Groupes opérant : rappels

$(G, \cdot)$ est un groupe multiplicatif et on note 1 (ou 1_G si nécessaire) l'élément neutre. E est un ensemble non vide et $\mathcal{S}(E)$ est le groupe des permutations de E.

1.1 Définitions et exemples

Définition 1.1 *On dit que G opère (à gauche) sur E si on a une application :*

$$\begin{array}{ccc} G \times E & \rightarrow & E \\ (g, x) & \mapsto & g \cdot x \end{array}$$

telle que :

$$\left\{ \begin{array}{l} \forall x \in E,\ 1 \cdot x = x \\ \forall (g, g', x) \in G^2 \times E,\ g \cdot (g' \cdot x) = (gg') \cdot x \end{array} \right.$$

Une telle application est aussi appelée action (à gauche) de G sur E.

Remarque 1.1 *On peut définir de manière analogue l'action à droite d'un groupe sur un ensemble non vide comme une application :*

$$\begin{array}{ccc} G \times E & \rightarrow & E \\ (g, x) & \mapsto & x \cdot g \end{array}$$

telle que :

$$\left\{ \begin{array}{l} \forall x \in E,\ x \cdot 1 = x \\ \forall (g, g', x) \in G^2 \times E,\ (x \cdot g) \cdot g' = x \cdot (gg') \end{array} \right.$$

Pour tout $g \in G$, l'application :

$$\begin{array}{rccc} \varphi(g) : & E & \rightarrow & E \\ & x & \mapsto & g \cdot x \end{array}$$

est alors une bijection de E sur E, c'est-à-dire que $\varphi(g) \in \mathcal{S}(E)$. En effet, de $1 \cdot x = x$ pour tout $x \in E$, on déduit que $\varphi(1) = Id_E$ et avec $g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = 1 \cdot x = x$ et $g^{-1} \cdot (g \cdot x) = x$ on déduit que $\varphi(g) \circ \varphi(g^{-1}) = \varphi(g^{-1}) \circ \varphi(g) = Id_E$, ce qui signifie que $\varphi(g)$ est bijective d'inverse $\varphi(g^{-1})$.

De plus avec $g \cdot (g' \cdot x) = (gg') \cdot x$, pour tous g, g', x, on déduit que $\varphi(gg') = \varphi(g) \circ \varphi(g')$, c'est-à-dire que l'application φ est un morphisme de groupes de $(G, \cdot)$ dans $(\mathcal{S}(E), \circ)$.

Le noyau de ce morphisme φ est le noyau de l'action à gauche de G sur E.

Réciproquement un tel morphisme φ définit une action à gauche de G sur E avec :

$$g \cdot x = \varphi(g)(x)$$

Exemple 1.1 *G agit sur lui même par translation à gauche :*

$$(g,h) \in G \times G \mapsto g \cdot h = gh$$

Exemple 1.2 *Un groupe G agit sur lui même par conjugaison :*

$$(g,h) \in G \times G \mapsto g \cdot h = ghg^{-1}$$

le morphisme de groupes correspondant de $(G,\cdot)$ dans $(\mathcal{S}(G),\circ)$ est noté :

$$\mathrm{Ad}(g) : \begin{array}{rcl} G & \rightarrow & G \\ h & \mapsto & ghg^{-1} \end{array}$$

L'image de Ad *est le groupe* $\mathrm{Int}(G)$ *des automorphismes intérieurs de G.*

Exercice 1.1 *Montrer que* $\mathrm{Int}(G)$ *est isomorphe au groupe quotient $G/Z(G)$, où $Z(G)$ est le centre de G.*

Solution 1.1 Le noyau du morphisme de groupes $\mathrm{Ad} : G \rightarrow \mathcal{S}(G)$ est formé des $g \in G$ tels que $\mathrm{Ad}(g) = Id_G$, c'est-à-dire des $g \in G$ tels que $ghg^{-1} = h$ pour tout $h \in G$, ce qui équivaut à $gh = hg$ pour tout $h \in G$. Le noyau de Ad est donc le centre $Z(G)$ de G. Comme $\mathrm{Im}(\mathrm{Ad}) = \mathrm{Int}(G)$, on en déduit que $G/Z(G) = G/\ker(\mathrm{Ad})$ est isomorphe à $\mathrm{Im}(\mathrm{Ad}) = \mathrm{Int}(G)$.

Exemple 1.3 *Un groupe G agit sur tout sous-groupe distingué H par conjugaison :*

$$(g,h) \in G \times H \mapsto g \cdot h = ghg^{-1} \in H$$

Exemple 1.4 *Le groupe $\mathcal{S}(E)$ agit naturellement sur E par :*

$$(\sigma,x) \in \mathcal{S}(E) \times E \mapsto \sigma \cdot x = \sigma(x) \in E$$

1.2 Orbites et stabilisateurs

Définition 1.2 *Soit G un groupe opérant sur un ensemble non vide E. Pour tout $x \in E$, le sous-ensemble de E :*

$$G \cdot x = \{g \cdot x \mid g \in G\}$$

est appelé **orbite** *de x sous l'action de G.*

On vérifie facilement que la relation $x \sim y$ si, et seulement si, il existe $g \in G$ tel que $y = g \cdot x$ est une relation d'équivalence sur E ($x = 1 \cdot x$ donne la réflexivité, $y = g \cdot x$ équivalent à $x = g^{-1} \cdot y$ donne la symétrie et $y = g \cdot x$, $z = h \cdot y$ qui entraîne $z = (hg) \cdot x$ donne la transitivité) et la classe de $x \in E$ pour cette relation est l'orbite de x. Il en résulte que les orbites forment une partition de E.

