158 Groupe opérant sur un ensemble. Exemples et applications.

Notations : $(G, \times)$ un groupe de neutre 1_G.
E un ensemble non vide.
$(S(E), \circ)$ le groupe des permutations sur E.

Références : Skandalis, p. 8–11
Gourdon, p. 21–22
Rombaldi, p. 19–23

Définition : G opère (à gauche) sur E s'il existe une application :

$$\cdot : \begin{array}{rcl} G \times E & \longrightarrow & E \\ (g, x) & \longmapsto & g \cdot x \end{array}$$

telle que :

→ $\forall x \in E, \ 1_G \cdot x = x$ (1)

→ $\forall (g, g') \in G, \forall x \in E$:
$g \cdot (g' \cdot x) = (g \times g') \cdot x$ (2)

Une telle application est appelée action ou opération de G sur E.

Définition alternative / Propriété :
Une action de G sur E est un morphisme de groupes :

$$\varphi : \begin{array}{rcl} (G, \times) & \longrightarrow & (S(E), \circ) \\ g & \longmapsto & \begin{array}{rcl} E & \longrightarrow & E \\ x & \longmapsto & \varphi(g)(x) \end{array} \end{array}$$

On peut alors noter :
$$g \cdot x = \varphi(g)(x).$$

Preuve :

* Si on a une action $\cdot$ de G sur E, alors :

$\forall g \in G$, l'application $m_g : \begin{array}{rcl} E & \longrightarrow & E \\ x & \longmapsto & m_g(x) = g \cdot x \end{array}$ est bijective :

$$\begin{aligned} \forall y \in E : \quad m_g^{-1}(\{y\}) &= \{x \in E \mid m_g(x) = y\} \\ &= \{x \in E \mid g \cdot x = y\} \quad \text{G gpe} \\ &= \{x \in E \mid g^{-1} \cdot (g \cdot x) = g^{-1} \cdot y\} \quad (2) \\ &= \{x \in E \mid (g^{-1} \times g) \cdot x = g^{-1} \cdot y\} \\ &= \{x \in E \mid 1_G \cdot x = g^{-1} \cdot y\} \quad (1) \\ &= \{x \in E \mid x = g^{-1} \cdot y\} \\ &= \{g^{-1} \cdot y\} \end{aligned}$$

qui est de cardinal 1.

* Réciproquement, si $\varphi : G \to S(E)$ est un morphisme alors si on pose $\forall g \in G, \forall x \in E, \ g \cdot x = \varphi(g)(x)$ alors :

→ $\forall x \in E, \ 1_G \cdot x = \varphi(1_G)(x) = id(x) = x$
φ morphisme

→ $\forall g, g' \in G, \forall x \in E, \ g \cdot (g' \cdot x) = g \cdot (\varphi(g')(x)) = \varphi(g) \circ \varphi(g')(x) = \varphi(g \times g')(x)$
$= (g \times g') \cdot x$

Exemples :

- S_n agit sur $\{1,\dots,n\}$
- Translation à gauche : G agit sur lui-m̂ : $g\cdot h = gh \ \forall g,h \in G$
- Conjugaison : H ss-gpe distingué de G :

$$\begin{aligned} G\times H &\longrightarrow H \\ (g,h) &\longmapsto g\cdot h = ghg^{-1} \quad (\in H \text{ car } H \text{ distingué}). \end{aligned}$$

Définition : Une action de G sur E est fidèle si le morphisme associé $g \mapsto m_g$ est injectif.

ie :

$$\left.\begin{array}{l} g\in G \\ \forall x\in E,\ g\cdot x = x \end{array}\right\} \Leftrightarrow g = 1_G$$

Ex : $E=\mathbb{C}$ et $G=\{id, r\}$ avec $r=$ réflexion d'axe (Ox) :

$$\begin{aligned} G\times\mathbb{C} &\longrightarrow \mathbb{C} \\ (g,z) &\longmapsto g\cdot z = g(z). \end{aligned}$$

$$\Rightarrow \varphi : \begin{aligned} G &\longrightarrow S(\mathbb{C}) \\ id &\longmapsto id \\ r &\longmapsto (z\mapsto \bar{z}) \neq id \end{aligned}$$

donc φ est injective, donc l'action est fidèle.

