Leçon 101 : Groupe opérant sur un ensemble. Exemples et applications.

Notations : Soient G un groupe multiplicatif d'élément neutre e et X un ensemble.

I Généralités et premiers exemples. [CaP]

Déf : - Une opération (à gauche) de G sur X est la donnée d'une application φ de $G\times X$ vers X : $(g,x)\mapsto g\cdot x$ telle que :

$$\forall (g_1,g_2)\in G^2\ \forall x\in X,\quad g_1\cdot(g_2\cdot x)=(g_1g_2)\cdot x \text{ et } e\cdot x = x.$$

- Si G opère sur X, on dira que X est un <u>G-ensemble</u> ou que G agit sur X.

Prop : Soit G un groupe opérant sur X. Alors :

i) $\forall g\in G$, l'application $\gamma_g : \begin{array}{l} X\to X \\ x\mapsto g\cdot x\end{array}$ est une permutation de X.

ii) L'application $\gamma : \begin{array}{l} G\to S_X \\ g\mapsto \gamma_g\end{array}$ est un morphisme de groupe (dit associé à l'action) et $\mathrm{Ker}\,\gamma$ est appelé <u>noyau de l'action</u> de G sur X.

Rq : La réciproque est vraie : la donnée d'un morphisme de G sur S_X définit une action de G sur X.

Prop : Si H est un sous groupe de G et si G agit sur X alors H agit sur X par restriction.

Exemples : - G opère sur G et $\mathcal{P}(G)$ par translation à gauche

- Si $H\leq G$ alors G opère par translation à gauche sur G/H l'ensemble des classes à gauche de G modulo H.
- G opère sur G et $\mathcal{P}(G)$ par conjugaison.
- S_X opère de façon "naturelle" sur X, en particulier S_n opère sur tout ensemble de cardinal n.

Déf-Prop : Soit X un G-ensemble :

- Le sous groupe $\mathrm{Stab}_G(x)=\{g\in G\ ;\ g\cdot x = x\}$ de G associé à $x\in X$ est appelé <u>stabilisateur</u> de x.
- La relation $\mathcal{R}$ définie sur X par $x\mathcal{R}y \iff \exists g\in G,\ y=g\cdot x$ est une relation d'équivalence. La classe d'équivalence modulo $\mathcal{R}$ d'un élément $x\in X$ est appelée <u>orbite</u> et notée $\Omega_x=\{g\cdot x,\ g\in G\}$. On note l'ensemble des orbites X/G.
- On pose $\mathrm{Fix}_X(g)=\{x\in X,\ g\cdot x = x\}$ et $X^G=\bigcap_{g\in G}\mathrm{Fix}_X(g)=\{x\in X,\ g\cdot x = x\ \forall g\in G\}$

X^G est l'<u>ensemble de points fixes</u> de l'action i.e. l'ensemble des éléments ayant une orbite ponctuelle.

Prop : Si X est un G-ensemble et $y=g\cdot x$ pour $(y,x)\in X^2$ et $g\in G$ alors

$$\mathrm{Stab}_G(y)=g\,\mathrm{Stab}_G(x)\,g^{-1}$$

Déf : - On dit que l'action de G sur X est <u>transitive</u> si $\forall (x,y)\in X^2$, $\exists g\in G$ tel que $y=g\cdot x$.

- On dit que l'action de G sur X est <u>simplement transitive</u> si

$$\forall (x,y)\in X^2,\ \exists!\, g \text{ tel que } y=g\cdot x.$$

- On dit que l'action est <u>fidèle</u> si l'homomorphisme associé est injectif i.e. $\mathrm{Ker}\,\gamma=\{e\}$ i.e. $(g\cdot x = x\ \forall x\in X)\Rightarrow g=e$

Rq : On a toujours $G/\mathrm{Ker}\,\gamma$ opère fidèlement sur X. [Per]

Exemples : - Si $\sigma\in S_n$, le groupe cyclique $\langle\sigma\rangle$ opère sur $\{1,\dots,n\}$ et σ se décompose en produit de cycles disjoints. [Per]

- $GL(E)$ agit de façon simplement transitive sur l'ensemble de bases de l'ev. de dim. finie E. [...]
- Si $H\leq G$, l'action de G sur G/H par translation à gauche est transitive.

Application : * $\mathrm{Ker}\,\gamma=\bigcap_{g\in G} gHg^{-1}$ est le plus grand sous groupe distingué de G contenant H.

* Si G est infini et H distinct de G, d'indice fini dans G alors G n'est pas simple. [Per]

- L'action de G sur lui-même par translation à gauche est fidèle.

Application : <u>Théorème de Cayley</u> : Si G est fini de cardinal n, G est isomorphe à un sous groupe de S_n. [Per]

Prop : Soit X un G-ensemble. Alors $\forall x\in X$, l'application $\theta : \begin{array}{l}\Omega_x\to G/\mathrm{Stab}_G(x) \\ g\cdot x\mapsto g\,\mathrm{Stab}_G(x)\end{array}$ est bijective et donc $|\Omega_x|=[G:\mathrm{Stab}_G(x)]$ $\forall x\in X$.

