8. Complément I : Filtrations et le théorème de Jordan-Hölder

Si G est un groupe, on appelle *filtration* de G de longueur n la donnée d'une suite finie décroissante [16] $G_\bullet$ de sous-groupes

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{1\}$$

avec G_{i+1} distingué dans G_i pour tout $0 \leqslant i < n$. On appelle alors *gradués* de $G_\bullet$ les n groupes quotients $\mathrm{gr}_i\, G_\bullet := G_i/G_{i+1}$ pour $0 \leqslant i < n$. Une filtration est dite *de Jordan-Hölder* si ses gradués sont des groupes simples.

Proposition 8.1. *Tout groupe fini admet une filtration de Jordan-Hölder.*

Démonstration — On procède par récurrence sur le cardinal du groupe fini G. Si G est simple, il n'y a rien à démontrer (prendre $G_0 = G$ et $G_1 = \{1\}$). Sinon, soit H un sous-groupe distingué de G de cardinal maximal et $\neq G$. Comme les sous-groupes distingués de G/H sont en bijection avec les sous-groupes distingués de G contenant H (Proposition 6.19 Chap. 2), le groupe quotient G/H est simple. Si $H_\bullet$ est une filtration de Jordan-Hölder de H, alors $G \supset H \supset H_1 \supset H_2 \cdots \supset H_n = \{1\}$ en est une de G. □

Remarque 8.2. Un groupe admet en général plusieurs filtrations de Jordan-Hölder. Par exemple, le groupe abélien p-élémentaire $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension 2, admet exactement $p+1$ sous-groupes $H \simeq \mathbb{Z}/p\mathbb{Z}$ (nécessairement distingués), et pour tous ces groupes on a $G/H \simeq \mathbb{Z}/p\mathbb{Z}$, de sorte que $G \supset H \supset \{1\}$ est de Jordan-Hölder.

Théorème 8.3. (Jordan-Hölder) *Si $G_\bullet$ et $G'_\bullet$ sont deux filtrations de Jordan-Hölder d'un même groupe G, alors elles ont même longueur, disons n, et il existe $\sigma \in \mathrm{S}_n$ tel que $\mathrm{gr}_i G_\bullet \simeq \mathrm{gr}_{\sigma(i)} G'_\bullet$ pour tout $0 \leqslant i < n$.*

En particulier, les gradués d'une filtration de Jordan-Hölder d'un groupe fini G sont bien définis à permutation et isomorphisme près : on les appelle les *facteurs de Jordan-Hölder* de G. Noter que dans le cas $G = \mathrm{S}_n$, le théorème de Jordan-Hölder découle facilement des Théorèmes 5.1 et 5.2. Ils démontrent :

Corollaire 8.4. *Pour $n \geqslant 5$, les facteurs de Jordan-Hölder de S_n sont A_n et $\mathbb{Z}/2\mathbb{Z}$. Le facteurs de Jordan-Hölder de S_4 sont $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, et ceux de S_3 sont $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$.*

Pour démontrer le théorème de Jordan-Hölder, nous aurons besoin du lemme suivant. Soit $G_\bullet$ une filtration du groupe G. Si H est un sous-groupe de G, alors $H_i := G_i \cap H$ définit manifestement une filtration du groupe H. De plus, si H est distingué dans G, et si $\pi : G \to G/H$ est la projection canonique, alors $K_i := \pi(G_i)$ définit manifestement une filtration du groupe $K := G/H$ (Exemple 6.4 Chap. 2). Ces deux filtrations ont même longueur que $G_\bullet$ et sont dites *induites* par cette dernière. Comparons leurs gradués.

16. Il est plus souple de ne pas imposer aux G_i d'être distincts. La terminologie *suite de composition* (ou *composition series* en anglais) est parfois utilisée pour *filtration*. Nous préférons la seconde pour éviter la confusion avec les suites exactes, juste introduites. Noter enfin que les G_i avec $i > 1$ ne sont pas nécessairement distingués dans G.

