-groupe de G}} H'$$

d'où $gD(G)g^{-1} = \langle g[h,k]g^{-1} \mid h,k \in G\rangle$.

On observe que pour pour tout $h,k \in G$, on a $g[h,k]g^{-1} = [ghg^{-1}, gkg^{-1}]$, on en déduit

$$gD(G)g^{-1} \subset D(G)$$

donc $D(G)$ est distingué. □

1.9. Relation d'équivalence

Motivation On a vu que le noyau d'un morphisme de groupes $f : G \to H$ est un sous-groupe distingué de G. On souhaite savoir si tout sous-groupe distingué de G est le noyau d'un certain morphisme $f : G \to H$. Plus précisément, pour tout sous-groupe distingué K de G, existe-il un groupe H et un morphisme $f : G \to H$ tel que $K = \ker(f)$?

Définition 1.9.1. *Soit E un ensemble. Une relation sur E est une partie $R \subset E \times E$. On écrit $x \sim_R y$ si $(x,y) \in R$. On dit que R est une relation d'équivalence si les conditions suivantes sont satisfaites*

(i) pour tout $x \in E$, $x \sim_R x$ [Réfléxivité].
(ii) Si $x \sim_R y$ alors $y \sim_R y$ [Symétrie].
(iii) Si $x \sim_R y$ et $y \sim_R z$ alors $x \sim_R z$.[Transitivité]

Exemple 1.9.2. *Une décomposition de E en parties disjointes $E = \cup_i E_i$ fournit une relation d'équivalence sur E, définie comme suit :*

$$x \sim y \text{ si } \exists i \text{ tel que } x,y \in E_i.$$

Inversement, une relation d'équivalence R sur E fournit une décomposition de E en parties disjointes. Pour $x \in E$ on définit

$$[x] := \{y \in E \mid x \sim y\}$$

Lemme 1.9.3. — $[x] \cap [y] \neq \emptyset$ *ssi* $x \sim y$.
— *si* $[x] \cap [y] \neq \emptyset$ *alors* $[x] = [y]$.

Notation 1.9.4. *On appelle $[x]$ la classe d'équivalence de x. On utilise également les notation $\bar{x}$ pour la classe d'équivalence de x.*

En choisissant un représentant de chaque classe d'équivalence on obtient un ensemble K des représentants des classes d'équivalence, on peut alors écrire

$$E = \cup_{x\in K}[x].$$

Définition 1.9.5. *Le quotient d'un ensemble E par une relation d'équivalence R est l'ensemble de classes d'équivalence de R. Il est noté par R/E. La projection canonique. $\pi : E \to E/R$ est l'applicaton. $x \mapsto [x]$.*

@

1.9.1. Classes à gauche et à droite. On fixe H un sous-groupe de G. On définit la relation ($x \sim y$ si $xH \cap yH \neq \emptyset$) sur G. On souhaite montrer que $\sim$ est une relation d'équivalence. La réflexivité et symétrie sont claires, par contre la transitivité n'est pas claire. Cela nécessite une partie de la structure de groupe : l'inversion.

LEMME 1.9.6. *Les trois assertions suivantes sont équivalentes.*

(1) $gH \cap g'H \neq \emptyset$.
(2) $g^{-1}g' \in H$.
(3) $gH = g'H$.

DÉMONSTRATION. (1 $\Rightarrow$ 2) Soit $x \in gH \cap g'H$. On a $x = gh_1$ et $x = g'h_1$, d'où $gh_1 = g'h_2$ et $g^{-1}g' = h_2h_1^{-1} \in H$.
(2 $\Rightarrow$ 3) : Soit $h = g^{-1}g' \in H$ d'où $g' = gh$ et

$$g'H = (gh)H = g(hH) = gH$$

car H est un sous-groupe et $h \in H$ (rappelez-vous que la translation à gauche par h est une bijection de H sur H). (3 $\Rightarrow$ 1) Celle-ci est évident. □

On peut maintenant montrer que $\sim$ est transitive : si $x \sim y$ et $y \sim z$ alors $xH = yH$ et $yH = zH$ d'où $xH = zH$ et $x \sim z$.

Les classes à gauche de H dans G sont par définition les classes d'équivalence de la cette relation d'équivalence. L'ensemble des classes est noté par G/H.

L'indice de H de G est par définition la cardinalité de G/H,

$$[G : H] :=\mid G/H \mid$$

NOTATION 1.9.7. *La classes (d'équivalence) à gauche de $g \in G$ est notée par $[g]$ ou gH ou $\bar{g}$.*

Soit K un ensemble des représentants des classes à gauche. On a une réunion en partie disjointes

$$G = \cup_{g \in K}[g].$$

Si $\mid G \mid < +\infty$, on a

$$\mid G \mid = \sum_{g \in K} \mid [g] \mid$$

On calcule $\mid [g] \mid$,

$$[g] = \{g' \in G \mid g' \sim g\} = \{g' \mid g^{-1}g' \in H\} = \{g' \mid g' \in gH\} = \{gh \mid h \in H\}$$

L'application $h \mapsto gh$ est une bijection (translation à gauche L_g restreinte à H est une bijection sur de H sur gH). On obtient donc

$$\mid [g] \mid =\mid gH \mid =\mid H \mid$$

d'où

$$\mid G \mid = \sum_{g \in K} \mid H \mid =\mid H \mid \times \mid K \mid =\mid H \mid \times [G : H]$$

et

$$[G : H] = \frac{\mid G \mid}{\mid H \mid} \tag{1.1}$$

Une conséquence

THEOREM 1.9.8. *(Théorème de Lagrange) Si H est sous-groupe de un groupe d'ordre fini G, alors $|H|$ divise $|G|$.*

COROLLAIRE 1.9.9. *Soit G un groupe d'ordre fini. Pour g,* $\mathrm{Ord}(g)$ *divise* $|\ G\ |$.

DÉMONSTRATION. Tout d'abord $\mathrm{Ord}(g)$ est fini sinon $k \mapsto g^k$ sera une bijection par la proposition 1.5.2 et donc G contient un ensemble infini $\{g^k \mid k \in \mathbb{Z}\}$. Cela contredit la finitude de G. Donc $\mathrm{Ord}(g) < \infty$ et $\langle g\rangle = \{g^k \mid k \in \mathbb{Z}\} = \{e, g, \cdots, g^{\mathrm{Ord}(g)-1}\}$. Comme $\langle g\rangle$ est un sous-groupe de G, par le théorème de Lagrange, $\mathrm{Ord}(\langle g\rangle) \mid |G|$. □

Une autre simple conséquence des calculs ci-dessus est,

COROLLAIRE 1.9.10. *Soient H et H' deux sous-groupes de G tel que $H \subset H'$. Alors*

$$[G : H] = [G : H'][H' : H].$$

DÉMONSTRATION. Comme $H \subset H'$, H est un sous-groupe de H', on peut donc écrire.

$$[G : H'][H' : H] = \frac{|G|}{|H'|}\frac{|H'|}{|H|} = \frac{|G|}{|H|}$$

□

PROPOSITION 1.9.11. *Soit $\phi : G \to H$ un morphisme surjectif de groupes. Pour tout sous-groupe $K \leq H$, on a*

$$[G, \phi^{-1}(K)] = [H : K].$$

DÉMONSTRATION. Par la proposition (1.7.10), $L := \phi^{-1}(K)$ est un sous-groupe de G. On considère l'application $\bar{\phi} : G/L \to H/K$ définie par $\bar{\phi}(gL) = \phi(g)K$. On vérifie que $\bar{\phi}$ est bien définie : Si $g_1L = g_2L$ alors $g_2^{-1}g_1 \in L = \phi^{-1}(K)$. Donc $\phi(g_2)^{-1}\phi(g_1) = \phi(g_2^{-1}g_1) \in K$ d'où $\phi(g_1)K = \phi(g_2)K$.

On montre que $\bar{\phi}$ est surjective : Soit $hK \in H/K$. Puisque ϕ est surjective, il existe $g \in G$ tel que $h = \phi(g)$. On a $\bar{\phi}(gL) = \phi(g)K = hK$ donc $hK \in \mathrm{Image}(\bar{\phi})$.

$\bar{\phi}$ est injective car : si $\bar{\phi}(g_1)L = \bar{\phi}(g_2)L$, alors $\phi(g_1)K = \phi(g_2)K$ et donc $\phi(g_2^{-1}g_1) = \phi(g_2)^{-1}\phi(g_1) \in K$ d'où $g_2^{-1}g_1 \in L = \phi^{-1}(K)$ et $g_1L = g_2L$.

□

1.10. Le groupe quotient G/H et les théorèmes structurels

Dans cette section on explique la structure du groupe sur les classes à gauches d'un sous-groupe distingué H dans G.

La structure du groupe. : On définit le produit de deux classes xH et yH par

$$xH.yH = xyH.$$

Tout d'abord on doit vérifier que le produit est bien défini, c'est-à-dire si le produit ci-dessus ne dépend pas du choix des représentants :

(1) Si $xH = x'H$ alors $x^{-1}x' \in H$. On a $xH.yH = xyH$, $x'H.yH = x'yH$ et

$$(xy)^{-1}(x'y) = y^{-1}x^{-1}x'y \in y^{-1}Hy = H,$$

et donc $x'yH = xyH$.

(2) $yH = y'H$, $y^{-1}y' \in H$. On a $xH.yH = xyH$, $xH.yH = xy'H$ et

$$(xy)^{-1}(xy') = y^{-1}x^{-1}xy' = y^{-1}y' \in H,$$

et donc $x'yH = xyH$.

Alors si $xH = x'H$ et $yH = y'H$, en utilisant (1) et (2) on a $xH.yH = x'H.yH = x'H.y'H$, et $xH.yH = x'H.y'H$ et donc le produit est bien défini.

L'associativité est claire :

$$(xH.yH).zH = xyH.zH = (xy)zH = x(yz)H = xH.zyH = xH.(yH.zH).$$

L'élément neutre est la classe d'élément neutre $[e] = eH = H$.

$$eH.xH = exH = xH = xeH = xH.eH$$

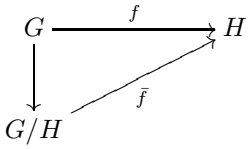
PROPOSITION 1.10.1. *La structure du groupe sur G/H introduite ci-dessus est l'unique structure de groupe faisant de la projection canonique $\pi : G \to G/H$ est un morphisme de groupes. De plus* $\ker(\pi) = H$.

DÉMONSTRATION. Soient α et $\beta \in G/H$. Puisque π est surjective, il existe $x, y \in G$ tel que $\pi(x) = xH = \alpha$ et $\pi(y) = yH = \beta$. Si π est un morphisme de groupes pour une certaine loi de composition $*$ sur G/H, on $\alpha * \beta = \pi(x) * \pi(y) = \pi(xy)$ d'où $xH * yH = xyH$ donc $*$ est précisément celle définie ci-dessus.