Exemple 1.5 *Pour l'action de $\mathcal{S}(E)$ sur E il y a une seule orbite. En effet, pour tout $x \in E$, on a :*

$$\mathcal{S}(E) \cdot x = \{\sigma(x) \mid \sigma \in \mathcal{S}(E)\} = E$$

(tout $y \in E$ s'écrit $y = \tau(x)$, où τ est la transposition $\tau = (x,y)$ si $y \neq x$, $\tau = Id$ si $y = x$).

Exemple 1.6 *Pour l'action de G sur lui même par conjugaison, les orbites sont appelées* **classes de conjugaison** *:*

$$\forall h \in G,\ G \cdot h = \left\{ghg^{-1} \mid g \in G\right\}$$

Le groupe G est commutatif si, et seulement si, $G \cdot h = \{h\}$ pour tout $h \in G$.

Exemple 1.7 *Si H est un sous-groupe de G, il agit par translation à droite sur G :*

$$(h, g) \in H \times G \mapsto h \cdot g = gh^{-1}$$

($1 \cdot g = g1 = g$ et $h_1 \cdot (h_2 \cdot g) = \left(gh_2^{-1}\right) h_1^{-1} = g\,(h_1 h_2)^{-1} = (h_1 h_2) \cdot g$) et pour tout $g \in G$ l'orbite de g est la classe à gauche modulo H :

$$\begin{aligned} H \cdot g &= \{h \cdot g \mid h \in H\} = \left\{gh^{-1} \mid h \in H\right\} \\ &= \{gk \mid k \in H\} = gH \end{aligned}$$

L'ensemble de ces orbites est l'ensemble quotient G/H des classes à gauche modulo H.
En utilisant les translations à gauche sur G :

$$(h, g) \in H \times G \mapsto h \cdot g = hg$$

les orbites sont les classes à droite modulo H :

$$H \cdot g = \{hg \mid h \in H\} = Hg$$

Exemple 1.8 *Soit E un ensemble non vide. Pour $\sigma \in \mathcal{S}(E)$, le groupe des permutations de E, on fait agir le groupe cyclique $H = \langle \sigma \rangle$ sur E par :*

$$(\sigma^r, x) \in H \times E \mapsto \sigma^r \cdot x = \sigma^r(x)$$

et l'orbite de $x \in E$ pour cette action est l'ensemble :

$$H \cdot x = \{\gamma \cdot x \mid \gamma \in H\} = \{\sigma^r(x) \mid r \in \mathbb{Z}\}$$

On dit $H \cdot x$ est l'orbite de la permutation σ. On note, dans ce contexte, $Orb_\sigma(x)$ une telle orbite.

Un **cycle** est une permutation $\sigma \in \mathcal{S}(E)$ pour laquelle il n'existe qu'une seule orbite non réduite à un point.

En utilisant le fait que les σ-orbites forment une partition de E et que chaque σ-orbite non réduite à un point permet de définir un cycle, on déduit que toute permutation $\sigma \in \mathcal{S}(E) \backslash \{Id_E\}$ se décompose en produit de cycles de supports deux à deux disjoints (théorème **??**).

Exercice 1.2 *Soit $\sigma = (x_1, x_2, \cdots, x_r)$ un cycle de longueur paire. Montrer que σ^2 n'est pas un cycle.*

Solution 1.2 Soit $r = 2p$ la longueur de σ avec $p \geq 1$. Pour $p = 1$, $\sigma^2 = Id_E$ n'est pas un cycle et pour $p \geq 2$, on a :

$$Orb_{\sigma^2}(x_1) = \{x_1, x_3, \cdots, x_{2p-1}\} \text{ et } Orb_{\sigma^2}(x_2) = \{x_2, x_4, \cdots, x_{2p}\}$$

et σ^2 n'est pas un cycle.

Définition 1.3 *On dit que l'action de G sur E est* **transitive** *[resp.* **simplement transitive** *] si :*

$$\forall (x,y) \in E^2,\ \exists g \in G \mid y = g \cdot x$$
$$\textit{resp. } \forall (x,y) \in E^2,\ \exists! g \in G \mid y = g \cdot x$$

Dans le cas d'une action transitive ou simplement transitive, il y a une seule orbite.

Définition 1.4 *On dit que l'action de G sur E est* **fidèle** *si le morphisme de groupes :*

$$\varphi : g \in G \mapsto (\varphi(g) : x \mapsto g \cdot x) \in \mathcal{S}(E)$$

est injectif, ce qui signifie que :

$$(g \in G \text{ et } \forall x \in E,\ g \cdot x = x) \Leftrightarrow (g = 1)$$

Une action fidèle permet d'identifier G à un sous-groupe de $\mathcal{S}(E)$.

Théorème 1.1 (Cayley) *L'action de G sur lui même par translation à gauche est fidèle et G est isomorphe à un sous-groupe de $\mathcal{S}(G)$.*

Démonstration. Pour $g \in G$, on a $g \cdot h = gh = h$ pour tout $h \in G$ si, et seulement si, $g = 1$, donc φ est injectif. ■

Exercice 1.3 *On considère, pour $n \geq 1$, l'action de $\mathcal{O}_n(\mathbb{R})$ sur $\mathbb{R}^n$ définie par :*

$$\forall (A,x) \in \mathcal{O}_n(\mathbb{R}) \times \mathbb{R}^n,\ A \cdot x = A(x)$$

Montrer que les orbites sont les sphères de centre 0.