LEMME 8.5. *Soient $G_\bullet$ une filtration de longueur n du groupe G, H un sous-groupe de G, ainsi que $H_\bullet$ et $K_\bullet$ les filtrations induites par $G_\bullet$ sur H et $K := G/H$. Pour tout $0 \leqslant i < n$ on a une suite exacte naturelle*

$$1 \to \mathrm{gr}_i\, H_\bullet \to \mathrm{gr}_i\, G_\bullet \to \mathrm{gr}_i\, K_\bullet \to 1.$$

DÉMONSTRATION — Soit $\pi : G \to K$ la projection canonique. Soit π_i la composé des morphismes surjectifs naturels $G_i \xrightarrow{\pi} K_i \to K_i/K_{i+1}$. On a clairement $H_iG_{i+1} \subset \ker \pi_i \subset G_i$. Précisément, pour $g \in G_i$ on a les équivalences

$$g \in \ker \pi_i \;\Leftrightarrow\; \pi(g) \in K_{i+1} \;\Leftrightarrow\; \exists g' \in G_{i+1},\ \pi(g) = \pi(g') \Leftrightarrow g \in (G_{i+1}H) \cap G_i = H_i \cap G_{i+1}.$$

Considérons le morphisme $\iota_i : H_i \to G_i/G_{i+1}, h \mapsto hG_{i+1}$. On a montré que la suite

$$H_i \xrightarrow{\iota_i} G_i/G_{i+1} \xrightarrow{\overline{\pi_i}} K_i/K_{i+1} \to 1$$

est exacte. Il ne reste qu'à voir que le noyau de ι_i est H_{i+1}. Mais c'est l'ensemble des $h \in H_i$ tels que $hG_{i+1} = G_{i+1}$, c'est donc bien $H_i \cap G_{i+1} = H_{i+1}$. □

DÉMONSTRATION — (du théorème de Jordan-Hölder) On raisonne par récurrence sur $|G|$. Il n'y a rien à démontrer si G est simple. Sinon, fixons $1 \subsetneq H \subsetneq G$ un sous-groupe distingué strict de G. Soit $G_\bullet$ une tour de Jordan-Hölder de G de longueur n, ainsi que $H_\bullet$ et $K_\bullet$ les filtrations induites par $G_\bullet$ comme ci-dessus sur H et $K = G/H$. Par hypthèse, $\mathrm{gr}_i\, G$ est simple pour tout i. La suite exacte montre donc que pour tout i, on a donc soit $\mathrm{gr}_i\, H_\bullet \simeq \mathrm{gr}_i\, G_\bullet$ (simple) et $\mathrm{gr}_i\, K_\bullet \simeq 1$, soit $\mathrm{gr}_i\, H_\bullet \simeq 1$ et $\mathrm{gr}_i\, G_\bullet \simeq \mathrm{gr}_i\, K_\bullet$ (simple). Notons I et J l'ensemble des indices i dans le premier et second cas respectivement, de sorte que $\{1, \ldots, n\} = I \coprod J$. Par hypothèse de récurrence appliquée à H et G/H, les gradués de $H_\bullet$ et $K_\bullet$ (modulo isomorphismes et permutations) ne dépendent pas de ces filtrations de H et K respectivement. La même chose vaut donc pour les gradués de G, qui sont réunion avec multiplicité, de ceux de H et de K. □

EXEMPLE 8.6. (*Où l'on retrouve ... le théorème fondamental de l'arithmétique !*) Remarquons que ce théorème appliqué à $\mathbb{Z}/n\mathbb{Z}$ redémontre l'unicité de la décomposition d'un entier en facteurs premiers. En effet, à toute écriture $n = p_1 \ldots p_r$ avec les p_i premier, on peut associer une filtration de Jordan-Hölder du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ de gradués les $\mathbb{Z}/p_i\mathbb{Z}$.

Dans le reste de ce complément, on rediscute de la notion de résolubilité en terme de filtrations à gradués abéliens. Commençons par une traduction des Propositions 6.11 et 4.4.

PROPOSITION 8.7. *Soit $1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$ une suite exacte de groupes. Alors G est résoluble si, et seulement si, H et K le sont.*

Une filtration $G_\bullet$ de G est dite *normale* si on a $G_i \lhd G$ pour tout i.

