101 - Groupe opérant sur un ensemble. Exemples et applications

Cadre : G désigne un groupe qui sera noté multiplicativement (sauf mention contraire). X désigne un ensemble non vide, et $n \in \mathbb{N}^*$. On notera $S(X)$ l'ensemble des permutations de X, i.e. les bijections de X dans X.

I. Action de groupe. Équation aux classes

[Per]
1) Définition et premières propriétés.

Déf. ①: On dit que G agit sur X, noté $G \curvearrowright X$ s'il existe une application $\bullet : \begin{array}{l} G \times X \to X \\ (g,x) \mapsto g \cdot x \end{array}$ appelée action de G sur X telle que:

13 1) $\forall x \in X$, $1_G \cdot x = x$

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

Prop. ②: Il est équivalent de se donner une action de G sur X et un morphisme de G vers $S(X)$:

$$\begin{array}{ccc} \{\text{actions de } G \text{ sur } X\} & \longleftrightarrow & \mathrm{Hom}(G, S(X)) \\ \bullet & \longmapsto & \sigma : g \mapsto (\sigma_g : x \mapsto g \cdot x) \\ \bullet : (g,x) \mapsto \sigma(g)(x) & \longleftarrow & \sigma \end{array}$$

Déf. ③: Une action $G \curvearrowright X$ est dite:

1) transitive si : $\forall x, y \in X, \exists g \in G \ / \ g \cdot x = y$

14 2) fidèle si : σ de Prop. ② est injectif, i.e. $g \cdot x = x \ \forall x \in X \Rightarrow g = 1$

[Ber] **Ex. ④:** 1) $G \curvearrowright G$ par translation à gauche : $(g,x) \mapsto gx$. Cette action est fidèle et transitive.

170

171 2) Si $H \lhd G$, $G \curvearrowright H$ par conjugaison : $(g,h) \in G \times H \mapsto ghg^{-1}$. Cette action n'est a priori ni fidèle, ni transitive (prendre G abélien par exemple).

Th. ⑤ : (Cayley)

177 Si G est fini et $|G| = n$, alors G est isomorphe à un sous-groupe de S_n (où $S_n = S(\{1, \dots, n\})$).

[Ber]
2) Équation aux classes

Déf./Prop. ⑥: Soit $G \curvearrowright X$ et $x \in X$.

1) Le stabilisateur de x (pour $G \curvearrowright X$) est $\mathrm{Stab}_x = \{g \in G \ / \ g \cdot x = x\} \subset G$.

172 C'est un sous-groupe de G (pas nécessairement distingué !).

2) L'orbite de x (pour $G \curvearrowright X$) est $\omega(x) = \{g \cdot x, g \in G\} \subset X$. La relation "être dans une même orbite" est une relation d'équivalence sur X. 173

Ex. ⑦: Dans l'action de G sur G par conjugaison, les orbites sont les classes de conjugaison.

Déf. ⑧: Soit $G \curvearrowright X$. L'ensemble des points fixes de X pour l'action de G est $X^G = \{x \in X \ / \ \forall g \in G, g \cdot x = x\}$. Si $g \in G$, le fixateur de g est $\mathrm{Fix}(g) = \{x \in X \ / \ g \cdot x = x\}$.

Rq ⑨: 1) $x \in X^G \iff |\omega(x)| = 1 \iff \mathrm{Stab}_x = G$ 173

2) $G \curvearrowright X$ est transitive $\iff \omega(x) = X \ \forall x \in X \iff$ il n'y a qu'une seule orbite

Th. ⑩: Soit $G \curvearrowright X$ et $x \in X$. Alors $\begin{array}{l} G/\mathrm{Stab}_x \to \omega(x) \\ \bar{g} \mapsto g \cdot x \end{array}$ est bien définie et bijective. 174

Th. ⑪: (équation aux classes)

Soit $G \curvearrowright X$ où X est fini. Soit Ω un système de représentants de chaque orbite. ~173

Alors, $|X| = \sum_{x \in \Omega} |\omega(x)| = \sum_{x \in \Omega} \left| G/\mathrm{Stab}_x \right|$. Si G est fini, $|X| = \sum_{x \in \Omega} \frac{|G|}{|\mathrm{Stab}_x|}$

Rq ⑫: On se permettra d'écrire $\sum_{x \in X}$ au lieu de $\sum_{x \in \Omega}$, mais "$x \in X$" est à comprendre comme "un x dans chaque orbite".

