ACTION D'UN GROUPE SUR UN ENSEMBLE

1. Définition

Définition. Soit $(G, \cdot)$ un groupe d'élément neutre e et soit E un ensemble. On appelle *action* (ou *opération*) de G sur E la donnée d'une application

$$\begin{array}{rcl} G \times E & \to & E \\ (g, x) & \mapsto & g * x \end{array}$$

vérifiant les conditions suivantes :

(1) $e * x = x$ pour tout $x \in E$ (l'élément neutre du groupe agit trivialement) ;

(2) $g * (h * x) = (g \cdot h) * x$ pour tous $g, h \in G$, $x \in E$ (compatibilité entre action et loi interne du groupe).

Exemples. (a) Le groupe $(\mathrm{GL}_n(\mathbb{R}), \times)$ des matrices de taille n inversibles agit sur l'ensemble $E = \mathcal{M}_{n,p}(\mathbb{R})$ des matrices de format (n, p) par multiplication : lorsque $P \in \mathrm{GL}_n(\mathbb{R})$ et $A \in \mathcal{M}_{n,p}(\mathbb{R})$, on pose $P * A = PA$.

[Pour tout $A \in \mathcal{M}_{n,p}(\mathbb{R})$, on a bien $I_2 * A = I_2 A = A$, et pour tous $P, Q \in \mathrm{GL}_n(\mathbb{R})$: $P * (Q * A) = P(QA) = (PQ)A = (PQ) * A$ par associativité du produit matriciel.]

(b) Le groupe $G = \mathrm{GL}_p(\mathbb{R})$ agit sur l'ensemble $E = \mathcal{M}_{n,p}(\mathbb{R})$ par multiplication à droite combinée avec inverse : pour $P \in \mathrm{GL}_p(\mathbb{R})$ et $A \in \mathcal{M}_{n,p}(\mathbb{R})$, on pose $P * A = AP^{-1}$.

[On a $I_2 * A = AI_2^{-1} = A$ et $P * (Q * A) = (AQ^{-1})P^{-1} = A(Q^{-1}P^{-1}) = A(PQ)^{-1} = (PQ) * A$.]

En posant $P *' A = A({}^tP)$, on obtient pareillement une action.

En revanche, la définition $P *'' A = AP$ (où on ne combine pas la multiplication à droite avec l'inverse ni avec la transposée) ne donne pas lieu à une action, car en général $P *'' (Q *'' A) = AQP = (QP) *'' A$ ne coïncide pas avec $(PQ) *'' A = APQ$.

(c) On peut combiner les exemples précédents : le groupe $G = \mathrm{GL}_n(\mathbb{R})$ agit sur l'ensemble $\mathcal{M}_n(\mathbb{R})$ par conjugaison : pour $P \in \mathrm{GL}_n(\mathbb{R})$ et $A \in \mathcal{M}_n(\mathbb{R})$, on pose $P * A = PAP^{-1}$.

(d) Le groupe des permutations $(\mathfrak{S}_n, \circ)$ agit naturellement sur l'ensemble des entiers $E = \{1, \ldots, n\}$: pour $\sigma \in \mathfrak{S}_n$ et $i \in \{1, \ldots, n\}$, on pose $\sigma * i = \sigma(i)$.

Le même groupe agit aussi sur l'ensemble $E' = \{1, \ldots, n\} \times \{1, \ldots, n\}$ des couples d'entiers : on pose $\sigma * (i, j) = (\sigma(i), \sigma(j))$.

(e) On a aussi une action de $G = \mathfrak{S}_n$ sur l'ensemble $E = \mathcal{M}_{n,p}(\mathbb{R})$ des matrices que l'on peut définir à l'aide de la matrice de permutation M_σ : pour $\sigma \in \mathfrak{S}_n$ et $A \in \mathcal{M}_{n,p}(\mathbb{R})$, on pose $\sigma * A = M_\sigma A$.