PROPOSITION 8.8. *Soit G un groupe. Il y a équivalence entre :*

(i) G est résoluble,

(ii) G possède une filtration normale à gradués abéliens,

(iii) G possède une filtration à gradués abéliens.

De plus, tout groupe résoluble fini possède une filtration à gradués cycliques d'ordre premier.

Démonstration — Si G est résoluble de classe n, alors les $G_i := \mathrm{D}^i(G)$, pour $i = 0, \ldots, n$, définissent une filtration de longueur n de G à gradués $\mathrm{D}^i(G)_{\mathrm{ab}}$ abéliens. Cette filtration est normale car $\mathrm{D}^i(G)$ est caractéristique dans G pour tout i, donc distingué. Cela montre (i) $\Rightarrow$ (ii). L'implication (ii) $\Rightarrow$ (iii) est évidente. Supposons enfin que $G_\bullet$ est une filtration de longueur n de G à gradués abéliens. L'hypothèse $G_n = 1$, la Proposition 8.7 et, pour $i = 0, \ldots, n-1$, les suites exactes naturelles

$$1 \to G_{i+1} \to G_i \to \mathrm{gr}_i\, G_\bullet \to 1$$

entraînent successivement que G_{n-1}, G_{n-2}, $\ldots$, G_1, $G_0 = G$ sont résolubles. Cela montre (iii) $\Rightarrow$ (i).

Supposons maintenant G résoluble fini. Considérons une filtration de Jordan-Hölder de G. Par la Proposition 8.7, ses gradués sont résolubles. Ils sont aussi simples et finis. Mais un groupe simple résoluble H est de groupe dérivé $\mathrm{D}(H)$ trivial (sinon on aurait $\mathrm{D}^n(H) = H$ pour tout $n \geqslant 1$), donc H est abélien, puis cyclique d'ordre premier par l'Exemple 6.14. □

9. Complément II : Groupe de Galois d'un polynôme (culturel)

C'est Galois qui introduit le premier, vers 1830, la notion et la terminologie de *groupe*, dans ses recherches sur la *résolubilité par radicaux* des racines d'un polynôme P à une variable (dans la lignée de travaux de Lagrange). Informellement, on entend par là le fait de pouvoir écrire ou non les racines de P comme somme de radicaux emboités de termes dépendant simplement des coefficients de P.

Galois, tout comme Lagrange, s'intéresse aux relations de nature algébrique entre les différentes racines d'un même polynôme à une variable. De manière moderne, on considère le sous-groupe

$$\Sigma = \mathrm{Aut}(\mathbb{C}) \subset \mathrm{S}_{\mathbb{C}}$$

de tous les automorphismes du corps $\mathbb{C}$. Par exemple, la conjugaison complexe $z \mapsto \overline{z}$ est un élément de Σ, mais il y en a beaucoup d'autres, en fait, une infinité indénombrable ! Noter qu'un élément $\sigma \in \Sigma$ vérifie toujours $\sigma(x) = x$ pour $x \in \mathbb{Q}$, puis $\sigma(P(x_1, \ldots, x_n)) = P(\sigma(x_1), \ldots, \sigma(x_n))$ pour tout $P \in \mathbb{Q}[X_1, \ldots, X_n]$ et $x_1, \ldots, x_n \in \mathbb{C}$. En particulier, σ préserve l'ensemble des zéros des polynômes à coefficients rationnels.

Fixons donc $P \in \mathbb{Q}[X]$, et notons $R \subset \mathbb{C}$ l'ensemble fini de ses racines. [17] L'action naturelle de $\mathrm{Aut}(\mathbb{C})$ sur $\mathbb{C}$ préserve R, ce qui fournit un morphisme de groupes

$$\mathrm{Aut}(\mathbb{C}) \to \mathrm{S}_R.$$

L'image de ce morphisme est par définition le groupe de Galois du polynôme P. Il est noté $\mathrm{Gal}(P/\mathbb{Q})$. Autrement dit, ce sont les permutations des racines de P induites par un automorphisme du corps $\mathbb{C}$. Il est non trivial : on montre par exemple assez formellement que si P est irréductible dans $\mathbb{Q}[X]$ alors $\mathrm{Gal}(P/\mathbb{Q})$ agit transitivement sur R.