Prop. ⑬: (formule de Burnside)

Soit $G \curvearrowright X$ où G et X sont finis et $\Omega = \{\omega(x), x \in X\}$. 176

Alors $|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$.

II. Théorèmes de Sylow

[Ber]

$p \in \mathbb{N}$ désigne un nombre premier.

1) p-groupes

Déf. ⑭: G est un p-groupe si $|G| = p^\alpha$, $\alpha \in \mathbb{N}$. 180

Th. ⑮: Soit G un p-groupe, X un ensemble fini tels que $G \curvearrowright X$. 181

Alors, $|X| \equiv |X^G| \ [p]$.

Coro. ⑯: Le centre d'un p-groupe n'est pas trivial.

Appli. ⑰: Si $|G| = p^2$, alors G est abélien. ♡

[Ber] **Th. (18) : (Cauchy)**

179 Tout p-groupe possède un élément d'ordre p.

Coro. (19) : Soit G un p-groupe, $|G| = p^\alpha$. Alors pour tout $0 \leq k \leq \alpha$,
♡ G possède un sous-groupe de cardinal p^k.

2) Théorèmes de Sylow

[Per] **Déf. (20) :** Soit G un groupe fini, $|G| = p^\alpha m$ où $\alpha \in \mathbb{N}$, $m \in \mathbb{N}^*$ et $p \nmid m$.
18 Un p-Sylow de G est un sous-groupe S de G tel que $|S| = p^\alpha$.

Lemme (21) : Soit G un groupe fini et $p \mid |G|$. On suppose qu'il existe S un
19 p-Sylow de G, et on considère $H \leq G$. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.

18 **Th. (22) : (Sylow)**
DVP1 Soit G un groupe de cardinal $|G| = p^\alpha m$, $p \nmid m$.
19 1) Il existe (au moins) un p-Sylow de G.
2) Si $H \leq G$ est un p-sous-groupe, alors il existe un p-Sylow S tel que $H \subset S$
3) Les p-Sylow sont tous deux à deux conjugués.
4) Si $n_p = |\{p\text{-Sylow de } G\}|$, on a $n_p \equiv 1\ [p]$ et $n_p \mid m$

Coro. (23) : Si $|G| = p^\alpha m$, $p \nmid m$, alors G contient des sous-groupes d'ordre p^k pour tout $0 \leq k \leq \alpha$.

20 **Coro. (24) :** Si S est un p-Sylow de G, alors : $S \triangleleft G \iff n_p = 1$

Appli (25) : Un groupe d'ordre 63 n'est jamais simple.

III. Groupe symétrique. Groupe alterné. $n \geq 2$

1) Généralités sur le groupe symétrique

Rappel (26) : $(S_n, \circ)$ est un groupe de cardinal $n!$. Pour $\sigma, \tau \in S_n$, on écrira $\sigma\tau$ pour $\sigma \circ \tau$. On supposera connues les notions de k-cycle, transposition, support, ... et leurs propriétés élémentaires (ordre, commutativité, ...). On pose $E = \{1 \dots n\}$.

[Ber] 209 **Prop (27) :** Soit $(a_1 \dots a_k)$ un k-cycle et $\sigma \in S_n$. Alors $\sigma(a_1 \dots a_k)\sigma^{-1} = (\sigma(a_1) \dots \sigma(a_k))$

204 **Th. (28) :** Toute permutation s'écrit comme produit de cycles à support disjoint, unique à l'ordre des permutations près.

