

101: groupe opérant sur un ensemble. Applications

Pierre Lissy

May 6, 2010

1 Définition. Exemples. Premières applications

1.1 Action de groupe.[1]

Définition 1. Soit $(G, \cdot)$ un groupe noté multiplicativement, d'élément neutre 1. Soit X un ensemble. Une action du groupe G sur X est une application $\psi : G \times X \rightarrow X$ vérifiant:

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

On dit alors que X est un G -ensemble et que G opère (ou agit) sur X .

Remarque 1. Il revient au même de se donner un morphisme de groupe $\varphi : G \rightarrow \text{Bij}(X)$, en posant $\varphi(g) := x \mapsto \psi(g, x)$. On dit alors que φ est une action de groupe donnée par automorphismes. Si ce morphisme est injectif, on dit que l'action est fidèle. En particulier, $G/\text{Ker}\varphi$ opère fidèlement sur X .

Dans toute la suite, l'action sera simplement notée $\cdot$.

1.2 Actions par translation.[1]

Définition-proposition 1. Soit G un groupe. On appelle action par translation à gauche l'action de G sur lui-même définie par $g.a := ga$. G opère fidèlement sur G pour cette action.

Application 1 (Théorème de Cayley). Tout groupe d'ordre n peut s'écrire comme un sous-groupe du groupe symétrique $\mathcal{S}_n$.

On peut définir d'autres actions par translation.

Exemple 1. On fait agir $GL_n(k)$ sur $M_{n,m}(k)$ par translation: $G.M \mapsto GM$. De même par translation à droite.

Définition 2. Soit G un groupe et H un sous-groupe distingué de G . On appelle action par translation à gauche sur le quotient l'action de G sur le groupe quotient G/H définie par $g.(aH) := gaH$. G n'opère pas fidèlement pour cette action (le noyau est H).

Application 2. Soit G un groupe infini et H un sous-groupe de G distinct de G d'indice fini. Alors en faisant agir G sur G/H on montre que G n'est pas simple.

1.3 Actions par conjugaison.[1]

Définition 3. Soit G un groupe. On appelle action par conjugaison l'action de G sur lui-même définie par $g.a := gag^{-1}$. Cette action n'est pas fidèle.

Définition 4. Soit G un groupe. On appelle action par conjugaison sur les sous-groupes l'action de G sur l'ensemble de ses sous-groupes définie par $g.H := gHg^{-1}$. Cette action n'est pas fidèle.

On peut aussi définir d'autres actions par conjugaison.

Exemple 2. $GL_n(k)$ agit sur $M_n(k)$ par conjugaison, mais pas fidèlement en général. $O_n(k)$ agit sur $S_n(\mathbb{R})$ par conjugaison, pas fidèlement en général.

1.4 Groupes d'applications.

Définition 5. Soit G un groupe (pour la composition) d'applications de E dans E . Alors G agit sur F par l'action $f.x = f(x)$, et donc agit fidèlement.

Exemple 3. Soit E un espace vectoriel. $GL(E)$ (ou $GL_n(k)$) agit (fidèlement) sur E^* (ou sur k^*)

Exemple 4. S_n agit sur $\{1, \dots, n\}$ fidèlement.

1.5 Exemples d'actions provenant de la géométrie.

Exemple 5. [1] On note D_n le groupe diédral, ie l'ensemble des isométries qui laissent invariantes un polygone régulier à n côtés P_n . Alors D_n agit sur P_n fidèlement.

Exemple 6. [4][page 75] Soit $ABCD$ un carré orienté dans le sens direct. On appelle Δ l'ensemble de ses diagonales. Alors le groupe diédral D_2 agit sur Δ par l'action $\sigma.d = \sigma(d)$ fidèlement.

Exemple 7. [2][page 42] Si E est un espace vectoriel, $GL(E)$ agit sur l'ensemble des sev de E noté $\mathcal{F}$. $GL(E)$ n'agit pas fidèlement sur $\mathcal{F}$, mais $PGL(E)$ agit fidèlement sur $\mathcal{F}$.

Exemple 8. [1] On note G un sous-groupe du groupe des rotations sur espace euclidien de dimension 3. On appelle X l'ensemble des pôles (ie les intersections des axes des éléments de G avec la sphère unité). Alors G agit sur X par $g, x \mapsto g(x)$.