Définition : Si G agit sur E, on appelle orbite de x sous l'action de G ($\forall x\in E$) :

$$\Theta(x) = G\cdot x = \{g\cdot x \mid g\in G\}$$

Si $\forall x\in E$, $\Theta(x)=E$, on dit que l'action est transitive. (il y a une seule orbite)

Propriété :
L'ensemble des orbites forme une partition de E.

Preuve :
La relation suivante $x\sim y \Leftrightarrow y\in\Theta(x)$
$\Leftrightarrow \exists g\in G$ tq $y = g\cdot x$
est une relation d'équivalence :

→ $x = 1_G\cdot x$ donc $x\in\Theta(x)$ donc $x\sim x$
donc $\sim$ est réflexive.

→ $x\sim y \Rightarrow \exists g\in G$ tq $y = g\cdot x$
$\Rightarrow \exists g\in G$ tq $g^{-1}\cdot y = g^{-1}\cdot(g\cdot x) = (g^{-1}g)\cdot x = 1_G x = x$
$\Rightarrow x\in\Theta(y)$
$\Rightarrow y\sim x$
donc $\sim$ est symétrique.

→ $$\left.\begin{array}{l} x\sim y \\ y\sim z\end{array}\right\} \Rightarrow \left\{\begin{array}{l} \exists g\in G \text{ tq } y = g\cdot x \\ \exists h\in G \text{ tq } z = h\cdot y\end{array}\right\} \Rightarrow \exists g,h\in G \text{ tq : } \begin{aligned} z &= h\cdot(g\cdot x) \\ &= (hg)\cdot x \end{aligned}$$

$\Rightarrow x\sim z \Rightarrow \sim$ est transitive.

Donc les orbites sont les classes d'équivalence pour $\sim$. ☒

Thm de Cayley :

Tout groupe d'ordre n est isomorphe à un sous-groupe de S_n.

Preuve :

Si G est d'ordre n.

1) G est isomorphe à un sous-groupe de $S(G)$:

Prenons l'action de multiplication à gauche :

$$G \times G \longrightarrow G$$
$$(g, h) \longmapsto g \cdot h = gh$$

Pour $g \in G$ on a $g \cdot h = gh = h \ \forall h \in G$ ssi $g = 1$ donc le morphisme associé est injectif.

On construit la surjection en restreignant l'espace d'arrivée et on a bien la bijection entre G et un sous-groupe de $S(G)$.

2) $S(G)$ est isomorphe à S_n :

→ On numérote les éléments de $G = \{g_i \mid i \in [\![1; n]\!]\}$.
$N(g_i) = i \Rightarrow N$ est une bijection.

→ $\forall f \in S(G)$, on pose $\varphi(f) = N \circ f \circ N^{-1}$
$\Rightarrow \varphi^{-1}(\sigma) = N^{-1} \circ \sigma \circ N$

→ φ est un isomorphisme.

☒

Définition : $\forall x \in E$, on appelle le stabilisateur de x sous l'action de G :

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

Si $\forall x \in E$, $G_x = \{1_G\}$ (tous les stabilisateurs sont triviaux), on dit que l'action ~~de~~ est libre.

Propriété :

libre $\Rightarrow$ fidèle.

Preuve : $\cdot$ est libre donc $\forall x \in E$, $G_x = \{1_G\}$.

$\Rightarrow \forall x \in E, \forall g \in G, \ g \cdot x = x \Leftrightarrow g = 1_G$

$\Rightarrow \cdot$ est fidèle.

☒

Propriété :

$\forall x \in E$: $\quad \mathrm{Card}(\mathcal{O}(x)) = [G : G_x] \overset{\text{si } G \text{ est fini}}{=} \dfrac{|G|}{|G_x|}$

Preuve : Soit $x \in E$. Posons : $\varphi : (G/G_x)_g \longrightarrow \mathcal{O}(x)$
$\qquad g G_x \longmapsto g \cdot x$

Montrons que φ est bijective :

* φ est surjective par construction.