Solution 1.3 Pour $x \in \mathbb{R}^n$, on a :

$$\mathcal{O}_n(\mathbb{R}) \cdot x = \{A(x) \mid A \in \mathcal{O}_n(\mathbb{R})\}$$

Pour tout $y \in \mathcal{O}_n(\mathbb{R}) \cdot x$, il existe $A \in \mathcal{O}_n(\mathbb{R})$ telle que $y = A(x)$ et $\|y\| = \|A(x)\| = \|x\|$, donc $\mathcal{O}_n(\mathbb{R}) \cdot x \subset S(0, \|x\|)$.
Réciproquement si $y \in S(0, \|x\|)$ avec $x \neq 0$, on a $y \neq 0$ et on peut construire deux bases orthonormées $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ et $\mathcal{B}' = (e'_i)_{1 \leq i \leq n}$ de $\mathbb{R}^n$ telles que $e_1 = \dfrac{1}{\|x\|} x$ et $e'_1 = \dfrac{1}{\|y\|} y$. La matrice de base de $\mathcal{B}$ à $\mathcal{B}'$ est alors orthogonale et $y = \|y\| e'_1 = \|x\| A(e_1) = A(x)$, donc $y \in \mathcal{O}_n(\mathbb{R}) \cdot x$. On a donc $\mathcal{O}_n(\mathbb{R}) \cdot x = S(0, \|x\|)$ pour $x \neq 0$.
Pour $x = 0$, on a $\mathcal{O}_n(\mathbb{R}) \cdot x = \{0\} = S(0, \|x\|)$.

Exercice 1.4 *Soient n, m deux entiers naturels non nuls et $\mathbb{K}$ un corps commutatif. On fait agir le groupe produit $G = GL_n(\mathbb{K}) \times GL_m(\mathbb{K})$ sur l'ensemble $E = \mathcal{M}_{n,m}(\mathbb{K})$ des matrices à n lignes et m colonnes par :*

$$\forall (P,Q) \in G,\ \forall A \in E,\ (P,Q) \cdot A = PAQ^{-1}$$

Montrer que les orbites correspondantes sont les ensembles :

$$\mathcal{O}_r = \{A \in E \mid \mathrm{rg}(A) = r\}$$

où r est compris entre 0 et $\min(n,m)$.

Solution 1.4 On rappelle qu'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est de rang r si et seulement si elle est équivalente à $A_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.
Rappelons une démonstration de ce résultat.
Pour $r = 0$, on a $A = 0 = A_0$. Pour $r \geq 1$, en désignant par $u \in \mathcal{L}(\mathbb{K}^n)$ l'endomorphisme de matrice A dans la base canonique de $\mathbb{K}^n$, H un supplémentaire de $\ker(u)$ dans $\mathbb{K}^n$, $\mathcal{B}_1 = (e_i)_{1\leq i\leq r}$ une base de H et $\mathcal{B}_2$ une base de $\ker(u)$, le système $u(\mathcal{B}_1) = (u(e_1))_{1\leq i\leq r}$ qui est libre dans $\mathbb{K}^n$ (si $\sum_{k=1}^{r} \lambda_k u(e_k) = 0$, alors $\sum_{k=1}^{r} \lambda_k e_k \in H \cap \ker(u) = \{0\}$ et tous les λ_k sont nuls) se complète en une base $\mathcal{B} = \{u(e_1), \cdots, u(e_r), f_{r+1}, \cdots, f_n\}$ de $\mathbb{K}^n$ et la matrice de u dans les bases $\mathcal{B}_1 \cup \mathcal{B}_2$ et $\mathcal{B}$ a alors la forme indiquée. La réciproque est évidente.
Il en résulte que :

$$\begin{aligned} \mathcal{O}_r &= \{A \in E \mid \mathrm{rg}(A) = r\} \\ &= \left\{A \in E \mid \exists (P,Q) \in G \mid A = PI_rQ^{-1}\right\} = G \cdot I_r \end{aligned}$$

et :

$$E = \bigcup_{r=0}^{\min(n,m)} \mathcal{O}_r = \bigcup_{r=0}^{\min(n,m)} G \cdot I_r$$

ce qui nous donne toutes les orbites.

Définition 1.5 *Soit G un groupe opérant sur un ensemble non vide E. Pour tout $x \in X$, le sous-ensemble de G :*

$$G_x = \{g \in G \mid g \cdot x = x\}$$

est le **stabilisateur** *de x sous l'action de G.*

On vérifie facilement que ces stabilisateurs G_x sont des sous-groupes de G (en général non distingués).

Exemple 1.9 *Soit un ensemble E non réduit à un point. En faisant agir sur E son groupe de permutations $G = \mathcal{S}(E)$, par $\sigma \cdot x = \sigma(x)$, le stabilisateur de $x \in E$ est isomorphe à $\mathcal{S}(E \setminus \{x\})$. À $\sigma \in G_x$, on associe la restriction σ' de σ à $E \setminus \{x\}$, ce qui définit un isomorphisme de G_x sur $\mathcal{S}(E \setminus \{x\})$.*

Théorème 1.2 *Soit $(G, \cdot)$ est un groupe opérant sur un ensemble E. Pour tout $x \in E$ l'application :*

$$\begin{array}{rccl} \varphi_x : & G/G_x & \rightarrow & G \cdot x \\ & \overline{g} = gG_x & \mapsto & g \cdot x \end{array}$$

est bien définie et bijective. Dans le cas où G fini, on a :

$$\mathrm{card}(G \cdot x) = [G : G_x] = \frac{\mathrm{card}(G)}{\mathrm{card}(G_x)}$$