[On a $\mathrm{id} * A = M_{\mathrm{id}} A = I_n A = A$ et, pour tous $\sigma, \sigma' \in \mathfrak{S}_n$, on a $\sigma * (\sigma' * A) = M_\sigma(M_{\sigma'} A) = (M_\sigma M_{\sigma'})A = M_{\sigma \circ \sigma'} A = (\sigma \circ \sigma') * A$ d'après les propriétés des matrices de permutations.]

Remarque : $M_\sigma A$ est obtenue en permutant les lignes de A : la $\sigma(i)$-ème ligne de $M_\sigma A$ est la i-ème ligne de A. En particulier si $p=1$, on obtient une action sur les n-uplets : $\sigma * \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\sigma^{-1}(1)} \\ \vdots \\ x_{\sigma^{-1}(n)} \end{pmatrix}$.

Conséquence de la définition. Dans la définition, on ne demande pas de condition liée à l'inverse g^{-1} d'un élément g du groupe G. En revanche, la conditions requises dans la définition entraînent que pour tous $g \in G$, $x \in E$, on a :

$$(*) \qquad g^{-1} * (g * x) = (g^{-1}g) * x = e * x = x.$$

Autrement dit si on a $y = g * x$ alors on aura $x = g^{-1} * y$.

Reformulation de la définition. Étant donnée une action de G sur E, chaque $g \in G$ donne lieu à une application

$$f_g : E \to E,\ x \mapsto g * x.$$

De plus d'après $(*)$ ci-dessus, on a $f_{g^{-1}} \circ f_g = \mathrm{id}_E$ et pareillement (en remplaçant g par g^{-1} dans la formule précédente) $f_g \circ f_{g^{-1}} = \mathrm{id}_E$. Ainsi f_g est une bijection de E dans E.

L'ensemble $\mathrm{Bij}(E)$ des bijections de E dans E est un groupe pour l'opération $\circ$. Pour tous $g, h \in G$ et $x \in E$, la condition (2) de la définition d'action de groupe entraîne :

$$f_g \circ f_h(x) = g * (h * x) = (gh) * x = f_{gh}(x)$$

ce qui donne : $f_g \circ f_h = f_{gh}$. Il résulte que $\varphi : G \to \mathrm{Bij}(E)$, $g \mapsto f_g$ est un morphisme de groupes.

En fait se donner une action de G sur E revient à se donner un morphisme de groupes de G vers le groupe $(\mathrm{Bij}(E), \circ)$.

2. Notions d'orbites et stabilisateurs

Soit G un groupe agissant sur un ensemble E.

Définition. Soit $x \in E$.

(a) On appelle *orbite de x sous l'action de G* l'ensemble $G * x = \{g * x : g \in G\}$. Il s'agit d'un sous-ensemble de E.

(b) On appelle *stabilisateur de x sous l'action de G* l'ensemble $S_x = \{g \in G : g * x = x\}$. Il s'agit d'un sous-ensemble de G.

Remarque. L'orbite $G * x$ contient toujours x, en particulier elle est toujours non vide. Le stabilisateur S_x contient toujours e, en particulier il est toujours non vide.

Exemples. (a) Considérons $G = \mathfrak{S}_3 = \{\mathrm{id}, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$ et son action naturelle sur $E = \{1,2,3\}$. On a alors $G * 1 = G * 2 = G * 3 = \{1,2,3\}$ et $S_1 = \{\mathrm{id}, (2\,3)\}$, $S_2 = \{\mathrm{id}, (1\,3)\}$, $S_3 = \{\mathrm{id}, (1\,2)\}$.

(b) Considérons à présent l'action de $G = \mathfrak{S}_3$ sur $E' = \{1,2,3\} \times \{1,2,3\}$. Alors $G * (1,2) = \{(i,j) : 1 \leq i \neq j \leq 3\}$, $S_{(1,2)} = \{\mathrm{id}\}$, tandis que $G * (1,1) = \{(1,1), (2,2), (3,3)\}$, $S_{(1,1)} = \{\mathrm{id}, (2\,3)\}$.

Propriété. Pour tout $x \in E$, le stabilisateur S_x est un sous-groupe de G.