17. Si P est irréductible dans $\mathbb{Q}[X]$, alors il est premier à P' dans $\mathbb{Q}[X]$, et donc par Bezout P n'a pas de racine multiple dans $\mathbb{C}$: ainsi, P a exactement $\deg P$ racines complexes.

Exemple 9.1. En guise d'exemple, considérons $P = X^4 - 2$. On a

$$R = \{\alpha, i\alpha, -\alpha, -i\alpha\} \quad \text{avec } i^2 = -1 \text{ et } \alpha = \sqrt[4]{2}.$$

Identifions respectivement $\alpha, i\alpha, -\alpha, -i\alpha$ à $1, 2, 3, 4$, et donc $\mathrm{Gal}(P/\mathbb{Q})$ à un sous-groupe G de S_4. L'élément de G induit par la conjugaison complexe τ est la transposition $(2\,4)$, mais il y a bien d'autres éléments dans G. Par exemple, P étant irréductible dans $\mathbb{Q}[X]$ l'action de G sur $\{1, 2, 3, 4\}$ doit être transitive, et donc il doit exister $\sigma \in \mathrm{Gal}(P/\mathbb{Q})$ tel que $\sigma(\alpha) = i\alpha$. La relation $i^2 = -1$ montre $\sigma(i)^2 = -1$, puis $\sigma(i) = \pm i$. Quitte à remplacer σ par $\tau\sigma$ on peut donc supposer $\sigma(i) = i$ et $\sigma(\alpha) = i\alpha$. On constate alors que σ agit comme le 4-cycle $(1\,2\,3\,4)$, puis que G contient le groupe D_8, car on a $\mathrm{D}_8 = \langle(1\,2\,3\,4), (2\,4)\rangle$. En fait, on peut montrer $G = \mathrm{D}_8$. En effet, la relation $\sigma(-x) = -\sigma(x)$ pour tout $\sigma \in \mathrm{Aut}(\mathbb{C})$ montre que les éléments G commutent avec la double transposition $(1\,3)(2\,4)$, dont le commutant dans S_4 est en fait D_8.

Un résultat spectaculaire de Galois est le fait que P est résoluble par radicaux si, et seulement si, le groupe $\mathrm{Gal}(P/\mathbb{Q})$ est *résoluble* au sens de la Définition 6.9. Comme un polynôme générique de degré n a pour groupe de Galois S_n, et que ce dernier n'est résoluble que pour $n \leqslant 4$ (Proposition 6.7), il retrouve que le polynôme générique n'est pas résoluble par radicaux en degré $\geqslant 5$, un résultat déjà connu de Abel et Ruffini. De même, la résolubilité du groupe D_8 est compatible avec l'écriture par radicaux triviale des racines de $X^4 - 2$. Ces résultats, et bien d'autres, feront l'objet du cours d'algèbre 2. Ils constituent une motivation forte à l'étude des sous-groupes de S_n.

10. Complément III : Le groupe affine et un théorème de Galois

Soit V un espace vectoriel[18] sur un corps k. On rappelle qu'une bijection $f : V \to V$ est dite *affine* si on a, pour tout $x, y \in V$ et tout $\lambda, \mu \in k$ avec $\lambda + \mu = 1$,

$$f(\lambda x + \mu y) \ = \ \lambda f(x) + \mu f(y).$$

Alternativement, il est équivalent de demander que f est affine et :

(a) qu'il existe $\vec{f} \in \mathrm{GL}(V)$, nécessairement unique et appelée *application linéaire tangente*, vérifiant $f(x + h) = f(x) + \vec{f}(h)$ pour tout $x, h \in V$.

(b) qu'il existe $a \in \mathrm{GL}(V)$ et $b \in V$ avec $f(x) = a(x) + b$. On a alors nécessairement $a = \vec{f}$ et $b = f(0)$.

Définition 10.1. *On note* $\mathrm{Aff}(V) \subset \mathrm{S}_V$ *le sous-groupe des bijections affines* f *de* V.