Th. (29) : Les parties suivantes sont génératrices de S_n : 212
1) les transpositions 2) $\{(1,i),\ 2 \leq i \leq n\}$ 3) $\{(i,i+1),\ 1 \leq i \leq n-1\}$ 213
4) $\{(1\,2),\ (1\,2 \dots n)\}$

2) Classes de conjugaison

Déf. (30) : $\sigma, \sigma' \in S_n$ sont conjuguées s'il existe $\tau \in S_n$ tel que $\sigma' = \tau\sigma\tau^{-1}$

Prop. (31) : Deux k-cycles sont conjugués. [Ber]

Th. (32) : $\sigma, \sigma' \in S_n$ sont conjuguées SSI pour tout $2 \leq k \leq n$, σ et σ' ont le même nombre de cycles de longueur k dans leur décomposition en produit de cycles à support disjoint. ~209

Ex. (33) : $(1\,3\,5)(2\,4)$ et $(1\,2\,3)(6\,7)$ sont conjuguées dans S_7 210

Déf. (34) : Soit $n \in \mathbb{N}^*$. Une partition de n est une suite $(p_k)_{k \geq 1}$ d'entiers, 211
décroissante et nulle à partir d'un certain rang telle que $\sum_{k \geq 1} p_k = n$.
On note $\mathcal{P}(n)$ l'ensemble des partitions de n.

Ex. (34) : $\mathcal{P}(4) = \{(4), (3,1), (2,2), (2,1,1), (1,1,1,1)\}$

Déf. (35) : Soit $\sigma \in S_n$. Le type de σ est la partition de n correspondant aux cardinaux des cycles de la décomposition de σ, rangés par ordre décroissant. On le note p_σ.

Ex. (36) : Si $\sigma = (1\,3)(4\,7\,6\,5) \in S_9$, $p_\sigma = (4,2,1,1,1)$

Rq (37) : Le Th (32) se réécrit : σ et σ' sont conjuguées SSI $p_\sigma = p_{\sigma'}$.
Il y a donc $\mathcal{P}(n)$ orbites pour l'action par conjugaison de S_n sur lui-même.

Ex. (38) : S_4 possède 5 classes de conjugaison dont un système de représentants est $\{(1\,2\,3\,4), (1\,2\,3), (1\,2)(3\,4), (1\,2), id\}$ 212

3) Signature, groupe alterné

[Ber]

Th./Déf. (39) : Il existe un unique morphisme de groupes surjectif
$\varepsilon : (S_n, \circ) \to (\{\pm 1\}, \cdot)$. De plus, ε vaut -1 sur les transpositions. ~ 213
ε est appelé (morphisme) signature, et $\varepsilon(k\text{-cycle}) = (-1)^{k-1}$.

215 <u>Déf. 40</u> : Le groupe alterné d'ordre n est $\mathcal{A}_n = \ker \varepsilon$.

<u>Prop. 41</u> : $|\mathcal{A}_n| = \frac{n!}{2}$ et $\mathcal{A}_n \lhd S_n$

<u>Ex. 42</u> : 1) Les double transpositions, les 3-cycles sont dans $\mathcal{A}_n$
2) $\mathcal{A}_2 = \{1\}$, $\mathcal{A}_3 = \{1, \sigma, \sigma^2\}$ où $\sigma = (1\,2\,3)$

<u>Th. 43</u> : $n \geq 3$. $\mathcal{A}_n$ est engendré par :
216 1) les double transpositions (pas nécessairement à support disjoint).
2) les 3-cycles.

213 <u>Lemme 44</u> : Si $n \geq 5$, les 3-cycles sont conjugués dans $\mathcal{A}_n$

[Per] <u>Rq 45</u> : Faux si $n=3$ car $\mathcal{A}_3$ est abélien, et si $n=4$ car $|\{3\text{ cycles}\}| = 8$,
16 $|\mathcal{A}_4| = 12$ et $8 \nmid 12$.

28 <u>Prop. 46</u> : Si $n \geq 2$, $\mathcal{D}(S_n) = \mathcal{A}_n$. Si $n \geq 5$, $\mathcal{D}(\mathcal{A}_n) = \mathcal{A}_n$.
(où $\mathcal{D}(G)$ est le sous-groupe dérivé de G).

<u>Th. 47</u> : $\mathcal{A}_n$ est simple pour $n \geq 3$ et $n \neq 4$.