(donc $\mathrm{card}(G \cdot x)$ *divise* $\mathrm{card}(G)$*).*

Démonstration. En remarquant que pour g, h dans G et $x \in E$, l'égalité $g \cdot x = h \cdot x$ équivaut à $(h^{-1}g) \cdot x = x$, soit à $h^{-1}g \in G_x$ ou encore à $\overline{g} = \overline{h}$ dans G/G_x, on déduit que l'application φ_x est bien définie et injective. Cette application étant clairement surjective, elle définie une bijection de G/G_x sur $G \cdot x$. Dans le cas où G fini, on a :

$$\mathrm{card}(G \cdot x) = \mathrm{card}(G/G_x) = \frac{\mathrm{card}(G)}{\mathrm{card}(G_x)}$$

■

Exercice 1.5 *En utilisant l'action naturelle de $\mathcal{S}(E)$ sur E, montrer que si E est un ensemble fini à n éléments, on a alors* $\operatorname{card}(\mathcal{S}(E)) = n!$

Solution 1.5 On utilise l'action de $\mathcal{S}(E)$ sur E définie par :

$$\forall (\sigma, x) \in \mathcal{S}(E) \times E,\ \sigma \cdot x = \sigma(x)$$

Cette action est transitive (il y a une seule orbite), donc $\mathcal{S}(E) \cdot x = E$ pour tout $x \in E$. Le stabilisateur de $x \in E$ est :

$$\mathcal{S}(E)_x = \{\sigma \in \mathcal{S}(E) \mid \sigma(x) = x\}$$

et l'application qui associe à $\sigma \in \mathcal{S}(E)_x$ sa restriction à $F = E \setminus \{x\}$ réalise un isomorphisme de $\mathcal{S}(E)_x$ sur $\mathcal{S}(F)$. On a donc $\operatorname{card}(\mathcal{S}(E)_x) = \operatorname{card}(\mathcal{S}(F))$ et :

$$\begin{aligned}\operatorname{card}(\mathcal{S}(E)) &= \operatorname{card}(\mathcal{S}(E) \cdot x) \operatorname{card}(\mathcal{S}(E)_x) \\ &= \operatorname{card}(E) \operatorname{card}(\mathcal{S}(F)) = n \operatorname{card}(\mathcal{S}(F))\end{aligned}$$

On conclut alors par récurrence sur $n \geq 1$.

1.3 Équation des classes

Théorème 1.3 (équation des classes) *Soit $(G, \cdot)$ est un groupe fini opérant sur un ensemble fini E. En notant $G \cdot x_1, \cdots, G \cdot x_r$ toutes les orbites deux à deux distinctes, on a :*

$$\operatorname{card}(E) = \sum_{i=1}^{r} \operatorname{card}(G \cdot x_i) = \sum_{i=1}^{r} \frac{\operatorname{card}(G)}{\operatorname{card}(G_{x_i})}$$

Démonstration. Si E est fini, on a alors un nombre fini d'orbites $G \cdot x_1, \cdots, G \cdot x_r$ qui forment une partition de E et :

$$\operatorname{card}(E) = \sum_{i=1}^{r} \operatorname{card}(G \cdot x_i).$$

En utilisant la bijection de G/G_x sur $G \cdot x_i$, on déduit que si G est aussi fini, on a alors :

$$\operatorname{card}(E) = \sum_{i=1}^{r} \frac{\operatorname{card}(G)}{\operatorname{card}(G_{x_i})}.$$

■

Si $(G, \cdot)$ est un groupe opérant sur un ensemble E, on note alors :

$$E^G = \{x \in E \mid G \cdot x = \{x\}\}$$

C'est l'ensemble des éléments de E dont l'orbite est réduite à un point.

En séparant dans la formule des classes les orbites réduites à un point des autres, elle s'écrit :

$$\operatorname{card}(E) = \operatorname{card}\left(E^G\right) + \sum_{\substack{i=1 \\ \operatorname{card}(G \cdot x_i) \geq 2}}^{r} \operatorname{card}(G \cdot x_i)$$

(la somme étant nulle si toutes les orbites sont réduites à un point).

Définition 1.6 *Si $p \geq 2$ est un nombre premier, on appelle* p**-groupe** *tout groupe de cardinal p^α où α est un entier naturel non nul.*

Corollaire 1.1 *Si $p \geq 2$ est un nombre premier et $(G, \cdot)$ est un p-groupe opérant sur un ensemble fini E, alors :*

$$\mathrm{card}\left(E^G\right) \equiv \mathrm{card}\,(E) \pmod{p}.$$

Démonstration. Dans le cas d'un p-groupe de cardinal p^α avec $\alpha \geq 1$, pour toute orbite $G \cdot x_i$ non réduite à un point (s'il en existe), on a :

$$\mathrm{card}\,(G \cdot x_i) = \mathrm{card}\left(\frac{G}{G_{x_i}}\right) = \frac{\mathrm{card}\,(G)}{\mathrm{card}\,(G_{x_i})} \geq 2$$

donc $\mathrm{card}\,(G_{x_i}) = p^{\beta_i}$ avec $0 \leq \beta_i < \alpha$ et $\mathrm{card}\,(G \cdot x_i) = p^{\alpha - \beta_i}$ avec $1 \leq \alpha - \beta_i \leq \alpha$. Il en résulte que :

$$\mathrm{card}\,(E) = \mathrm{card}\left(E^G\right) + \sum_{\substack{i=1 \\ \mathrm{card}(G \cdot x_i) \geq 2}}^{r} \mathrm{card}\,(G \cdot x_i) \equiv \mathrm{card}\left(E^G\right) \pmod{p}$$