$*$ Supposons $\varphi(g_1 G_x) = \varphi(g_2 G_x)$

$\Rightarrow g_1 \cdot x = g_2 \cdot x$

$\Rightarrow g_2^{-1} \cdot (g_1 \cdot x) = x$

$\Rightarrow (g_2^{-1} \cdot g_1) \cdot x = x$

$\Rightarrow g_2^{-1} \cdot g_1 \in G_x$

$\Rightarrow g_1 \in g_2 G_x$

$\Rightarrow \forall g \in G_x, \quad g_1 g \in g_2 G_x$

$\Rightarrow g_1 G_x \subseteq g_2 G_x$

Par symétrie on a $g_2 G_x \subseteq g_1 G_x$ donc $\varphi(g_1 G_x) = \varphi(g_2 G_x) \Rightarrow g_1 G_x = g_2 G_x$ donc φ est <u>injective</u>.

Comme φ est bijective on a $\mathrm{Card}(\Theta(x)) = \mathrm{Card}(G/G_x) = [G : G_x]$.

Dans le cas fini, le théorème de Lagrange nous donne l'égalité $[G : G_x] = \frac{|G|}{|G_x|}$.

$\boxtimes$

<u>Théorème</u> : <u>Formule des classes</u> :

Supposons E fini et $\mathcal{A} = \{\text{représentants des orbites}\}$.

Alors :

$$\mathrm{Card}(E) = \sum_{x \in \mathcal{A}} \frac{|G|}{|G_x|}$$

<u>Preuve</u> :

Les orbites forment une partition de E donc

$$\mathrm{Card}(E) = \sum_{x \in \mathcal{A}} \mathrm{Card}(\Theta(x)) \underset{\text{ppté ci-dessus}}{=} \sum_{x \in \mathcal{A}} [G : G_x] \underset{E \text{ fini} + \text{Lagrange}}{=} \sum_{x \in \mathcal{A}} \frac{|G|}{|G_x|}$$

$\boxtimes$

<u>Corollaire de la formule des classes</u> :

Soit $\mathcal{A}$ un ensemble de représentants des classes de conjugaison* ($\forall (g,x) \in G \times G$: $g \cdot x = g x g^{-1} \in G$), alors :

$$|G| = |Z(G)| + \sum_{x \in \mathcal{A}} \frac{|G|}{|Z(x)|}$$

* non réduites à 1 élément

<u>Définition/notation</u> : $\forall x \in G$:

- Centralisateur de x :
  $Z(x) = \{ g \in G \mid gx = xg \}$
- On a l'équivalence : pour l'action de conjugaison
  $x \in Z(G) \Leftrightarrow \Theta(x) = \{x\}$

<u>Preuve</u> :

Découle directement de l'équivalence ci-contre et du théorème.

$\boxtimes$

Application : p-groupes :

Définition : Soit $p \in \mathbb{P}$.
On appelle p-groupe tout groupe de cardinal p^α, $\alpha \in \mathbb{N}^*$.

$E^G = \{x \in E \mid \overset{,,\Theta(x)}{G \cdot x} = \{x\}\}$
ens. des élém^ts de E dont l'orbite est réduite à 1 élément.

Propriété : (*)
Soit $p \in \mathbb{P}$ et G un p-groupe opérant sur l'ens. fini E. Alors :
$\text{Card}(E^G) \equiv \text{Card}(E)\ [p]$

Preuve :
Notons $\{x_i\}_{i \in [\![1;r]\!]}$ les représentants des orbites, et $|G| = p^\alpha$, $\alpha \in \mathbb{N}^*$.