$\ker(\pi) = \{x \in G | xH = eH\} = \{x \in G | e^{-1}x \in H\} = \{x \in G | x \in H\}$ □

PROPOSITION 1.10.2. *Soient $f : G \to H$ un morphisme de groupes et $K \subset \ker(f)$ un sous-groupe distingué de G. Alors il existe un unique morphisme de groupes $\bar{f} : G/K \to H$ faisant le diagramme ci-dessous commutatif.*

(1.1)



Lorsque $K = \ker(f)$, l'application induite $\bar{f} : G/\ker(f) \to H$ est injective.

DÉMONSTRATION. L'application $\bar{f}$ est définie par $\bar{f}([x]) = f(x)$ o'où $[x] \in G/K$ est une classe à gauche. D'abord on vérifie que $\bar{f}$ est bien définie : Si $[x] = [y] \in G/K$, alors $y^{-1}x \in K \subset \ker(f)$, et donc $f(y)^{-1}f(x) = f(y^{-1})f(x) = f(y^{-1}x) = e_H$, d'où $f(y) = f(x)$ et $\bar{f}([x]) = \bar{f}([y])$.

$\bar{f}$ est un morphisme de groupes car,

$$\bar{f}([x].[y]) = \bar{f}([xy]) = f(xy) = f(x).f(y) = \bar{f}([x])\bar{f}([y]).$$

le diagramme est commutatif parce que $(\bar{f} \circ \pi)(x) = \bar{f}(\pi(x)) = \bar{f}([x]) = f(x)$ d'où

$$f = \bar{f} \circ \pi.$$

Pour montrer l'unicité, supposons que $g : G/K \to H$ soit un morphisme satisfaisant la condition $f = g \circ \pi$. Soit $[x] \in G/K$ une classe à gauche avec $x \in G$ comme représentant, donc $[x] = \pi(x)$. On a $g([x]) = g(\pi(x)) = (g \circ \pi)(x) = f(x) = \bar{f}([x])$ d'où $g = \bar{f}$ et l'unicité de $\bar{f}$.

Maintenant on suppose que $K = \ker(f)$. Soit $[x] \in \ker(\bar{f})$. On a $e_H = \bar{f}([x]) = f(x)$. Donc $x \in \ker(f)$ et la classe à gauche $[x] \in G/\ker(f)$ est triviale. On conclut que $\ker(\bar{f}) = \{e_{G/Ker(f)}\}$ et $\bar{f}$ est injective. □

DÉFINITION 1.10.3. *L'ensemble des classes à gauche G/H muni de la loi de composition ci-dessus est appelé le groupe quotient.*

THEOREM 1.10.4. *(Le premier théorème d'isomorphisme). Soit $f : G \to H$ un morphisme de groupes. Alors l'application induite $\bar{f} : G/\ker(f) \to \text{Image}(f)$ est un isomorphisme.*

DÉMONSTRATION. Par la proposition 1.10.2 $\bar{f}$ est un morphisme injectif. Pour montrer la surjectivité, supposons que $y \in \text{Image}(f)$. Alors il existe $x \in G$ tel que. $y = f(x)$, d'où $y = f(x) = \bar{f}([x])$ et la surjectivité de $\bar{f}$.

□

Par la suite on identifie les sous-groupes du groupe quotient.

THEOREM 1.10.5. *Il y a une bijection entre les sous-groupes de G/H et les sous-groupes de G contenants H.*

DÉMONSTRATION. On pose $A := \{K \leq G \mid H \subset K\}$ et soit B l'ensemble des sous-groupes de G/H. On donne une bijection entre A et B.

Soit $\pi : G \to G/H$ la projection canonique, la bijection souhaitée $\psi : A \to B$ est donnée par $\psi(K) := \pi(K)$ et son inverse est $\Psi'(L) := \pi^{-1}(L)$ pour tout sous-groupe L de G/H.

Par la proposition 1.7.10 (1), l'image par π d'un sous-groupe de G est un sous-groupe de G/H, donc ψ est bien une application de A dans B.

D'autre part, pour un sous-groupe $L \in B$ de G/H, $H = \pi^{-1}\{e\} \subset \pi^{-1}(L)$, car $e_{G/H} \in L$. Donc $\Psi'(L) \in A$ et Ψ' est une application de B dans A, Il reste à montrer que $\Psi \circ \Psi' = id_B$ et $\Psi' \circ \Psi = id_A$.

On fixe $K \in A$, on a $\Psi'(\Psi(A)) = \pi^{-1}(\pi(K))$. On rappelle que $K \subset \pi^{-1}(\pi(K))$, il faut donc montrer que $\pi^{-1}(\pi(K)) \subset K$. Soit $x \in \pi^{-1}(\pi(K))$. Donc $\pi(x) \in \pi(K)$ et il existe $y \in K$ tel que $\pi(x) = \pi(y) \in G/H$ i.e. $[x] = [y]$ d'où $y^{-1}x \in K \subset H$. On a donc $y^{-1}x \in K$ et puisque K est un sous-groupe et $y \in K$, on conclut que $x \in K$. On vient de monter que $\pi^{-1}(\pi(K)) \subset K$ d'où $K = \pi^{-1}(\pi(K)) = \Psi'(\Psi(K))$ et $\Psi' \circ \Psi = id_A$.

Maintenant on fixe $L \in B$. On a $\Psi(\Psi'(L)) = \pi(\pi^{-1}(L)) = L$ car π est surjectif. On a donc montré que $\Psi \circ \Psi' = id_B$

□

THEOREM 1.10.6. *(Deuxième théorème d'isomorphisme) Soient H, K deux sous-groupes de G o'où K est distingué dans G. Alors il existe un isomorphisme de groupes*

$$\frac{HK}{K} \simeq \frac{H}{K \cap H}$$

DÉMONSTRATION. Puisque K est distingué dans G, K et $H \cap K$ sont respectivement distingués HK et H.

L'isomorphisme $f : \frac{H}{H \cap K} \to \frac{HK}{K}$ est donné par $f(x(H \cap K)) = xK$ o'où $x \in H \subset HK$, autrement dit l'image de la classe à gauche dans $H/K \cap H$ représentée par x est la classe dans HK/K toujours représentée par $x \in H \subset HK$.

f est un morphisme est assez clair : $f([x][y]) = f([xy]) = [xy] = [x][y]$

f est surjectif car pour tout $x = hk \in HK$,

$$xK = hkK = hK = f(h(H \cap K)).$$

Montrons l'injectivité : si $f(x(H \cap K)) = xK = eK$, alors $x \in H \cap K$.

□

THEOREM 1.10.7. *(Troisième théorème d'isomorphisme) Soient H et K deux sous-groupes distingués de G, tels que $K \subset H$. Alors il existe un isomorphisme de groupes*

$$\frac{G/K}{H/K} \simeq \frac{G}{H} \tag{1.2}$$

DÉMONSTRATION. On considère l'application $\phi : G/K \to G/H$ donnée par $\phi(gK) = gH$. D'abord on vérifie qu'elle est bien définie : Si $g_1K = g_2K$ alors $g_2^{-1}g_1 \in K$, puisque $K \subset H$ on a donc $g_2^{-1}g_1 \in H$ et $g_1H = g_2H$ d'où $\psi(g_1K) = \psi(g_2K)$.

La surjectivité est assez claire car pour $g \in G$, $gH = f(gK)$.

Identifions le noyau : $gH = f(gK) = eH$ si et seulement si $g \in H$. C'est-à-dire que

$$\ker(\phi) = \{hK | h \in H\} = H/K = \pi(H),$$

o'où $\pi : G \to G/K$ est la projection canonique. Donc par le premier théorème d'isomorphisme ϕ induit un isomorphisme $\bar{\phi} : (G/K)/(H/K) \to G/H$

□

THEOREM 1.10.8. *Soit H, K deux sous-groupes distingués de G tels que $H \cap K = \{e\}$ et $HK = G$. Alors il existe un isomorphisme de groupes $G \simeq H \times K$.*

DÉMONSTRATION. D'abord on montre que pour tout $h \in H$ et $k \in K$,

$$hk = kh.$$

Pour ce faire on montre que $hkh^{-1}k^{-1} \in H \cap K = \{e\}$. Puisque. H est distingué $kh^{-1}k^{-1} \in H$ et donc $h.kh^{-1}k^{-1} \in H$. De la mà^{a}me manière, $hkh^{-1} \in K$ parce que K est distingué, et donc $hkh^{-1}.k \in H$. d'où $hkh^{-1}k^{-1} \in H \cap K = \{e\}$, et

$$hkh^{-1}k^{-1} = e \Longrightarrow hk = kh.$$

On définit l'application $f : H \times K \to G$ par

$$f(h, k) = hk.$$

f est un morphisme parce que

$$f((h_1, k_1)(h_2, k_2)) = f(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_2h_2k_2 = f(h_1, k_1)f(h_2, k_2)$$

Ci-dessus on a utilisé $h_2k_1 = k_1h_2$.
f est injectif : si $f(h, k) = hk = e$ alors $h = k^{-1}$ et $h \in H \cap K = \{e\}$ d'où $k = e$ et (h, k) est l'élément neutre.

Enfin f est surjectif car $\text{Image}(f) = HK = G$ par l'hypothèse. □

1.11. Groupes cycliques

On rappelle qu'un groupe cyclique est un groupe G engendré par un seul élément $g \in G$, i.e

$$G = \langle g \rangle.$$

PROPOSITION 1.11.1. *On suppose que $G = \langle g \rangle$ est un groupe cyclique. Alors soit $G \simeq \mathbb{Z}$ ou $G \simeq \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ o'ù $n = \text{Ord}(g) < +\infty$.*

DÉMONSTRATION. Soit $n = \text{Ord}(g)$. On définit $\phi : \mathbb{Z} \to G$ par $\phi(n) = g^n$. Comme $G = \langle g \rangle$, alors ϕ est surjectif.

Si $n = +\infty$, alors par la proposition 1.5.2 (3) ϕ est injectif et donc ϕ est un isomorphisme. Si $n < +\infty$ alors par la proposition 1.5.2 (2), $\ker(\phi) = \langle n \rangle$, et donc par le premier théorème d'isomorphisme 1.10, $\mathbb{Z}/n\mathbb{Z} \simeq G$. □

PROPOSITION 1.11.2. *Si $(m, n) = 1$, alors on a un isomorphisme de groupes*

$$\mathbb{Z}_{mn} \simeq \mathbb{Z}_n \times \mathbb{Z}_m.$$

DÉMONSTRATION. On considère l'application $f : \mathbb{Z} \to \mathbb{Z}/\mathbb{Z}_n \times \mathbb{Z}/\mathbb{Z}_m$,

$$f(x) = ([x], [x]) = (x + n\mathbb{Z}, x + m\mathbb{Z}) \in \mathbb{Z}/\mathbb{Z}_n \times \mathbb{Z}/\mathbb{Z}_m.$$

f est un morphisme de groupes car par la proposition 1.10.1 ses composantes $x \mapsto x + n\mathbb{Z}$ et $x \mapsto x + m\mathbb{Z}$ sont des morphismes de groupes.

