Fiche 3 : un exercice abordé mais peu détaillé en td

Exercice 12 *Soit p un nombre premier, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/\mathbb{Z}_p$ et on identifie $\mathfrak{S}_p$ avec le groupe de bijections de $\mathbb{F}_p$. On note $GA(p)$ le groupe des bijections affines de $\mathbb{F}_p$, i.e. l'ensemble des applications*

$$\begin{array}{rccc} f_{a,b} & : \mathbb{F}_p & \longrightarrow & \mathbb{F}_p \\ & x & \longmapsto & ax+b \ , \end{array}$$

où $a \in \mathbb{F}_p^*$ et $b \in \mathbb{F}_p$. On pose $t = f_{1,1}$ et $m_a = f_{a,0}$.

(a) *Montrer que le groupe $GA(p)$ est résoluble.*

Réponse : Nous démontrerons un peu plus que ce qui est demandé : $GA(p) = T \rtimes M$ avec $T = \langle t \rangle$ et $M = \{m_a \mid a \in \mathbb{F}_p\}$. Les tâches de vérifier que $GA(p)$ est un ensemble de permutations de $\mathbb{F}_p$ et que, muni de la composition des permutations, il est un sous-groupe de $\mathfrak{S}_p$ sont laissées aux lecteurs. Il en est de même pour M. Notez aussi que M est un groupe commutatif, en fait il est isomorphe au groupe $(\mathbb{F}_p^\times, .)$. Par ailleurs, T est isomorphe au groupe $(\mathbb{F}_p, +)$.

Pour démontrer la décomposition en produit semi-direct recherchée, nous vérifierons les trois conditions pour les produits semi-directs. Vérifons d'abord que $T \cap M = \{1\}$. Il suffit de comparer deux éléments arbitrairement choisis, l'un de T l'autre de M :

$$t^b(x) \ = \ m_a(x) \ \text{ si et seulement si } \ x+b \ = \ ax \ \text{ si et seulement si } \ b=0 \text{ et } a=1 \ .$$

Ensuite, vérifions que $T \lhd GA(p)$. En effet, si $m_a \in M$, $t \in T$ et $b \in \mathbb{F}_p$, alors

$$m_a t m_a^{-1} \ = \ m_a t^b(a^{-1}x) \ = \ m_a(a^{-1}+b) \ = \ x+ab \ = \ t_{ab}(x) \ .$$

Finalement, vérifions que le groupe $GA(p)$ se factorise comme produit de T et de M, en d'autres termes, que $GA(p) = TM$. En effet, pour tout $f_{a,b} \in GA(p)$ et tout $x \in \mathbb{F}_p$,

$$f_{a,b}(x) \ = \ ax+b \ = \ t^b(ax) \ = \ t^b(m_a(x)) \ .$$

A ce stade, un calcul assez rapide (faites-le) montre que le groupe dérivé $GA(p)' = T$ si $p \neq 2$ et $GA(p)' = \{1\}$ si $p = 2$. Comme T est commutatif, si $p \neq 2$, alors $GA(p)$ est résoluble de classe 2. Quand $p = 2$, $GA(p)$ est commutatif, donc résoluble de classe 1.

(b) *Soit G un sous-groupe de $\mathfrak{S}_p$ transitif, montrer que tout sous-groupe distingué non trivial de G est encore transitif.*

Réponse : Soient G comme dans l'énoncé, et N un sous-groupe distingué de G. Nous supposons $N \neq \{1\}$. Montrons que N agit transitivement sur $\mathbb{F}_p$.

