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

Soit G un groupe et X un ensemble non vide.

I - Opération d'un groupe sur un ensemble. [PER]

A - Premières définitions. [PER]

Définition 1 : Définition d'action de groupe.

Remarque 2 : Se donner une action revient à se donner un morphisme de groupe.

Définition 3 : Action transitive, fidèle.

Exemples 4 : $\mathfrak{S}_n$ agit transitivement et fidèlement sur $[\![1,n]\!]$, $\mathrm{GL}_n(\mathbb{C})$ agit transitivement et fidèlement sur $\mathbb{C}^n\backslash\{0\}$, $\mathrm{O}_n(\mathbb{R})$ agit transitivement sur $\mathbb{R}^n$.

Remarque 5 : Si G opère sur X alors $G/\mathrm{Ker}(\varphi)$ agit fidèlement sur X.

Remarque 6 : Soit E un $\mathbb{K}$-ev, pour l'action de $\mathrm{GL}(E)$ sur $\mathbb{P}(E)$, $\mathrm{Ker}(\varphi) = \mathrm{Z}(\mathrm{GL}(E)) = \mathbb{K}^\times Id_E$ et donc $\mathrm{PGL}(E)$ agit fidèlement sur $\mathbb{P}(E)$.

B/ Orbites et stabilisateurs. [PER]

Définition 7 : Relation $\mathcal{R}$: $x\mathcal{R}y \iff \exists g \in G,\ y = g\cdot x$

Définition 8 : Orbites.

Définition 9 : Stabilisateurs.

Proposition 10 : $\mathrm{Stab}(x)$ est un sous-groupe de G.

Remarque 11 : Être transitif c'est n'avoir qu'une seule orbite.

Remarque 12 : Les orbites pour l'action de $\mathrm{O}_n(\mathbb{R})$ sur $\mathbb{R}^n$ sont les sphères, dans celle de $\mathfrak{S}_n$ le stabilisateur d'un point est isomorphe à $\mathfrak{S}_{n-1}$.

C/ Dénombrer à l'aide des orbites. [PER] [ROM]

Proposition 13 : ${}^{G}/_{\mathrm{Stab}(x)}$ est en bijection avec $\omega(x)$.

Théorème 14 : Équation aux classes.

Développement 1

Application 15 : Dénombrement des endomorphismes diagonalisables de $\mathbb{F}_q^n$

Théorème 16 : Formule de Burnside.

Application 17 : Problème de la roulette : on se donne une roulette à n segments et c couleurs et on dit que deux roulettes ont la même coloration si l'on peut passer de l'une à l'autre après rotation de la roulette, il y a donc $\frac{1}{n}\sum_{d|n}\varphi(d)c^{\frac{n}{d}}$ colorations possibles.

II/ Actions sur les groupes finis

A/ Action par translation. [PER]

Définition 18 : Action par translation.

Remarque 19 : Cette action est simplement transitive et fidèle.

Application 20 : Théorème de Cayley.

B/ Action par conjugaison. [PER]

Proposition 21 : Action par conjugaison, centralisateur.

Remarque 22 : Principe de conjugaison.

Application 23 : Théorème de Wedderburn : Tout anneau à division fini est commutatif.

Application 24 : Le centre d'un p-groupe n'est pas réduit au neutre.

C/ Application aux théorèmes de Sylow. [PER]

Définition 25 : p-sous-groupe de Sylow.

Théorème 26 : Théorème de Sylow 1 : Existence des p-Sylows.

Théorème 27 : Théorème de Sylow 2 : Dénombrement des p-Sylows et ils sont tous conjugués.

Corollaire 28 : Un p-Sylow est unique ssi il est distingué.

Application 29 : Un sous-groupe d'ordre 63 n'est pas simple. Les groupes d'ordre pq avec p et q premiers distincts ne sont pas simples.

III/ Applications dans d'autres domaines des mathématiques.

A/ Isomorphismes exceptionnels. [CAL] [PER]

Définition 30 : Définition groupes projectifs linéaires.

Proposition 31 : Dénombrement sur les corps finis : $\mathrm{GL}_n(\mathbb{F}_q)$, $\mathbb{P}^n(F_q)$, $\mathrm{SL}_n(\mathbb{F}_q)$, $\mathrm{PGL}_n(\mathbb{F}_q)$ et $\mathrm{PSL}_n(\mathbb{F}_q)$.

Lemme 32 : Si H est un sous-groupe d'indice n de $\mathfrak{S}_n$ alors $H \simeq \mathfrak{S}_{n-1}$.

Théorème 33 : Isomorphismes exceptionnels.

B/ En géométrie : Isométries préservant les polytopes. [CAL]

Définition 34 : On note $I_S(X)$ les isométries laissant stable X.