■

Corollaire 1.2 *Soit G un groupe fini que l'on fait opérer sur lui même par conjugaison ($g \cdot h = ghg^{-1}$, pour $(g, h) \in G \times G$). En notant $G \cdot h_1, \cdots, G \cdot h_r$ toutes les orbites deux à deux distinctes, on a :*

$$\begin{aligned}
\mathrm{card}\,(G) &= \mathrm{card}\,(Z\,(G)) + \sum_{\substack{i=1 \\ \mathrm{card}(G \cdot h_i) \geq 2}}^{r} \mathrm{card}\,(G \cdot h_i) \\
&= \mathrm{card}\,(Z\,(G)) + \sum_{\substack{i=1 \\ \mathrm{card}(G \cdot h_i) \geq 2}}^{r} \frac{\mathrm{card}\,(G)}{\mathrm{card}\,(G_{h_i})}.
\end{aligned}$$

Démonstration. Une orbite $G \cdot h$ est réduite à $\{h\}$ si et seulement si $ghg^{-1} = h$ pour tout $g \in G$, ce qui revient à dire que $gh = hg$, ou encore que $h \in Z\,(G)$. On a donc $Z\,(G) = G^G$ et le résultat annoncé. ■

Théorème 1.4 *Pour tout nombre premier p, le centre d'un p-groupe n'est pas réduit à $\{1\}$.*

Démonstration. Soit G un p-groupe à p^α éléments.

On a, avec les notations des corollaires qui précèdent :

$$\mathrm{card}\,(Z\,(G)) = \mathrm{card}\left(G^G\right) \equiv \mathrm{card}\,(G) \pmod{p}$$

et comme $\mathrm{card}\,(Z\,(G)) \geq 1$, il en résulte que $\mathrm{card}\,(Z\,(G)) \geq p$ et $Z\,(G)$ est non trivial. ■

Théorème 1.5 *Tout groupe d'ordre p^2 avec p premier est commutatif.*

Démonstration. Soit G d'ordre p^2. On sait que $Z\,(G)$ est non trivial, il est donc de cardinal p ou p^2 et il s'agit de montrer qu'il est de cardinal p^2.

Si $Z\,(G)$ est de cardinal p, il est alors cyclique, soit $Z\,(G) = \langle g \rangle$.

Un élément h de $G \setminus Z\,(G)$ ne pouvant être d'ordre p^2 (sinon $G = \langle h \rangle$ et G serait commutatif ce qui contredit l'hypothèse $G \neq Z\,(G)$), il est d'ordre p et $Z\,(G) \cap \langle h \rangle = \{1\}$ (exercice **??**)

En utilisant l'application :

$$\begin{array}{cccc} \varphi : & \{0,1,\cdots,p-1\}^2 & \to & G \\ & (i,j) & \mapsto & g^i h^j \end{array}$$

nous déduisons que tout élément de G s'écrit de manière unique $g^i h^j$. Pour ce faire il suffit de montrer que φ est injective. Si $g^i h^j = g^{i'} h^{j'}$, alors $g^{i-i'} = h^{j'-j} \in Z(G) \cap \langle h \rangle = \{1\}$ et $g^{i-i'} = h^{j'-j} = 1$ ce qui entraîne que p divise $i-i'$ et $j-j'$ et comme $|i-i'| < p$, $|j-j'| < p$, on a nécessairement $i = i'$, $j = j'$. Avec les cardinaux il en résulte que φ est une bijection.

Si k, k' sont dans G, il s'écrivent $k = g^i h^j$ et $k' = g^{i'} h^{j'}$ et comme g commute à tout G, on en déduit que k et k' commutent. Le groupe G serait alors commutatif ce qui est contraire à l'hypothèse $G \neq Z(G)$.

En définitive $Z(G)$ ne peut être de cardinal p, il est donc de cardinal p^2 et G est commutatif.

■

Remarque 1.2 *Si G d'ordre p^2 a un élément d'ordre p^2, il est alors cyclique isomorphe à $\dfrac{\mathbb{Z}}{p^2\mathbb{Z}}$. Dans le cas où tous ses éléments sont d'ordre p, il est isomorphe à $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$.*

1.4 Le théorème de Cauchy

Soient G un groupe fini de cardinal $n \geq 2$, $p \geq 2$ un nombre premier et :

$$E = \{(g_1, \cdots, g_p) \in G^p \mid g_1 \cdots g_p = 1\}$$

Lemme 1.1 *Avec ces notations, on a :*

$$\mathrm{card}(E) = n^{p-1}.$$

Démonstration. L'application $(g_1, \cdots, g_{p-1}) \mapsto \left(g_1, \cdots, g_{p-1}, (g_1 \cdots g_{p-1})^{-1}\right)$ réalise une bijection de G^{p-1} sur E (de l'égalité $g_1 \cdots g_p = 1$, on déduit que la connaissance des g_i pour $1 \leq i \leq p-1$ détermine g_p de manière unique). On a donc :

$$\mathrm{card}(E) = n^{p-1}.$$

■

On désigne par $H = \langle \sigma \rangle$ le sous-groupe de $\mathcal{S}_p$ engendré par le p-cycle $\sigma = (1, 2, \cdots, p)$ et on fait agir H sur E par :

$$\left(\sigma^k, (g_1, \cdots, g_p)\right) \mapsto \left(g_{\sigma^k(1)}, \cdots, g_{\sigma^k(p)}\right)$$