- f **est surjectif** : Puisque. $(m, n) = 1$, il existe r, s tels que $rm + sn = 1$. Soient $p, q \in \mathbb{Z}$, on a

$$rmp + snp = p, \text{ d'où } \boxed{rmp \equiv p \mod (n)} \tag{1.1}$$

$$rmqd + snq = q, \text{ d'où } \boxed{snq \equiv q \mod (m)} \tag{1.2}$$

On a,

$$\begin{aligned}\phi(rmp + snq) &= (rmp + snq + n\mathbb{Z}, rmp + snq + m\mathbb{Z}) = (rmp + n\mathbb{Z}, snq + m\mathbb{Z}) \\ &= (p + n\mathbb{Z}, q + m\mathbb{Z}) = ([p], [q]) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}\end{aligned}$$

et f est surjectif.

- $\ker(f)$: Si $f(x) = ([x], [x]) = ([0], [0]) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, on a alors $x \in n\mathbb{Z}$ et $x \in m\mathbb{Z}$, i.e. $n|x$ et $m|x$ d'où $mn|x$ parce que $(m, n) = 1$. Donc $\ker(f) \subset mn\mathbb{Z}$. Réciproquement si $x \in mn\mathbb{Z}$, alors $x \in n\mathbb{Z}$ et $x \in m\mathbb{Z}$, et puis $x + n\mathbb{Z} = 0 + n\mathbb{Z}$ et $x + m\mathbb{Z} = 0 + m\mathbb{Z}$,

$$f(x) = ([0], [0]) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

on conclut que $\ker f = mn\mathbb{Z}$ et par le premier théorème d'isomorphisme, f induit un isomorphisme $\bar{f} : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

□

PROPOSITION 1.11.3. *L'application diagonale $f : \mathbb{Z} \to \mathbb{Z}/\mathbb{Z}_n \times \mathbb{Z}/\mathbb{Z}_m$ induit un morphisme injectif $\bar{f} : (\mathbb{Z}/nm\mathbb{Z})^* \to (\mathbb{Z}/\mathbb{Z}_n)^* \times (\mathbb{Z}/\mathbb{Z}_m)^*$.*

On doit d'abord montrer que l'application $\bar{f}$ est bien définie Soit $\bar{x} \in (\mathbb{Z}/nm\mathbb{Z})^*$. On a $(x, mn) = 1$ d'où $(x, n) = (x, m) = 1$ et donc $(\bar{x}, \bar{x}) \in (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$.

$\bar{f}$ est un morphisme est assez clair :

$$\bar{f}(\bar{x}\bar{y}) = \bar{f}(\overline{xy}) = (\overline{xy}, \overline{xy}) = (\bar{x}\bar{y}, \bar{x}\bar{y}) = (\bar{x}, \bar{x})(\bar{y}, \bar{y}) = \bar{f}(\bar{x})\bar{f}(\bar{x}).$$

injectivité si $\bar{f}(x) = (\bar{x}, \bar{x}) = (\bar{1}, \bar{1}) \in (\mathbb{Z}/\mathbb{Z}_n)^* \times (\mathbb{Z}/\mathbb{Z}_m)^*$, alors $n|x - 1$ et $m|x - 1$. Puisque $(m, n) = 1$, on obtient $mn|x - 1$ d'où $\bar{x} = \bar{1} \in (\mathbb{Z}/nm\mathbb{Z})^*$. Donc $\bar{f}$ est injective.

PROPOSITION 1.11.4. *Soit G un groupe. Pour tout $g \in G$ d'ordre fini,*

$$\mathrm{Ord}(g^k) = \frac{\mathrm{Ord}(g)}{pgcd(k, \mathrm{Ord}(g))}$$

.

DÉMONSTRATION. On pose $n = \mathrm{Ord}(g)$ et $d = pgcd(k, \mathrm{Ord}(g))$, donc $d|k$ et $d|n$ et

$$(\frac{k}{d}, \frac{n}{d}) = 1.$$

On a $(g^k)^{n/d} = g^{n\frac{k}{d}} = (g^n)^{\frac{k}{d}} = e^{\frac{k}{d}} = e$ car $\frac{k}{d}$ est un entier.

Si pour un entier l,

$$(g^k)^l = e,$$

par la proposition 1.5.2 (2), $n|kl$, d'où

$$\frac{n}{d} \mid \frac{k}{d}l.$$

Puisque $(\frac{k}{d}, \frac{n}{d}) = 1$ on obtient $\frac{n}{d}|l$. On conclut donc $\mathrm{Ord}(g^k) = \frac{n}{d}$. □

COROLLAIRE 1.11.5. *$\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ est un générateur si et seulement $(k, n) = 1$.*

DÉMONSTRATION. Par proposition 1.11.4, $n = \mathrm{Ord}(\bar{k}) = \frac{n}{pgcd(n,k)}$ si et seulement si $pgcd(n, k) = 1$. □

DÉFINITION 1.11.6. *Fonction d'Euler (ou ϕ d'Euler ou indicatrice d'Euler) Pour $n \in \mathbb{N}^*$, on définit*

$$\phi(n) := \#\{k | 1 \leq k \leq n \quad \& \quad (k, n) = 1\} = \mathrm{Ord}((\mathbb{Z}/n\mathbb{Z})^*)$$

LEMME 1.11.7. *(1) Soient G_1 et G_2 deux groupes et $g_1 \in G_1$ et $g_2 \in G_2$ deux éléments d'ordre fini. Alors, pour $(g_1, g_2) \in G_1 \times G_2$,*

$$\mathrm{Ord}((g_1, g_2)) = ppcm(\mathrm{Ord}(g_1), \mathrm{Ord}(g_2)).$$

(2) On suppose que $(m, n) = 1$. Alors $(\bar{a}, \bar{b}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z}$ est un générateur si et seulement si $\bar{a} \in Z/n\mathbb{Z}$ et $\bar{b} \in \mathbb{Z}/m\mathbb{Z}$ sont deux générateurs.

DÉMONSTRATION. (1) On pose $k = ppcm((\mathrm{Ord}(g_1), \mathrm{Ord}(g_2))$, donc $\mathrm{Ord}(g_1)|k$ et $\mathrm{Ord}(g_2)|k$ d'où $g_1^k = e_{G_1}$ et $g_2^k = e_{G_2}$. On a $(g_1, g_2)^k = (g_1^k, g_2^k) = (e_{G_1}, e_{G_2}) \in G_1 \times G_2$.

D'autre part si pour un entier l, $(g_1, g_2)^l = (e_{G_1}, e_{G_2})$, on a $g_1^l = e_{G_1}$ et $g_2^l = e_{G_2}$ d'où $\mathrm{Ord}(g_1) \mid l$ et $\mathrm{Ord}(g_2) \mid l$, et donc $k \mid l$. Cela montre que $k = \mathrm{Ord}((g_1, g_2))$

(2) Puisque $(m, n) = 1$, $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/mn$, donc $(\bar{a}, \bar{b})$ est un générateur si et seulement $\mathrm{Ord}(\bar{a}, \bar{b}) = mn$, on a

$$mn = \mathrm{Ord}(\bar{a}, \bar{b}) \overset{Lem 1.11.7}{=} ppcm(\mathrm{Ord}(\bar{a}), \mathrm{Ord}(\bar{b})) = \frac{\mathrm{Ord}(\bar{a})\,\mathrm{Ord}(\bar{b})}{pgcd(\mathrm{Ord}(\bar{a}), \mathrm{Ord}(\bar{b}))}.$$

D'autre part $\mathrm{Ord}(\bar{a}) \mid n$ et $\mathrm{Ord}(\bar{b}) \mid m$ donc $\frac{\mathrm{Ord}(\bar{a})\,\mathrm{Ord}(\bar{b})}{pgcd(\mathrm{Ord}(\bar{a}), \mathrm{Ord}(\bar{b}))} \leq mn$. Donc $\mathrm{Ord}(\bar{a}, \bar{b}) = mn$ si et seulement si $\mathrm{Ord}(\bar{a}) = n$ et $\mathrm{Ord}(\bar{b}) = m$.

□

PROPOSITION 1.11.8. *(1) Un groupe cyclique d'ordre n a précisément $\phi(n)$ générateurs.*

(2) $\phi(p^k) = p^{k-1}(p - 1)$

(3) Si $(m, n) = 1$, alors $\phi(mn) = \phi(m)\phi(n)$.

(4) Si $(m, n) = 1$, alors l'application $\bar{f}$ de la proposition 1.11.3 est un isomorphisme de groupes.

(5) Pour tous nombres premiers distincts $p_1, \cdots p_k$,

$$\phi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \prod_{i=1}^{k} p_i^{\alpha_i}(p_i - 1)$$

DÉMONSTRATION. (1) Ceci suit du corollaire 1.11.5.

(2) Puisque p est un premier, les diviseurs de p^k sont de la forme p^l. On a $\phi(p^k) = \#\{1 \leq x \leq p^k \mid (x, p^k) = 1\} = p^k - \#\{1 \leq x \leq p^k \mid (x, p^k) \neq 1\}$ et $(x, p^k) \neq 1$ si et seulement si $p \mid x$. Il faut donc compter le nombre des x entre 1 et p^k qui sont de la forme py :

$$1 \leq py \leq p^k. \iff 1 \leq y \leq p^{k-1}$$

cela montre que $\phi(p^k) = p^k - p^{k-1}$.

(3) Par (1), $\phi(mn)$ est le nombre des générateurs de $\mathbb{Z}/mn\mathbb{Z}$ qui est isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ si $(m,n) = 1$. Par le lemme 1.11.7, le nombre des générateurs de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est égale au produit des nombres des générateurs de $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$, i.e. $\phi(m)\phi(n)$.

(4) Le morphisme $\bar{f}$ est injectif par la proposition 1.11.3, puisque la source et l'arrivée ont la màªme cardinalité $\phi(mn) = \phi(m)\phi(n)$, $\bar{f}$ est surjectif et donc bijectif.

