

§4 Groupe opérant sur un ensemble

1. Définition.

On dit qu'un groupe G opère à gauche sur un ensemble E , si l'on définit une loi externe $G \times E \longrightarrow E$

$$(g, x) \longrightarrow g \cdot x$$

telle que
$$\begin{cases} g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x \\ e \cdot x = x \end{cases}, \quad \forall g_1, g_2 \in G, \quad \forall x \in E$$

on dit alors que E est un G -ensemble.

2. Proposition.

La donnée d'une opération à gauche $(g, x) \longrightarrow g \cdot x$ du groupe G sur l'ensemble E équivaut à la donnée d'un homomorphisme $G \longrightarrow S(E)$ (où $S(E)$ le groupe des bijections de E).

Preuve: Si E est un G -ensemble, soit $T: G \longrightarrow S(E)$, $g \longrightarrow T(g) = T_g$ telle que $T_g: E \longrightarrow E, x \longrightarrow T_g(x) = g \cdot x$

T est un homomorphisme de groupes (à vérifier)

inversement, si $T: G \longrightarrow S(E)$ un homomorphisme, $g \longrightarrow T(g) = T_g$, on notera alors $\forall x \in E, T_g(x) = g \cdot x$, on a donc une opération à gauche de G sur E par l'application $G \times E \longrightarrow E, (g, x) \longmapsto T_g(x) = g \cdot x$

3. Exemples.

Soit G un groupe

1) G opère sur lui-même par translation à gauche :
 $\forall g \in G$ la translation à gauche $T_g: G \rightarrow G$
 $n \mapsto T_g(n) = g \cdot n = gn$, est une bijection de G sur G
 donc $G \rightarrow S(G)$, $g \mapsto T_g$, est un homomorphisme
 de groupes et par suite G opère sur lui-même par la
 loi $G \times G \rightarrow G$, $(g, n) \mapsto g \cdot n = gn$.

2) G opère sur lui-même par conjugaison :
 L'application $G \rightarrow S(G)$, $g \mapsto T_g$ telle
 que $T_g: G \rightarrow G$, $n \mapsto T_g(n) = g n g^{-1}$
 est un homomorphisme de groupes, donc G opère sur lui
 même par la loi $G \times G \rightarrow G$, $(g, n) \mapsto g \cdot n = g n g^{-1}$

3) G opère sur $\mathcal{H}$ l'ensemble des s/g de G par
 conjugaison :

L'application $T_g: \mathcal{H} \rightarrow \mathcal{H}$, $H \mapsto g H g^{-1}$
 est une bijection et l'application $G \rightarrow \mathcal{H}$

$g \mapsto T_g$ est un homomorphisme de groupes, donc
 G opère sur $\mathcal{H}$ par la loi $G \times \mathcal{H} \rightarrow \mathcal{H}$
 $(g, H) \mapsto g H g^{-1}$.

4) Soit H s/g de G , G opère sur $(\frac{G}{H})_g = \{nH / n \in G\}$
 l'ensemble des classes à gauche de G modulo H ,
 par translation à gauche :

G opère sur $(\frac{G}{H})_g$ par la loi $G \times (\frac{G}{H})_g \rightarrow (\frac{G}{H})_g$

$$(g, xH) \rightarrow (gu)H.$$

4. Soit G un groupe opérant sur un ensemble E . On considère la relation R dans E définie par:

$$x R y \Leftrightarrow (\exists g \in G / y = g \cdot x)$$

R est une relation d'équivalence sur E . Soit $x \in E$,

$\pi = \{g \cdot x / g \in G\}$ qu'on appelle orbite de x pour le groupe G et on la note Ω_x . L'ensemble noté $C_x = \{g \in G / g \cdot x = x\}$ est un sous groupe de G qu'on appelle stabilisateur de x dans G .

5. Proposition

Soit E un G -ensemble et soit Ω une orbite pour G . Si x et y sont dans Ω , alors les stabilisateurs C_x et C_y sont conjugués dans G .