Proposition 35 : Triangle équilatéral $I_S(X) \simeq \mathfrak{S}_3$. Pour le polygone régulier c'est le groupe diédral.

Proposition 36 : Groupe isométries tétraèdre.

Développement 2

Proposition 37 : Détermination du groupe des isométries du cube et colorations des cubes à c couleurs.

C/ Actions sur les groupes de matrices. [ROM]

Proposition 38 : Action $(P, A) \mapsto PA$ et orbites (lien avec les opérations élémentaires, on agit ici sur les lignes de la matrice A)

Proposition 39 : Action $(P, A) \mapsto AP^{-1}$ et orbites (lien avec les opérations élémentaires, on agit ici sur les colonnes de la matrice A)

Proposition 40 : Il existe une unique matrice échelonnée réduite dans chaque orbite.

Proposition 41 : Action de Steinitz ($(P, Q, A) \mapsto PAQ$) et orbites.

Proposition 42 : Connexité et adhérence de ces orbites.

Proposition 43 : Action par conjugaison : $(P, A) \mapsto PAP^{-1}$.

Proposition 44 : Dans $\mathbb{C}$ l'orbite de M est fermée ssi M est diagonalisable.

Références :

— [PER] Perrin p. 13-20
— [ROM] Rombaldi 2nde édition p. 21 et p. 197
— [CAL] Caldéro Histoires hédonistes tome 1 p. 250-257, p. 264, p. 363 et p. 376

Exercices/Questions autour de la leçon 101 :

Exercice 1 : Quel est le nombre d'orbites de l'action par congruence $\mathrm{GL}_n(\mathbb{C}) \times S_n(\mathbb{C}) \to S_n(\mathbb{C})$? Quel représentant privilégié dans les orbites ?

Solution exercice 1 : Cela revient à considérer le théorème de réduction des formes quadratiques sur $\mathbb{C}$, il y a donc $n+1$ orbites. On a donc $S_n(\mathbb{C}) = \bigcup_{k=0}^{n} O_r$ où O_r est l'orbite de $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.

Exercice 2 : Quelles sont les orbites de l'action par congruence sur $\mathbb{R}$?

Solution exercice 2 : Penser au théorème d'inertie de Sylvester, dans chaque orbite on a un représentant privilégié qui est $\begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_q & 0 \\ 0 & 0 & 0 \end{pmatrix}$ avec $p+q=r$ où r est le rang.

Exercice 3 : Quelles sont les orbites par l'action par conjugaison ?

Solution exercice 3 : Deux matrices sont semblables ssi elles ont les mêmes invariants de similitude (réduction de Frobenius).

Exercice 4 : Soit G fini tel que $\mathrm{Aut}(G)$ agit transitivement sur $G\backslash\{1\}$. Montrer que $Z(G) \neq \{1\}$.

Solution exercice 4 : La transitivité de l'action implique que les ordres de tous les éléments distinct de 1 sont égaux, notons o cet ordre commun. Pour p diviseur premier de $n = |G|$, on a qu'il existe un élément d'ordre p (théorème de Cauchy), donc $o = p$ puis $n = p$. Ainsi G est un groupe d'ordre p et on conclut par l'application 24.

Exercice 5 : Un groupe d'ordre 200 n'est pas simple.

Solution exercice 5 : $200 = 2^3 \times 5^2$, on compte les 5-Sylow, il n'y en a qu'un donc le 5-Sylow est distingué et un groupe d'ordre 200 n'est pas simple.

Exercice 6 : Classifier les groupes d'ordre p^2.

Solution exercice 6 : Ils sont tous abéliens et soit isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$ ou isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$. (Regarder le centre du groupe).

Exercice 7 : Soit p premier. Quel est l'ordre des p-Sylow de $\mathfrak{S}_p$?

Solution exercice 7 : $|\mathfrak{S}_p| = p! = p \times (p-1)!$, comme p ne divise pas $(p-1)!$ alors ils sont d'ordre p.

Exercice 8 : Combien $\mathfrak{S}_p$ contient de p-cycles ?

Solution exercice 8 : On les compte en faisant agir $\mathfrak{S}_p$ sur les p-cycles, c'est une action transitive et on obtient par la formule des classes : $(p-1)!$. (On peut aussi le compter à la main en faisant attention que deux p-cycles sont les mêmes si on passe de l'un à l'autre par permutation circulaire des éléments).

Exercice 9 : En déduire le nombre de p-Sylow de $\mathfrak{S}_p$.

Solution exercice 9 : Les sous-groupes d'ordre p premier sont cycliques dont les p-Sylow sont engendrés par les p-cycles (car pas d'autres éléments d'ordre p que les p-cycles car p premier). Le sous-groupe engendré par un p-cycle contient toutes ses puissances donc il y en $p-1$ différents dans chaque p-Sylow. On a donc $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow dans $\mathfrak{S}_p$.