(5) On a $(p_1^{\alpha_1}, p_2^{\alpha_2} \cdots p^{\alpha_k}) = 1$, donc par (3)

$$\phi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})\phi(p_3^{\alpha_3} \cdots p_k^{\alpha_k}) = \cdots =$$
$$\phi(p_1^{\alpha_1}) \cdots \phi(p_k^{\alpha_k}) = \prod p_i^{\alpha_i - 1}(p_i - 1)$$

□

Proposition 1.11.9. *Soit $G = \langle g \rangle$ un groupe cyclique d'ordre fini $n := \mathrm{Ord}(G) < +\infty$.*

(1) Pour tout diviseur d de n, G possède précisément un unique sous-groupe d'indice d.

(2) Pour tout diviseur d de n, il y a exactement $\phi(d)$ éléments d'ordre d.

(3) $n = \sum_{d|n} \phi(d)$.

Démonstration. (1) On considère l'application $f : \mathbb{Z} \to G$ donnée par $f(n) = g^n$. Soit H un sous-groupe de G. On pose $H' = f^{-1}(H)$. Tout sous-groupe de $\mathbb{Z}$ est de la forme $d\mathbb{Z}$, donc il existe d tel que $H' = d\mathbb{Z}$. Par la proposition 1.9.11 $[\mathbb{Z}, f^{-1}(H)] = [G, H]$ d'où $d = [\mathbb{Z}, d\mathbb{Z})] = [G, H]$. Donc l'indice de H détermine d et donc $H' = d\mathbb{Z}$. Puisque f est surjectif, $H = f(f^{-1}(H)) = f(H')$. On conclut que l'indice de H détermine H et donc H est unique.

(2) Pour $x \in G$ d'ordre d, le sous groupe $\langle x \rangle$ est d'indice $n/d = [G, \langle x \rangle]$. Par (1), il existe un seul sous-groupe d'indice n/d, donc tous les éléments d'ordre d engendrent le màªme sous-groupe autrement dit, si $\mathrm{Ord}(x) = \mathrm{Ord}(y)$, $\langle x \rangle = \langle y \rangle$. Donc si on fixe un élément x d'ordre d, tous les éléments d'ordre d de G sont les générateurs de $\langle x \rangle$ et par la proposition 1.11.8 $\langle x \rangle$ a précisément $\phi(d)$ générateurs.

(3) On peut considérer la réunion disjointes

$$G = \cup_{d|n} \{x \in G | \, \mathrm{Ord}(x) = d\}$$

et donc $n = \mathrm{Ord}(G) = \sum_{d|n} \#\{x \in G | \, \mathrm{Ord}(x) = d\} = \sum_{d|n} \phi(d)$

□

Définition 1.11.10. *Soit G un groupe. On dit que $x \in G$ est de période k si $x^k = e$.*

Proposition 1.11.11. *Soit G un groupe fini tel que pour tout $p \in \mathbb{N}$ le nombre des éléments de période p est inférieur à p, alors G est cyclique.*

Démonstration. Pour x un élément d'ordre d, le sous-groupe $\langle x \rangle = \{e, x, \cdots, x^{d-1}\}$ contient d éléments (distincts) de période d, donc il contient tout les éléments de période d , y compris tout les éléments d'ordre d. On remarque qu'un élément d'ordre d dans $\langle x \rangle$ est forcement un générateur de $\langle x \rangle$ et par la proposition 1.11.9 (1), $\langle x \rangle$ précisément $\phi(d)$ générateurs. Donc, s'il existe un élément d'ordre d dans G, alors il existe précisément $\phi(d)$ éléments d'ordre d. On considère la réunion disjointe,

$$G = \cup_{d|n} \{x \in G | \, \mathrm{Ord}(x) = d\}$$

qui donne

$$n = \mathrm{Ord}(G) = \sum_{d|n} \#\{x \in G | \mathrm{Ord}(x) = d\} \leq \sum_{d|n} \phi(d) = n.$$

d'où on conclut que G a précisément $\phi(d)$ éléments d'ordre d, pour tout diviseur d de n. En particulier G, $\phi(n) \geq 1$ élément d'ordre $n = \mathrm{Ord}(G)$. Pour un tel élément $\langle x \rangle = G$ et G est cyclique. □

1.12. Action de groupes

Définition 1.12.1. *Soient G un groupe et E un ensemble. Une action de G sur E est une application $\alpha : G \times E \to E$ satisfaisant les conditions suivantes :*

(1) $\alpha(e, x) = x$

(2) $\alpha(gh, x) = \alpha(g, \alpha(h, x))$.

Autrement dit, α associe à chaque élément $g \in G$ une application $\alpha_g : E \to E$ donnée par $\alpha_g(x) := \alpha(g, x)$. Il s'avère que α_g est une bijection ; on a

$$(\alpha_{g^{-1}} \circ \alpha_g)(x) = \alpha_{g^{-1}}(\alpha(g, x)) = \alpha(g^{-1}, \alpha(g, x)) = \alpha(g^{-1}g, x) = \alpha(e, x) = x,$$

d'où $\alpha_{g^{-1}} \circ \alpha_g = id_E$. De même, $\alpha_g \circ \alpha_{g^{-1}} = id_E$. Donc , pour tout $g \in G$, α_g est une bijection de E sur E.

Pour un ensemble E, on note par $\mathrm{Per}(E)$ l'ensembles des permutations de E,i.e.

$$\mathrm{Per}(E) := \{f : E \to E | \quad f \text{ est bijective}\}$$

Proposition 1.12.2. *Soient G un groupe et E un ensemble. Il y a une bijection entre les actions de G sur E et les homomorphismes de G dans* $\mathrm{Per}(E)$.

Démonstration. A une action $\alpha : G \times E \to E$ on associe le morphisme $\phi_\alpha : G \to \mathrm{Per}(E)$ donné par $\phi_\alpha(g) = \alpha_g$. Vérifions que ϕ est un morphisme : pour $x \in E$ et $g_i \in G$,

$$(\phi_\alpha(g_1) \circ \phi_\alpha(g_2))(x) = \phi_\alpha(g_1)(\phi_\alpha(g_2)(x)) = \alpha_{g_1}(\alpha_{g_2}(x)) =$$
$$\alpha(g_1, \alpha(g_2, x)) = \alpha(g_1 g_2, x) = \alpha_{g_1 g_2}(x) = \phi_\alpha(g_1 g_2)(x),$$

d'où $\phi_\alpha(g_1 g_2) = \phi_\alpha(g_1) \circ \phi_\alpha(g_2)$.

On construit l'application réciproque : Soit $\phi : G \to \mathrm{Per}(E)$ un morphisme. On définit l'action $\alpha_\phi : G \times E \to E$ par

$$\alpha(g, x) := \phi(g)(x).$$

Il faut montrer que l'une est l'inverse de l'autre

$\alpha_{\phi_\alpha}(g, x) = \phi_\alpha(g)(x) = \alpha_g(x) = \alpha(g, x)$,

d'où $\alpha_{\phi_\alpha} = \alpha$. Réciproquement,

$\phi_{\alpha_\phi}(g)(x) = (\alpha_\phi)_g(x) = \alpha_\phi(g, x) = \phi(g)(x)$ d'où $\phi_{\alpha_\phi}(g) = \phi(g)$ pour tout $g \in G$, i.e.

$$\phi = \phi_{\alpha_\phi}.$$

□

Définition 1.12.3. *Pour une action α, on définit le noyau*

$$\ker(\alpha) := \ker(\phi_\alpha) = \{g \in | \phi_\alpha(g) = \alpha_g = id_E\} = \{g \in G | \forall x \in E, \quad \alpha(g, x) = x\}.$$

Proposition 1.12.4. $\ker(\alpha)$ *est un sous-groupe distingué de G.*

Démonstration. ϕ_α est un morphisme de groupes donc $\ker(\alpha) = \ker(\phi_\alpha)$ est un sous-groupe distingué. □

Définition 1.12.5. *On dit que α est fidèle si* $\ker(\alpha) = \{e\}$. *Autrement dit, si pour tout x , $\alpha(g, x) = x$ alors $g = e$.*

Notation 1.12.6. *Pour simplifier l'écriture, on utilise $g.x$ à la place de $\alpha(g, x)$.*

Définition 1.12.7. *L'orbite d'un élément $x \in E$ est*

$$\mathrm{Orb}(x) := \{g.x| \quad g \in G\}.$$

Le stabilisateur de x est par définition

$$G_x := \{g \in G | g.x = x\}.$$

Par la définition de $\ker(\alpha)$ c'est clair que :

Proposition 1.12.8.

$$\ker(\alpha) = \cap_{x \in E} G_x$$

Proposition 1.12.9. *G_x est un sous-groupe de G.*

Démonstration. Tout d'abord $e \in G_x$ donc $G_x \neq \emptyset$. Supposons $g, h \in G_x$. On a $h.x = x$, d'où $h^{-1}(h.x) = (h^{-1}h).x = x$ et

$$(gh^{-1}).x = g.(h^{-1}.x) = g.x = x.$$

On a donc $gh^{-1} \in G_x$. □

Proposition 1.12.10. *Pour tout $g \in G$,*

$$gG_xg^{-1} = G_{gx}.$$

Démonstration. Soit $h \in G_x$, on a

$$(ghg^{-1})(gx) = gh.x = g.(h.x) = g.x.$$

On conclut que $ghg^{-1} \in G_{g.x}$.

□

Exemple 1.12.11. *Le cercle $S^1 = \{z \in \mathbb{C} || z| = 1\} = \{e^{i\theta} | \theta \in \mathbb{R}\}$ agit sur $\mathbb{C}$ par multiplication : $\alpha(z, x) = zx$. On peut aisément identifier les orbites et les stabilisateurs de $x \neq 0$.*

$$\mathrm{Orb}(x) = \{zx \mid |z| = 1\},$$

On a $|zx| = |z|.|x| = 1.|x| = |x|$. Réciproquement si $|y| = |x|$, alors $|y/x| = 1$, et $y = (y/x).x$, donc $y \in \mathrm{Orb}(x)$. On conclut $\mathrm{Orb}(x) = \{y \mid |y| = |x|\}$. *Quant au stabilisateur, de l'équation $zx = x$ on conclut que $z = 1$ car on avait supposé que $x \neq 0$. Donc le stabilisateur est le sous-groupe trivial $\{1\}$. Pour $x = 0$, on a* $\mathrm{Orb}(0) = \{0\}$ *et le stabilisateur est le groupe entier S^1.*

Définition 1.12.12. *Soit $F \subset E$ une partie. On dit que F est stable sous l'action de G si pour tout $g \in G$, $gF \subset F$.*

En fait si F est stable, on a $gF = F$ pour tout g. La raison est que $F = gg^{-1}F = g(g^{-1}F) \subset gF$. On a donc $gF = F$.

