

## THÉORIE DES GROUPES 2024 - 25, SOLUTIONS 10

**Exercice 1.** À faire vous-même.

**Exercice 2.** Soit  $G/H$  l'ensemble des classes à gauche de  $H$  dans  $G$ . Alors  $|G/H| = p$  et il existe donc un homomorphisme induit  $\varphi : G \rightarrow S_p$  par l'action de  $G$  sur  $G/H$ . Soit  $K$  le noyau de  $\varphi$ , et considérons les deux lemmes suivants.

**Lemme A :** La cardinalité de  $G/K$  est  $p$ .

**Lemme B :** Nous avons une inclusion de sous-groupes  $K \subseteq H$ .

En supposant les lemmes, puisque l'indice de  $K$  et de  $H$  dans  $G$  est  $p$  et que  $K \subseteq H$ , nous pouvons conclure que  $H = K$ . Le fait que  $K$  soit un noyau d'un homomorphisme implique que  $H = K$  est un sous-groupe normal. Nous laissons la preuve du Lemme B au lecteur et prouvons le Lemme A.

**Preuve du Lemme A :** Soit  $q$  un facteur premier de  $|G/K|$ . Puisque  $p$  est supposé être le plus petit premier divisant  $|G|$  et que  $|G/K| \mid |G|$ , nous avons  $q \geq p$ . Par le premier théorème d'isomorphisme appliqué à  $\varphi$ , nous obtenons que  $G/K$  est isomorphe à un sous-groupe de  $S_p$ . Par conséquent  $q \mid |G/K| \mid p!$  et donc  $q \leq p$ . Ainsi, nous obtenons  $q = p$ . Donc  $|G/K| = p^n$  mais  $|G/K| \mid p!$  implique également que  $n = 1$ . Par conséquent  $|G/K| = p$ .

**Exercice 3.** (1) Par un exercice d'une série précédente, un  $p$ -groupe d'ordre  $n$  possède des sous-groupes normaux d'ordre  $p^k$  pour tout  $1 \leq k \leq n$ , ce qui prouve l'énoncé.

(2) Supposons sans perte de généralité  $p > q$ . Par les théorèmes de Sylow, le nombre de  $p$ -sous-groupes de Sylow du groupe divise  $q$  et a un reste de 1 modulo  $p$ . Comme  $p$  et  $q$  sont des premiers distincts, il doit être égal à 1, et par un exercice de la série 9, ce sous-groupe sera normal.

(3) Si  $q < p$ , dans ce cas, il existe un unique  $p$ -sous-groupe de Sylow de  $G$ , et il est donc normal dans  $G$ . Supposons maintenant que  $p < q$ . Il ne peut pas être le cas que  $p$  ait un reste 1 modulo  $q$ , donc le nombre de  $q$ -sous-groupes de Sylow, que nous notons  $n_q$ , doit vérifier  $n_q = 1$  ou  $n_q = p^2$ . Si  $n_q = 1$ , alors le groupe  $G$  n'est pas simple. Supposons donc  $n_q = p^2$ . Puisqu'un  $q$ -sous-groupe de Sylow a un ordre  $q$  et que deux  $q$ -sous-groupes de Sylow distincts s'intersectent trivialement,  $G$  a  $p^2(q-1)$  éléments d'ordre  $q$ . Par conséquent, le  $p$ -sous-groupe de Sylow contient tous les  $p^2$  éléments restants de  $G$ . Dans ce cas, nous concluons que le  $p$ -sous-groupe de Sylow est unique, donc normal dans  $G$ .

(4) Sans perte de généralité, supposons que  $p < q < r$ . Si le nombre  $n_s$  de  $s$ -sous-groupes de Sylow est 1 pour  $s = p, q$  ou  $r$ , alors le  $s$ -sous-groupe de Sylow est normal. Supposons

donc maintenant que  $n_p$ ,  $n_q$  et  $n_r$  sont tous strictement supérieurs à 1. En utilisant les théorèmes de Sylow, nous en déduisons que  $n_p \geq 1$ ,  $n_q \geq r$  et  $n_r \geq pq$ . Puisque, pour  $s = p, q, r$ , les  $s$ -sous-groupes de Sylow sont en intersection triviale (comme dans le point précédent), nous pouvons compter les éléments de ces  $s$ -sous-groupes de Sylow (ces éléments sont d'ordre  $s$ ) et constater que

$$\begin{aligned} |G| &\geq n_p(p-1) + n_q(q-1) + n_r(r-1) \\ &\geq q(p-1) + r(q-1) + pq(r-1) \\ &= qp - q + rq - r + pqr - pq \\ &= pqr + r(q-1) - q \\ &\geq |G| + q(q-2) \\ &> |G|, \end{aligned}$$

une contradiction.

**Exercice 4.** Remarquons que tout entier positif  $m$  inférieur à 60 peut s'écrire sous l'une des formes suivantes :

- (1)  $p^n$  pour un premier  $p$  et  $n \geq 0$ ,
- (2)  $p^a q^b$  pour des premiers distincts  $p, q$  et  $a > 0, b > 0$ ,
- (3)  $pqr$  pour des premiers distincts  $p, q, r$ .

Soit  $G$  un groupe non abélien d'ordre  $m$  tel que  $m < 60$ . Si  $m$  est de la forme  $p^n, pqr$ , alors  $G$  n'est pas simple par l'exercice 3.

