Algèbre – Devoir à la maison I

*Le devoir est à rendre au plus tard le **vendredi 11 Octobre 2024**. Vous pouvez le rédiger en **français ou en anglais**. Le devoir est à rendre de l'une des façons suivantes : **directement lors de séance de TD** ou **par mail en un UNIQUE fichier pdf avec votre nom** dans le nom du fichier à l'adresse* `kevin.destagnol@universite-paris-saclay.fr` *pour le groupe de TD 1. Vous pouvez également bien sûr me contacter à cette adresse mail en cas de questions ou si vous repérez ce qui vous semble être une erreur d'énoncé.*

Problème 1 — Nombres cycliques. Soit $n \in \mathbb{N}^*$. On dit que n est un *nombre cyclique* si tout groupe de cardinal n est cyclique.

1. Justifier qu'un nombre premier est cyclique et que, pour $p < q$ deux nombres premiers tels que $p \nmid q-1$, pq aussi.

Le reste du problème est consacré à la démonstration du fait que si

$$n \text{ est } \textit{sans facteur carré} \text{ et si pour tout paire de nombres premiers } p < q \text{ divisant } n, \text{ on a } p \nmid q-1, \qquad (*)$$

alors n est cyclique.
On rappelle qu'un entier est *sans facteur carré* s'il n'est divisible par le carré d'aucun nombre premier. On note φ l'indicatrice d'Euler et on rappelle que pour tout entier naturel non nul, $\varphi(n) = \{m \in \{1, \dots, n\} \ : \ \text{pgcd}(m, n) = 1\}$.

2. Établir qu'un entier n satisfait la condition $(*)$ ci-dessus si, et seulement si, $\text{pgcd}(n, \varphi(n)) = 1$.
On pourra montrer que si ℓ et k sont premiers entre eux, $\varphi(\ell k) = \varphi(\ell)\varphi(k)$ et calculer $\varphi(p^\alpha)$ pour p premier et $\alpha \in \mathbb{N}$.

3. On raisonne par récurrence sur les entiers vérifiant la condition $(*)$. On suppose que $n > 1$ et que tous les groupes d'ordre $k < n$ avec k vérifiant $(*)$ sont cycliques. On cherche à montrer que tout groupe d'ordre n avec n satisfaisant $(*)$ est cyclique. Raisonnons alors par l'absurde en considérant un groupe G d'ordre n vérifiant $(*)$ tel que G ne soit pas cyclique.

a) Justifier que tous les sous-groupes et les quotients de G distincts de G sont cycliques.

b) Montrer que G est non abélien et en déduire que $Z(G) = \{e\}$.
On pourra supposer G abélien et construire un élément d'ordre n, puis, on pourra considérer le quotient $G/Z(G)$.

c) On dit qu'un sous-groupe M de G est *maximal* si $M \neq G$ et si pour tout sous-groupe H tel que $M \subseteq H \subseteq G$, alors $H = G$. On définit également pour tout $x \in G$ le *centralisateur* de x comme étant le stabilisateur de x pour l'action de G sur lui-même par conjugaison. Montrer que pour tout $x \in G \setminus \{e\}$, $Z(x)$ est un sous-groupe maximal de G.

d) Soit M un sous-groupe maximal de G. Montrer réciproquement que $M = Z(x)$ pour tout $x \in M \setminus \{e\}$.

e) Montrer que deux sous-groupes maximaux M et M' sont d'intersection triviale.

f) Soit N un sous-groupe distingué de G. Montrer que l'action par conjugaison de G sur N fournit un morphisme $\rho : G \longrightarrow \text{Aut}(N)$. Montrer que le cardinal de $G/\text{Ker}(\rho)$ divise à la fois n et $\varphi(n)$. Conclure à la simplicité de G.

g) Soit M un sous-groupe maximal de G. Montrer que le nombre de sous-groupes de la forme gMg^{-1} avec $g \in G$ est donné par $\dfrac{\#G}{\#N_G(M)}$, où $N_G(M) = \left\{g \in G \ : \ gMg^{-1} = M\right\}$ est le *normalisateur* de M dans G. En déduire que

$$1 + \frac{\#G}{2} \leqslant \#\left(\bigcup_{g \in G} gMg^{-1}\right) < \#G.$$

h) On choisit alors $x \in G \setminus \left(\bigcup_{g \in G} gMg^{-1}\right)$ et on pose $M' = Z(x)$. Minorer le cardinal de

$$\left(\bigcup_{g \in G} gMg^{-1}\right) \cup \left(\bigcup_{g \in G} gM'g^{-1}\right).$$

Conclure.

Problème 2 — Module de permutation. Soient G un groupe fini et X un ensemble sur lequel G agit. Soit k un corps de caractéristique nulle.

1. Montrer que G agit linéairement sur l'espace vectoriel k^X des applications de X dans k via $(g \cdot f)(x) = f(g^{-1} \cdot x)$ pour tous $x \in X$, $g \in G$ et $f \in X^k$.

2. Montrer que le sous-espace vectoriel $k^{(X)}$ des applications à support fini est un sous-G-module de k^X dont une base est donnée par $(\delta_x)_{x \in X}$ où $\delta_x(y) = 1$ si $y = x$ et 0 sinon pour tout $y \in X$. Vérifier que $g \cdot \delta_x = \delta_{gx}$ pour tous $g \in G$ et $x \in X$.
On appelle le G-module $k^{(X)}$ *le G-module de permutation* associé à X et on le note X^σ.

On suppose dans le reste du problème que l'ensemble X est **fini.**

3. On note
$$(X^\sigma)^G = \{f \in X^\sigma \ : \ \forall g \in G,\ g \cdot f = f\}\,.$$
Calculer $(X^\sigma)^G$ puis $\chi_{X^\sigma}(g)$ pour tout $g \in G$.

4. En déduire la formule de Burnside
$$r = \frac{1}{|G|}\sum_{g\in G} |X^g|\,,$$
où r désigne le nombre d'orbites de X sous l'action de G et $X^g = \{x \in X \ : \ g \cdot x = x\}$.

Dans les question **5.** à **9.**, on suppose que $|X| \geqslant 2$ et $|X/G| = 1$.

5. Montrer qu'il existe $g \in G$ sans point fixe.

6. Montrer que les propriétés ci-dessous sont équivalentes :

- **(i)** L'action de G sur X est doublement transitive, c'est-à-dire que pour tous $x \neq y$ et $x' \neq y'$ dans X, il existe $g \in G$ tel que $x' = g \cdot x$ et $y' = g \cdot y$.
- **(ii)** L'action de G sur $X \times X$ a deux orbites : la diagonale et son complémentaire.
- **(iii)** On a $\displaystyle\sum_{g\in G} |X^g|^2 = 2|G|$.

7. Montrer que $(X^\sigma)^G$ admet un unique supplémentaire G-stable, que l'on notera V et que l'on déterminera.

8. Montrer que si les propriétés de la question **6.** sont vérifiées, alors V est un G-module irréductible. En déduire les sous-G-modules de X^σ.

9. Montrer que si V est un G-module irréductible et k est algébriquement clos, alors les propriétés de la question **6.** sont vérifiées.

10. Soit $n \geqslant 2$. En déduire que si k est un corps de caractéristique nulle, alors le $\mathfrak{S}_n$-module k^n obtenu par permutation des coordonnées se décompose en somme directe de deux représentations irréductibles non isomorphes dont l'une est la représentation triviale.
La seconde s'appelle la *représentation standard*.