

Condition nécessaire et suffisante pour qu'un sous-groupe transitif soit résoluble

Cortex

October 15, 2026

Présentation Ce développement présente une condition nécessaire et suffisante pour qu'un sous-groupe transitif de $\mathfrak{S}_p$ soit résoluble, avec p un nombre premier.

Remarques préliminaires Je trouve ce résultat passionnant par la simplicité de la condition et par tout le cheminement qu'il faut effectuer pour le prouver. C'est un développement ambitieux qui nécessite d'être à l'aise avec les permutations et les actions de groupe, mais le développement présente beaucoup de résultat et fourni donc beaucoup de recasage.

Notations Dans la suite, $p > 2$ désigne un nombre premier et $\mathfrak{S}_p := \mathfrak{S}(\mathbf{F}_p)$.

- Je note $e := \text{Id}_{\mathbf{F}_p}$.
- Le groupe $\text{Aff}_p \leq \mathfrak{S}_p$ est le groupe des transformations affines de $\mathbf{F}_p$, i.e.

$$\text{Aff}_p := \{x \in \mathbf{F}_p \mapsto ax + b \in \mathbf{F}_p \mid a \in \mathbf{F}_p^\times, b \in \mathbf{F}_p\}$$

- Je note $\tau : x \in \mathbf{F}_p \mapsto x + 1 \in \mathbf{F}_p$ et pour $a \in \mathbf{F}_p^\times$, $m_a : x \in \mathbf{F}_p \mapsto ax \in \mathbf{F}_p$. On a $\tau, m_a \in \text{Aff}_p$.

Résultats admis Soit $p \geq 2$ un nombre premier :

- Si $t \in \mathfrak{S}_p$ est d'ordre p , alors c'est un p -cycle.
- Si $t \in \mathfrak{S}_p$ est un cycle transitif, alors c'est un p -cycle.
- Aff_p est engendré par τ et $(m_a)_{a \in \mathbf{F}_p^\times}$.
- Le groupe Aff_p est transitif et résoluble.

Développement

Le résultat que l'on va démontrer est le suivant.

Théorème 1 : Soit $G \leq \mathfrak{S}_p$ un sous-groupe transitif, alors il y a équivalence entre

- G est résoluble.
- Le seul élément de G avec au moins deux points fixes est e .

Pour démontrer ce résultat, nous allons utiliser un lemme.

Lemme 2 : Soit $G \leq \mathfrak{S}_p$. Si G est transitif et résoluble alors il est conjugué à un sous-groupe de Aff_p , i.e. qu'il existe $\varphi \in \mathfrak{S}_p$ et $H \leq \text{Aff}_p$ tels que $\varphi G \varphi^{-1} = H$.

Preuve du Lemme 2 Soit G un sous-groupe transitif et résoluble. Comme G est fini, je dispose d'une suite de Jordan-Hölder

$$G =: G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{r-1} \triangleright G_r = \{e\}$$

Et comme G est résoluble, pour tout $0 \leq i \leq r-1$, on a G_i/G_{i+1} cyclique d'ordre premier.

La preuve du lemme consiste à faire un "aller-retour" dans la suite ci-dessus. On parvient à faire descendre la transitivité du groupe jusqu'à G_{r-1} pour obtenir le fait que G_{r-1} est conjugué à un sous-groupe de Aff_p , et cette dernière propriété, on parvient à la faire remonter jusqu'à G .

Etape 1 Je considère $H \triangleleft G$ non trivial, montrons que H est transitif. Soient $x \neq y \in G$. Je dispose de $g \in G$ tel que $x = g(y)$. Je note $\omega_x, \omega_y \subset \mathbf{F}_p$ les orbites de x et de y sous l'action de H . Dans ce cas, si $x' \in \omega_x$, je dispose de $h \in H$ avec $x' = h(x)$ et

$$g(x') = gh(x) = ghg^{-1}(g(x)) = ghg^{-1}(y)$$

comme $ghg^{-1} \in H$ par hypothèse, il vient $g(x') \in \omega_y$. Ainsi, g induit une application

$$g : \omega_x \rightarrow \omega_y$$

d'inverse g^{-1} , donc $\text{Card}(\omega_x) = \text{Card}(\omega_y)$. En notant Ω l'ensemble des orbites et n_0 leur cardinal commun, il vient

$$\text{Card}(\mathbf{F}_p) = p = \sum_{\omega \in \Omega} \text{Card}(\omega) = n_0 \text{Card}(\Omega)$$

Mais comme H n'est pas trivial, $n_0 > 1$ et comme p est premier, $\text{Card}(\Omega) = 1$ ce qui signifie que H est transitif.

