

Leçon N° 101: Groupes opérant sur un ensemble. Exemples et Applications.

Donne toute cette leçon, G adérisque un groupe et X un ensemble.

I) Actions de groupes.

1) Définitions et exemples.

Définition 1: On dit que G opère sur X si on a été donné une opération $G \times X \rightarrow X$

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

vérifiant les axiomes suivants:

- 1) $\forall g, g' \in G, \forall x \in X, g \cdot (g' \cdot x) = (gg') \cdot x$
- 2) $\forall x \in X, 1 \cdot x = x.$

Remarque 2: Il revient au même de se donner un morphisme $\varphi: G \rightarrow \mathcal{S}(X)$ en posant $g \cdot x = \varphi(g)(x)$

Exemple 3: 1) G agit sur lui-même par translation à gauche:

$$(gg') \cdot x \mapsto g \cdot (g' \cdot x) \mapsto g \cdot x$$

2) G agit sur lui-même par conjugaison:

$$g \cdot x \mapsto g \cdot x \cdot g^{-1}$$

Le morphisme de groupes correspondant de $(G, \cdot)$ dans $(\mathcal{S}(G), \circ)$ est noté $\text{Int}(G)$

$\text{Int}(G)$ est le groupe intérieur de G . Les automorphismes intérieurs de G .

3) G agit sur tout sous-groupe distingué H par conjugaison:

$$G \times H \rightarrow H$$

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

4) $\mathcal{S}(X)$ agit naturellement sur X par:

$$\mathcal{S}(X) \times X \rightarrow X$$

$$(\sigma, x) \mapsto \sigma \cdot x = \sigma(x)$$

Définition 4: 1) On dit que G opère transitivement sur X lorsque $\forall x \in X, \forall y \in X, \exists g \in G$ tq $g \cdot x = y$.

2) On dit que G opère fidèlement lorsque $\forall g \in G$ on a $g \cdot e = e$. Lorsque $g \cdot e = e \Rightarrow g = 1$.

Exemple 5: G agit fidèlement sur X .

Définition 6: On dit que G opère simplement transitivement lorsque $\forall (a, b) \in G^2, \exists ! g \in G$ tq $g \cdot a = b$. (avec $g = ba^{-1}$).

Proposition 7: Si G opère simplement transitivement alors il opère fidèlement.

Exemple 8: L'action par translation à gauche est simplement transitive donc fidèle.

Proposition 9: (Cayley) Si G est fini de cardinal n , c'est isomorphe à un sous-groupe de $\mathcal{S}_n$.

2) Équivalence avec équiv.

Définition 10: Si G opère sur X , alors $\forall x \in X$, le sous-ensemble $\omega_x = \{g \cdot x \mid g \in G\}$ est appelé orbite de x sous l'action de G .

Remarque 11: La relation $x \sim y$ si $\exists g \in G$ tq $x = g \cdot y$ est une relation d'équivalence sur X dont les classes sont les orbites.

Les orbites forment donc une partition de X .

Définition 12: Si G opère sur X , alors $\forall x \in X$ le sous-ensemble $\text{Stab}(x) = \{g \in G, g \cdot x = x\}$ est le stabilisateur de x sous l'action de G .

Proposition 13: Les stabilisateurs sont des sous-groupes de G .

Proposition 14: Si G opère sur X , $\forall x \in X$, l'application:

$\varphi: G \rightarrow H$ est bien définie et linéaire.

$\varphi = \varphi_{\text{Stet}(n)} \mapsto \varphi_n$

En particulier si G est fini, on a $|\text{Stet}(n)| = \frac{|G|}{|\text{Aut}(n)|}$.

Théorème 15: (Équation aux dérivées). Si G agit sur X et si G est fini et si X est fini. En notant $G_1, \dots, G_n$ les toutes les orbites deux-à-deux disjointes, on a $|X| = \sum_{i=1}^n |G_i|$

$$= \sum_{i=1}^n \frac{|G|}{|\text{Stet}(n_i)|}$$

Corollaire 16: Si G est fini, la le précédent s'écrit lui-même par composition en notant $G_1, \dots, G_n$ toutes les orbites deux-à-deux disjointes, on a: $|G| = |Z(G)| + \sum_{i=1}^n |G_i|$

$$= |Z(G)| + \sum_{i=1}^n \frac{|G|}{|\text{Stet}(n_i)|}$$

Application 17: (Les dérivées quadratiques). Soient p et q deux nombres premiers impairs distincts. Montrer $\binom{p}{q} \binom{q}{p} = (-1)^{p-1} \frac{p-1}{2} \frac{q-1}{2}$

$$\text{on } \binom{p}{q} = a^{p-1} = \begin{cases} 1 & \text{si } a \in \mathbb{F}_p^\times \\ 0 & \text{si } a = 0 \end{cases}$$

2) Formule de Burnside.