Comme G est un groupe de permutations, l'action de G sur $\mathbb{F}_p$ n'a pas de noyau, en d'autres termes aucun élément de G ne fixe $\mathbb{F}_p$ entièrement. Rappelons aussi que pour tous $g \in G$ et $x \in \mathbb{F}_p$

$$\mathrm{Stab}_G(gx) = g\mathrm{Stab}_G(x)g^{-1} \ .$$

Ainsi, comme $N \lhd G$ et que G agit transitivement sur $\mathbb{F}_p$,

$$\text{pour tout } x \in \mathbb{F}_p, \ N \not\leq \mathrm{Stab}_G(x) \ .$$

Soulignons que ce raisonnement monre en fait le lemme général suivant :

Lemme : *Soit Γ un groupe de permutations d'un ensemble X. Si N est un sous-groupe distingué et non trivial de Γ, alors pour tout $x \in X$, $N \not\leq \mathrm{Stab}_\Gamma(x)$; en d'autres termes, le stabilisateur d'un point arbitraire ne contient pas de sous-groupe non trivial distingué dans Γ.*

Par ailleurs,

$$\begin{aligned} |\mathrm{orb}_N(x)| &= |N/\mathrm{Stab}_N(x)| \\ &= |N/\mathrm{Stab}_G(x) \cap N| \\ &= |\mathrm{Stab}_G(x)N/N| \ . \end{aligned}$$

Notons aussi que N étant un sous-groupe distingué de G, l'ensemble $N\mathrm{Stab}_G(x)$ est en fait un sous-groupe de G. Les calculs de cardinal ci-dessus montre que $N\mathrm{Stab}_G(x)$ est un sous-groupe strictement plus grand que $\mathrm{Stab}_G(x)$. Comme G agit transitivement sur $\mathbb{F}_p$, $[G : \mathrm{Stab}_G(x)] = p$. Ainsi, il n'y a qu'une possibilité pour $N\mathrm{Stab}_G(x)$, notamment $G = \mathrm{Stab}_G(x)N$. Ceci équivaut à dire que chaque classe de $\mathrm{Stab}_G(x)$ contient un élément de N, en d'autres termes N agit transitivement sur $\mathbb{F}_p$.

(*c*) *Soit G un sous-groupe de $\mathfrak{S}_p$ transitif et résoluble. On note $(H_i)_{1\leq i\leq r}$ la suite décroissante des groupes dérivés ($H_r = \{1\}$).*
(*i*) *Montrer que H_{r-1} est conjugué au groupe T.*
(*ii*) *Soit $\sigma \in \mathfrak{S}_p$ tel que $\sigma\tau\sigma^{-1} \in GA(p)$. Montrer que σ est dans $GA(p)$.*
(*iii*) *En déduire que G est un conjugué à un sous-groupe de $GA(p)$.*
Réponse : (i) Nous suivrons la notation de l'énoncé. Alors, H_{r-1} est un sous-groupe non trivial, commutatif et distingué de G. Etant non trivial et distingué, c'est un sous-groupe transitif. Comme c'est un sous-groupe commutatif, tous ses sous-groupes sont distingués. Alors, il découle du lemme général du point (b) que $\mathrm{Stab}_{H_{r-1}}(x) = \{1\}$. Par conséquent $|H_{r-1}| = p$. En particulier, H_{r-1} est un groupe cyclique. Si τ est un générateur de H_{r-1}, alors il induit une permutation de la forme

$$(\ 0 \ \tau(0) \ \dots \ \tau^{p-1}(0) \ ) \ ,$$

avec 0 l'élément neutre de $(\mathbb{F}_p, +)$. Comme l'élément t aussi induit une telle permutation, ils sont conjugués dans $\mathfrak{S}_p$.

(ii) Soit $\sigma \in \mathfrak{S}_p$ tel que $\sigma t\sigma^{-1} \in GA(p)$. Alors, comme $|GA(p)| = p(p-1)$ et que $|M| = p-1$, il existe $i \in \{1, \dots, p-1\}$ tel que $\sigma t\sigma^{-1} = t^i$. Il s'ensuit de cette conclusion que pour tout $x \in \mathbb{F}_p$,

$$\sigma t\sigma^{-1}(x) \ = \ x + i \ .$$

Par conséquent,

$$\sigma^{-1}(x) + 1 \ = \ \tau\sigma^{-1}(x) \ = \ \sigma^{-1}(x + i) \ .$$

Il en découle que pour tout $x \in \mathbb{F}_p$, $\sigma^{-1}(x) = i^{-1}x + \sigma^{-1}(0)$, c'est la formule d'une *droite affine sur* $\mathbb{F}_p$. Ainsi σ^{-1}, et donc σ, appartiennent à $GA(p)$.