Définition 1.12.13. *On dit que x est un point fixe de $g \in G$ si $gx = x$ et on note par* $\mathrm{Fix}(g)$ *l'ensemble de points fixes de g. On dit que $x \in E$ est un point fixe de G, si l'ensemble $\{x\}$ est stable, autrement dit pour tout g, $gx = x$. C'est équivalent à dire que* $\mathrm{Orb}(x) = \{x\}$.

La situation opposée à l'existence d'un point fixe est

Définition 1.12.14. *On dit que l'action de G sur E est libre si pour tout x , $G_x = \{e\}$.*

Proposition 1.12.15. *Une action libre est fidèle*

DÉMONSTRATION. On a $G_x = \{e\}$, pour tout x, donc $\ker(\alpha) = \cap_x G_x = \{e\}$. □

On a vu qu'avoir une action α est équivalent à avoir un morphisme de groupes $\phi_\alpha : G \to \mathrm{Per}(E)$. D'autre part on peut (pré)composer par un morphisme avec un autre morphisme de groupes $f : H \to G$ et obtenir un nouveau morphisme $\phi_\alpha \circ f : H \to \mathrm{Per}(E)$ et donc une action de H sur E.

PROPOSITION 1.12.16. *Soit $\alpha : G \times E \to E$ une action. Un morphisme de groupes $f : H \to G$ induit (naturellement) une action de H de sur G dont le morphisme de groupe $H \to \mathrm{Per}(E)$ est $\phi_\alpha \circ f$.*

DÉMONSTRATION. On définit l'action $\alpha_f : H \times E \to E$ par

$$\alpha_f(h, x) = \alpha(f(h), x) :$$

Vérifions les conditions :

(1) $\alpha_f(e_H, x) = \alpha(f(e_H), x) = \alpha(e_G, x) = x$
(2) $\alpha_f(hh', x) = \alpha(f(hh'), x) = \alpha(f(h)f(h'), x) = \alpha(f(h), \alpha(f(h'), x)) = \alpha_f(h, \alpha_f(h', x))$.

Identifions le morphisme ϕ_{α_f} comme expliqué dans la proposition 1.12.2 : Pour $x \in E$

$$\phi_{\alpha_f}(h)(x) = \alpha_f(h, x)) = \alpha(f(h), x) = \phi_\alpha(f(h))(x) = (\phi_\alpha \circ f)(h)(x),$$

d'où $\phi_{\alpha_f} = \phi_\alpha \circ f$. □

EXEMPLE 1.12.17. *Soit G un groupe. G agit sur G par translation à gauche : Pour $g, x \in G$*

$$\alpha(g, x) = gx$$

Cette action est fidèle et libre. Donc le morphisme induit $G \to \mathrm{Per}(G)$ est injectif.

Donc on vient de démontrer :

PROPOSITION 1.12.18. *Tout groupe fini G est isomorphe à un sous-groupe du groupe symétrique S_n o'ù $n = \mathrm{Ord}(G)$.*

DÉFINITION 1.12.19. *L'action de G sur E est dite transitive si $\mathrm{Orb}(x) = E$ pour tout $x \in E$.*

L'exemple 1.12.17 est une action transitive.

PROPOSITION 1.12.20. *Soient $x, y \in E$. Les conditions suivantes sont équivalentes.*

(1) $y \in \mathrm{Orb}(x)$
(2) $\mathrm{Orb}(x) \cap \mathrm{Orb}(y) \neq \emptyset$
(3) $\mathrm{Orb}(x) = \mathrm{Orb}(y)$

DÉMONSTRATION. $(1 \Rightarrow 2)$ est évident car pour y , $y \in \mathrm{Orb}(y)$. Donc si $y \in \mathrm{Orb}(x)$ alors, $y \in \mathrm{Orb}(x) \cap \mathrm{Orb}(y)$.
$(2 \Rightarrow 3)$: Soit $z \in \mathrm{Orb}(x) \cap \mathrm{Orb}(y)$, on a $z = g_1.x = g_2.y$ d'où $x = g_1^{-1}g_2.y$ et $y = g_2^{-1}g_1.x$

Tout élément w de l'orbite de x est de la forme $w = g.x = g(g_1^{-1}g_2.y) = (gg_1^{-1}g_2).y \in \mathrm{Orb}(y)$, donc $\mathrm{Orb}(x) \subset \mathrm{Orb}(y)$. Similairement, $\mathrm{Orb}(y) \subset \mathrm{Orb}(x)$ et donc $\mathrm{Orb}(y) = \mathrm{Orb}(x)$. $(3 \Rightarrow 1)$ C'est évident car $y \in \mathrm{Orb}(y) = \mathrm{Orb}(x)$.

□

Une relation d'équivalence :
Il est clair que

$$x \sim y \Leftrightarrow \mathrm{Orb}(x) = \mathrm{Orb}(y)$$

définit une relation d'équivalence. Par la proposition 1.12.20 la classe d'équivalence de $x \in E$ est

$$[x] = \mathrm{Orb}(x).$$

NOTATION 1.12.21. *On note par E/G l'ensemble des orbites. Si $I = \{x_1, \cdots\}$ désigne l'ensemble des représentants des classes d'équivalence, alors $|I| = |E/G|$.*

EXEMPLE 1.12.22. *Soit H est un sous-groupe de G. Il existe une action naturelle de H sur G donnée par,*

$$\alpha(h, g) = gh^{-1}.$$

Le stabilisateur est trivial, i.e. $G_g = \{e\}$, donc l'action est fidèle et libre.

Identifions les orbites et classes d'équivalence : Si $x \sim y$ alors il existe $h \in H$ tel que $xh^{-1} = y$, autrement dit $x = yh$ ce qui veut que dire les classes à gauche sont égales ,i.e. $xH = yH$.

On conclut donc qu'il y a une bijection entre les orbites (donc les classes d'équivalence) et les classes à gauches de H.

EXEMPLE 1.12.23. *G agit sur G par conjugaison : $\alpha : G \times G \to G$:*

$$\alpha(g, h) = ghg^{-1}$$

$g, h \in G$.

Le stabilisateur $G_x = \{g \mid gxg^{-1} = x\} = \{g \mid gx = xg\}$ est noté $C_x(G)$. On appelle $C_x(G)$ le centralisateur de x dans G. Le noyau $\ker(\alpha) = \cap G_x = \cap C_x(G) = Z(G)$. Donc l'action est fidèle si le centre de G est trivial.

EXEMPLE 1.12.24. *Comme on a vu dans l'exemple précédent, G agit sur G par conjugaison. Cette action induit une action de G sur l'ensemble des sous-groupes de G : $(g, H) \mapsto gHg^{-1}$. On peut voir aisément que les points fixes de cette action sont les sous-groupes distingués.*

Essayons d'identifier le stabilisateur d'un sous-groupe H :

$$G_H := \{g \in G \mid gHg^{-1} = H\}$$

On utilise la notation $N_G(H)$ pour le stabilisateur de H qui est appelé le normalisateur de H, pour la raison suivante :

PROPOSITION 1.12.25. *Pour $H \leq G$, on pose $N_G(H) := \{g \in G \mid gHg^{-1} = H\}$*

(1) $N_G(H)$ est un sous-groupe de G et $H \leq N_G(H)$.
(2) $H \trianglelefteq N_G(H)$.
(3) $N_G(H)$ est le plus grand sous-groupe de G contant H comme un sous-groupe distingué.

DÉMONSTRATION. (1) Par la propositionè 1.12.9 un stabilisateur est un sous-groupe. Pour $g \in H$, $gHg^{-1} \subset H$ cart H est sous-groupe, donc $H \subset N_G(H)$.

(2) Pour $g \in N_G(H)$, par définition on a $gHg^{-1} \subset H$, donc H est distingué dans $N_G(H)$.

(3) Soit $K \subset G$ un sous-groupe contenant H comme un sous-groupe distingué. Alors pour tour $g \in K$, $gHg^{-1} \subset K$, et donc $g \in N_G(H)$, d'où $K \subset N_G(H)$.

□

EXEMPLE 1.12.26. *Soit H un sous-groupe de G. Alors G agit sur les classes à gauche de H par*

$$\alpha(g, xH) = gxH.$$

Cette action est transitive.

EXEMPLE 1.12.27. *Soit A un ensemble. On fixe E un ensemble munit d'un action d'un groupe G. Cette action induit une action sur*

$$Fonc(E, A) = \{f \mid f : E \to A\}$$

donnée par

$$(g.f)(x) = f(g^{-1}x)$$

où $x \in E$ et $g \in G$.

$$((gh).f)(x) = f((gh)^{-1}x) = f((h^{-1}g^{-1}x)$$

et

$$(g.(h.f))(x) = (h.f)(g^{-1}x) = f(h^{-1}g^{-1}x).$$

Donc $g.(h.f) = (gh).f$.

PROPOSITION 1.12.28. *Supposons que G agit sur E. Pour tout $x \in E$, on a une bijection $G/G_x \simeq \mathrm{Orb}(x)$.*

DÉMONSTRATION. On définit l'application $\phi : G/G_x \to \mathrm{Orb}(x)$ par $\phi(gG_x) = g.x$.
ϕ est bien définie : Si g_1 et g_2 sont tels que $g_1G_x = g_2G_x$, alors $g_2^{-1}g_1 \in G_x$ d'où $(g_2^{-1}g_1).x = x$ et $g_2.x = g_1.x$, i.e. $\phi(g_1G_x) = \phi(g_2G_x)$.

ϕ est injective : Si $\phi(g_1G_x) = \phi(g_2G_x)$ alors $g_1.x = g_2.x$ d'où $(g_2^{-1}g_1).x = x$ et $g_2^{-1}g_1 \in G_x$ i.e. $g_1G_x = g_2G_x$.
Pour $g \in G$, $gx = \phi(gG_x)$ d'où la surjectivité de ϕ.