* Si $x_i \notin E^G$ alors :

$$\text{Card}(\Theta(x_i)) = \text{Card}(G/G_{x_i}) = \frac{|G|}{|G_{x_i}|} \geq 2$$

Car $|G_{x_i}| > 1$ car $x_i \notin E^G$.
De plus G_{x_i} est un sous groupe de G donc d'après le théorème de Lagrange : $|G_{x_i}| \mid |G|$
donc $|G_{x_i}| = p^{\beta_i}$ avec $0 \leq \beta_i < \alpha$.

$$\Rightarrow \text{Card}(\Theta(x_i)) = p^{\alpha - \beta_i} \text{ avec } 1 \leq \alpha - \beta_i \leq \alpha.$$

* On a alors (formule des classes) :

$$\text{Card}(E) = \text{Card}(E^G) + \sum_{\substack{i=1 \\ x_i \notin E^G}}^{r} p^{\alpha - \beta_i} \equiv \text{Card}(E^G)\ [p].$$

$\boxtimes$

Thm :
$\forall p \in \mathbb{P}$, le centre d'un p-groupe est non trivial.

Preuve :
Soit G un p-groupe, notons $|G| = p^\alpha$, $\alpha \in \mathbb{N}^*$.
D'après le corollaire de la formule des classes :

$$\text{Card}(G) = \underbrace{\text{Card}(Z(G))}_{= \text{Card}(G^G)} + \sum_{\substack{i=1 \\ x_i \notin G^G}}^{r} \frac{|G|}{|G_{x_i}|}$$

$$\Rightarrow \text{Card}(Z(G)) = \text{Card}(G^G) \overset{\text{ppté précédente}}{\equiv} \text{Card}(G)\ [p]$$
$$\equiv p^\alpha\ [p]$$

Or $1_G \in Z(G) \Rightarrow \text{Card}(Z(G)) \geq 1$
Donc $\text{Card}(Z(G)) \geq p \Rightarrow Z(G) \neq \{1_G\}$.

$\boxtimes$

Thm:
Tout groupe d'ordre p^2 avec $p \in \mathbb{P}$ est commutatif.

Preuve:
Soit G d'ordre p^2, $p \in \mathbb{P}$.
Pour montrer que G est commutatif, il faut mq $Z(G) = G$.
Or on sait que $Z(G)$ est non trivial (voir thm précédent) et que $|Z(G)| \mid |G|$ par le thm de Lagrange, donc $\underline{|Z(G)| \in \{p, p^2\}}$.
$\underline{\text{Il faut donc mq } |Z(G)| = p^2}$:
Supposons par l'absurde que $|Z(G)| = p$, c'est-à-dire que G n'est pas commutatif.

* $|Z(G)| = p \Rightarrow Z(G)$ est cyclique
$\Rightarrow \exists g \in G$ tq $\underline{Z(G) = \langle g \rangle}$.

Posons $\underline{h \in G \setminus Z(G)}$ (non vide car $|Z(G)| = p < p^2 = |G|$):
→ Si $ord(h) = p^2$ alors $G = \langle h \rangle$ et G est commutatif, ce qui contredit notre hypothèse.
Donc $\underline{ord(h) = p}$.

* $Z(G) \cap \langle h \rangle$ est un sous-gpe de $Z(G)$ donc $|Z(G) \cap \langle h \rangle| \in \{1; p\}$.
→ Si $|Z(G) \cap \langle h \rangle| = p$ alors $Z(G) \cap \langle h \rangle = Z(G)$ et $h \in Z(G)$, absurde car on a pris $h \in G \setminus Z(G)$
Donc $|Z(G) \cap \langle h \rangle| = p$, donc $\underline{Z(G) \cap \langle h \rangle = \{1_G\}}$.

* Soit $\varphi : [\![0; p-1]\!]^2 \longrightarrow G$
$(i,j) \longmapsto g^i h^j$

→ $\underline{\varphi \text{ est injective}}$ car:
$\varphi(i,j) = \varphi(i',j') \Rightarrow g^i h^j = g^{i'} h^{j'} \Rightarrow g^{i-i'} = h^{j'-j} \in Z(G) \cap \langle h \rangle$
$\Rightarrow \begin{cases} g^{i-i'} = 1_G \\ h^{j'-j} = 1_G \end{cases} \Rightarrow \begin{cases} p \mid i-i' \\ p \mid j'-j \end{cases} \Rightarrow \begin{cases} i = i' \\ j = j' \end{cases} \Rightarrow (i,j) = (i',j')$

$i, i', j, j' \in [\![0, p-1]\!] \Rightarrow \begin{cases} |i-i'| < p \\ |j'-j| < p \end{cases}$

Or $\text{Card}([\![0; p-1]\!]^2) = p^2 = |G| \Rightarrow \underline{\varphi \text{ est une bijection}}$.

