Algèbre – Interrogation I

*Vous disposez de **45 minutes** pour résoudre les cinq exercices suivants qui sont tous indépendants. Vous pouvez admettre le résultat d'une question pour résoudre une question ultérieure même sans l'avoir traitée. Vous pouvez utiliser librement tous les résultats du cours. Ce qui a été vu uniquement en TD est à redémontrer. En cas de questions ou si vous repérez ce qui vous semble être une erreur d'énoncé, n'hésitez pas à me solliciter. On prendra soin de rédiger de façon propre et rigoureuse.*

Exercice 1. Soit G un groupe et $Z(G)$ son centre.

1. Rappeler la définition de $Z(G)$ et montrer que $Z(G)$ est distingué et caractéristique.
2. On suppose que $G/Z(G)$ est cyclique. Montrer que G est abélien.

Solution.

1. On a par définition
$$Z(G) = \{g \in G \ : \ \forall h \in G,\ hg = gh\}.$$
Montrons que $Z(G)$ est caractéristique, ce qui implique distingué par le cours. Soient $\varphi \in \mathtt{Aut}(G)$ et $g \in Z(G)$. On doit montrer que $\varphi(g) \in Z(G)$. Soit alors $h \in G$, on doit montrer que $h\varphi(g) = \varphi(g)h$. Puisque φ est un automorphisme, il est en particulier surjectif et il existe $h' \in G$ tel que $h = \varphi(h')$. Mais alors,
$$h\varphi(g) = \varphi(h')\varphi(g) = \varphi(h'g)$$
car φ est un morphisme. Comme $g \in Z(G)$, $h'g = gh'$ et donc
$$h\varphi(g) = \varphi(gh') = \varphi(g)\varphi(h') = \varphi(g)h,$$
ce qu'il fallait démontrer.
2. Notons $\pi : G \to G/Z(G)$ la surjection canonique[1]. Par hypothèse, il existe $a \in G$ tel que $\pi(a)$ engendre $G/Z(G)$. Soient alors $x, y \in G$. On a l'existence de m et n deux entiers tels que $\pi(x) = \pi(a)^n = \pi(a^n)$ et $\pi(y) = \pi(a)^m = \pi(a^m)$. Cela implique qu'il existe $g_1, g_2 \in Z(G)$ tels que $x = a^n g_1$ et $y = a^m g_2$. On a alors
$$xy = a^n g_1 a^m g_2 = a^{n+m} g_1 g_2 = yx$$
car g_1 et g_2 commutent à tout élément de G. On a donc bien que G est abélien.

Exercice 2. Montrer qu'un groupe d'ordre 200 n'est pas simple.

Solution. Soit G un groupe d'ordre 200. On a $200 = 2^3 \times 5^2$. En notant n_5 le nombre de 5-Sylow, il vient $n_5 \mid 8$ (soit $n_5 \in \{1, 2, 4, 8\}$) et $n_5 \equiv 1 \pmod 5$. Cela exclut 2, 4 et 8. On a donc $n_5 = 1$ et un unique 5-Sylow distingué. On en déduit que G n'est pas simple.

Exercice 3. Soient p un nombre premier et $H \lhd G$ un sous-groupe distingué non trivial d'un p-groupe G. Montrer que $H \cap Z(G) \neq \{e\}$.
On pourra adapter la preuve du cours du fait que le centre d'un p-groupe est non trivial.

Solution. Puisque H est distingué, on peut faire agir G sur H par conjugaison. L'équation aux classes fournit alors
$$\#H = \sum_{\substack{\omega \in \Omega \\ \#\omega = 1}} 1 + \sum_{\substack{\omega \in \Omega \\ \#\omega = 1}} \frac{\#G}{\#\mathrm{Stab}_\omega}.$$
Puisque H est un sous-groupe non trivial d'un p-groupe, il vient modulo p que
$$\sum_{\substack{\omega \in \Omega \\ \#\omega = 1}} 1 \equiv 0 \pmod p.$$
Or, l'orbite de $h \in H$ est de cardinal 1 si, et seulement si, pour tout $g \in G$, $ghg^{-1} = h$ soit si, et seulement si, $gh = hg$. Il vient
$$\sum_{\substack{\omega \in \Omega \\ \#\omega = 1}} 1 = \{h \in H \ : \ h \in Z(G)\} = H \cap Z(G).$$
Comme $e \in H \cap Z(G)$, $\#H \cap Z(G) > 0$ et $\#H \cap Z(G) \equiv 0 \pmod p$ si bien que $\#H \cap Z(G) \geqslant p$ et en particulier $H \cap Z(G) \neq \{e\}$.

Exercice 4. Soient p un nombre premier et $G = \mathfrak{S}_p$.