Démonstration. Comme $e * x = x$ alors $e \in S_x$. Si $g, h \in S_x$, alors $(gh) * x = g * (h * x) = g * x = x$ donc $gh \in S_x$. Enfin si $g \in S_x$, alors $g^{-1} * x = g^{-1} * (g * x) = (g^{-1} g) * x = e * x = x$ donc $g^{-1} \in S_x$. $\square$

Propriété/Définition. Pour $x, y \in E$, on pose $x \sim y$ s'il existe $g \in G$ tel que $g * x = y$. On obtient alors une relation d'équivalence sur E, appelée *relation d'intransitivité*.

De plus, on a $\overline{x} = G * x$ (la classe d'équivalence de x coïncide avec l'orbite de x).

Démonstration. On montre d'abord que $\sim$ est une relation d'équivalence :

(1) Comme $e * x = x$ alors $x \sim x$ pour tout $x \in E$. La relation est donc réflexive.

(2) Si $x \sim y$ alors il existe $g \in G$ tel que $g * x = y$, ce qui entraîne $g^{-1} * y = x$, et donc $y \sim x$. La relation est donc symétrique.

(3) Si $x \sim y$ et $y \sim z$, alors il existe $g, h \in G$ tels que $g * x = y$ et $h * y = z$ et donc $(hg) * x = h * (g * x) = h * y = z$, d'où $x \sim z$. La relation est donc transitive.

On justifie ensuite la dernière égalité de l'énoncé : $\overline{x} = \{y \in E : x \sim y\} = \{y \in E : \exists g \in G,\ g * x = y\} = \{g * x : g \in G\} = G * x$. $\square$

Conséquences. (1) Les orbites forment une partition de l'ensemble E.

(2) Deux orbites sont soit disjointes, soit égales.

(3) Si $y \in G * x$ alors on a $G * x = G * y$.

Définition. Une action est dite *transitive* si elle n'admet qu'une seule orbite, ce qui revient à dire que pour tout couple (x, y) d'éléments de E, il existe toujours un élément $g \in G$ tel que $g * x = y$.

Remarque. L'action est donc transitive lorsque la relation d'intransitivité est "triviale", c'est-à-dire telle que $x \sim y$ pour tous $x, y \in E$.

Dans l'exemple (a) ci-dessus, l'action est transitive. Mais pas dans l'exemple (b) : E est alors la réunion disjointe des deux orbites $G * (1, 2)$ et $G * (1, 1)$. Au vu de la conséquence (3) ci-dessus, on peut aussi affirmer que $G * (1, 2) = G * (i, j)$ pour tout couple (i, j) pour lequel $i \neq j$. Et pareillement $G * (1, 1) = G * (2, 2) = G * (3, 3)$.

3. Cas d'un groupe fini agissant sur un ensemble fini

On suppose désormais que G est un groupe fini agissant sur E un ensemble fini. On note par $\mathrm{card}(E)$ le cardinal de E. On rappelle que dans le cas d'un groupe le cardinal est aussi appelé ordre de G, et on note $|G| = \mathrm{card}(G)$.

Pour $x \in E$, le stabilisateur S_x étant un sous-groupe de G, on sait que $|S_x|$ divise $|G|$ (par le théorème de Lagrange). On peut être cependant plus précis :

Propriété. Pour tout $x \in E$, on a : $|G| = |S_x| \times \mathrm{card}(G * x)$.

Démonstration. On note $G * x = \{x_1, x_2, \ldots, x_k\}$ où $k = \mathrm{card}(G * x)$. Par définition de $G * x$, pour tout $i \in \{1, \ldots, k\}$ il existe $g_i \in G$ tel que $g_i * x = x_i$. On considère l'application

$$f : G \to G * x = \{x_1, \ldots, x_k\},\ g \mapsto g * x$$

qui est bien définie et surjective, par définition de $G * x$.