(iii) Une conséquence du point (ii) est que $N_{\mathfrak{S}_p}(\langle t\rangle) = GA(p)$. Maintenant, d'après le point (i), le sous-groupe H_{r-1} est conjugué au sous-groupe $\langle t\rangle$. Il en découle que G, étant un sous-groupe de $N_G(H_{r-1})$ est conjugué à un sous-groupe de $N_G(\langle t\rangle)$. Or, nous venons de remarquer que ce dernier normalisateur est exactement $GA(p)$.

(*d*) *Soit G un sous-groupe transitif de $\mathfrak{S}_p$. Montrer que G est résoluble si et seulement si l'identité est le seul élément de G ayant deux points fixes.*
Réponse : La nécessité de la condition sur les points fixes découle des points précédents. En effet, si G est un sous-groupe transitif et résoluble de $\mathfrak{S}_p$, alors G est conjugué à un sous-groupe de $GA(p)$ d'après le point (c). Or, le groupe $GA(p)$ satisfait à la condition dont nous essayons de vérifier la nécessité à la résolubilité de G.

Supposons maintenant que G soit un sous-groupe transitif de $\mathfrak{S}_p$ qui satisfait à la condition sur les points fixes. D'après l'exercice 8 (b) de la fiche 2, G a un élément qui ne fixe aucun point. Appelons τ un tel élément de G. Nous montrerons que τ est un p-cycle. Puisque pour tout $x \in \mathbb{F}_p$,

$$|\mathrm{orb}_{\langle\tau\rangle}(x)| = \frac{|\tau|}{|\mathrm{Stab}_{\langle\tau\rangle}(x)|} = |\tau| \ ,$$

la formule suivante, où la somme est décrite par un élément x et un seul de chaque orbite sous l'action de $\langle\tau\rangle$:

$$p \ = \ \sum_x \ |\mathrm{orb}_{\langle\tau\rangle}(x)| \ .$$

Il s'ensuit que $|\tau| \mid p$. Ainsi $|\tau| = p$, et τ agit transitivement sur $G/\mathrm{Stab}_G(x)$.

Le dernier paragraphe montre que $G = \langle\tau\rangle\mathrm{Stab}_G(x)$. L'élément τ étant d'ordre p,

$$\langle\tau\rangle \cap \mathrm{Stab}_G(x) = \{1\} \ .$$

Par ailleurs, d'après la condition sur le nombre de points fixes,

$$\mathrm{Stab}_G(x) \cap \mathrm{Stab}_G(y) \;=\{1\} \;\text{ si et seulement si } x \neq y \;.$$

Il en découle que $N_G(\mathrm{Stab}_G(x)) = \mathrm{Stab}_G(x)$ (vérifiez les détails qui mènent à cette conclusion). Nous déduisons alors la formule suivante :

$$|G| = |\tau||\mathrm{Stab}_G(x)| = |\tau|(|\mathrm{Stab}_G(x)| - 1) + 1 + |\text{les éléments qui ne fixent aucun point}| \;.$$

Ces égalités montrent que $\langle\tau\rangle$ est formé par l'élément neutre et tous éléments de G qui ne fixent aucun point de $\mathbb{F}_p$. Ainsi $\langle\tau\rangle \lhd G$, et finalement,

$$G \;=\; \langle\tau\rangle \rtimes \mathrm{Stab}_G(x) \;.$$

L'élément τ étant un p-cycle, nous pouvons conjuguer τ à t dans $\mathfrak{S}_p$. Puisque $N_{\mathfrak{S}_p}(\langle t\rangle) = GA(p)$, cette dernière conjugaison implique que $\mathrm{Stab}_G(x)$ soit un groupe abélien. Par conséquent G est résoluble. $\square$