Pour $g = (g_1, \cdots, g_p) \in E$, on a :

$$g_2 \cdots g_p g_1 = g_1^{-1} g_1 = 1$$

donc $\left(g_{\sigma(1)}, \cdots, g_{\sigma(p)}\right) = (g_2, \cdots, g_p, g_1) \in E$. Il en résulte que pour tout entier k compris entre 0 et $p-1$, $\left(g_{\sigma^k(1)}, \cdots, g_{\sigma^k(p)}\right) \in E$ et l'application :

$$\left(\sigma^k, (g_1, \cdots, g_p)\right) \mapsto \sigma^k \cdot (g_1, \cdots, g_p) = \left(g_{\sigma^k(1)}, \cdots, g_{\sigma^k(p)}\right)$$

est bien à valeurs dans E. Cette application définit bien une action puisque :

$$Id \cdot (g_1, \cdots, g_p) = (g_1, \cdots, g_p)$$

et

$$\begin{aligned} \sigma^j \cdot \left(\sigma^k \cdot (g_1, \cdots, g_p)\right) &= \sigma^j \cdot \left(g_{\sigma^k(1)}, \cdots, g_{\sigma^k(p)}\right) = \left(g_{\sigma^{j+k}(1)}, \cdots, g_{\sigma^{k+j}(p)}\right) \\ &= \sigma^{j+k} \cdot (g_1, \cdots, g_p) = \left(\sigma^j \circ \sigma^k\right) \cdot (g_1, \cdots, g_p) \end{aligned}$$

Lemme 1.2 *Avec ces notations, on a :*

$$E^H = \{x \in E \mid H \cdot x = \{x\}\} \neq \emptyset$$

et $\mathrm{card}\left(E^H\right)$ *est divisible par* p *si* p *est un diviseur premier de* n.

Démonstration. En remarquant que $x = (1, \cdots, 1)$ est dans E^H, on déduit que E^H est non vide.

Comme H est de cardinal p (un p-cycle est d'ordre p dans $\mathcal{S}_p$), on a :

$$\mathrm{card}\left(E^H\right) \equiv \mathrm{card}\,(E) \pmod{p}$$

(corollaire 1.1) avec $\mathrm{card}\,(E) = n^{p-1}$ divisible par p comme n, ce qui entraîne que $\mathrm{card}\left(E^H\right)$ est également divisible par p. ∎

Théorème 1.6 (Cauchy) *Si* G *est un groupe fini, alors pour tout diviseur premier* p *de son ordre* n, G *possède un élément d'ordre* p *(et donc un sous-groupe d'ordre* p*).*

Démonstration. On utilise les notations qui précèdent.

De $\mathrm{card}\left(E^H\right) \geq 1$ et $\mathrm{card}\left(E^H\right)$ divisible par p, on déduit que $\mathrm{card}\left(E^H\right) \geq p \geq 2$ et en remarquant que $x = (g_1, \cdots, g_p) \in E^H$ équivaut à dire que $g_1 = \cdots = g_p = g$ avec $g \in G$ tel que $g^p = 1$, on déduit qu'il existe $g \neq 1$ tel que $g^p = 1$, ce qui signifie que g est d'ordre p. ∎

Exercice 1.6 *Soit* $(G, \cdot)$ *est un groupe fini opérant sur un ensemble fini* E. *Pour tout* $g \in G$, *on note :*

$$\mathrm{Fix}\,(g) = \{x \in E \mid g \cdot x = x\}$$

Montrer que le nombre d'orbites est :

$$r = \frac{1}{\mathrm{card}\,(G)} \sum_{g \in G} \mathrm{card}\,(\mathrm{Fix}\,(g))$$

(formule de Burnside).

Solution 1.6 L'idée est de calculer le cardinal de l'ensemble :

$$F = \{(g, x) \in G \times E \mid g \cdot x = x\}$$

de deux manières en utilisant les partitions :

$$F = \bigcup_{g \in G} \{(g, x) \mid x \in \mathrm{Fix}\,(g)\} = \bigcup_{x \in E} \{(g, x) \mid g \in G_x\}$$

ce qui donne :

$$\mathrm{card}\,(F) = \sum_{g \in G} \mathrm{card}\,(\mathrm{Fix}\,(g))$$

et en notant $G \cdot x_1, \cdots, G \cdot x_r$ les orbites distinctes :

$$\begin{aligned} \mathrm{card}\,(F) &= \sum_{x \in E} \mathrm{card}\,(G_x) = \sum_{x \in E} \frac{\mathrm{card}\,(G)}{\mathrm{card}\,(G \cdot x)} \\ &= \sum_{i=1}^{r} \sum_{x \in G \cdot x_i} \frac{\mathrm{card}\,(G)}{\mathrm{card}\,(G \cdot x)} = \sum_{i=1}^{r} \mathrm{card}\,(G) \left(\sum_{x \in G \cdot x_i} \frac{1}{\mathrm{card}\,(G \cdot x)} \right) \\ &= \sum_{i=1}^{r} \mathrm{card}\,(G) \left(\sum_{x \in G \cdot x_i} \frac{1}{\mathrm{card}\,(G \cdot x_i)} \right) = \sum_{i=1}^{r} \mathrm{card}\,(G) = r\,\mathrm{card}\,(G) \end{aligned}$$

du fait que $G \cdot x = G \cdot x_i$ pour $x \in G \cdot x_i$ (la relation $x \sim y$ si $y = g \cdot x$ est d'équivalence et les classes d'équivalence sont les orbites). Ce qui donne le résultat annoncé.