Un sous-groupe important de $\mathrm{Aff}(V)$ est le sous-groupe $\mathrm{T}(V)$ constitué des translations, *i.e.* des applications de la forme $\tau_v(x) = x + v$, avec $v \in V$. L'application $v \mapsto \tau_v$ est un isomorphisme $V \simeq \mathrm{T}(V)$. Le groupe $\mathrm{Aff}(V)$ agit naturellement sur

18. Le cadre le plus clair, mais évité ici pour aller droit au but, serait en fait de se placer dans un espace affine général sous V, c'est-à-dire d'un ensemble muni d'un action libre et transitive de l'espace vectoriel V. Dans un espace affine, non seulement on ne favorise pas d'origine, mais on distingue deux groupes identifiés ici potentiellement de manière perturbante : le sous-groupe $\mathrm{GL}(V)$ de $\mathrm{Aff}(V)$ fixant 0, et le quotient $\mathrm{GL}(V)$ de $\mathrm{Aff}(V)$ des applications linéaires tangentes.

V, et ce transitivement, car c'est déjà le cas de $\mathrm{T}(V)$. Le stabilisateur de l'origine 0 de V coïncide avec $\mathrm{GL}(V)$. On a un morphisme

$$d : \mathrm{Aff}(V) \to \mathrm{GL}(V), f \mapsto \vec{f}$$

(le vérifier !). Ce morphisme d est surjectif car on a $df = f$ pour $f \in \mathrm{GL}(V)$. Son noyau est le sous-groupe $\mathrm{T}(V)$ (c'est clair sur (b)), qui est donc distingué dans $\mathrm{Aff}(V)$.

Proposition 10.2. *On a une suite exacte courte naturelle*

$$1 \longrightarrow V \xrightarrow{v \mapsto \tau_v} \mathrm{Aff}(V) \xrightarrow{d} \mathrm{GL}(V) \longrightarrow 1.$$

Le sous-groupe $\mathrm{GL}(V)$ *de* $\mathrm{Aff}(V)$ *est un complément de* $\mathrm{T}(V)$*, et on a* $\mathrm{Aff}(V) \simeq V \rtimes_\alpha \mathrm{GL}(V)$ *pour le morphisme tautologique* $\alpha : \mathrm{GL}(V) \to \mathrm{Aut}(V)$.

Démonstration — On a clairement $\mathrm{T}(V) \cap \mathrm{GL}(V) = \{1\}$ et $\mathrm{Aff}(V) = \mathrm{T}(V)\mathrm{GL}(V)$ (propriété (b)), donc $\mathrm{GL}(V)$ est un complément de $\mathrm{T}(V)$ dans $\mathrm{Aff}(V)$. Ainsi, on a $\mathrm{Aff}(V) = \mathrm{T}(V) \rtimes \mathrm{GL}(V)$ (produit semi-direct interne). Pour $g \in \mathrm{GL}(V)$ et $v \in V$ on a la formule immédiate $g\tau_v g^{-1} = \tau_{g(v)}$. On conclut par suivi des isomorphismes (Proposition 7.8 appliquée à $a : V \xrightarrow{\sim} \mathrm{T}(V), v \mapsto \tau_v$ et $b = \mathrm{id}$). □

Considérons le cas de la dimension 1. Le groupe $\mathrm{Aff}(k)$ est simplement le groupe des bijections de k de la forme $x \mapsto ax + b$ avec $a \in k^\times$ et $b \in k$. Il est dans une suite exacte $1 \to k \to \mathrm{Aff}(k) \to k^\times \to 1$, et les deux groupes k et $k^\times$ sont abéliens, on en déduit :

Corollaire 10.3. *Le groupe* $\mathrm{Aff}(k)$ *est résoluble.*

Plutôt que de développer de la géométrie affine, on se propose dans ce complément de voir comment le groupe $\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$ intervient, suivant Galois, dans la classification des sous-groupes résolubles de S_p qui sont *transitifs*, *i.e.* agissant transitivement sur $\{1, \ldots, p\}$. Commençons par donner quelques conditions nécessaires et suffisantes simples pour qu'un sous-groupe de S_p avec p premier soit transitif.

Lemme 10.4. *Soit G un sous-groupe de* S_p *avec p premier. Les conditions suivantes sont équivalentes :*

(i) G est transitif,

(ii) p divise $|G|$,

(iii) G contient un p-cycle.

