103 – Exemples de sous-groupes distinguées et de groupes quotients. Applications.

Références : Gourdon Algèbre, Cortella, Rombaldi, Perrin

Cadre : Soit $(G, \times)$ un groupe et H un sous-groupe de G.

1 La relation d'équivalence modulo H

1.1 Indice d'un groupe

Définition 1. On définit la relation d'équivalence R sur G par : $xRy \iff xy^{-1} \in H$.
La classe d'équivalence de $g \in G$ est de la forme $gH = \{gh \mid h \in H\}$.
L'ensemble des classes est noté $G/H = \{gH \mid g \in G\}$ et est appellé ensemble des classes à gauches modulo H.
De la même manière, on définit $H = \{Hg \mid g \in G\}$ l'ensemble des classes à droites modulo H.
On définit l'indice du sous-groupe H comme le cardinal de G/H, noté $[G : H]$.

Remarque 2. On note $\pi_H : g \mapsto gH$ qui est surjective de G dans G/H.

Lemme 3 (Des Bergers). *L'ensemble G/H forme une partition de G.*

Théorème 4 (De Lagrange). *Soit G un groupe fini d'ordre $2 \leq n$ et H un sous-groupe de G. Alors :*

$$\#(G) = [G : H]\#(H)$$

Autrement dit, l'ordre de tout sous-groupe de G divise l'ordre de G.

1.2 Les sous-groupes distingués

Définition 5. On dit qu'un sous-groupe H de G est distingué dans G si $\forall g \in G$, $Hg = gH$. Autrement dit les classes à gauches et à droites modulo H sont les mêmes

Proposition 6. *Soit H un sous-groupe de G. H est distingué dans $G \iff \forall x \in G$, $xHx^{-1} \subset H$.*

Exemple 7.
- Les groupes $\{e\}$ et G sont distingués dans G
- L'intersection de deux sous-groupes distingués est un sous-groupe distingué
- Si G est abélien, tout les sous-groupes sont abéliens. C'est le cas des sous-groupes de $(\mathbb{Z}, +)$: ses sous-groupes sont les $n\mathbb{Z}$, qui sont distingués.
- Le centre $Z(G)$ d'un groupe est un sous-groupe distingué

Proposition 8. *Soit $\varphi : G \to G'$ un morphisme entre deux groupes et H, H' deux sous-groupes respectifs de G, G'. Alors*
- *Si φ est surjective et H est distingué, φ, alors $\varphi(H)$ est distingué dans G'*
- *Si H' est distingué, alors $\varphi^{-1}(H')$ est distingué dans G*
- *En particulier, $\ker(\varphi)$ est toujours un sous-groupe distingué de G*

Définition 9. Un groupe G est dit simple si ses seuls sous-groupes distingués sont $\{e\}$ et lui-même.

Exemple 10. Soit H un sous-groupe de G d'indice 2, alors H est distingué dans G

2 Le passage au quotient

2.1 Groupe quotient

Théorème 11. *Soit H un sous-groupe distingué de G. On peut munir G/H d'une loi $'\times'$ qui vérifie $\forall (x, y) \in G^2$: $\pi_H(xy) = \pi_H(x)\pi_H(y)$, ce qui fait de $(G/H, \times)$ un groupe d'ordre $[G : H]$. Dans ce cas, π_H est un morphisme de groupe surjectif entre G et G/H.*

Remarque 12. L'élément neutre de $(G/H, \times)$ est $\pi_H(1) = H$.

Théorème 13. *(d'isomorphisme) Soit $\varphi : G \to G'$ un morphisme de groupe. Il existe alors un unique isomorphisme de groupe $\bar{\varphi} : G/\ker(\varphi) \to Im(\varphi)$.*

Corollaire 14. *Soit $\varphi : G \to G'$ un morphisme de groupe. Si G est d'ordre finie, alors :*

$$\#(G) = \#(\ker(\varphi))\#(Im(\varphi))$$

Exemple 15. Soit $\mathbb{K}$ un corps. Alors $SL_n(\mathbb{K})$ est un sous-groupe distingué de $GL_n(\mathbb{K})$, et le groupe quotient $GL_n(\mathbb{K})/SL_n(\mathbb{K})$ est isomorphe à $\mathbb{K}^*$ via le morphisme de groupe surjectif $\det : GL_n(\mathbb{K}) \to \mathbb{K}^*$.