1.5 Groupe des isométries laissant une partie invariante

On désigne par $\mathcal{E}$ un espace affine euclidien de dimension $n \geq 2$ et de direction E.

Pour A, B dans $\mathcal{E}$, on note $d(A, B) = \left\| \overrightarrow{AB} \right\|$ la distance de A à B.

On rappelle qu'une isométrie affine est une application affine $\varphi : \mathcal{E} \to \mathcal{E}$ telle que $d(\varphi(A), \varphi(B)) = d(A, B)$ pour tout couple (A, B) de points de $\mathcal{E}$.

Une application affine $\varphi : \mathcal{E} \to \mathcal{E}$ est une isométrie affine si, et seulement si, son application linéaire associée $\overrightarrow{\varphi} : \overrightarrow{AB} \mapsto \overrightarrow{\varphi(A)\varphi(B)}$ est une isométrie vectorielle de E.

On note $Is(\mathcal{E})$ le groupe des isométries de E, $Is^+(\mathcal{E})$ le sous-groupe des déplacements de $\mathcal{E}$ (i. e. des isométries telles que $\det(\overrightarrow{\varphi}) = 1$) et $Is^-(\mathcal{E})$ l'ensemble des antidéplacements de $\mathcal{E}$ (i. e. des isométries telles que $\det(\overrightarrow{\varphi}) = -1$).

Pour toute partie $\mathcal{P}$ de $\mathcal{E}$ ayant au moins 2 éléments, on note $Is(\mathcal{P})$ [resp. $Is^+(\mathcal{P}), Is^-(\mathcal{P})$] l'ensemble des isométries [resp. des déplacements, antidéplacements] φ de $\mathcal{E}$ qui conservent $\mathcal{P}$, c'est-à-dire telles [resp. tels] que $\varphi(\mathcal{P}) = \mathcal{P}$.

Si $\varphi \in Is(\mathcal{P})$, alors sa restriction à $\mathcal{P}$ est une permutation de $\mathcal{P}$.

Théorème 1.7 *Si $\mathcal{P}$ est une partie non vide de $\mathcal{E}$, alors :*

1. *$Is(\mathcal{P})$ est un sous-groupe de $Is(\mathcal{E})$ et $Is^+(\mathcal{P})$ est un sous-groupe distingué de $Is(\mathcal{P})$;*
2. *l'application Φ qui associe à $\varphi \in Is(\mathcal{P})$ sa restriction à $\mathcal{P}$ est un morphisme de groupes de $Is(\mathcal{P})$ dans $\mathcal{S}(\mathcal{P})$ (donc dans $\mathcal{S}_m$ si $\mathcal{P}$ est de cardinal m) ; dans le cas où $\mathcal{P}$ contient un repère affine de $\mathcal{E}$, Φ est injective et si $\mathcal{P}$ est un repère affine, alors $Is(\mathcal{P})$ est isomorphe à un sous-groupe de $\mathcal{S}_{n+1}$;*
3. *si $Is^-(\mathcal{P}) \neq \emptyset$, alors pour toute isométrie $\sigma \in Is^-(\mathcal{P})$, l'application $\rho \mapsto \sigma \circ \rho$ réalise une bijection de $Is^+(\mathcal{P})$ sur $Is^-(\mathcal{P})$; dans le cas où $\mathcal{P}$ est fini, on a $\operatorname{card}(Is(\mathcal{P})) = 2\operatorname{card}(Is^+(\mathcal{P}))$;*
4. *si $\mathcal{P}$ est fini, alors toute isométrie $\varphi \in Is(\mathcal{P})$ laisse fixe l'isobarycentre de $\mathcal{P}$.*

Démonstration.