□

Soit $E/G := \{\omega_i\}_{i\in J}$ l'ensemble des orbites et $I = \{x_i\}_{i\in J}$ un ensemble des représentants pour les orbites. On a $|I| = |J| = |E/G|$,

$$|E| = \sum_{x\in I} |\,\mathrm{Orb}(x)| = \sum_{x\in I} \frac{|G|}{|G_x|}$$

Formule de Burnside. Supposons que G agit sur E. On pose

$$F = \{(x, g) \mid g.x = x\}.$$

On a la réunion disjointe $F = \cup_x\{(x, g) \mid g.x = x\}$ d'où

$$\begin{aligned} |F| &= \textstyle\sum_x \mid \{(x,g) \mid g.x = x\} \mid = \sum_{x\in E} \mid G_x \mid = \sum_{x\in E} \frac{|G|}{|\mathrm{Orb}(x)|} \\ &= \mid G \mid \textstyle\sum_{x\in E} \frac{1}{|\mathrm{Orb}(x)|} = \mid G \mid \sum_{\omega_i, i\in J} \sum_{x\in\omega_i} \frac{1}{|\omega_i|} = \mid G \mid \sum_{\omega_i, i\in J} |\omega_i| \frac{1}{|\omega_i|} \\ &= \mid G \mid \textstyle\sum_{\omega_i, i\in J} 1 = \mid G \mid .|E/G| \end{aligned}$$

D'autre part, on a la réunion disjointe $F = \cup_{g\in G} \mathrm{Fix}(g) \times \{g\}$ d'où $|F| = \sum_{g\in G} |\,\mathrm{Fix}(g)|$.

$$\boxed{\sum_{g\in G} |\operatorname{Fix}(g)| = |\ G\ | \ .|E/G|} \tag{1.1}$$

DÉFINITION 1.12.29. *Supposons que G agit sur E. L'ensemble des points fixes globaux est $E^G := \{x \in E \mid \forall g \in G \quad g.x = x\} = \cap_{g\in G} \operatorname{Fix}(g)$. En particulier pour $G = \langle g\rangle$,*

$$E^{\langle g\rangle} = \operatorname{Fix}(g)$$

Avec cette notation, la formule de Burnside s'écrit comme

$$\boxed{\sum_{g\in G} |E^{\langle g\rangle}| = |\ G\ | \ .|E/G|} \tag{1.2}$$

EXEMPLE 1.12.30. *Si G agit E, alors G agit G sur $Fonc(E, A)$ (voir Exemple 1.12.27). Calculons les points fixes globaux.*

$$\begin{aligned} Fonc(E,A)^G &= \{f : E \to \mathbb{R} \mid g.f = f \forall g \in G\} = \{f : E \to A \mid f(g^{-1}x) = f(x), \forall x \in E \quad \forall g \in G\} \\ &= \{f : E \to A \mid f(x) = f(gx), \forall x \quad \forall g \in G\}. \end{aligned}$$

Donc $f \in Fonc(E, \mathbb{R})^G$ si et seulement si f est constante sur chaque orbite, plus précisément

$$Fonc(E, A)^G = Fonc(E/G, A), \tag{1.3}$$

Au cas particulier $G = \langle g\rangle$, $Fix(g) = Fonc(E, A)^{\langle g\rangle} = Fonc(E/\langle g\rangle, A)$

Par la formule de Burnside, on obtient

PROPOSITION 1.12.31.

$$|Fonc(E, A)/G| = \frac{1}{|G|}\sum_{g\in G} |Fonc(E, A)^{\langle g\rangle}| \overset{(1.3)}{=} \frac{1}{|G|}|Fonc(E/\langle g\rangle, A)|$$

1.12.1. Application : Les nombres de colliers. On peut voir un collier de longueur n faits avec deux types de perles comme une fonction de $f : \mathbb{Z}/n\mathbb{Z} \to \{0, 1\}$. Mais deux telles fonctions donnent(géométriquement) le mà[a]me collier si elles sont dans la mà[a]me orbite de l'action de $\mathbb{Z}/n\mathbb{Z}$ sur $Fonc(\mathbb{Z}/n\mathbb{Z}, \{0, 1\})$. Donc par la proposition 1.12.31 le nombre des colliers $T(n)$ est

$$\begin{aligned} T(n) &= |Fonc(\mathbb{Z}/n\mathbb{Z}, \{0, 1\})^{Z/n\mathbb{Z}}| = \tfrac{1}{n}\textstyle\sum_{g\in\mathbb{Z}/n\mathbb{Z}} |Fonc(\mathbb{Z}/n\mathbb{Z}/\langle g\rangle, \{0, 1\})| \\ &= \tfrac{1}{n}\textstyle\sum_{d|n}\sum_{\mathrm{Ord}(g)=d} 2^{n/d} = \tfrac{1}{n}\sum_{d|n} 2^{n/d}\phi(d) \end{aligned}$$

1.13. Groupes Symétriques

Soit $E; = \{1, \cdots n\}$.

DÉFINITION 1.13.1. *Le support de $\sigma \in S_n$ est*

$$\operatorname{Supp}(\sigma) := \{x \in E | \sigma(x) \neq x\}.$$

Le support est le complémentaire de l'ensemble des points fixes :

$$\operatorname{Fix}(\sigma) = \{x \in E \mid \sigma(x) = x\}$$

LEMME 1.13.2. *(1)* $\operatorname{Fix}(\sigma^{-1}) = \operatorname{Fix}(\sigma)$ *et* $\operatorname{Supp}(\sigma) = \operatorname{Supp}(\sigma^{-1})$.
(2) $\operatorname{Fix}(\sigma) \subset \operatorname{Fix}(\sigma^n)$.
(3) $\operatorname{Supp}(\sigma^n) \subset \operatorname{Supp}(\sigma)$.

(4) $\mathrm{Fix}(\sigma\gamma\sigma^{-1}) = \sigma(\mathrm{Fix}(\gamma))$ *et* $\mathrm{Supp}(\sigma\gamma\sigma^{-1}) = \sigma(\mathrm{Supp}(\gamma))$

(5) Si $\mathrm{Supp}\,\tau \cap \mathrm{Supp}\,\sigma = \emptyset$ *et* $\sigma\tau = 1$ *alors* $\sigma = 1$ *et* $\tau = 1$.

DÉMONSTRATION. (1) σ est une bijection, alors $\sigma^{-1}(x) = x$ si et seulement $x = \sigma(x)$, d'où $\mathrm{Fix}(\sigma^{-1}) = \mathrm{Fix}(\sigma)$ et donc $\mathrm{Supp}(\sigma) = \mathrm{Supp}(\sigma^{-1})$.

(2) Si $\sigma(x) = x$, alors $\sigma(\sigma(x)) = \sigma(x) = x$, et ... par récurrence $\sigma^n(x) = \sigma^{n-1}(x) = \cdots = \sigma(x) = x$.

(3) Par (2), $\mathrm{Fix}(\sigma) \subset \mathrm{Fix}(\sigma^n)$ d'où $\mathrm{Fix}(\sigma^n)^c \subset \mathrm{Fix}(\sigma)^c$ et donc $\mathrm{Supp}(\sigma^n) \subset \mathrm{Supp}(\sigma)$.

(4) Si $(\sigma\gamma\sigma^{-1})(x) = x$ alors $\gamma\sigma^{-1}(x) = \sigma^{-1}(x)$ d'où $\sigma^{-1}(x) \in \mathrm{Fix}(\gamma)$ et donc $\mathrm{Fix}(\sigma\gamma\sigma^{-1}) = \sigma(\mathrm{Fix}(\gamma))$

(5) Soit $x \in \mathrm{Supp}\,\sigma$. Alors $x \notin \mathrm{Supp}\,\tau$ et $\tau(x) = x$, d'où $\sigma(\tau(x)) = \sigma(x)$. Or par l'hypothèse $\sigma(\tau(x)) = x$ donc $\sigma(x) = x$ et $x \notin \mathrm{Supp}(\sigma)$ nous menant à une contradiction. Cela veut dire que $\mathrm{Supp}(\sigma) = \emptyset$ et $\sigma = 1$. A partir de l'identité $\sigma\tau = 1$ il maintenant claire $\tau = 1$.

□

DÉFINITION 1.13.3. *A toute paire* (i, j) *on peut associer une transposition* $\sigma = (i, j) \in S_n$ *définie par*

$$\sigma(x) = \begin{cases} x \ si\ x \neq i, j \\ j \ si\ x = i \\ i \ si\ x = j \end{cases} \tag{1.1}$$

En généralisant cette idée, on définit les cycles. A une liste $(a_1, \cdots, a_m)$, $a_i \neq a_j$ *et* $n > 1$, *on associe* $\gamma \in S_n$,

$$\gamma(x) = \begin{cases} x \ si\ x \notin \{a_1, \cdots, a_m\} \\ a_{i+1} \ si\ x = a_i, \quad i = 1, \cdots, m-1 \\ a_1 \ si\ x = a_m \end{cases}$$

Donc $\mathrm{Supp}(\gamma) = \{a_1, \cdots, a_m\}$. *La longueur de* γ *est par définition*

$$|\gamma| = m.$$

PROPOSITION 1.13.4. *Soit* $\gamma = (a_1, \cdots, a_m) \in S_n$ *un cycle de longueur* n.

(1) $\mathrm{Ord}(\gamma) = |\gamma|$

(2) $\gamma^{-1} = (a_m, \cdots, a_1)$

(3) Pour tout $\sigma \in S_n$, $\sigma\gamma\sigma^{-1}$ *est le cycle* $(\sigma(a_1), \cdots, \sigma(a_m))$.

(4) Pour $x \in \mathrm{Supp}(\gamma)$, $\gamma = (x, \gamma(x), \gamma^2(x), \ldots, \gamma^{m-1}(x))$ *et donc* $\mathrm{Supp}\,\gamma = \{x, \gamma(x), \cdots, \gamma^{m-1}(x))$.

DÉMONSTRATION. (1) Soit $x \in \{1, \cdots n, \}$. Si $x \notin \mathrm{Supp}\,\gamma$ alors $\gamma(x) = x$ d'où $\gamma^n(x) = x$. Si $x = a_i$ alors $\gamma^n(a_i) = \gamma^{n-1}(a_{i+1 \mod n} = \cdots a_{i+n \mod n} = a_i$. Donc dans tous les cas, $\gamma^n(x) = x$.

(2) On pose $\sigma = (a_m, \cdots, a_1)$. Alors $\mathrm{Supp}(\sigma) = \mathrm{Supp}(\gamma)$. Donc si $x \notin \mathrm{Supp}(\sigma) = \mathrm{Supp}(\gamma)$, alors $(\sigma \circ \gamma)(x) = x$. Si $x = a_i$, alors $(\sigma \circ \gamma)(a_i) = \sigma(\gamma(a_i)) = \sigma(a_{i+1 \mod n}) = a_{i+1-1 \mod n} = a_i$. Donc tous les cas $(\sigma \circ \gamma)(x) = x$ d'où $\sigma = \gamma^{-1}$.

(3) D'abord on identifie les points fixes de $\sigma\gamma\sigma^{-1}$. Si $(\sigma\gamma\sigma^{-1})(x) = x$ alors $\gamma\sigma^{-1}(x) = \sigma^{-1}(x)$ d'où $\sigma^{-1}(x) \in \mathrm{Fix}(\gamma)$ et donc $\mathrm{Fix}(\sigma\gamma\sigma^{-1}) = \sigma(\mathrm{Fix}(\gamma))$. Puisque σ est une bijection, on conclut que $\mathrm{Supp}(\sigma\gamma\sigma^{-1}) = \sigma(\mathrm{Supp}(\gamma)) = \{\sigma(a_1), \cdots, \sigma(a_m)\}$. Donc pour si $x \notin \{\sigma(a_1), \cdots, \sigma(a_m)\}$, $(\sigma\gamma\sigma^1)(x) = x$,

et si $x = \sigma(a_i)$ alors $(\sigma\gamma\sigma^1)(x) = \sigma\gamma\sigma^1)(\sigma(a_i)) = \sigma(\gamma(a_i)) = \sigma(a_{i+1})$. On a donc montré que $\sigma\gamma\sigma^1 = (\sigma(a_1), \cdots, \sigma(a_n))$.