Notation 18: Si G agit sur X , alors $\forall g \in G$, on pose

$$\text{Fix}(g) = \{x \in X, g \cdot x = x\}$$

i.e. $\text{Fix}(g)$ est l'ensemble des points fixes de la permutation $x \mapsto g \cdot x$.

Théorème 19 (Formule de Burnside) Si G est fini et agit sur E lui-même fini. On note Σ l'ensemble des éléments de E non fixés par aucun de G .

On a alors $|\Sigma| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$.

Lemme 20: Les groupes d'automorphismes du cube sont:

$$- I_5 + (CC) \cong G_4$$

$$- I_5 (CC) \cong G_4 \times \mathbb{Z}/2\mathbb{Z}$$

Application 21: Le nombre de coloriage du cube à 2 couleurs (noir et blanc) est $\frac{1}{24} (C^6 + 6C^5 + 6C^4 + 3C^3 + 6C^2)$ pour C couleurs.

II) Actions sur les groupes finis.

1) p-groupes.

Définition 22: Soit p un nombre premier. Un p -groupe est un groupe fini G dont l'ordre est une puissance de p .

Proposition 23: Si G est un p -groupe agissant sur X , alors $|X| \equiv |X^G| \pmod{p}$.

Application 24: (Cauchy) Si G est fini et p premier $\nmid p \nmid \text{Card}(G)$ alors G possède au moins un élément d'ordre p .

Corollaire 25: Si G est un p -groupe non trivial. Alors son centre $Z(G)$ est non trivial.

Application 26: Tout groupe d'ordre p^2 est p -groupe et commutatif.

2) p-sylow.

Définition 27: Si G est fini de cardinal $n = p^\alpha m$ avec p premier $\nmid m$. Un p -sylow de G est un sous-groupe de cardinal p^α .

Lemme 28: $|G|_p = (p^\alpha - 1) (p^\alpha - p) \dots (p^\alpha - p^{\alpha-1})$.

Lemme 29: Si G est fini et p premier, alors $|G| \equiv p^a \pmod{p^2}$ et il y a une unique de G . Supposons que G admette un p -sylow S . Alors $\exists g \in G$ $g \notin S$, $g^{-1} \notin S$ et g agit sur S par conjugaison. Aut 2.

Théorème 30: (Sylow) Si G est fini, p premier, q p -diviseur de $|G| = p^a q^b$ avec $m \geq 0$ et $p \nmid q$. Alors:

- 1) Il existe p -Sylow et tout p -Sylow groupe de G est contenu dans un p -Sylow.
- 2) Le conjugué d'un p -Sylow de G est un p -Sylow de G et tous les p -Sylow de G sont conjugués.
- 3) Si N_p est le nombre de p -Sylow de G , on a $N_p \equiv 1 \pmod{p}$ et $N_p \mid q$.

Lemme 31: Si S est un p -Sylow de G , alors $S \trianglelefteq G$ si et seulement si G est l'unique p -Sylow de G .

Application 32: 1) Un groupe d'ordre 63 n'est pas simple.

2) Un groupe d'ordre 33 est cyclique.

III) Applications à la géométrie.

Définition 33: Soit $\mathbb{F}_q$ le corps à q éléments et $n \in \mathbb{N}^*$.

On définit le groupe projectif linéaire $PGLn(\mathbb{F}_q) := \frac{GL_n(\mathbb{F}_q)}{\mathbb{F}_q^* I_n}$.

Définition 34: On définit l'ensemble des droites vectorielles de $\mathbb{F}_q^n$

$$P(\mathbb{F}_q^n) := \mathbb{F}_q^n \setminus \{0\} / \mathbb{F}_q^*.$$

Proposition 35: L'application $GL_n(\mathbb{F}_q) \times P(\mathbb{F}_q^n) \rightarrow P(\mathbb{F}_q^n)$
 $(T, \overline{v}) \mapsto \overline{Tv}$

est une action de $GL_n(\mathbb{F}_q)$ sur $P(\mathbb{F}_q^n)$ qui passe au quotient

en une action fidèle de $PGLn(\mathbb{F}_q)$ sur $P(\mathbb{F}_q^n)$.

Exercices:

- 1) $PG_{L,2}(\mathbb{F}_2) \cong S_3$
- 2) $PG_{L,2}(\mathbb{F}_3) \cong S_4$
- 3) $PG_{L,2}(\mathbb{F}_4) \cong S_5$
- 4) $PG_{L,2}(\mathbb{F}_5) \cong S_5$.