Preuve:

Puisque x et y sont dans la même orbite, il existe $g \in G$ tel que $y = g \cdot x$, l'application $C_y \xrightarrow{\varphi} C_x$
 $g \mapsto g^{-1} g_1 g$ est un homomorphisme bijectif et par suite
 $C_x = \varphi(C_y) = g^{-1} C_y g$ c.q.f.d

6. Soit E un G -ensemble, $x \in E$ et $f_x: G \rightarrow E$

$g \mapsto g \cdot x$, $\theta: \frac{G}{C_x} \rightarrow f_x(G) = \Omega_x$
 la correspondance de $\frac{G}{C_x}$ définie par $\theta(\bar{g}) = f_x(g) = g \cdot x$

montrons que θ est une bijection

$$\bar{g}_1 = \bar{g}_2 \Leftrightarrow g_1^{-1} g_2 \in C_n \Leftrightarrow g_1^{-1} g_2 \cdot n = n$$

$$\Leftrightarrow g_2 \cdot n = g_1 \cdot n \Leftrightarrow \theta(\bar{g}_1) = \theta(\bar{g}_2)$$

donc θ est une application injective. Soit $g_1 \cdot n \in \Omega_n$ alors $\theta(\bar{g}_1) = g_1 \cdot n$ d'où θ est bijective.

Si le groupe G est fini on aura donc

$$\text{card } \Omega_n = \text{card} \left(\frac{G}{C_n} \right) = [G : C_n] = \frac{\text{card } G}{\text{card } C_n}$$

7. Exemple

Soit G un groupe opérant par conjugaison sur l'ensemble $\mathcal{H}$ de ses sous-groupes ($G \times \mathcal{H} \rightarrow \mathcal{H}$, $(g, H) \mapsto gHg^{-1}$). Soit $H \in \mathcal{H}$, l'orbite de H est $\Omega_H = \{gHg^{-1} / g \in G\}$ qui est l'ensemble des conjugués de H . Le stabilisateur de H est $\{g \in G / gHg^{-1} = H\} = N_G(H)$ = le normalisateur de H . Si G fini, on a $\text{card } \Omega_H = \text{card} \left(\frac{G}{N(H)} \right) = \frac{\text{card } G}{\text{card } N(H)}$

(ie) le nbre de sous-groupe conjugués de H est l'indice du normalisateur de H .

8. Soit E un G -ensemble. Si E est fini, chaque orbite est fini, soit P un sous-ensemble de E qui contient un élément et un seul de chaque orbite, les orbites

forment une partition de E , $\text{card } E = \sum_{n \in P} |\Omega_n| =$
 $= \sum_{n \in P} \frac{\text{card } G}{\text{card } C_n}$ Relation très importante dite
 "Equation des classes".

9. Exemple.

Soit G groupe fini qui opère sur lui-même par conjugaison
 $(G \times G \rightarrow G, (g, u) \rightarrow g u g^{-1})$ Soit $u \in G$,

$C_u = \{g \in G / g u g^{-1} = u\} = \{g \in G / g u = u g\}$
 le stabilisateur de u , on a

$u \in Z(G)$ centre de G ($\{a \in G / \forall y \in G: a y = y a\}$)

$(\Rightarrow) C_u = G \Leftrightarrow \text{card } \Omega_u = 1$

Soit P un sous ensemble de G , qui contient un élé et un seul
 de chaque orbite, $\forall u \in Z(G): \text{card } \Omega_u = 1$
 donc $\forall u \in Z(G), u \in P$ d'où $Z(G) \subseteq P$.

On a $P = Z(G) \cup (P - Z(G)) = Z(G) \cup P_1$

car $P_1 = P - Z(G)$

L'équation des classes s'écrit donc :

$$\text{card } G = \sum_{u \in P} \text{card } \Omega_u = \sum_{u \in Z(G)} \text{card } \Omega_u + \sum_{u \in P_1} \text{card } \Omega_u$$

$$= \text{card } Z(G) + \sum_{u \in P_1} \frac{\text{card } G}{\text{card } C_u}$$

$$\text{card } G = \text{card } Z(G) + \sum_{u \in P_1} \frac{\text{card } G}{\text{card } C_u}$$

10. Applications.

1) Si $\text{card } G = p^k$, $k \geq 1$, alors $Z(G) \neq \{e\}$
en effet: on a l'équation

$$\text{card } G = \text{card } (Z(G)) + \sum_{n \in P_1} [G : C_n]$$

$$(ie) \quad p^k = \text{card } Z(G) + \sum_{n \in P_1} [G : C_n]$$

$$\forall n \in P_1 : \text{card } C_n = [G : C_n] = \frac{\text{card } G}{\text{card } C_n} \neq 1$$

$$\text{Card } C_n \text{ divise } \text{card } G = p^k \text{ donc } \text{card } C_n \equiv 0 \pmod{p}$$
$$\text{donc } \text{card } Z(G) = p^k - \sum_{n \in P_1} \text{card } C_n \equiv 0 \pmod{p}$$

donc $Z(G) \neq \{e\}$.

