M1 - Théorie de Galois et représentations
Corrigé du DS du 28 octobre 2022

Exercice 1

(1) Soit $\varphi \in \mathrm{Aut}_{\mathrm{gr}}(\mathbf{Q})$. Si $\alpha = \varphi(1) \in \mathbf{Q}$, et $x \in \mathbf{Q}$, on peut écrire $x = \frac{u}{v}$ avec $u \in \mathbf{Z}$ et $v \in \mathbf{N}_{>0}$: on a $v\varphi(x) = \varphi(vx) = \varphi(u) = u\varphi(1) = \alpha u$, de sorte que $\varphi(x) = \alpha x$. Comme φ est un automorphisme, on a $1 \in \mathrm{Im}(\varphi)$ ce qui montre que $\alpha \in \mathbf{Q}^\times$. Réciproquement, si $\alpha \in \mathbf{Q}^\times$, notons $m_\alpha \colon \mathbf{Q} \to \mathbf{Q}$ la multiplication par α. C'est un morphisme de groupes, et $m_\alpha \circ m_{\alpha^{-1}} = m_1 = \mathsf{Id}_{\mathbf{Q}}$ ce qui montre qu'en fait $m_\alpha \in \mathrm{Aut}_{\mathrm{gr}}(\mathbf{Q})$. On dispose donc de l'application surjective

$$\begin{aligned} \mathbf{Q}^\times &\to \mathrm{Aut}_{\mathrm{gr}}(\mathbf{Q}) \\ \alpha &\mapsto m_\alpha. \end{aligned}$$

Elle est bijective parce que $\alpha = m_\alpha(1)$, et il est immédiat que c'est un isomorphisme de groupes.

(2) L'application $G \to \mathrm{Aut}(G)$ qui à $g \in G$ associe l'automorphisme intérieur $x \mapsto g^{-1}xg$ est un morphisme de groupes de noyau $\mathsf{Z}(G)$ (le centre de G) : il induit un morphisme injectif $G/\mathsf{Z}(G) \to \mathrm{Aut}(G)$. Si $\mathrm{Aut}(G)$ est monogène (isomorphe à $\mathbf{Z}$ ou à $\mathbf{Z}/n\mathbf{Z}$ avec $n \in \mathbf{N}_{>0}$), il en est de même de ses sous-groupes, donc de $G/\mathsf{Z}(G)$: il existe $g \in G$ tel que $G/\mathsf{Z}(G) = \langle \overline{g} \rangle$, donc $G = \langle g, \mathsf{Z}(G) \rangle$ est abélien.

Remarque. Bien entendu, il ne suffit pas que G soit abélien pour que $\mathrm{Aut}(G)$ soit cyclique : par exemple, $\mathrm{Aut}((\mathbf{Z}/2\mathbf{Z})^2) = \mathsf{GL}_2(\mathbf{Z}/2\mathbf{Z})$ n'est pas cyclique (il n'est pas abélien).

Exercice 2

(1) On sait que $\mathfrak{A}_n$ est simple : on a $H \cap \mathfrak{A}_n \in \{\{\mathsf{Id}\}, \mathfrak{A}_n\}$. Si $H \cap \mathfrak{A}_n = \{\mathsf{Id}\}$, alors H s'identifie, via la signature, à un sous-groupe de $\{\pm 1\}$: il est d'ordre 1 ou 2. S'il était d'ordre 2, il serait de la forme $H = \langle g \rangle$ avec $g \in \mathfrak{S}_n$ d'ordre 2 : comme $H \trianglelefteq \mathfrak{S}_n$, on a $\sigma^{-1}g\sigma \in H \setminus \{\mathsf{Id}\} = \{g\}$ et donc $\sigma g = g\sigma$ pour tout $\sigma \in \mathfrak{S}_n$, soit encore $g \in \mathsf{Z}(\mathfrak{S}_n) = \{\mathsf{Id}\}$ ce qui est absurde. On a donc nécessairement $H = \{\mathsf{Id}\}$ dans ce cas. Si $H \cap \mathfrak{A}_n = \mathfrak{A}_n$, on a $\mathfrak{A}_n \subset H$, et donc $H \in \{\mathfrak{A}_n, \mathfrak{S}_n\}$ vu que $(\mathfrak{S}_n : \mathfrak{A}_n) = 2$.