Pour tout $i \in \{1, \ldots, k\}$ on note $G_i = f^{-1}(\{x_i\}) = \{g \in G : f(g) = x_i\}$ l'ensemble des antécédents de x_i par f. Clairement les ensembles $G_1, \ldots, G_k$ sont deux-à-deux disjoints et leur réunion est G, donc $|G| = |G_1| + \ldots + |G_k|$. On affirme que $\mathrm{card}(G_i) = |S_x|$ pour tout $i \in \{1, \ldots, k\}$. Si cela est vrai, alors il résulte :

$|G| = |S_x| \times k = |S_x| \times \mathrm{card}(G * x)$. Il reste donc à justifier cette affirmation pour que la démonstration soit complète.

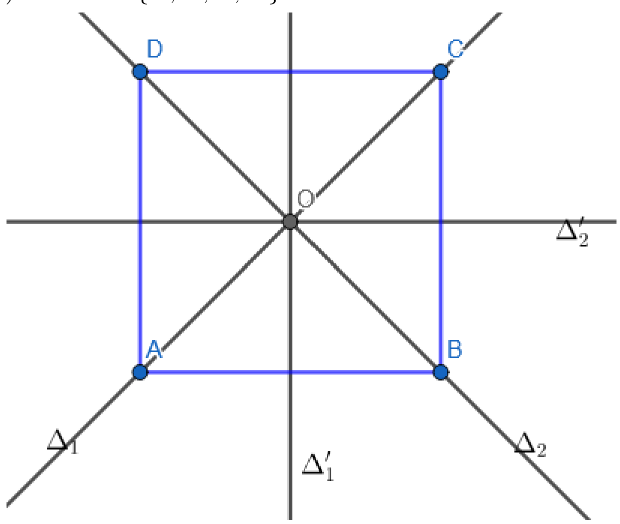
Pour $g \in G$, on a

$$g \in G_i \Leftrightarrow g * x = x_i \Leftrightarrow g * x = g_i * x \Leftrightarrow (g_i^{-1} g) * x = x \Leftrightarrow g_i^{-1} g \in S_x.$$

On obtient donc que l'application $\phi : G_i \to S_x,\ g \mapsto g_i^{-1} g$ qui est bien définie et bijective, de réciproque $\psi : S_x \to G_i,\ h \mapsto g_i h$. Donc $\mathrm{card}(G_i) = |S_x|$ comme affirmé. □

Remarque. La propriété entraîne donc que, non seulement l'ordre du stabilisateur S_x divise l'ordre du groupe G, mais en plus le cardinal de toute orbite $G*x$ divise $|G|$.

Exemples. (a) Soit $E = \{A, B, C, D\}$ l'ensemble des sommets d'un carré.



On considère le groupe diédral G formé par les transformations affines du plan qui préservent ce carré :

$$G = \{\mathrm{id}, r_{\pi/2}, r_\pi, r_{3\pi/2}, s_{\Delta_1}, s_{\Delta_2}, s_{\Delta_1'}, s_{\Delta_2'}\}.$$

Le groupe G ayant 8 éléments, une orbite pour une action de G sera toujours de cardinal 1, 2, 4 ou 8.

On considère l'action naturelle de G sur E. On a alors $G * A = \{A, B, C, D\}$ et $S_A = \{\mathrm{id}, s_{\Delta_1}\}$. Dans ce cas l'action est transitive.

On considère ensuite l'action de G sur l'ensemble E' des couples de sommets distincts : $E' = \{(A, B), (B, A), (A, C), (C, A), (A, D), (D, A), (B, C), (C, B), (B, D), (D, B), (C, D), (D, C)\}$. Dans ce cas, l'action ne peut pas être transitive puisque le cardinal d'une orbite est au plus 8 tandis que E' a 12 éléments. On a en fait que E' est la réunion de deux orbites : la première

$$G * (A, B) = \{(A, B), (B, A), (B, C), (C, B), (C, D), (D, C), (D, A), (A, D)\}$$

est formée par les couples de sommets situés sur un côté du carré ; on a $S_{(A,B)} = \{\mathrm{id}\}$. La seconde

$$G * (A, C) = \{(A, C), (C, A), (B, D), (D, B)\}$$

est formée par les couples de sommets diagonalement opposés ; on a $S_{(A,C)} = \{\mathrm{id}, s_{\Delta_1}\}$.