Exemple 16. $O_n(\mathbb{R})/SO_n(\mathbb{R}) \sim \dfrac{\mathbb{Z}}{2\mathbb{Z}}$

Exemple 17. Exemple supplémentaire dans le Cortella

Application 18. *Soit G un groupe opérant sur un ensemble X. Alors $\forall x \in X$ l'application $\varphi_x : gStab_x \mapsto O(x)$ est un isomorphisme entre $G/Stab_x$ et l'ensemble des orbites de x sous G. Dans le cas où G est fini, on à :*

$$\#(G) = [G : Stab_x]\#(Stab_x)$$

Application 19 (Equations aux classes). *Avec le lemme des bergers et l'application ci-dessus, on à, dans le cas où G est fini :*

$$\#(X) = \sum_{Syst\ de\ repré\ \ x_i} \frac{\#(G)}{\#(Stab_{x_i})}$$

2.2 Théorèmes de Sylows

Définition 20. Soit G un groupe d'ordre $n = p^a m$ avec p qui ne divise pas m. On appelle p-sylow tout sous-groupe de G d'ordre p^a.

Exemple 21. On exhibe un p-sylow de $GL_n(\mathbb{F}_p)$.

Théorème 22 (1er et 2ème théorème de Sylow). *Soit G un groupe d'ordre $n = p^a m$ avec p qui ne divise pas m. Alors il existe un sous-groupe de G d'ordre p^a.*
De plus, tout les p-Sylows de G sont conjugués

Théorème 23 (3ème théorème de Sylow). *On note N_p le nombre de p-Sylows de G, il vérifie $N_p | m$ et $N_p \equiv 1 \pmod p$*

Application 24. *Soit G un groupe fini d'ordre $n = p^a m$ avec p qui ne divise pas m. Si G possède un unique p-sylow, alors celui-ci est distingué dans G*

Exemple 25. Il n'existe pas de groupe simple d'odre 63.

2.3 Groupe dérivée

Définition 26. Soit G un groupe. On appelle sous-groupe dérivée de G le sous-groupe engendré par les commutateurs de G , c'est-à-dire : $D(G) = \{xyx^{-1}y^{-1} \mid (x,y) \in G^2\}$.

Proposition 27. *$D(G)$ est un sous-groupe distingué de G.*

Exemple 28.
— Si G est abélien, $D(G) = 1$
— Si G=S_3, $D(G) = \{1, c_{1\to 3}, c_{1\to 3}\}$

Théorème 29. *Le groupe dérivée est le plus petit sous-groupe distingué H de G tel que le groupe G/H soit commutatif.*

3 Deux exemples fondamentaux

3.1 Le groupe $\frac{\mathbb{Z}}{n\mathbb{Z}}$

Définition 30. Comme les $n\mathbb{Z}$ sont des sous-groupes distingués de $\mathbb{Z}$, $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est bien un groupe à n éléments.

Exemple 31. Par le théorème d'isomorphisme : $\frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \mu_n$

Proposition 32. *$\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un groupe cyclique à n éléments. Tout groupe cyclique d'ordre n lui est isomorphe.*

Proposition 33. *$\overline{k}$ est générateur de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ $\iff$ $k \wedge n = 1$*

Application 34. *$\frac{\mathbb{Z}}{n\mathbb{Z}}$ est simple $\iff$ n est premier.*

Théorème 35.
— *Les sous-groupes de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ sont cycliques d'ordre d qui divise n.*
— *Réciproquement, pour tout d qui divise n, il existe un unique sous-groupe de $\frac{\mathbb{Z}}{n\mathbb{Z}}$. Il s'agit de l'ensemble des éléments de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ d'ordre qui divise d. Ses générateurs sont les éléments d'ordre d.*

Application 36. $n = \sum_{d|n} \varphi(d)$

Pour n=$2, 4, p^\alpha, 2p^\alpha$ $(p > 2)$, $(\frac{\mathbb{Z}}{n\mathbb{Z}})^\times$ est cyclique.

3.2 Le groupe symétrique S_n

Définition 37. On définit le groupe alternée A_n comme le noyau de la signature ε.

Proposition 38. *A_n est un sous-groupe distingué de S_n, d'indice 2, de cardinal $\frac{n!}{2}$, engendré par les 3-cycles.*

Lemme 39. *Les 3-cycles sont conjuguées dans A_n*

Théorème 40. *Pour tout $n > 4$, A_n est simple.*

Proposition 41. *Pour $n > 4$, $D(A_n) = A_n$ et $D(S_n) = S_n$.*