Démonstration — Soient $X = \{1, 2, \ldots, p\}$ et $x \in X$. Supposons (i). Alors l'orbite de x sous G est $\mathrm{O}_x = X$. La formule orbite-stabilisateur montre $|G| = |\mathrm{G}_x|\,|X|$, et donc p divise $|G|$. On a montré (ii). Si p divise $|G|$ alors par Cauchy G contient un élément c d'ordre p. L'ordre d'un élément de S_p étant le ppcm des longueurs de ces cycles, cela montre que c est produit de p-cycles à supports disjoints, puis c est un p-cycles car $|X| = p$. On a montré (ii) $\implies$ (iii). L'implication (iii) $\implies$ (ii) est évidente. □

Considérons la bijection $\{1,\dots,p\} \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}$, $i \mapsto \bar{i}$. Elle permet d'identifier S_p avec $\mathrm{S}_{\mathbb{Z}/p\mathbb{Z}}$, et nous verrons définitivement $\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$ comme un sous-groupe de S_p au moyen de cette identification. Par exemple, la translation $\tau(x) = x+1$ coïncide alors avec le p-cycle $(1\,2\,\dots\,p)$. Ainsi, $\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$ est un sous-groupe résoluble et transitif de S_p. D'après la Proposition 10.2, il est de cardinal $|\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})| = p(p-1)$. On se propose de démontrer le résultat suivant, dû à Galois.[19]

Théorème 10.5. (Galois) *Soit G un sous-groupe transitif de S_p avec p premier. Il y a équivalence entre :*

(i) G est résoluble,

(ii) G possède un sous-groupe distingué d'ordre p,

(iii) G est conjugué à un sous-groupe de $\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$,

(iv) tout élément de G fixant 2 points de $\{1,\dots,p\}$ est l'identité,

(v) on a $|G| \leqslant p(p-1)$.

Nous aurons besoin du lemme suivant.

Lemme 10.6. *Soient p premier, c un élément d'ordre p dans S_p (i.e. un p-cycle), $C = \langle c\rangle$ et $N = \{\sigma \in \mathrm{S}_p \mid \sigma C \sigma^{-1} = C\}$ le normalisateur de C dans S_p. Alors :*

(a) il existe $g \in \mathrm{S}_p$ tel que $gNg^{-1} = \mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$.

(b) le centralisateur de c dans S_p est C.

Démonstration — Quitte à remplacer c par un conjugué, on peut supposer que c est la translation $x \mapsto x+1$ via l'identification $\mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} \{1,\dots,p\}$ ci-dessus, et donc $\mathrm{T}(\mathbb{Z}/p\mathbb{Z}) = C$. Soit $\sigma \in \mathrm{S}_p$ commutant avec c. On a alors

$$\sigma(x+1) = \sigma(x)+1, \quad \forall\, x \in \mathbb{Z}/p\mathbb{Z}.$$

On en déduit $\sigma(x) = x + \sigma(0)$, et donc $\sigma = c^k$ avec $k \equiv \sigma(0)$. Cela montre le (b). De même, supposons que $\sigma \in \mathrm{S}_p$ normalise C. Il existe $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ avec $\sigma c \sigma^{-1} = c^k$, car c^k doit engendrer $\langle c\rangle$. Mais $\sigma c = c^k \sigma$ s'écrit

$$\sigma(x+1) = \sigma(x) + k, \quad \forall\, x \in \mathbb{Z}/p\mathbb{Z}.$$

Cela implique $g(x) = kx + g(0)$: on a montré $N \subset \mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$. L'autre inclusion est claire car $\mathrm{T}(\mathbb{Z}/p\mathbb{Z}) = \langle c\rangle$ est distingué dans $\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$. □