2) Tout groupe fini d'ordre p^2 , p premier, est abélien.
en effet:

d'après 1) $\text{card } Z(G) \neq 1$ et divise $\text{card } G = p^2$
donc $\text{card } Z(G) = p$ ou p^2

si $\text{card } Z(G) = p^2$ alors $G = Z(G)$ abélien

si $\text{card } Z(G) = p$, on a $\frac{G}{Z(G)}$ est d'ordre p ($Z(G)$

est un s/g distingué de G) donc $\frac{G}{Z(G)}$ est cyclique
engendré par $\bar{x}$ avec $x \in G$.

Soient $a, b \in G$, $\bar{a} = \pi^n$ et $\bar{b} = \pi^m$, avec m et n dans $\mathbb{N}$, donc $a = \pi^n z_1$ et $b = \pi^m z_2$ où $z_i \in Z(G)$, $ab = \pi^n z_1 \pi^m z_2 = \pi^n (\pi^m z_1) z_2 = \pi^{n+m} z_1 z_2 = \pi^{m+n} z_2 z_1 = ba$ d'où G est abélien.

11. Proposition:

Soit G un groupe fini d'ordre p^k , p premier et $k \in \mathbb{N}^*$. Si G opère sur un ensemble fini E , en notant $E_G = \{x \in E / \forall g \in G: g \cdot x = x\}$, on a:

$$\text{Card}(E_G) \equiv \text{Card}(E) \pmod{p}.$$

Preuve:

$$\forall x \in E, x \in E_G \Leftrightarrow \text{card } \Omega_x = 1.$$

Soit P un sous ensemble de E formé par l'ensemble d'un seul représentant de chaque orbite, on a

$$\text{Card}(E) = \sum_{x \in P} \text{card } \Omega_x, \text{ puisque } \forall x \in E_G,$$

$$\text{card } \Omega_x = 1 \text{ alors } E_G \subseteq P, \text{ donc}$$

$$\begin{aligned} \text{Card } E &= \sum_{x \in E_G} \text{card } \Omega_x + \sum_{x \in P - E_G} \text{card } \Omega_x \\ &= \text{Card } E_G + \sum_{x \in P - E_G} \text{card } \Omega_x. \end{aligned}$$

mais $\forall u \in P - E_G$, $\text{card } \Omega_{n+1} \neq 1$ et
 $\text{card } \Omega_n$ divise $\text{card } G = p^k$, donc $\forall u \in P - E_G$,

$\text{Card } \Omega_n \equiv 0 \pmod{p}$ et par suite

$\sum_{x \in P - E_G} \text{card } \Omega_n \equiv 0 \pmod{p}$, d'où

$$\text{card } E_G \equiv \text{card } E \pmod{p}$$

C.Q.F.D

12. Lemme:

Soient H et K deux s'g d'un groupe G tels que
 $[G:H] = k$ et $o(K) = p^n$ avec p premier qui ne
divise pas k et $n \in \mathbb{N}^*$. Alors K est contenu
dans un conjugué de H car $\exists u \in G$ tel que
 $K \subseteq uHu^{-1}$.

Preuve:

Soit $E = \left(\frac{G}{H}\right)_G = \{xH / x \in G\}$
on fait opérer K sur E par translation à gauche

$$K \times E \longrightarrow E$$

$$(g, uH) \longmapsto (gu)H.$$

Soit $E_K = \{uH \in E / \forall g \in K: guH = uH\}$

$$\begin{aligned} \text{d'après (11), } \text{card}(E_k) &\equiv \text{card}(E) \pmod{p} \\ &\equiv \text{card}(G_{\mathbb{F}_p})_g \pmod{p} \\ &\equiv k \pmod{p} \end{aligned}$$

Or p ne divise pas k donc $\text{card}(E_k) \neq 0$ (i.e.)
 $E_k \neq \emptyset$, et par suite il existe $xH \in E_k$,

donc $\forall g \in K : gxH = xH$ (i.e.) $\forall g \in K : gx \in xH$

(i.e.) $\forall g \in K : g \in xHx^{-1}$

donc $K \subseteq xHx^{-1}$.

C.Q.F.D.