Sous-groupe distingué

Samuel Rochetin

Mardi 2 mai 2017

Problème. *Soit G un groupe fini et p le plus petit diviseur premier de $|G|$. Supposons qu'il existe un sous-groupe H de G d'indice p, c'est-à-dire tel que $[G : H] = \#G/H = p$. Le but de l'exercice est de montrer que H est distingué dans G. Il s'agit d'une généralisation de l'exercice de cours traitant du cas où $p = 2$ (puisque 2 est le plus petit nombre premier).*

1. *Pour tout $(g, a) \in G^2$ et pour tout $aH \in G/H$, nous définissons $g \cdot aH := gaH$.*
   (a) *Montrer que l'application $f : G \times G/H \to G/H, (g, aH) \mapsto g \cdot aH$ est bien définie.*
   (b) *Montrer que l'application f définit une action de groupe.*
2. *Soit $g \in G$ fixé. Considérons l'application $\varphi_g : G/H \to G/H, aH \mapsto g \cdot aH$.*
   (a) *Montrer que φ_g est une bijection et déterminer son inverse.*
   (b) *En déduire qu'il existe un morphisme $\phi : G \to \mathfrak{S}_{G/H}$, où $\mathfrak{S}_{G/H}$ est le groupe des permutations de G/H.*
3. (a) *Soit $K = \ker \phi$. Montrer que K est un sous-groupe distingué de G.*
   (b) *Soit $x \in K$. Montrer que pour tout $a \in G, a^{-1}xa \in H$. En déduire que $K \subset H$.*
4. (a) *Montrer que $|\mathfrak{S}_{G/H}| = p!$.*
   (b) *Montrer qu'il existe un isomorphisme de G/K sur $\phi(G)$.*
   (c) *Montrer que $|\phi(G)|$ divise $p!$ et en déduire que $[G : K]$ divise $p!$.*
   (d) *Montrer que $[G : K] = p \times \dfrac{|H|}{|K|}$ et en déduire que $\dfrac{|H|}{|K|}$ divise $(p-1)!$.*
   (e) *Soit q un diviseur premier de $\dfrac{|H|}{|K|}$. Montrer que $q < p$ et que q divise $|G|$.*
   (f) *En déduire que $K = H$. Conclure.*

Corrigé. 1. (a) Tout d'abord, l'ensemble d'arrivée est bien G/H : en effet, $(g, a) \in G^2$ donc $ga \in G$ donc $gaH \in G/H$. Pour montrer que l'application f est bien définie, nous devons montrer que $(g, aH) = (g', a'H) \implies f(g, aH) = f(g', a'H)$. Si $(g, aH) = (g', a'H)$, alors $g = g'$ et $aH = a'H$. Donc $gaH = \{gx, x \in aH\} = \{gy, y \in a'H\} = \{g'y, y \in a'H\} = g'a'H$, autrement dit $f(g, aH) = f(g', a'H)$.

(b) Il suffit de vérifier les deux axiomes de la définition d'une action de groupe. Soit $(g, g', a) \in G^3$. Nous avons $g \cdot (g' \cdot aH) = g \cdot (g'aH) = g(g'aH) = (gg')aH = (gg') \cdot aH$ et $e \cdot aH = eaH = aH$. Donc f définit une action du groupe G sur l'ensemble G/H (multiplication à gauche).

2. (a) Soit $aH \in G/H$. Nous avons $aH = gg^{-1}aH = g \cdot (g^{-1}a)H$ et $(g^{-1}a)H \in G/H$, donc φ_g est surjective. Soit $(aH, a'H) \in (G/H)^2$ tel que $\varphi_g(aH) = \varphi_g(a'H)$. Alors $gaH = ga'H$, donc $(g^{-1}, gaH) = (g^{-1}, ga'H)$, et puisque nous avons montré que f était une application bien définie, $f(g^{-1}, gaH) = f(g^{-1}, ga'H)$, c'est-à-dire $aH = a'H$. Donc φ_g est injective. Donc φ_g est une bijection. Avec les axiomes définissant une action de groupe, nous pouvons vérifier aisément que $\varphi_g^{-1} = \varphi_{g^{-1}}$. En effet, $\varphi_{g^{-1}} \circ \varphi_g(aH) = g^{-1} \cdot (g \cdot aH) = g^{-1}gaH = aH$. De même pour $\varphi_g \circ \varphi_{g^{-1}}(aH)$.