Démonstration — (du Théorème de Galois) Montrons (i) implique (ii). Noter que G est non trivial (car transitif). Supposons G résoluble. Alors G possède un sous-groupe distingué abélien non trivial A. En effet, si on a $\mathrm{D}^n(G) = \{1\}$ et $\mathrm{D}^{n-1}(G) \neq \{1\}$, le sous-groupe $A = \mathrm{D}^{n-1}(G)$ convient (il est même caractéristique dans G). Vérifions que A agit transitivement sur $\{1,\dots,p\}$. Soient $\Omega_1,\dots,\Omega_r$ les orbites de A dans $\{1,\dots,p\}$. Les Ω_i sont permutées (transitivement) par G car A est distingué dans G : on a $gAx = gAg^{-1}gx = Agx$. En particulier, les Ω_i ont même cardinal s, et donc on a $p = rs$. Le cas $s = 1$ signifie $A = \{1\}$, qui est absurde car A est non trivial. On a donc bien $r = 1$: A agit transitivement sur $\{1,\dots,p\}$. Par le Lemme 10.4, A

19. Dans la théorie de Galois, ce résultat s'interprête notamment en disant que si un polynôme $P \in \mathbb{Q}[X]$ de degré premier est résoluble par radicaux, alors chaque racine de P s'exprime comme un polynôme à coefficients rationnels en deux quelconques des racines de P.

contient donc un p-cycle c de S_p. Mais le commutant de c est $\langle c\rangle$ par le Lemme 10.6 (b). On a donc $A = \langle c\rangle$ car A est abélien : on a montré le (ii).

L'implication (ii) $\Longrightarrow$ (iii) se déduit des Lemmes 10.4 et 10.6 (a).

L'implication (iii) $\Longrightarrow$ (iv) est une propriété générale de l'action naturelle de $\mathrm{Aff}(k)$ sur k. En effet, si l'équation $ax + b = x$ admet deux solutions $x \in k$, c'est qu'on a $b = 0$ et $a = 1$.

Pour l'implication (iv) $\Longrightarrow$ (v), on observe d'abord que l'application $G \to \{1, \ldots, p\} \times \{1, \ldots, p\}, g \mapsto (g(1), g(2))$, est injective par l'hypothèse. Son image est incluse dans le sous-ensemble X des couples (i, j) avec $j \neq i$. On on conclut car on a $|X| = p(p-1)$.

Montrons (iv) $\Longrightarrow$ (v). On sait que p divise $|G|$ car G est transitif. De plus, l'hypothèse (iv) implique que pour $i \in \{1, \ldots, p\}$, le stabilisateur G_i agit librement sur $\{1, \ldots, p\}\backslash\{i\}$, et donc $|G_i|$ divise $p - 1$ par l'Exercice 4.18. On en déduit que $|G| = p|G_i|$ divise $p(p-1)$.

Montrons enfin (v) $\Longrightarrow$ (ii). Soit C un sous-groupe cyclique d'ordre p de G (Lemme 10.4). Il suffit de montrer que C est distingué dans G. Sinon, il existe $g \in G$ tel que $C' := gCg^{-1}$ est distinct de C. On a donc $C \cap C' = \{1\}$ (c'est un sous-groupe strict de $C \simeq \mathbb{Z}/p\mathbb{Z}$). Mézalor l'application $C \times C' \to G, (c, c') \mapsto cc'$ est injective, et donc on a $|CC'| = p^2$. C'est absurde car on a $|G| \leqslant p(p-1)$ et $CC' \subset G$. □

Au passage, nous en déduisons le :

Corollaire 10.7. *Si p est premier, il existe à isomorphisme près, une et une seule action transitive de S_p sur un ensemble à $(p-2)!$ éléments. Elle a pour stabilisateurs les conjugués de $\mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$.*

Démonstration — D'après la classification des actions transitives, il suffit de montrer la seconde assertion. Mais un tel stabilisateur H est d'ordre $p(p-1)$. Par le Lemme 10.4, il agit transitivement sur $\{1, \ldots, p\}$. On conclut d'après le (v) $\Longrightarrow$ (iii) du Théorème. □

Dans le cas $p = 5$ on retrouve l'existence, et surtout l'unicité jusqu'alors laissée de côté !, de l'action exotique de S_5 sur 6 éléments :

Corollaire 10.8. *À isomorphisme près, il existe une unique action transitive de S_5 sur un ensemble à 6 éléments. Le groupe affine $\mathrm{Aff}(\mathbb{Z}/5\mathbb{Z})$ en est un stabilisateur.*