(4) Soit $\sigma = (x, \gamma(x), \gamma^2(x), \cdots, \gamma^{n-1}(x))$ Supposons que $x = a_i$. Alors pour tout $j \in \{1, \cdots n\}$, $a_j = \gamma^{j-i}(a_i)$

et donc $\operatorname{Supp}\sigma = \{x, \gamma(x), \gamma^2(x), \cdots, \gamma^{n-1}(x)\} = \{a_i \cdots a_n, a_1 \cdots a_{i-1}\} = \{a_1 \cdots a_n\} = \operatorname{Supp}\gamma$.

Pour pour $a_j \in \operatorname{Supp}\sigma = \operatorname{Supp}\gamma$, $\sigma(a_j) = \sigma(\gamma^{j-i}(x)) = \gamma^{j-i+1}(x) = \gamma^{j-i+1}(a_i) = \gamma(\gamma^{j-i}(a_i)) = \gamma(a_j)$, donc $\sigma = \gamma$ sur leur supports, d'où $\sigma = \gamma$

□

Proposition 1.13.5. *Soient τ et $\sigma \in S_n$ deux permutation telles que* $\operatorname{Supp}(\sigma) \cap \operatorname{Supp}(\tau) = \emptyset$. *Alors σ et τ commutent i.e. $\sigma\tau = \tau\sigma$.*

Démonstration. On obsèrve que

(1) Si $x \in \operatorname{Supp}(\sigma)$ alors $\sigma(x) \in \operatorname{Fix}(\tau)$, sinon $\sigma(x) \in \operatorname{Supp}(\tau) \subset \operatorname{Fix}(\sigma)$ et donc $\sigma(\sigma(x)) = \sigma(x)$ d'où $\sigma(x) = x$ et $x \in \operatorname{Fix}(\sigma)$ qui est une contraction.

(2) Puisque les supports $\operatorname{Supp}(\sigma)$ et $\operatorname{Supp}(\tau)$ sont disjoints, pour $x \in \{1, \cdots n\}$ il existe trois cas mutullement exclusive : $x \in \operatorname{Supp}(\sigma)$, $x \in \operatorname{Supp}(\tau)$ ou $x \in c(\operatorname{Supp}(\sigma) \cup \operatorname{Supp}(\tau))^c = \operatorname{Supp}(\sigma)^c \cap \operatorname{Supp}(\tau)^c = \operatorname{Fix}(\sigma) \cap \operatorname{Fix}(\tau)$.

Nous avons donc

$$\tau(\sigma(x)) = \begin{cases} x \text{ si } x \operatorname{Fix}(\sigma) \cap \operatorname{Fix}(\tau) \\ \sigma(x) \text{ si } x \in \operatorname{Supp}(\sigma) \subset \operatorname{Fix}(\tau) \\ \mu(x) \text{ si } x \in \operatorname{Supp}(\tau) \subset \operatorname{Fix}(\sigma) \end{cases} \tag{1.2}$$

et de la même manière,

$$\sigma(\tau(x)) = \begin{cases} x \text{ si } x \operatorname{Fix}(\sigma) \cap \operatorname{Fix}(\tau) \\ \sigma(x) \text{ si } x \in \operatorname{Supp}(\sigma) \subset \operatorname{Fix}(\tau) \\ \mu(x) \text{ si } x \in \operatorname{Supp}(\tau) \subset \operatorname{Fix}(\sigma) \end{cases} \tag{1.3}$$

ce qui mets en évidence l'identité $\tau\sigma = \sigma\tau$.

□

Corollaire 1.13.6. *Si* $\operatorname{Supp}(\sigma) \cap \operatorname{Supp}(\tau) = \emptyset$ *alors* $\operatorname{Ord}(\sigma\tau) = ppcm(\operatorname{Ord}(\sigma), \operatorname{Ord}(\tau))$.

Démonstration. Soit $k = ppcm(\operatorname{Ord}(\sigma), \operatorname{Ord}(\tau))$. Par la proposition 1.13.5, commutent et donc $(\sigma\tau)^k = \sigma^k\tau^k = 1.1 = 1$

D'autre part si pour un certain $m \in \mathbb{N}$, $(\sigma\tau)^m = 1$, alors $\sigma^m.\tau^m = 1$. Comme $\operatorname{Supp}(\sigma^m) \subset \operatorname{Supp}(\sigma)$ et $\operatorname{Supp}\tau^m \subset \operatorname{Supp}\tau$ alors $\operatorname{Supp}(\sigma^m) \cap \operatorname{Supp}\tau^m = \emptyset$ (voir Lemme 1.13.2). Donc de l'identité $\sigma^m\tau^m = 1$ on déduit que $\sigma^m = 1$ et $\tau^m = 1$ d'où $\operatorname{Ord}(\tau)|m$ et $\operatorname{Ord}(\sigma)|m$. Par la définition de ppcm, il est maintenant claire que $k|m$ et donc $k = \operatorname{Ord}(\sigma\tau)$. □

Theorem 1.13.7. *Toute permutation γ est produit des cycles d'une manière unique.*

Démonstration.

Existence de décomposition : Soit $\sigma \in S_n$. Le (sous-) groupe cyclique $\langle\sigma\rangle$ agit sur $E = \{1, \cdots n\}$, donc $E = \omega_1 \cup \omega_2 \cdots \cup \omega_N$ est la réunion disjointe des orbites de cette action. Chaque orbit ω_i est de la forme $\omega_i = \{x_i, \sigma(x_i), \cdots \sigma^k(x_i)\}$ pour un certain $x \in E$ et $k \in \mathbb{N}$. En particulier si $k = 0$, ça veut dire que x est un point fixe et $\omega_i = \{x_i\}$ est un singleton. A chaque orbit $\omega_i = \{x_i, \sigma(x_i), \cdots \sigma^k(x_i)\}$ on associe le cycle $\gamma_{\omega_i} = (x_i, \sigma(x_i), \cdots \sigma^k(x_i))$ et on va démontrer que $\sigma = \gamma_{x_1} \cdots \gamma_{x_N}$.Tout

d'abord on observe que les supports des $\gamma_{\omega_i} = \{x_i, \sigma(x_i), \cdots \sigma^k(x_i)\} = \omega_i$ sont mutullement disjoints, donc $\sigma^l(x_i) \in \operatorname{Fix} \gamma_{\omega_j}$ si $i \neq j$.

Soit $y \in E$, alors il existe un unique i tel que $y \in \omega_i$ et donc $y = \sigma^l(x_i)$ pour un certain (unique) l et $\sigma(y) = \sigma(\sigma^l(x_i)) = \sigma^{l+1}(x_i)$. D'autre part

$$\begin{aligned}(\gamma_{\omega_1} \cdots \gamma_{\omega_N})(y) = (\gamma_{\omega_1} \cdots \gamma_{\omega_i})(y) \qquad & (\text{car } y = \sigma^l(x_i) \in \operatorname{Fix}(\omega_{i+1} \cap \cdots \operatorname{Fix}(\omega_N)) \\ = ((\gamma_{\omega_1} \cdots \gamma_{\omega_{i-1}})(\gamma_{\omega_i}(\sigma^l(x_i)) & = (\gamma_{\omega_1} \cdots \gamma_{\omega_{i-1}})(\sigma^{l+1})(x_i)) \\ = \sigma^{l+1}(x_i) \text{ car } & (\text{car } y = \sigma^l(x_i) \in \operatorname{Fix}(\omega_1 \cap \cdots \operatorname{Fix}(\omega_{i-1}))\end{aligned}$$

On conclut que $\sigma(y) = (\gamma_{\omega_1} \cdots \gamma_{\omega_N})(y)$.

Unicité de décomposition : Supposons $\sigma = \gamma_1 \cup \gamma_2 \cdots \gamma_p = \tau_1 \cup \tau_2 \cdots \tau_q$ où γ_i et τ_i sont des cycles. On a donc deux réunions disjointes $\{1, \cdots, n\} = \operatorname{Supp} \gamma_1 \cup \cdots \cup \operatorname{Supp} \gamma_n = \operatorname{Supp} \tau_1 \cup \cdots \cup \operatorname{Supp} \tau_m$.

On peut écrire $\gamma_1 = (x, \cdots, \gamma_1^k(x))$ où $x \in \operatorname{Supp}(\gamma_1)$ et $k \in \mathbb{N}$. Comme $x \in \{1, \cdots, n\} = \operatorname{Supp} \tau_1 \cup \cdots \cup \operatorname{Supp} \tau_m$, donc il existe unique τ_i telle que $x \in \operatorname{Supp} \tau_i$. Puisque les τ_i's commuent (voir Lemma 1.13.5), en changeant l'indexation des τ's, on peut supposer que $i = 1$.

Parce que $x \in \operatorname{Fix}(\gamma_i)$, on a $\sigma(x) = (\gamma_1 \gamma_2 \cdots \gamma_p)(x) = \gamma_1(x)$, pour $i \neq 1$, l'orbite de x sous l''action de σ est égale à $\operatorname{Supp} \gamma_1$ (voir la proposition 1.13.4) et de la même manière $\sigma(x) = \tau_1(x)$ et $\operatorname{Orb}(x) = \operatorname{Supp} \tau_1$. On a alors $|\gamma_1| = |\tau_1| = \#\operatorname{Orb}(x)$ et $\gamma_1 = (x, \gamma(x) \cdots) = (x, \sigma(x), \cdots) = (x, \tau(x), \dots) = \tau_1$. En supprimant $\tau_1 = \gamma_1$ de l'identité $\gamma_1 \cdot \gamma_2 \cdots \gamma_p = \tau_1 \cdot \tau_2 \cdots \tau_q$ et répétant la même procédure, on obtiendra $p = q$ et une correspondance entre γ_i et τ_i. Plus précisément pour chaque, i il existe un unique $\phi(i)$ tel que $\gamma_i = \tau_{\phi(i)}$.