2 Orbites. Stabilisateurs. Applications

2.1 Orbites. Actions transitives.

Définition-proposition 2. Soit G un groupe agissant sur un ensemble X . Soit R la relation d'équivalence suivante: $xRy \Leftrightarrow \exists g \in G | y = g.x$. Alors R est une relation d'équivalence et les classes d'équivalence sont appelées les orbites de X sous G . L'orbite contenant un certain point x est notée $Orb(x)$. $Orb(x) = \{g.x | g \in G\}$. Une action n'ayant qu'une seule orbite est dite transitive. Elle est dite libre si et seulement si pour tout x et tout y dans X , il existe au plus un g dans G tel que $y = g.x$. Elle est dite n fois transitive si et seulement si étant donné n points distincts $a_1, \dots, a_n$ de X et n points distincts $b_1, \dots, b_n$ de X , on peut trouver $g \in G$ tel que $\forall i \in \{1, \dots, n\}$, $g.a_i = b_i$.

Exemple 9. L'action de translation à gauche est transitive et libre. Celle de translation sur les quotients est non libre et non transitive.

Exemple 10. L'action de D_2 sur Δ est transitive et libre.

Exemple 11. Les orbites pour l'action de conjugaison sont appelées classes de conjugaison de G . Pour l'action de conjugaison sur les sous-groupes, les éléments de $Orb(H)$ sont appelés les conjugués de H . L'action est non libre.

Exemple 12. Pour l'action de $GL_n(k)$ sur $M_n(k)$, $Orb(A)$ est appelée la classe de similitude de A . Les orbites sont décrites par ce qu'on appelle les invariants de similitude, une suite de polynômes se divisant les uns les autres dont les noyaux sont en somme directe et sur lesquels les endomorphismes induits sont cycliques. Deux matrices sont conjuguées ssi elles ont les mêmes invariants de similitude. De même pour l'action de $O_n(\mathbb{R})$ sur les matrices symétriques, les orbites sont paramétrées uniquement par les valeurs propres comptées avec multiplicité. (car les matrices de permutation sont orthogonales)

Exemple 13. $\mathcal{A}_n$ est $n - 2$ fois transitif sur $\{1, \dots, n\}$, et l'action est non libre.

Exemple 14. [2][page 42] L'action de $GL(E)$ sur les droites vectorielles est transitive et non libre en général; mais l'action de $SO(E)$ sur les droites vectorielles est transitive et libre si $\dim(E) = 2$! L'action de $GL(E)$ sur les sous-espaces vectoriels a $n + 1$ orbites, chaque orbite étant l'ensemble des sev de dimension n . Cette action est non libre.

Exemple 15. L'action de D_n sur P_n est non libre et non transitive.

Application 3 (Décomposition en cycle d'une permutation). Soit $\sigma \in \mathcal{S}_n$. En faisant agir $\langle \sigma \rangle$ sur $\{1, \dots, n\}$ et en s'intéressant aux orbites de cette action, on montre qu'il existe une unique (à l'ordre près) décomposition de σ en cycles de supports disjoints commutant deux à deux.

Application 4 (Espace affine). [2] Soit E un espace vectoriel. On appelle espace affine de direction E la donnée d'un ensemble $\mathcal{E}$ et d'une action de groupe transitive et libre de E sur $\mathcal{E}$. C'est l'outil de base de la géométrie affine. On montre que si E est de dimension finie n alors $\mathbb{E}$ est isomorphe au E considéré en tant qu'espace affine. (cf Frankel)

2.2 Stabilisateurs. Formule des classes.

Définition 6. Soit G un groupe opérant sur un ensemble X . Le Stabilisateur d'un élément x est $\text{Stab}(x) := \{g \in G \mid g.x = x\}$. C'est un sous-groupe de G .

Remarque 2. $\text{Stab}(g.x) = g\text{Stab}(x)g^{-1}$.

Exemple 16. Le stabilisateur d'un élément pour l'action de translation est le neutre. Le stabilisateur d'un élément pour l'action de translation sur les sous-groupes est H .

Exemple 17. Le stabilisateur de x pour l'action de conjugaison est appelé le centralisateur de x , noté $C_G(x)$. $C_G(x) := \{g \in X \mid gx = xg\}$

Exemple 18. Le stabilisateur de H pour l'action de conjugaison sur les sous-groupes est appelé le normalisateur de H . On montre que H est distingué dans $N_G(H)$ et que $N_G(H)$ est le plus grand sous-groupe vérifiant cette propriété.