(2) Le groupe G agit transitivement par conjugaison sur l'ensemble de ses 5-Sylow. Par cardinalité, N est le stabilisateur de P pour cette action : la relation orbite-stabilisateur implique que le nombre de 5-Sylow de G est précisément m. Les théorèmes de Sylow impliquent donc que $m \equiv 1 \mod 5$ et $m \mid \#G = 5!$ d'où en fait $m \mid 4! = 24$.

(3) Si $m = 1$, alors P est distingué dans $\mathfrak{S}_5$, contredisant la question (1). Comme $m \equiv 1 \mod 5$ et $m \leq 24$, on a $m \in \{6, 11, 16, 21\}$: cela montre que $m = 6$ (puisque $m \mid 24$). Comme $120 = \#\mathfrak{S}_5 = m\#N$, cela implique que $\#N = 20$.

Remarque. On pouvait aussi trouver que $m = 6$ en dénombrant les éléments d'ordre 5 dans $\mathfrak{S}_5$: ce sont les 5-cycles, il y en a $4! = 24$. Les 5-Sylow sont cycliques d'ordre 5 : chacun contient quatre 5-cycles, ce qui montre que $4m = 4!$ et donc $m = 6$.

(4) Le groupe $\mathfrak{S}_5$ agit transitivement par translations à gauche sur l'ensemble quotient $\mathfrak{S}_5/N$. Cette action correspond à un morphisme de groupes $\varphi \colon \mathfrak{S}_5 \to \mathfrak{S}_{\mathfrak{S}_5/N} \simeq \mathfrak{S}_6$. Si $\sigma \in \mathrm{Ker}(\varphi)$, on a $\sigma N = N$, et donc $\sigma \in N$, de sorte que $\mathrm{Ker}(\varphi) \leq N$, d'où $(\mathfrak{S}_5 : \mathrm{Ker}(\varphi)) \geq 5$. Par ailleurs, le sous-groupe $\mathrm{Ker}(\varphi)$ est distingué dans $\mathfrak{S}_5$: d'après la question (1), on a nécessairement $\mathrm{Ker}(\varphi) = \{e\}$, et φ est injectif.

(5) Posons $H = \mathrm{Im}(\varphi)$: c'est un sous-groupe de $\mathfrak{S}_6$ isomorphe à $\mathfrak{S}_5$. Soit $k \in \{1, \ldots, 6\}$. Comme l'action de $\mathfrak{S}_5$ sur $\mathfrak{S}_5/N$ est transitive, il existe $\sigma \in \mathfrak{S}_5$ tel que $k = \varphi(\sigma)(1)$, soit encore $k = h(1)$ où $h = \varphi(\sigma) \in H$, ce qui signifie que H agit transitivement sur $\{1, \ldots, 6\}$ (pour l'action naturelle).

Exercice 3

(1) Si on avait $n_p = 1$, l'unique p-Sylow de G serait distingué, donc égal à G par simplicité. Le groupe G serait donc un p-groupe simple, donc cyclique d'ordre p, contredisant le fait qu'il n'est pas abélien : on a nécessairement $n_p > 1$. L'action de G par conjugaison sur l'ensemble X de ses p-Sylow est transitive : elle correspond à un morphisme de groupes non trivial $\rho \colon G \to \mathfrak{S}_X \simeq \mathfrak{S}_{n_p}$. Comme G est simple et $\mathrm{Ker}(\rho) \neq G$, on a $\mathrm{Ker}(\rho) = \{e\}$ *i.e.* ρ est injectif, ce qui implique que $\#G \mid \#\mathfrak{S}_{n_p} = n_p!$. Par ailleurs, on a $n_p \mid m$ (théorème de Sylow), de sorte que $p^r m = \#G \mid n_p! \mid m!$: il vient $p^r \mid (m-1)!$ en divisant par m.

(2) Soit G un groupe d'ordre $945 = 3^3 \times 5 \times 7$. D'après les théorèmes de Sylow, on a $n_3 \equiv 1 \mod 3$ et $n_3 \mid 5 \times 7$, ce qui implique $n_3 \in \{1, 7\}$. Supposons G simple : on a $n_3 = 7$. Étant d'ordre non premier, G est non abélien, et la question précédente implique que $\#G \mid n_3!$, en particulier $3^3 \mid 7!$, ce qui n'est pas. Le groupe G n'est donc pas simple.