Si  $m$  est de la forme  $p^a q^b$ , alors  $G$  est résoluble par le théorème de Burnside. Mais alors, la résolubilité de  $G$  implique que  $H := [G, G]$  est un sous-groupe normal de  $G$  avec  $G \neq H$ . Comme  $G$  n'est pas abélien, nous avons également  $H$  non trivial. Ainsi,  $G$  n'est pas simple.

**Exercice 5.** D'après les théorèmes de Sylow, le nombre de 2-sous-groupes de Sylow doit être soit 1, soit 3. Dans le premier cas, ce sous-groupe est normal et le résultat est établi. Dans le second cas, il existe un homomorphisme de groupes  $G \rightarrow S_3$  donné par l'action de  $G$  sur l'ensemble des 2-sous-groupes de Sylow. Si  $G$  est simple, cet homomorphisme doit être injectif, ce qui implique que  $G$  a au plus 6 éléments, ce qui contredit l'hypothèse  $n \geq 2$ .

**Exercice 6.** (1) Soit  $\sigma \in \text{Aut}(K)$  tel que  $\sigma\varphi_1(L)\sigma^{-1} = \varphi_2(L)$ . Soit  $x \in L$  un générateur du groupe cyclique  $L$ . Alors, il existe  $a \in \mathbb{N}$  tel que  $\sigma \circ \varphi_1(x) \circ \sigma^{-1} = \varphi_2(x^a) = \varphi_2(x)^a$ . Maintenant, pour tout  $l \in L$ , il existe  $b \in \mathbb{N}$  tel que  $l = x^b$ , ce qui implique que

$$\begin{aligned} \sigma \circ \varphi_1(l) \circ \sigma^{-1} &= \sigma \circ \varphi_1(x^b) \circ \sigma^{-1} \\ &= (\sigma \circ \varphi_1(x) \circ \sigma^{-1})^b \\ &= (\varphi_2(x)^a)^b \\ &= \varphi_2(x^b)^a \\ &= \varphi_2(l)^a \end{aligned}$$

(1)

comme suggéré par l'indice. Nous définissons maintenant

$$\psi : K \rtimes_{\varphi_1} L \rightarrow K \rtimes_{\varphi_2} L$$

par  $\psi(k, l) = (\sigma(k), l^a)$ . Nous laissons au lecteur le soin de vérifier que  $\psi$  est un homomorphisme de groupes. Pour construire un inverse  $\phi : K \rtimes_{\varphi_2} L \rightarrow K \rtimes_{\varphi_1} L$  de  $\psi$ , il suffit d'inverser les rôles de  $\varphi_1$  et  $\varphi_2$  ci-dessus. Pour ce faire, nous manipulons l'équation (1) pour obtenir que

$$\sigma^{-1} \circ \varphi_2(l) \circ \sigma = \varphi_1(l)^b$$

pour  $b = -a + 1$ . Par conséquent, nous savons que  $\phi : (k, l) \mapsto (\sigma^{-1}(k), l^b)$  est un homomorphisme de groupes. Il est maintenant facile de vérifier que  $\phi$  et  $\psi$  sont des inverses l'un de l'autre.

- (2) Soient  $\varphi_1, \varphi_2 : L = \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/p^2\mathbb{Z})$  des homomorphismes de groupes non triviaux. D'après l'indication, nous savons que  $\text{Aut}(\mathbb{Z}/p^2\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$  pour un certain entier  $m$ . Comme les deux homomorphismes sont non triviaux, leur noyau doit être trivial et  $\varphi_1$  et  $\varphi_2$  sont donc injectifs. Il s'ensuit que  $\varphi_1(L)$  et  $\varphi_2(L)$  sont des sous-groupes d'ordre  $p$  dans  $\mathbb{Z}/m\mathbb{Z}$ . Mais les groupes cycliques ont des sous-groupes uniques pour chaque ordre, donc  $\varphi_1(L) = \varphi_2(L)$ . En particulier, ils sont conjugués, et nous concluons en utilisant la première partie de l'exercice.
- (3) Soient  $\varphi_1, \varphi_2 : L = \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} = K)$  des homomorphismes de groupes non triviaux. Pour identifier le codomaine, nous remarquons que tout automorphisme  $f : K \rightarrow K$  est un automorphisme linéaire d'espace vectoriel sur  $L$ . En effet, pour  $\alpha \in L$ , nous avons  $f(\alpha \cdot (a, b)) = \alpha \cdot f(a, b)$ . Il s'ensuit que les automorphismes  $L$  sont en bijection avec les matrices inversibles à coefficients dans  $L$ , et donc

$$|\text{Aut}(K)| = |\text{GL}_2(\mathbb{Z}/p\mathbb{Z})| = (p^2 - 1)(p^2 - p) = p(p^3 - p^2 - p - 1) = p \cdot r,$$

où  $r \in \mathbb{N}$  est un nombre pair. Il s'ensuit que les  $p$ -sous-groupes de Sylow sont d'ordre  $p$ , et donc tous les sous-groupes d'ordre  $p$  sont conjugués (d'après le théorème de Sylow). Comme au point précédent, les groupes  $\varphi_1(L)$  et  $\varphi_2(L)$  sont des sous-groupes de  $\text{Aut}(K)$  d'ordre  $p$ , et donc sont conjugués. Nous concluons par le premier point.