Exemple 19. Le stabilisateur pour l'action d'application est l'ensemble des éléments fixant x , ie l'ensemble des éléments tels que x est un point fixe. Pour $GL(E)$ où E est un ev c'est $\text{Ker}(f - \text{Id})$. etc!

Exemple 20. [2][page 42] Le stabilisateur d'un sev F pour l'action par $GL(E)$ est l'ensemble des éléments de $GL(E)$ qui laissent F stables, et donc si on complète une base de F en une base de E , c'est bien caractérisé matriciellement.

Exemple 21. Le stabilisateur de Δ est l'identité et le retournement suivant Delta.

Exemple 22. Stabilisateur pour l'action de conjugaison sur les matrices: c'est l'ensemble des éléments inversibles de l'algèbre que représente le commutant de u

Proposition 1. Si φ est une action de groupe définie par automorphismes, alors $\text{Ker } \varphi = \bigcap_{x \in X} \text{Stab}(x)$.

Définition 7. [3] Soit X et X' deux G -ensembles. Un morphisme de G -ensembles est une application $f : X \rightarrow X'$ vérifiant: $\forall g \in G, \forall x \in X, f(g.x) = g.(f(x))$. Un isomorphisme de G -ensemble est une application bijective $f : X \rightarrow X'$ telle que f et f^{-1} soient des G -morphisms. Il suffit pour cela que f en soit un.

Théorème 1. soit $x \in X$. Alors $\text{Orb}(x)$ est isomorphe en temps que G -ensemble à $G/\text{Stab}(x)$ [3] (l'action sur le quotient étant l'action de translation). Notamment si G est fini, $\text{Orb}(x)$ est fini et $|\text{Orb}(x)|$ divise $|G|$.

Corollaire 1 (Formule des classes). Supposons G et X finis. Soit ω un ensemble de représentants des orbites de X . Alors $|X| = \sum_{x \in \omega} \frac{|G|}{|\text{Stab}(x)|}$.

Application 5. En utilisant l'action de conjugaison, on montre que le centre d'un p -groupe n'est jamais trivial. [1] On en déduit que si G un groupe d'ordre p^α . Alors $\forall i \leq \alpha$, il existe un sous-groupe distingué d'ordre p^i . Un p -groupe n'est donc jamais simple (sauf si c'est $\mathbb{Z}/p\mathbb{Z}$).

Application 6 (Théorème de Cauchy). [2][page 45] Soit G un groupe d'ordre n et p un facteur premier de n . Alors on montre en faisant agir $\mathbb{Z}/p\mathbb{Z}$ sur G^p qu'il existe des éléments d'ordre p dans G .

Application 7 (Théorèmes de Sylow). [1][page 19] Soit G un groupe d'ordre $p^\alpha m$ avec $p \wedge m = 1$. Alors G admet au moins un sous-groupe d'ordre p^α , ces sous-groupes sont tous conjugués et leur nombre est un diviseur de m , congru à 1 modulo p .

Application 8 (Théorème de Wedderburn). [1][page 82] Soit k un corps fini. On montre en faisant agir k^* sur lui-même par conjugaison que l'hypothèse de commutativité dans la définition des corps découle des autres axiomes.

Application 9. [1][fin du chapitre 4]

$$GL(2, \mathbb{F}_2) = SL(2, \mathbb{F}_2) = PSL(2, \mathbb{F}_2) \simeq S_3.$$

$$PGL(2, \mathbb{F}_3) \simeq S_4; PSL(2, \mathbb{F}_3) \simeq A_4.$$

$$PGL(2, \mathbb{F}_3) = PGL(2, \mathbb{F}_3) \simeq A_5.$$

$$PGL(2, \mathbb{F}_5) \simeq S_5; PSL(2, \mathbb{F}_5) \simeq A_5.$$

2.3 Formule de Burnside[2][pages 43,44,50,170].

Théorème 2. Soit G un groupe fini agissant sur un ensemble fini X . Soit $g \in G$. on note $\text{fix}(g)$ l'ensemble des points fixes de g pour l'action de G sur X . Alors le nombre d'orbites vaut $\frac{1}{|G|} \sum_{g \in G} |\text{fix}(g)|$

Application 10. On se donne 4 perles rouges, 3 perles bleues et 2 perles jaunes. On peut à l'aide de ses éléments fabriquer 76 colliers différents. Si on se donne 4 perles rouges, 6 perles bleues et 4 perles jaunes, on peut fabriquer 7575 colliers différents.