Etape 2 Je considère $\sigma \in \mathfrak{S}_p$. Montrons que si $\sigma\tau\sigma^{-1} \in \text{Aff}_p$ alors $\sigma \in \text{Aff}_p$. Pour cela, je dispose, par hypothèse, de $a \in \mathbf{F}_p^\times$ et $b \in \mathbf{F}_p$ tels que

$$\sigma\tau\sigma^{-1} = \tau^b m_a$$

Pour tout $k \geq 1$, on a

$$\sigma\tau^k\sigma^{-1} = \tau^{n_k} m_{a^k}, \quad n_k := b \sum_{i=0}^{k-1} a^i \in \mathbf{F}_p$$

dans le cas où $a \neq 1$, on peut noter $n_k = b \frac{a^k - 1}{a - 1} \in \mathbf{F}_p$ et on constate que $n_{p-1} = 0$. Cependant,

$$\sigma\tau^{p-1}\sigma^{-1} \neq e$$

nécessairement, $a = 1$. Ainsi $\sigma\tau = \tau^b\sigma$, i.e.

$$\forall x \in \mathbf{F}_p, \sigma(x+1) = \sigma(x) + b$$

et il suit par une relation de récurrence que $\sigma = \tau^{\sigma(0)} m_b \in \text{Aff}_p$.

Étape 3 La précédente étape montre que si $H \triangleleft G$, $H \leq \text{Aff}_p$ et que $\tau \in H$ alors pour tout $g \in G$, on a $g\tau g^{-1} \in H \leq \text{Aff}_p$ donc $G \leq \text{Aff}_p$. Reprenons alors la suite de Jordan-Hölder. Par la première étape, $G_1, G_2, \dots, G_{r-1}$ sont transitifs. De plus, G_{r-1} est cyclique. Notons $t \in G_{r-1}$ tel que $\langle t \rangle = G_{r-1}$. t est transitive donc c'est un p -cycle. Comme tous les p -cycles sont conjugués entre-eux, je dispose de $\varphi \in \mathfrak{S}_p$ tel que

$$\varphi t \varphi^{-1} = \tau, \quad \varphi G_{r-1} \varphi^{-1} \leq \text{Aff}_p$$

Je note pour tout $0 \leq i \leq r-1$, $H_i := \varphi G_i \varphi^{-1}$. On a par récurrence

$$H_i \leq \text{Aff}_p, \quad H_i \triangleleft H_{i-1}$$

pour obtenir $H_0 = \varphi G \varphi^{-1} \leq \text{Aff}_p$, ce qui conclut le lemme.

Preuve du Théorème 1

Sens direct Si G est transitif et résoluble alors il s'agit du conjugué d'un sous-groupe de Aff_p . Comme la conjugaison préserve les propriétés géométriques, elle préserve également le nombre de point fixe. Comme une transformation affine d'une droite est déterminable en deux points, on en déduit que tout élément avec au moins deux points fixes est e .

Sens indirect Supposons que G soit transitif et que si $g \in G$ possède au moins deux points fixes, alors $g = e$. Dans ce cas, je peux séparer G en trois parties. Les ensembles des éléments avec i points fixes seront notés P_i ,

$$\text{Card}(G) = \text{Card}(P_0) + \text{Card}(P_1) + \text{Card}(P_2) = \text{Card}(P_0) + \text{Card}(P_1) + 1$$

Je considère l'action de G sur $\mathbf{F}_p$, pour $x \in \mathbf{F}_p$, on a par hypothèse

$$\text{Card}(G) = \text{Card}(\omega_x) \text{Card}(G_x) = p \text{Card}(G_x)$$

D'une part $p \mid \text{Card}(G)$ donc G possède un élément d'ordre p , d'autre part, $\text{Card}(G_x)$ ne dépend pas de x . Notons $q := \text{Card}(G_x)$. Si $x \neq y \in \mathbf{F}_p$ et $g \in G_x \cap G_y$, alors $g(x) = x$ et $g(y) = y$ donc $g = e$ par hypothèse. Ainsi, $G_x \cap G_y = \{e\}$. Comme

$$P_1 = \bigsqcup_{x \in \mathbf{F}_p} (G_x \setminus \{e\})$$

On a $pq = \text{Card}(G) = \text{Card}(P_0) + p(q-1) + 1$, d'où $\text{Card}(P_0) = p-1 \geq 1$.

Comme dit précédemment, G possède un élément d'ordre p , donc un p -cycle que je note t et on a

$$\langle t \rangle \subset P_0 \cup \{e\}, \quad p = \text{Card}(\langle t \rangle) \leq \text{Card}(P_0) + 1 = (p-1) + 1 = p$$

donc tous les éléments sans points fixes de G sont de la forme $\{t, \dots, t^{p-1}\}$.