Donc $\forall k, k' \in G$, $\exists (i, i', j, j') \in [\![0, p-1]\!]^4$ tq $\begin{cases} k = g^i h^j \\ k' = g^{i'} h^{j'} \end{cases}$

On $g \in Z(G)$ car $Z(G) = \langle g \rangle$, donc h et h' commutent. Donc G est commutatif, ce qui contredit l'hypothèse de départ.

Donc $|Z(G)| = p^2 \Rightarrow G = Z(G) \Rightarrow G$ est commutatif. ▨

Thm de Cauchy :

Soit G un gpe fini avec $|G| = m \geq 2$.
Pour tout $p \in \mathbb{P}$ tq $p \mid m$, $\exists g \in G$ tq $\mathrm{ord}(g) = p$.
(donc il existe un ss-gpe d'ordre p).

Preuve :

Soit G gpe fini avec $|G| = m \geq 2$.
Soit $p \in \mathbb{P}$, et $E = \{(g_1, \dots, g_p) \in G^p \mid g_1 \cdots g_p = 1_G\}$.

Lemme :
$\mathrm{Card}(E) = m^{p-1}$

Preuve :
$\varphi : (g_1, \dots, g_{p-1}) \longmapsto (g_1, \dots, g_{p-1}, (g_1 \cdots g_{p-1})^{-1})$
est bijective de $G^{p-1} \longrightarrow E$ car $g_1 \cdots g_p = 1_G$ détermine g_p de manière unique quand les $g_1, \dots, g_{p-1}$ sont fixés.
D'où $\mathrm{Card}(E) = \mathrm{Card}(G^{p-1}) = m^{p-1}$. ▨

* On note $\sigma = (1\ 2\ \cdots\ p)$ un p-cycle et on pose $H = \langle \sigma \rangle$ qui est donc un sous-groupe de S_p.

$\forall s \in H, \exists k \in [\![0;p]\!]$ tq $s = \sigma^k$.

H agit sur E ainsi :

$$\bullet : \begin{array}{ccc} H \times E & \longrightarrow & E \\ (\sigma^k, (g_1, \dots, g_p)) & \longmapsto & (g_{\sigma^k(1)}, \dots, g_{\sigma^k(p)}) \end{array}$$

→ $\forall g = (g_1, \dots, g_p) \in E$: $\left(\prod_{k=2}^{p} g_k\right) \cdot g_1 = g_1^{-1} g_1 = 1$

$\Rightarrow (g_{\sigma(k)})_{k \in [\![1;p]\!]} = (g_2, \dots, g_p, g_1) \in E$ aussi.

Donc $\forall k \in [\![0, p-1]\!]$: $(g_{\sigma^k(1)}, \dots, g_{\sigma^k(p)}) \in E$, donc $\bullet$ est bien à valeurs dans E.

$\rightarrow \sigma^j \cdot (\sigma^k \cdot (g_1, \dots, g_p)) = \sigma^j \cdot (g_{\sigma^k(1)}, \dots, g_{\sigma^k(p)})$

$= (g_{\sigma^{j+k}(1)}, \dots, g_{\sigma^{j+k}(p)})$

$= \sigma^{j+k} \cdot (g_1, \dots, g_p)$

$= (\sigma^j \circ \sigma^k) \cdot (g_1, \dots, g_p)$

Et $id \cdot (g_1, \dots, g_p) = (g_1, \dots, g_p)$
donc c'est bien une action.

Lemme :
Soit $E^H = \{x \in E \mid H \cdot x = \Theta(x) = \{x\}\}$.
E^H est non vide et $\mathrm{Card}(E^H)$ est divisible par p si p est un diviseur premier de m.