Corollaire : <u>Equation aux classes</u> : Soit X un G-ensemble fini. Si $(x_i)_{1\leq i\leq r}$ est une famille de représentants des orbites distinctes alors

$$|X|=\sum_{i=1}^{r}[G:\mathrm{Stab}_G(x_i)]$$

Conséquences : * Si X est un G-ensemble fini et G un p-groupe alors $|X^G| \equiv |X| \pmod p$

** Formule de Burnside : Si G est fini et X un G-ensemble fini alors
$$|X/G| = \frac{1}{|G|}\sum_{g\in G} |Fix_X(g)|.$$

II Applications à la théorie des groupes. [Gl]

Déf : G agit sur lui-même par conjugaison et le noyau de l'homomorphisme associé à cette action est appelé le centre de G et noté $Z(G)$.
$$Z(G) = \{g \in G,\ gh = hg\ \forall h \in G\}.$$

Prop : Si G est fini alors $|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|Stab_G(x_i)|}$

où $(x_i)_{1\le i\le r}$ est une famille de représentants des orbites non ponctuelles de l'action de G sur G par conjugaison.

Application : Théorème de Wedderburn : Tout corps fini est commutatif. [Per]

Théorème de Cauchy : Si G est un groupe fini et si p premier divise $|G|$ alors G a au moins un élément d'ordre p. [Gou AP]

Premier théorème de Sylow. Si G est tel que $|G| = sp^n$ avec p premier et $p \nmid s$ alors $\forall\ 1 \le r \le n$, il existe un sous groupe d'ordre p^r

Déf : Si G est fini d'ordre sp^n, p premier et $p \nmid s$ on appelle p-sous-groupe de Sylow de G, tout sous groupe de G d'ordre p^n.

Second théorème de Sylow : Soit G fini et p premier tel que $p \mid |G|$ alors :

i) tout p-sous-groupe de G est contenu dans un p sous groupe de Sylow.

ii) Les p-sous groupes de Sylow de G sont conjugués.

iii) Le nombre de p-sous groupes de Sylow de G est congru à 1 modulo p et divise l'ordre de G.

Corollaire : Si S est un p-sg de Sylow de G, on a :
$$S \lhd G \iff S \text{ est l'unique } p\text{-sg de Sylow de } G.$$

Applications : * Un groupe d'ordre 255 n'est pas simple [Per]

* Soit G d'ordre pq avec p et q premiers distincts alors on a :
  - si $q \not\equiv 1 \pmod p$ G a un unique p-sous groupe de Sylow
  - G n'est pas simple.
  - si $q \not\equiv 1 \pmod p$ et $p \not\equiv 1 \pmod q$ alors G est cyclique.

III. Applications en algèbre :

a) Actions de sous groupes de Matrices sur des ensembles de matrices.

* Action de $GL_n(\mathbb{R})$ sur $M_n(\mathbb{R})$ par conjugaison : $P.M = PMP^{-1}$

Les orbites sont caractérisées par les invariants de similitude ; un système de représentants est donné par
$$\left\{\begin{pmatrix} C_{P_1} & & (0) \\ & \ddots & \\ (0) & & C_{P_r}\end{pmatrix},\ r\in\mathbb{N}^*,\ P_1 | \cdots | P_r,\ \deg(P_1) | \cdots | \deg(P_r) = n\right\} \cup \{0\}$$
où $\forall i \in [\![1,r]\!]$, C_{P_i} est la matrice compagnon de $P_i \in \mathbb{R}[X]$ non nul, non inversible, unitaire

* Action de $GL_n(\mathbb{R})$ sur $S_n(\mathbb{R})$: $P.M = PM\,{}^tP$

conduit à la classification affine des coniques.

* Action de $O_n(\mathbb{R})$ sur $S_n(\mathbb{R})$: $O.M = OM\,{}^tO$

Un système de représentants des orbites est donné par : $\left\{\begin{pmatrix}\lambda_1 & & (0)\\ & \ddots & \\ (0) & & \lambda_n\end{pmatrix},\ \lambda_i \in \mathbb{R},\ \lambda_1 \le \cdots \le \lambda_n\right\}$

Application : classification euclidienne des coniques.

* Action de $U_n(\mathbb{C})$ sur $H_n(\mathbb{C})$: $U.M = UM\,{}^t\bar{U}$.

Un système de représentants est donné par $\left\{\begin{pmatrix}d_1 & & (0)\\ & \ddots & \\ (0) & & d_n\end{pmatrix},\ d_i \in \mathbb{R},\ d_1 \le \cdots \le d_n\right\}$

b) Actions sur $A[X_1, \dots, X_n]$

Théorème fondamental sur les polynômes symétriques : Soit A un anneau intègre commutatif.

Notons $\Sigma_k = \sum_{1\le i_1 < i_2 < \cdots < i_k \le n} X_{i_1} X_{i_2} \cdots X_{i_k}$ les polynômes symétriques élémentaires de $A[X_1, \dots, X_n]$ et notons $A[X_1,\dots,X_n]^{S_n}$ la sous-algèbre de $A[X_1,\dots,X_n]$ des polynômes symétriques.