Je dispose de $\varphi \in \mathfrak{S}_p$ tel que $\varphi t \varphi^{-1} = \tau$ et note $H := \varphi G \varphi^{-1}$. Soit $h \in H$, comme $h\tau h^{-1} \in H$ ne possède pas de point fixe, alors $h\tau h^{-1} \in \langle \tau \rangle \leq \text{Aff}_p$ et $h \in \text{Aff}_p$ d'où $H \leq \text{Aff}_p$.

Ainsi H est résoluble, et comme la résolubilité est préservée par conjugaison, G est résoluble.

Remarques a posteriori

- Pour les contre-exemples du Lemme 2. Le groupe $\mathfrak{A}_5$ est transitif et non-résoluble et comme $\text{Card}(\text{Aff}_5) = 4 \times 5 = 20$ et $\text{Card}(\mathfrak{A}_5) = 60$, $\mathfrak{A}_5$ n'est pas un sous-groupe conjugué de Aff_5 . Par ailleurs, Je pose l'injection $\mathfrak{S}_3 = \text{Aff}_3 \hookrightarrow \mathfrak{S}_5$, et note l'image G . Alors G est résoluble mais non transitif et $\text{Card}(G) = 2 \times 3 = 6$, ce qui ne peut pas être un sous-groupe de Aff_5 .

De même, la condition p premier est importante. Il y a deux manières de généraliser Aff_n pour n non premier. Si n est une puissance de nombre premier, alors on peut travailler dans $\mathbf{F}_n$, sinon, dans $\mathbf{Z}/n\mathbf{Z}$, ce qui donne respectivement,

$$\text{Aff}(\mathbf{F}_q) := \{x \in \mathbf{F}_q \mapsto ax + b \mid a \in \mathbf{F}_q^\times, b \in \mathbf{F}_q\}$$

ou

$$\text{Aff}(\mathbf{Z}/n\mathbf{Z}) := \{x \in \mathbf{Z}/n\mathbf{Z} \mapsto ax + b \in \mathbf{Z}/n\mathbf{Z} \mid a \in (\mathbf{Z}/n\mathbf{Z})^\times, b \in \mathbf{Z}/n\mathbf{Z}\}$$

Dans le deux cas, on prend $n = 4$, les groupes $\mathfrak{A}_4$, $\text{Aff}(\mathbf{Z}/4\mathbf{Z})$ et $\text{Aff}(\mathbf{F}_4)$. On a

$$\text{Card}(\mathfrak{A}_4) = \text{Card}(\text{Aff}(\mathbf{F}_4)) = 12, \quad \text{Card}(\text{Aff}(\mathbf{Z}/4\mathbf{Z})) = 8$$

Donc $\mathfrak{A}_4$ est un sous-groupe transitif et résoluble mais ce n'est pas un sous-groupe de $\text{Aff}(\mathbf{Z}/4\mathbf{Z})$ et $\text{Aff}(\mathbf{Z}/4\mathbf{Z})$ est un sous-groupe transitif et résoluble mais ce n'est pas un sous-groupe de $\text{Aff}(\mathbf{F}_4)$.

- Pour les contre-exemples du Théorème 1. La condition de transitivité à son importance : on peut reprendre l'injection $\mathfrak{S}_3 \hookrightarrow \mathfrak{S}_5$ ce qui donne un sous-groupe résoluble non transitif qui possède un élément avec deux points fixes qui n'est pas l'identité $((1 \ 2 \ 3))$.

De même, la condition être premier est importante. $\text{Aff}(\mathbf{Z}/4\mathbf{Z})$ est transitif et résoluble mais l'application $x \mapsto -x$ possède deux points fixes. En revanche, dans le sens réciproque, je n'ai pas de contre-exemple, il faudrait trouver $G \leq \mathfrak{S}_n$ qui ne soit ni transitif, ni résoluble et qui possède uniquement e comme élément avec 2 points fixes.

- Il faut être capable de prouver les résultats admis.
- Dans la preuve du Théorème 1, le sens indirect ne peut pas être simplifier en disant que G est transitif si et seulement s'il possède un p -cycle (ce qui est vrai) car il faut justifier qu'il n'y a pas d'autre p -cycle que $\{t, \dots, t^{p-1}\}$.
- Ce développement possède une application en Théorie de Galois : $P \in \mathbf{Q}[X]$ un polynôme irréductible de degré p premier et L le corps de décomposition de P . Alors P est résoluble si et seulement si deux racines suffisent à engendrer L . Par ailleurs, si L possède plus de trois racines, une racine complexe et au moins deux racines réelles, alors P n'est pas résoluble par radicaux.

Références La référence pour ce développement est J-P Escofier, *Théorie de Galois* 2nd édition de Dunod, à la page 172. On trouvera l'application sous forme d'exercice à la page 183.

Recasage Pour ce développement, on peut partir pour 101, 103, 104, 105, 121.

Il est risqué de le placer dans la 120 et la 123 car l'utilisation du corps $\mathbf{F}_p$ est assez anecdotique.