Preuve :
* $x = (1, \dots, 1) \in E^H$ car $\forall \sigma^k \in H$, $\sigma^k \cdot (1, \dots, 1) = (1, \dots, 1)$
  $\Rightarrow E^H \neq \emptyset$.
* $\mathrm{ord}(\sigma) = p$ dans S_p car σ est un p-cycle donc $|H| = |\langle \sigma \rangle| = p$ donc par la ppté (*) on a :
  $\mathrm{Card}(E^H) \equiv \mathrm{Card}(E)\ [p]$
* Or par le lemme précédent on a :
  $\mathrm{Card}(E) = m^{p-1}$.
  Or $p \mid m$ donc $p \mid m^{p-1}$ d'où $p \mid \mathrm{Card}(E)$ d'où $p \mid \mathrm{Card}(E^H)$.

Enfin :
E^H non vide $\Rightarrow \mathrm{Card}(E^H) \geq 1$, et $p \mid \mathrm{Card}(E^H)$
$\Rightarrow \mathrm{Card}(E^H) \geq p \geq 2$.

Or $(g_1, \dots, g_p) \in E^H \Leftrightarrow g_1 = \dots = g_p = g$ avec $g \in G$ tq $g^p = 1$.
Donc $\exists g \neq 1$ tel que $g^p = 1$, d'où $\mathrm{ord}(g) = p$. ☒

Résumé de la preuve : Poser l'ens. E.
* $\rightarrow$ Lemme 1 : $\mathrm{card}(E) = m^{p-1}$ par bijection
* $\rightarrow$ Poser H et vérifier l'action de H sur E.
* $\rightarrow$ Lemme 2 : Poser E^H et vérifier $p \mid \mathrm{Card}(E^H) \geq 1$.
* $\rightarrow$ Conclure avec E^H.

Thm : Formule de Burnside :

Si G et E sont finis. Notons $Fix(g) = \{x \in E \mid g \cdot x = x\}$, et $\Theta = \{\Theta(x) \mid x \in E\}$ l'ensemble des orbites. Alors :

$$|\Theta| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$$

Preuve :

Calculons de 2 manières le cardinal de l'ensemble :

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

* $$Card(F) = \sum_{g \in G} Card(\{x \in E \mid g \cdot x = x\}) = \sum_{g \in G} |Fix(g)|.$$

* $$Card(F) = \sum_{x \in E} Card(\{g \in G \mid g \cdot x = x\})$$

$$= \sum_{x \in E} Card(G_x)$$

$Card(\Theta(x)) = \dfrac{|G|}{|G_x|}$

$$= \sum_{x \in E} \frac{|G|}{Card(\Theta(x))}$$

$$= \sum_{\Theta(x) \in \Theta} \sum_{y \in \Theta(x)} \frac{|G|}{|\Theta(x)|}$$

$$= \sum_{\Theta(x) \in \Theta} \left[\frac{|G|}{|\Theta(x)|} \cdot \sum_{y \in \Theta(x)} 1 \right] = \sum_{\Theta(x) \in \Theta} \frac{|G|}{\cancel{|\Theta(x)|}} \times \cancel{|\Theta(x)|}$$

$$= |G| \cdot \sum_{\Theta(x) \in \Theta} 1 = |G| \times |\Theta).$$

Au final : $|G| \times |\Theta| = \sum_{g \in G} |Fix(g)|$, d'où le résultat recherché. ▨

Application : Combien peut-on faire de colliers avec 4 perles bleues, 3 blanches et 2 oranges ?

- G = gpe diédral d'ordre 18.
- E = {colorations des 9 perles}
- Chaque orbite correspond à une coloration (à rotation/réflexion près).
- Burnside : $|\Theta| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)| = \frac{1260 + 0 \times 8 + 12 \times 9}{18} = \boxed{76}$:

- $g = id \Rightarrow |Fix(g)| = \binom{9}{4} \times \binom{5}{3} \times \binom{2}{2} = 1260$ colorat$^{\circ}$s fixes.
- 8 autres rotations : pas de colorat$^{\circ}$ fixe $\Rightarrow |Fix(g)| = 0$
- 9 réflexions : 1 blanche sur axe $\Rightarrow |Fix(g)| = \binom{4}{2}\binom{2}{1} = 12$.