[Ber] 219 <u>Lemme 48</u> : si $n \geq 3$, alors $Z(S_n) = \{id\}$

220 <u>Coro. 49</u> : si $n \neq 4$, les sous-groupes distingués de S_n sont $\{id\}$, $\mathcal{A}_n$ et S_n.

[Per] DVP 2 30 <u>Th. 50</u> : Si $n \neq 6$, alors les automorphismes de S_n sont intérieurs.

IV. Action sur un groupe de matrices : action par congruence

<u>Cadre</u> : On supposera connues les notions de forme quadratique q, q-orthogonalité, ... sur un K-espace vectoriel où K est un corps commutatif de caractéristique $\neq 2$.

[H2G2] <u>Déf. 51</u> : $GL_n(K) \times \mathcal{S}_n(K) \longrightarrow \mathcal{S}_n(K)$ où $\mathcal{S}_n(K) = \{M \in \mathcal{M}_n(K) \,/\, {}^tM = M\}$
$(P, M) \longmapsto {}^tPMP$
250 est une action de groupe appelée action par congruence.

<u>Rq 52</u> : Deux matrices $M, N \in \mathcal{S}_n(K)$ congruentes sont les matrices d'une même forme quadratique sur K^n dans deux bases "différentes".

<u>Déf. 53</u> : $K^2 = \{x^2, x \in K\}$ et $K^{*2} = \{x^2, x \in K^*\}$.

<u>Déf. 54</u> : Si $M \in \mathcal{S}_n(K) \cap GL_n(K)$, le discriminant de M est $\delta(M) = \det M \mod K^{*2}$ 250

<u>Prop. 55</u> : Le rang, le discriminant sont invariants par l'action par congruence.

<u>Th. 56</u> : Soit q une forme quadratique sur K^n. Alors, il existe une base de K^n q-orthogonale. 251

<u>Th. 57</u> : <u>(lois d'inertie de Sylvester)</u>
1) <u>$K = \mathbb{C}$</u> : $M \in \mathcal{S}_n(\mathbb{C})$, $r = rg(M)$: $\exists P \in GL_n(\mathbb{C}) \,/\, {}^tPMP = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$. 254
$M, N \in \mathcal{S}_n(\mathbb{C})$ sont congruentes SSI $rg(M) = rg(N)$ ($\Rightarrow n+1$ classes)
2) <u>$K = \mathbb{R}$</u> : $M \in \mathcal{S}_n(\mathbb{R})$, $r = rg(M)$: $\exists! (p,q) \in \mathbb{N}^2$, $p+q = r$, $\exists P \in GL_n(\mathbb{R}) \,/$ 255
${}^tPMP = \begin{pmatrix} I_p & & \\ & -I_q & \\ & & 0 \end{pmatrix}$. (p,q) est appelé signature de M, notée $sgn(M)$.
$M, N \in \mathcal{S}_n(\mathbb{R})$ sont congruentes SSI $sgn(M) = sg(N)$ ($\Rightarrow \sum_{r=0}^{n}(r+1) = \frac{(n+1)(n+2)}{2}$ classes)
3) <u>$K = \mathbb{F}_q$</u> : Soit $\alpha \in \mathbb{F}_q^*$, $\alpha \notin \mathbb{F}_q^{*2}$. Il y a alors deux classes de congruence sur $\mathcal{S}_n(\mathbb{F}_q) \cap GL_n(\mathbb{F}_q)$: I_n et $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & \alpha \end{pmatrix}$. 256
$M, N \in \mathcal{S}_n(\mathbb{F}_q) \cap GL_n(\mathbb{F}_q)$ sont congruentes SSI $\delta(M) = \delta(N)$.

<u>Appli 58</u> : <u>(loi de réciprocité quadratique)</u>
Soient p, q premiers impairs. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}}$ 304

Références :

- [Ber] Berhuy, *Algèbre : le grand combat* (2e éd.)
- [Per] Perrin, *Cours d'algèbre*
- [H2G2] Caldero, *Nouvelles histoires....* Tome 1