Exercice 10 : Soit G un groupe d'ordre 15, combien a-t-il d'élements d'ordre 3 ? Et 5 ?

Solution exercice 10 : Il y a un unique 3-Sylow donc deux éléments d'ordre 3. Pareil pour 5 on a donc 4 éléments d'ordre 5 (Sylow cyclique car d'ordre un nombre premier).

Exercice 11 : Montrer que G d'ordre 15 est cyclique.

Solution exercice 11 : En effet, en comptant il reste nécessairement 8 éléments d'ordre 15.

Exercice 12 : Montrer que $O_2^+(\mathbb{R})$ agit transitivement sur le cercle unité de $\mathbb{R}^2$.

Solution exercice 12 : Oui si on prend deux points A et B on considère la rotation d'angle (OA, OB).

Exercice 13 : Démontrer que $O_3^+(\mathbb{R})$ agit transitivement sur la sphère unité de $\mathbb{R}^3$.

Solution exercice 13 : On prend deux points A et B sur la sphère unité. Soit P le plan contenant O, A et B et D la droite perpendiculaire à P passant par O. On considère alors la rotation d'axe D transformant A en B par la rotation d'angle (OA,OB). (Résultat prolongeable sur $O_n(\mathbb{R})$ en prenant comme espace stable un espace de dimension $n-2$)

Exercice 14 : Un groupe de 35 éléments agit sur un ensemble à 19 éléments sans fixer aucun d'entre eux. Combien y-a-t-il d'orbites ? Combien d'éléments contiennent-elles ?

Solution exercice 14 : Une orbite a un cardinal divisant 35. Comme ne fixe aucun d'entre eux, pas 1. Comme au plus de cardinal 19, la seule possibilité est que cela vaille 7 (disons qu'il y en a m) ou 5 (disons qu'il y en a n). Les orbites réalisant une réunion disjointe de l'ensemble à 19 éléments, on doit avoir $5n+7m=19$; la seule possibilité est $n=1$ et $m=2$. Il y a donc 3 orbites, l'une à 5 éléments, les deux autres à 7 éléments.

Exercice 15 : Montrer qu'un groupe de cardinal 6 non abélien est isomorphe à $\mathfrak{S}_3$.

Solution exercice 15 : On compte les 3-Sylows et 2-Sylows sachant qu'il n'y a pas d'élément d'ordre 6. Ensuite un élément d'ordre 3 ne commute pas avec un élément d'ordre 2 car sinon le produit est d'ordre 6. On crée donc un morphisme envoyant un élément d'ordre 2 de G sur une transposition de $\mathfrak{S}_3$ et de même pour l'ordre 3.

Exercice 16 : Montrer qu'un sous-groupe d'ordre 30 possède un sous-groupe distingué non trivial.

Solution exercice 16 : $30 = 2\times 3\times 5$. Par le deuxième théorème de Sylow $n_2 \in \{1,3,5,15\}$, $n_3 \in \{1,10\}$ et $n_5 \in \{1,6\}$. Supposons qu'aucun des trois ne soit 1, on suppose alors que $n_2 = 3$, $n_3 = 10$ et $n_5 = 6$. Or 2,3 et 5 sont premiers donc les Sylows sont tous cycliques et d'intersection neutre (sinon ils sont tous égaux). On compte alors le nombre d'éléments du groupe G dans cette configuration : 1 (neutre) + 3×1 (éléments engendrant un 2-Sylow) + $10\times 2+6\times 4 > 30$ c'est absurde et donc au moins un des trois est 1, un groupe d'ordre 30 n'est donc pas simple.

Exercice 17 : Montrer qu'un groupe d'ordre 35 est cyclique.

Solution exercice 17 : On regarde les Sylow, il n'y a qu'un seul 3-Sylow S_3 et un seul 5-Sylow S_5, l'intersection est réduite au neutre, ils sont cycliques et x_5 (générateur de S_5) et x_7 (générateur de S_7) commutent alors on factorise l'application $(k,l)\mapsto x_5^k x_7^l$ et on obtient le résultat avec le théorème chinois.

Exercice 18 : Montrer qu'un groupe de cardinal 255 admet au moins 3 sous-groupes distingués.

Solution exercice 18 : On regarde les Sylows, il y a un seul 17-Sylow. Pour les deux autres au moins un des deux vaut 1 sinon trop d'élément disons que $n_3 = 1$. On introduit $K = < S_{17}, S_3 >$ le sous-groupe engendré et il convient comme 3ème sous-groupe distingué.

Exercice 19 : Montrer que tout groupe d'ordre 48 admet un sous-groupe distingué d'ordre 8 ou 16.