□

COROLLARY 1.13.8. *Le groupe symétrique S_n est engendré par par les transposition,*

$$S_n = \langle (i,j) | i, j \in \{1, \cdots n\} \rangle.$$

DÉMONSTRATION. Par le théorème précédent S_n est engendré par les cycles, il suffit donc de montrer qu'un cycle le produit des transpositions ce qui n'est pas difficile car

$$(a_1, a_2, \cdots, a_n) = (a_1, a_2)(a_2, a_3) \cdots (a_{n-1}, a_n)$$

□

Il y a d'autres présentations pour S_n, notamment grâce aux identités

$$(i,j) = (1,i)(1,j)(1,i)$$

on peut donc écrire

$$S_n = \langle (1,i) | i \in \{2, \cdots, n\} \rangle. \tag{1.4}$$

On peut également montrer que

$$S_n = \langle (1,2), (2,3), \cdots (n-1,n) \rangle \tag{1.5}$$

pour lequel il suffit de montrer que les générateurs (voir 1.4) $(1,i) \in \langle (1,2), (2,3), \cdots (n-1,n) \rangle$ Pour ce faire on observe que

$$(1,3) = (1,2)(2,3), (1,2) \in \langle (1,2), (2,3), \cdots (n-1,n) \rangle.$$

En suite,

$$(3,4) = (1,3)(1,4)(1,3) \in \langle (1,2), (2,3), \cdots (n-1,n) \rangle,$$

etc.

En fin la présentation le plus simple (i.e. avec 2 générateurs) est donnée par

$$S_n = \langle \tau = (1,2), \sigma = (1,2,3,\cdots,n) \rangle \tag{1.6}$$

Il suffit de vérifier que $(k-1,k) = \sigma^k \tau \sigma^{-k}$.

La question qui se pose naturellement est : Quel est l'effet de conjugaison sur les décompositions en cycle. Soit $\sigma = \gamma_1 \cdots \gamma_m$ une décomposition en cycles disjoints et $\pi \in S_n$ une permutation. On a

$$\pi\sigma\pi^{-1} = (\pi\gamma_1\pi^{-1})(\pi\gamma_2\pi^{-1}) \cdots (\pi\gamma_m\pi^{-1}), \tag{1.7}$$

où $((\pi\gamma_i\pi^{-1})$ sont des cycles (voir la proposition 1.13.4). P uisque $\mathrm{Supp}(\pi\gamma_i\pi^{-1}) = \pi(\mathrm{Supp}(\gamma_i))$, les supports de $\pi\gamma_i\pi^{-1}$'s sont disjoints,

$$\begin{aligned} \mathrm{Supp}(\pi\gamma_i\pi^{-1}) \cap \mathrm{Supp}(\pi\gamma_j\pi^{-1}) &= \pi(\mathrm{Supp}(\gamma_i)) \cap \pi(\mathrm{Supp}(\gamma_j) \\ &= \pi(\mathrm{Supp}(\gamma_i) \cap \mathrm{Supp}(\gamma_j)) = \pi(\emptyset) = \emptyset \end{aligned}$$

Alors (1.7) est la décomposition de $\pi\sigma\pi^{-1}$ en cycles disjoints. Il est claire que γ_i et $\pi\gamma\pi^{-1}$ ont les même longueurs et pour $n_i := |\gamma_i| = |\pi\gamma\pi^{-1}|$ on a $n = n_1 \cdots + n_m$.

Ce calcul nous montre que deux permutations conjuguées fournissent la même partition de n. On peut naturellement se demander si deux permutations fournissent la même ppartition, sont conjuguées. Par la suite on répond à cette question affirmativement.

Définition 1.13.9. *Soit $n \in \mathbb{N}$. Une partition de n est une suite croissante $n_1 \geq n_2 \geq \cdots \geq n_k$ dans $\mathbb{N}$ telle que ,*

$$n = n_1 + n_2 + \cdots + n_k.$$

Proposition 1.13.10. *Il y a une bijection entre les classes de conjugaison dans S_n et les partitions de n.*

Démonstration. On a vu ci-dessous qu'une permutation σ nous fournit une partition $n_1 \geq n_2 \geq n_k$ de n. Il suffit de prendre la décomposition de $\sigma = \gamma_1\gamma_2 \cdots \gamma_n$ et . Puisque les γ_i's commuent alors, si nececessaire, on peut changer l'ordre de sort que la suite $ni := |\gamma_i$, longueurs de γ_i's, est croissante.

Et à l'inverse à une partition $n_1 \geq n_2 \geq \cdots \geq n_k$ de n,on peut associer une permutation

$$\sigma = (1,\cdots,n_1)(n_1{+}1,\cdots n_1{+}n_2)(n_1{+}n_2{+}1 \cdots n_1{+}n_2{+}n_3) \cdots (n_1{+}n_2{+}\cdots n_{k-1}{+}1,\cdots n_1{+}n_2{+}\cdots n_{k-1}{+}n_k)$$

xxCi-dessus on a vu que deux permutations conjuguées fournissent la même permutation.

Donc Il reste à démontrer que si deux permutation fournissent la même permutation alors elles sont conjuguées. Soient σ et τ deux permutations telles que leurs decompositions en cycles

$$\sigma = \gamma_1 \cdots \gamma_k$$

$$\tau = \mu_1 \cdots \mu_k$$

fournissent la même partition i.e. $|\gamma_i| = |\mu_i|$. On pose $p_i := |\gamma_i| = |\mu_i|$. Supposons que $\gamma_j = (\alpha_{j1},\cdots,\alpha_{jp_j})$ et $\mu_i = (\beta_{j1},\cdots,\beta_{ji_{p_j}})$. Alors on définit la permutation π par

$$\pi = \begin{pmatrix} \alpha_{11},\cdots,\alpha_{1p_1}, & \alpha_{21},\cdots,\alpha_{2p_2} & \cdots, \\ \beta_{11},\cdots,\beta_{1p_1}, & \beta_{21},\cdots,\beta_{2p_2} & \cdots \end{pmatrix} \tag{1.8}$$

On peut aisément vérifier que $\pi\sigma\pi^{-1} = \tau$

□

1.14. Signature

On a vu qu'on peut écrire n'importe quelle permutation comme un produit des transpositions. Est-ce que le nombre des transpositions nécessaire est bien défini ? Il s'avère que seulement la parité de ce nombre est bien défini. Autrement dit les longueurs de deux décomposition d'une permutation en transpositions diffère par un multiple de 2.

PROPOSITION 1.14.1. *Il existe un unique morphisme de groupe $S : S_n \to \mathbb{Z}_2$, appelé la signature, qui envoie toutes les transpositions à (-1).*

DÉMONSTRATION. La signature est donnée par

$$S(\tau) = \prod_{1\leq i<j\leq n} \frac{\sigma(i)-\sigma(j)}{i-j} = \frac{\prod_{1\leq i<j\leq n}(\sigma(i)-\sigma(j))}{\prod_{1\leq i<j\leq n}(i-j)}$$

Puisque σ est une bijection, les éléments des ensembles $\{\sigma(i)-\sigma(j)|1 \leq i < j \leq n\}$ et $\{i-j|1 \leq i < j \leq n\}$ sont identiques à un signe près, donc $S(\tau) \in \{\pm 1\}$.

Par la formule ci-dessus, il est évident que la signature d'une transposition est (-1).

Afin de montrer que σ est un morphisme de groupe, on présente une nouvelle formule pour la signature : Soit $P_2(E) := \{(i,j)|i,j \in E\}$ l'ensemble des tous les sous-ensemble à 2 éléments de E. On remarque que pour tout i, j

$$\frac{\sigma(i)-\sigma(j)}{i-j} = \frac{\sigma(j)-\sigma(i)}{j-i}$$

Donc dans la formule de la signature l'ordre $i < j$ n'est pas importante et on peut donc écrire

$$S(\tau) = \prod_{\{i,j\}\in P_2(E)} \frac{\sigma(i)-\sigma(j)}{i-j}$$

□

Puisque que $\tau : E \to E$ est une bijection, elle induit une bijection de $P_2(E)$ sur $P_2(E)$, autrement dit $P_2(E) = \{\ \{\tau(i),\tau(j)\}|\{i,j\} \in P_2E)\}$. On en déduit

$$\begin{aligned} S(\sigma\tau) &= \prod_{\{i,j\}\in P_2(E)} \frac{(\sigma\tau)(i)-(\sigma\tau)(j)}{i-j} = \prod_{\{i,j\}\in P_2(E)} \frac{(\sigma(\tau(i))-(\sigma(\tau(j))}{i-j} \\ &= \prod_{\{i,j\}\in P_2(E)} \frac{(\sigma(\tau(i))-(\sigma(\tau(j))}{\tau(i)-\tau(j)} \prod_{\{i,j\}\in P_2(E)} \frac{\tau(i)-\tau(j)}{i-j} \qquad (1.1) \\ &= \prod_{\{i,j\}\in P_2(E)} \frac{\sigma(i)-(\sigma(j)}{i-j} \prod_{\{i,j\}\in P_2(E)} \frac{\tau(i)-\tau(j)}{i-j} = S(\sigma)S(\tau) \end{aligned}$$

Unicité : Supposons que $S, S' : S_n \to \{\pm 1\}$ sont deux morphismes qui envoient les transposition à -1. Soit $\sigma \in S_n$ une permutation quelconque. Par le corollaire 1.13.8, on peut écrire $\sigma = \tau_1 \cdots \tau_k$ où τ_i's sont des transpositions. $S(\sigma) = S(\tau_1 \cdots \tau_k) = S(\tau_1) \cdots S(\tau_k) = (-1)(-1) \cdots (-1) = (-1)^k = S'(\tau_1) \cdots S'(\tau_k) = S'(\tau_1 \cdots \tau_k) = S'(\sigma)$

COROLLARY 1.14.2. *Si $\sigma = \tau_1 \cdots \tau_k$ est la décomposition de σ en produit des transpositions, alors $S(\sigma) = (-1)^k$. Donc la parité de k est déterminée par la signature de σ.*

DÉFINITION 1.14.3. *On appelle le noyau du morphisme S le groupe alterné ; il est noté par A_n. Parce que $S_n/A_n \simeq \mathbb{Z}_2$, A_n est d'indice 2 et donc distingué. Le quotient S_n/A_n consiste de deux classes : A_n et τA_n où τ est une transposition quelconques autrement dit $S_n = A_n \cup \tau A_n$.*

PROPOSITION 1.14.4. *S_n est isomorphe a un sous-groupe de A_{n+2}.*

DÉMONSTRATION. On a vu dans l'exemple 1.7.12 que l'application $i_{n+1}i_n$: $S_n \to S_{n+2}$ est injective. Mais l'image de cette application n'est pas forcement inclue dans A_{n+1} et donc nécessite une correction. L'injection southaitée $S_n \hookrightarrow A_{n+2}$ est donnée par $\sigma \to \sigma(n, n+1)^{\frac{S(\sigma)+1}{2}}$. □