1. Noter que par la question précédente, on a bien un groupe car $Z(G) \lhd G$.

1. Déterminer le cardinal des p-Sylow de G. En déduire l'ordre de tout élément distinct de Id et appartenant à un p-Sylow de G.
2. Combien G possède-t-il de p-cycles ?
3. En déduire le nombre de p-Sylow de G puis que

$$(p-1)! \equiv -1 \pmod{p} \qquad \text{(théorème de Wilson).}$$

Solution.

1. On a $\#\mathfrak{S}_p = p! = p \times (p-1)!$. On a alors que p est premier avec $(o-1)!$ car p est premier. Il s'ensuit qu'un p-Sylow de G est de cardinal p, donc cyclique isomorphe à $\mathbf{Z}/p\mathbf{Z}$, et dont tous les éléments non triviaux sont d'ordre p.
2. Pour un p-cycle $(a_1\ a_2 \cdots a_p)$, on a p choix pour a_1, $p-1$ choix pour a_2, jusqu'à 1 choix pour a_p mais alors on a compté p fois le même cycle[2] si bien qu'on obtien $\frac{p!}{p} = (p-1)!$ p-cycles dans G.
3. On constate qu'un élément d'ordre p de G n'est rien d'autre qu'un p-cycle. Par ailleurs, comme en TD, puisque les p-Sylow de G sont cycliques, deux p-Sylow distincts sont d'intersection triviale. Il vient que si on a n_p p-Sylow, alors cela forunit $n_p(p-1)$ éléments d'ordre p dans G. Or, on a vu qu'on en avait $(p-1)!$. Cela entraîne que $n_p = (p-2)!$. Les théorèmes de Sylow impliquent alors que $n_p \equiv 1 \pmod{p}$ soit $(p-2)! \equiv 1 \pmod{p}$ et finalement[3] $(p-1)! \equiv -1 \pmod{p}$.

Exercice 5. Soient G un groupe, $H \lhd G$ un sous-groupe distingué de G et P un p-Sylow de G avec p premier tel que $p \mid |G|$.

1. Justifier que HP est un sous-groupe de G et que P est un p-Sylow de HP.
2. Justifier que $|H \cap P| = \frac{|P| \times |H|}{|HP|}$.
   On pourra penser à un théorème d'isomorphisme.
3. En déduire que $H \cap P$ est un p-Sylow de H.
   On pourra écrire $|H| = p^m r$, $|P| = p^n$ et $|HP| = p^n s$.
4. Montrer que HP/H est un p-Sylow de G/H.

Solution.

1. Comme $H \lhd G$, HP est un sous-groupe de G et je vous renvoie au cours pour la preuve. On a alors si $\#G = p^n m$ avec $p \nmid m$, $\#P = p^n$. Mais alors par Lagrange, $\#HP = p^{n'} s$ avec $n' \leqslant n$ et $s \mid m$. Mais par définition, P est un sous-groupe de HP donc par Lagrange à nouveau, $p^n \mid p^{n'} s$, ce qui impose $n \leqslant n'$. On a donc $n' = n$ et $\#HP = p^n s$ et P est un sous-groupe de HP d'ordre p^n, soit un p-Sylow de HP.
2. Par un théorème d'isomorphisme du cours, on a $PH/H \cong P/(P \cap H)$ et il suffit de passer aux cardinaux.
3. Avec les notations de l'indication, $|H \cap P| = p^m \frac{r}{s}$ où $s \mid r$ car HP est un sous-groupe, de H. D'autre part, $H \cap P$ est un sous-groupe de P qui est un p-groupe donc par Lagrange, $r = s$ et $|H \cap P| = p^m$ si bien que $H \cap P$ est un p-Sylow de H.
4. On a $\#G/H = p^{n-m} \frac{m}{r}$ où $r \mid m$. Par ailleurs, $\#HP/H = p^{n-m} \frac{s}{r} = p^{n-m}$ car on a vu que $r = s$. On a donc le résultat.

2. Car

$$(a_1\ a_2 \cdots a_p) = (a_p\ a_1\ a_2 \cdots a_{p-1}) = \cdots = (a_2\ a_3 \cdots a_p\ a_1).$$

3. On appelle ce résultat le théorème de Wilson. On a en fait

$$p \text{ premier} \iff (p-1)! \equiv -1 \pmod{p}.$$

Ce critère de primalité est particulièrement peu efficace du fait de l'explosion de la taille de $(p-1)!$. Je rappelle que pour démontrer le théorème de Wilson de façon élémentaire, on écrit

$$(p-1)! \equiv \prod_{x \in \mathbf{F}_p^\times} x \pmod{p}$$

et regroupant chaque $x \neq \pm 1$ avec son inverse x^{-1} qui vérifie $x \neq x^{-1}$, on obtient que $(p-1)! \equiv 1 \times (-1) \equiv -1 \pmod{p}$.