Application 11. Il y a 57 manières de colorier le cube avec 3 couleurs (ou moins). Il y a $\frac{1}{24} * (|C|^6 + 6 * |C|^3 + 8 * |C|^2 + 6 * |C|^3 + 3 * |C|^4)$ manières de colorier le cube avec C couleurs (ou moins).

Faire de même avec tétraèdre et icosaèdre en utilisant la formule $\frac{1}{|G|} \sum |C|^{\gamma(g)}$ où $\gamma(g)$ désigne le nombre de cycles de g dans sa décomposition en cycles à supports disjoints

Application 12 (sous-groupes du groupe des déplacements[2][page 171]). En utilisant l'action d'un sous-groupe fini sur ses pôles décrites précédemment, tout sous-groupe fini d'ordre supérieur ou égal à 2 de l'ensemble des déplacements de l'espace est isomorphe soit au sous-groupes des racines n -ièmes de l'unité, soit au groupe diédral $D_{n/2}$, soit à A_4 ou A_5 ou S_5 .

Application 13 (Fermat [2][page 170]). n^p est congru à n modulo p .

3 Produits semi-directs

Définition 8. Soit N et H deux groupes et φ une action de H sur N définie par automorphismes de groupes (ie tombe dans $\text{Aut}(N)$!!!!!!). La loi suivante sur $N \rtimes H$: $(n, h)(n', h') = (n\varphi(h)n', hh')$ définit une loi de groupe $N \rtimes H$ appelé produit semi-direct de N par H noté $N \rtimes_\varphi H$.

Remarque 3. N est un sous-groupe distingué de $N \rtimes_\varphi H$ au contraire de H qui n'en est pas un en général. On a même:

Théorème 3. $N \rtimes_\varphi H$ abélien $\Leftrightarrow \varphi$ trivial $\Leftrightarrow H$ distingué.

Remarque 4. Si N est distingué dans G et que H est un sous-groupe de G alors NH est un groupe.

Théorème 4. Soit G un groupe, H et N , avec N distingué dans G , $NH = G$ et $N \cap H = 1$. Alors G s'écrit comme produit semi-direct $H \rtimes K$.

Remarque 5. Il existe des groupes qui ne sont pas décomposables en produits semi-directs de la forme $\mathbb{Z}/\mathbb{Z}$, par exemple parmi les 5 groupes d'ordre 8, on en a trois abéliens, le diédral D_4 et le groupe des quaternions H_8 pas décomposable.

3.1 Dévissage des groupes diédraux, symétriques, et de $Aut(S_6)$

Théorème 5. *Le groupe S_n est isomorphe à un produit semi-direct $A_n \rtimes Z_2$, la section étant n'importe quelle transposition (on envoie sur sa signature), cela donne les mêmes produits.*

Théorème 6. *Le groupe diédral D_n est isomorphe à un produit semi-direct $Z/nZ \rtimes Z_2$.*

Application 14. *Les sous-groupes d'ordre 8 sont les sous-groupes abéliens, le groupe diédral et le groupe des quaternions*

Théorème 7. *Le groupe $Aut(S_6)$ est isomorphe à $S_6 \rtimes Z_2$.*

3.2 Groupes d'ordre p et p^2

Proposition 2. *Tout sous-groupe d'ordre p est abélien et même cyclique isomorphe à Z_p .*

Exemple 23. $NA(1) = NA(3) = \dots = NA(59)$.

Application 15. *Tout sous-groupe d'ordre p^2 est commutatif et isomorphe à Z/p^2Z ou $Z/pZ \times Z/pZ$.*

Exemple 24. *valable pour 4, 9, 32, 49, 64..*

3.3 Groupes d'ordre pq

Théorème 8. *Tout sous-groupe d'ordre pq est isomorphe à $Z/pZ \times Z/qZ$ si p et $q-1$ sont premiers entre eux, si p divise $q-1$ alors on a deux classes d'isomorphie, $Z/pZ \times Z/qZ$ et au produit semi-direct $Z/pZ \rtimes Z/qZ$*

Exemple 25. *Sous-groupes d'ordre 6: S_3 et $Z/3Z$. Sous-groupes d'ordre 15, 33, 51, 35: seulement ceux abéliens. Sous-groupes d'ordre 10, 14, 21, 22, 26, 34, 38, 58: l'abélien et le produit semi-direct.*

References

[1] Perrin

[2] Combes

[3] Quéré

[4] Lelong-Ferrand Arnaudiès Algèbre

Rajouter les produits semi-directs.