   (b) Nous venons de voir qu'à chaque élément $g \in G$, nous pouvions associer une (unique) bijection $\varphi_g \in \mathfrak{S}_{G/H}$. Nous avons donc une application $\phi : G \to \mathfrak{S}_{G/H}$. Il reste à montrer que ϕ est un morphisme. Soit $(g, g') \in G^2$. Avec les axiomes définissant une action de groupe, nous avons $\phi(gg') = \varphi_{gg'} = \varphi_g \circ \varphi'_g = \phi(g) \circ \phi(g')$, donc ϕ est bien un morphisme.

3. (a) K est le noyau du morphisme $\phi : G \to \mathfrak{S}_{G/H}$, donc K est un sous-groupe distingué de G (proposition du cours).

   (b) Si $x \in K$, alors $\phi(x) = Id_{\mathfrak{S}_{G/H}}$. Donc pour tout $a \in G, aH = xaH$, donc $H = a^{-1}xaH$, donc $a^{-1}xa \in H$. Ceci étant valable pour tout $a \in G$, ça l'est en particulier pour $a = e$, et il vient $x \in H$. Donc $K \subset H$.

4. (a) Par définition, $[G : H] = \#G/H = p$, donc $|\mathfrak{S}_{G/H}| = p!$.

   (b) Nous avons un morphisme de groupes $\phi : G \to \mathfrak{S}_{G/H}$ de noyau K, donc d'après le premier théorème d'isomorphisme, il existe un isomorphisme de G/K sur $\phi(G)$.

   (c) $\phi(G)$ est un sous-groupe de $\mathfrak{S}_{G/H}$, donc d'après le théorème de Lagrange, $|\phi(G)|$ divise $|\mathfrak{S}_{G/H}| = p!$. D'après le théorème de Lagrange et le premier théorème d'isomorphisme, nous avons $[G : K] = \dfrac{|G|}{|K|} = |\phi(G)|$. Donc $[G : K]$ divise $p!$.

   (d) D'après le théorème de Lagrange, $[G : K] = \dfrac{|G|}{|K|} = \dfrac{|G|}{|H|} \times \dfrac{|H|}{|K|} = [G : H] \times \dfrac{|H|}{|K|} = p \times \dfrac{|H|}{|K|}$. Or, $[G : K]$ divise $p!$, donc $p \times \dfrac{|H|}{|K|}$ divise $p! = p \times (p-1)!$, c'est-à-dire $\dfrac{|H|}{|K|}$ divise $(p-1)!$.

   (e) q divise $\dfrac{|H|}{|K|}$ et $\dfrac{|H|}{|K|}$ divise $(p-1)!$ donc q divise $(p-1)!$. Puisque p est premier et que $(p-1)! = 1 \times 2 \times \cdots \times (p-1)$, tout diviseur

premier de $(p-1)!$ est nécessairement inférieur à $p-1$, donc $q < p$. Ensuite, si q divise $\dfrac{|H|}{|K|}$, alors q divise $|H|$. Or, d'après le théorème de Lagrange, $|H|$ divise $|G|$, donc q divise $|G|$.

(f) Le résultat de la question précédente contredit la minimalité de p. Donc $\dfrac{|H|}{|K|}$ n'admet pas de diviseur premier et vaut 1, autrement dit $|K| = |H|$. Or, nous avons $K \subset H$, donc $K = H$. Or, K est un sous-groupe distingué de G, donc H est bien un sous-groupe distingué de G, ce que nous voulions démontrer.

□