1. On a $Id \in Is(\mathcal{P})$ et pour φ, ψ dans $Is(\mathcal{P})$, la composée $\varphi \circ \psi^{-1}$ est aussi dans $Is(\mathcal{P})$, donc $Is(\mathcal{P})$ est un sous-groupe de $Is(\mathcal{E})$ et $Is^+(\mathcal{P}) = Is(\mathcal{P}) \cap Is^+(\mathcal{E})$ un sous-groupe de $Is^+(\mathcal{E})$. Le groupe $Is^+(\mathcal{P})$ est distingué dans $Is(\mathcal{P})$ comme noyau du morphisme de groupes $\det : \varphi \in Is(\mathcal{P}) \to \det(\overrightarrow{\varphi}) \in \{-1, 1\}$ (on peut aussi dire que pour $\rho \in Is^+(\mathcal{P})$ et $\varphi \in Is(\mathcal{P})$, $\varphi^{-1} \circ \rho \circ \varphi \in Is^+(\mathcal{P})$).
2. Une isométrie $\varphi \in Is(\mathcal{P})$ reste injective sur $\mathcal{P}$ et elle est surjective de $\mathcal{P}$ sur $\mathcal{P}$ puisque $\varphi(\mathcal{P}) = \mathcal{P}$, c'est donc une permutation de $\varphi(\mathcal{P}) = \mathcal{P}$. Il est clair que l'application $\Phi : \varphi \mapsto \varphi_{|\mathcal{P}}$ est un morphisme de groupes.
   Si $\mathcal{P}$ contient un repère affine $(A_i)_{0 \leq i \leq n}$ de $\mathcal{E}$, l'application Φ est alors injective du fait que l'égalité $\varphi_{|\mathcal{P}} = \psi_{|\mathcal{P}}$ entraîne $\varphi(A_i) = \psi(A_i)$ pour tout i compris entre 0 et n et $\varphi = \psi$ puisque ces applications affines coïncident sur un repère affine. Dans le cas où $\mathcal{P} = \{A_0, \cdots, A_n\}$, Φ réalise un isomorphisme de $Is(\mathcal{P})$ sur $\mathcal{S}_{n+1}$.
3. Pour $\sigma \in Is^-(\mathcal{P})$, l'application $\Psi : \rho \mapsto \sigma \circ \rho$ est clairement injective de $Is^+(\mathcal{P})$ sur $Is^-(\mathcal{P})$ et pour tout $\sigma' \in Is^-(\mathcal{P})$, $\rho = \sigma^{-1} \circ \sigma' \in Is^+(\mathcal{P})$ est un antécédent de σ'. L'application Ψ est donc bijective. En utilisant la partition $Is(\mathcal{P}) = Is^+(\mathcal{P}) \cup Is^-(\mathcal{P})$, on en déduit dans le cas où $\mathcal{P}$ est fini que $\operatorname{card}(Is(\mathcal{P})) = 2\operatorname{card}(Is^+(\mathcal{P}))$.
4. Si $\mathcal{P} = \{A_1, \cdots, A_m\}$, tout application $\varphi \in Is(\mathcal{P})$ qui est affine va transformer l'isobarycentre O de $\mathcal{P}$ en l'isobarycentre de $\varphi(\mathcal{P}) = \mathcal{P}$ et nécessairement $\varphi(O) = O$.

■

Remarque 1.3 *On déduit du point 3. du théorème précédent que $Is(\mathcal{P}) = Is^+(\mathcal{P})$ s'il n'y a pas d'antidéplacement qui conserve $\mathcal{P}$ et que $Is(\mathcal{P}) = Is^+(\mathcal{P}) \cup (\sigma \circ Is^-(\mathcal{P}))$ s'il existe un antidéplacement σ qui conserve $\mathcal{P}$.*

Remarque 1.4 *On déduit du point 4. du théorème précédent que dans le cas où $\mathcal{P}$ est fini, l'étude de $Is(\mathcal{P})$ se ramène à une étude analogue dans l'espace vectoriel euclidien E.*
Dans le cas où $\mathcal{E}$ est un plan affine, une isométrie distincte de l'identité laissant fixe une partie finie d'isobarycentre O est soit une rotation de centre O, soit une réflexion d'axe passant par O.

Exercice 1.7 *Soit $\mathcal{P} = \{A_1, \cdots, A_m\}$ une partie finie du plan euclidien avec $m \geq 2$. Montrer que* $\operatorname{card}(Is^{\pm}(\mathcal{P})) \leq m$ *et* $\operatorname{card}(Is(\mathcal{P})) \leq 2m$.

Solution 1.7 Les éléments de $Is^+(\mathcal{P})$ sont des rotations de centre l'isobarycentre O de $\mathcal{P}$ et une telle rotation est uniquement déterminée par l'image d'un point fixé $A_k \neq O$ de $\mathcal{P}$, ce qui donne un maximum de m possibilités. On a donc $\operatorname{card}(Is^+(\mathcal{P})) \leq m$. Si $Is^-(\mathcal{P}) = \emptyset$, on a alors $\operatorname{card}(Is(\mathcal{P})) = \operatorname{card}(Is^+(\mathcal{P})) \leq m$, sinon on a $\operatorname{card}(Is(\mathcal{P})) = 2\operatorname{card}(Is^+(\mathcal{P})) \leq 2m$.

Exercice 1.8 *Montrer que le groupe des isométries du plan affine euclidien qui conservent les sommets d'un vrai triangle isocèle non équilatéral est isomorphe à $\mathcal{S}_2$.*

Solution 1.8 On note $\mathcal{P}$ le plan affine euclidien et on se donne un vrai triangle isocèle non équilatéral T de sommets A_1, A_2, A_3 avec $A_1A_2 = A_1A_3$ (figure 1.1).On note $Is(T)$ le groupe

FIGURE 1.1 –

des isométries de $\mathcal{P}$ qui conservent $E = \{A_1, A_2, A_3\}$.
Soit $\varphi \in Is(T)$. Par conservation des barycentres, on a $\varphi(O) = O$, en désignant par O le centre de gravité du triangle (l'isobarycentre de E) et $\varphi([A_2A_3])$ est un coté du triangle de même longueur que $[A_2A_3]$, c'est donc $[A_2A_3]$ puisque le triangle est non équilatéral et isocèle en A_1. On a donc $\varphi(\{A_2A_3\}) = \{A_2, A_3\}$ et nécessairement $\varphi(A_1) = A_1$. Si $\varphi(A_2) = A_2$, alors $\varphi = Id$ puisque ces deux applications coïncident sur le repère affine (O, A_1, A_2). Si $\varphi(A_2) = A_3$, alors φ est la réflexion σ d'axe (OA_1), la médiatrice de $[A_2A_3]$, puisque ces deux applications coïncident sur le repère affine (O, A_1, A_2). On a donc $Is(T) = \{Id, \sigma\} = \mathcal{S}(\{A_2, A_3\})$ qui est isomorphe à $\mathcal{S}_2$.