On a :
$$A[X_1,\dots,X_n]^{S_n} \simeq A[\Sigma_1, \dots, \Sigma_n].$$
[Gob]

Théorème de Molien. Soit V un $\mathbb{C}$-espace vectoriel de dimension finie n. [DVPT]
Soit G un sous groupe fini de $GL(V)$. Soit $A = \mathbb{C}[X_1, \dots, X_n]$. On fixe $\mathcal{B} = (e_1, \dots, e_n)$ une base de V. On définit une action : $G \times A \to A$, $(g, P) \mapsto \sigma_g(P)$ où $g(e_k) = \sum a_{jk} e_j \ \forall k \in [\![1,n]\!]$

et $\sigma_g(P)(X_1, \dots, X_n) = P(\sum a_{1j} X_j, \dots, \sum a_{nj} X_j)$

On pose A_k l'ensemble des polynômes homogènes à n variables de degré k ; $a_k = \dim(A_k)$;
$a_k(G) = \dim A_k^G$ où $A_k^G = \{P \in A_k \ / \ \forall g \in G \ g.P = P\}$.

Alors
$$\frac{1}{\operatorname{card} G} \sum_{g \in G} \frac{1}{\det(I - zg)} = \sum_{k=0}^{+\infty} a_k(G) z^k \in \mathbb{C}[\![z]\!].$$
[Lei].

IV Utilisation et applications à la géométrie.

* **Définition de angles non orientés** : Soit E un espace euclidien de dimension $n \geq 2$, $\mathcal{D}_0$ l'ensemble des demi-droites de E ; $\mathcal{D}$ l'ensemble des droites de E.
Alors $O(E)$ opère sur $\mathcal{D}^2$ (resp $\mathcal{D}_0^2$) par $g.(D_1, D_2) = (g(D_1), g(D_2))$; $(D_1, D_2) \in \mathcal{D}^2$ ou $\mathcal{D}_0^2$.

i) Soient $(D_1, D_2) \in \mathcal{D}^2$ (resp $\mathcal{D}_0^2$), on appelle angle non orienté de D_1 et D_2 l'orbite de (D_1, D_2) sous l'action de $O(E)$.

ii) On appelle angle non orienté de deux vecteurs non nuls de E l'angle non orienté des demi droites qu'ils déterminent. [Tau]

* **Définition d'espace affine** : Un espace affine attaché à un k-espace vectoriel E est un ensemble sur lequel le groupe additif de E opère simplement transitivement. [Tau].

* **Théorème : Sous groupes finis de $SO(3)$.**
Tout sous groupe fini de $SO(3)$ est isomorphe à l'un des groupes suivants :
$\mathbb{Z}/n\mathbb{Z}$; D_n ; $\mathcal{A}_4$; S_4 ; $\mathcal{A}_5$
[X-ens]
[Arn]

* **Action du groupe modulaire sur le demi plan de Poincaré**
On définit le groupe modulaire $PSL_2(\mathbb{Z})$ comme le groupe quotient $SL_2(\mathbb{Z})/\{\pm I_2\}$
On appelle demi-plan de Poincaré l'ensemble $\mathcal{P} = \{z \in \mathbb{C} \ ; \ \operatorname{Im}(z) > 0\}$
On pose $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ dans $SL_2(\mathbb{Z})$ et $\mathcal{D} = \{z \in \mathcal{P} \ ; \ |z| \geq 1 \text{ et } |\operatorname{Re}(z)| \leq \frac{1}{2}\}$

On a :
- $PSL_2(\mathbb{Z})$ agit fidèlement sur $\mathcal{P}$ par homographie
- $\mathcal{D}$ est un domaine fondamental pour cette opération i.e. toute orbite rencontre $\mathcal{D}$.
- $SL_2(\mathbb{Z})$ est engendré par S et T.

[Ale]

* **Un problème de dénombrement** : On peut réaliser 76 colliers différents à l'aide d'un fil, de 4 perles bleues, 3 perles blanches et 2 perles oranges. [Com]

Références :
[Col] : Éléments de théorie des groupes. Josette Calais PUF.
[Ale] : Thèmes de géométrie. M. Alessandri Dunod.
[Lei] : Exercices corrigés de maths. Polytechnique-ENS. Leichtnam Ellipses.
[Tau] : Géométrie P. Taurel Dunod
[Com] : Algèbre et géométrie Combes.
[Per] : Cours d'algèbre D. Perrin Ellipses
[Gou A] : Algèbre Gourdon Ellipse.
[Arn] : les cinq polyèdres réguliers de $\mathbb{R}^3$ et leur groupes. J. M. Arnaudiès Centre de documentation universitaire et SEDES. (polycopié disponible à l'IRMAR).
[X-ens] : Exercices oraux X-ens algèbre 1 Francinou-Gianella Nicolas.
[Gob] : Algèbre commutative R. Goblot