Solution exercice 19 : $48 = 3\times 2^4$. Le nombre de 2-sous-groupes de Sylow divise 3 et est impair. S'il est égal à 1, G possède un sous-groupe distingué d'ordre 16. Le quotient de G par le sous-groupe distingué d'ordre 16 est alors isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Sinon, G a 3 sous-groupes de Sylow d'ordre 16. L'opération de G sur l'ensemble des 3-sous-groupes de Sylow par conjugaison est transitive et définit un morphisme $G\to\mathfrak{S}_3$. L'image est d'ordre 3 ou 6. En effet, si l'image est d'ordre 2, l'action ne peut pas être transitive. Le noyau qui est distingué est donc d'ordre $8=\frac{48}{6}$ ou $16=\frac{48}{3}$ (en fait le dernier cas, n'est pas possible car cela signifierait qu'il y a un sous-groupe de Sylow distingué, ce qui est contradictoire avec l'hypothèse faite). On a donc montré le résultat.

Exercice 20 : Les groupes de cardinaux pqr ne sont pas simples.

Solution exercice 20 : Si G n'a pas de sous-groupe distingué, les nombres n_p, n_q et n_r sont strictement supérieurs à 1. On a $n_r | pq$ et $n_r \equiv 1[r]$. Donc si n_r est différent de 1, il est de la forme $1+rk$ avec $k>0$ et divise pq. Comme r est plus grand que p et q, il ne peut être égal à p ou q. Donc, il y aurait pq r-sous-groupes de Sylow. Il y aurait alors $pq(r-1)$ éléments d'ordre r. De même, $n_p|$qr, donc $n_p \geq q$ et $n_q|pr$ et $n_p \geq p$. Il y aurait donc au moins $q(p-1)$ éléments d'ordre p et $p(q-1)$ éléments d'ordre q. Ce qui donne au moins $pq(r-1)+q(p-1)+p(q-1)+1 = pqr+(q-1)(p-1)$ éléments, ce qui est plus que pqr. Donc un des entiers n_p, n_q ou n_r est égal à 1.

Exercice 21 : Soit G un groupe non abélien et Z son centre. Montrer que G/Z n'est pas monogène.

Solution exercice 21 : Montrons la réciproque. Supposons a générateur de G/Z alors si $x,y \in G$ on a $x = a^k g$ et $y = a^l g'$ où $(k,l) \in \mathbb{N}$ et $g,l \in Z$. Alors $xy = a^k g a^l g' = a^{k+l} g g' = a^l g' a^k g = yx$ donc G abélien.

Exercice 22 : Dénombrer le nombre de sous-espaces vectoriels de dimension r de $(\mathbb{F}_q)^n$.

Solution exercice 22 : Considérons ensuite l'action $\mathrm{GL}_n(\mathbb{F}_q) \times V_r \to V_r, (M,F) \mapsto MF$ où V_r est l'ensemble des sous-espaces vectoriels de dimension r. L'action est transitive (penser aux matrices de passage d'une base complétée de l'un sur une base complétée de l'autre). Calculons $|\mathrm{Stab}(V)|$ où $V \in V_r$. En se plaçant dans la bonne base, on voit que $M \in \mathrm{Stab}(V) \Longleftrightarrow \begin{pmatrix} M_V & \star \\ 0 & M_U \end{pmatrix}$ où $M_V \in \mathrm{GL}_r(\mathbb{F}_q)$ et $M_U \in \mathrm{GL}_{n-1}(\mathbb{F}_q)$. Donc $|\mathrm{Stab}(V)| = |\mathrm{GL}_r(\mathbb{F}_q)||\mathrm{GL}_{n-r}(\mathbb{F}_q)|q^{r(n-r)}$ et l'équation aux classes donne le résultat.

Exercice 23 : Dénombrer le nombre de k-cycles de $\mathfrak{S}_n$.

Solution exercice 23 : On fait agir $\mathfrak{S}_n$ sur les k-cycles par conjugaison cette action est transitive on cherche donc juste le stabilisateur d'un élément k-cycle. On a $\sigma \in \mathrm{Stab}((a_1,\ldots,a_n))$ ssi $\sigma(a_1)$ à choisir et le reste ne bouge pas. Donc $|\mathrm{Stab}((a_1,\ldots,a_n))| = k \times (n-k)!$, on déduit le résultat de l'équation aux classes.

Exercice 24 : Déterminer l'ensemble des isométries laissant stable un octaèdre. De même pour le dodécaèdre et l'icosaèdre.

Solution exercice 24 : Fait proprement dans Caldéro Histoires hédonistes tome 1. L'octaèdre est le dual du cube et a donc le même groupe d'isométries que le cube. On peut inscrire 5 cubes dans le dodécaèdre et faire agir sur ces cinq cubes. L'icosaèdre est le dual du dodécaèdre et a donc le même groupe d'isométries que le dodécaèdre.