École normale supérieure, année universitaire 2020-2021. Cours *Algèbre 1*, devoir à la maison, semaine du 16 novembre 2020.

Exercice 1. On note SO_3 le groupe des isométries directes de l'espace euclidien $\mathbf{R}^3$ (muni du produit scalaire usuel). On rappelle que si g appartient à SO_3 alors 1 est valeur propre de g, et que lorsque $g \neq \mathrm{Id}$ le sous-espace propre associé à 1 estr une droite (g est ce qu'on appelle une rotation, et cette droite est son axe).

Soit G un sous-groupe fini de SO_3. Le but de l'exercice est de montrer que G est isomorphe à l'un des groupes suivants :

$$\mathbf{Z}/n\mathbf{Z},\ D_n \text{ (pour } n \in \mathbf{N} \setminus \{0\}), \mathfrak{A}_4,\ \mathfrak{S}_4, \mathfrak{A}_5.$$

Le résultat est évident si G est trivial, et l'on suppose à partie de maintenant que $G \neq \{e\}$.

Soit $S^2 = \{(x_1, x_2, x_3) \in \mathbf{R}^3 \mid x_1^2 + x_2^2 + x_3^2 = 1\}$ la sphère unité de $\mathbf{R}^3$, sur laquelle SO_3 agit naturellement. Soit $X = \{x \in S^2 \mid \exists g \in G - \{\mathrm{Id}\},\ g \cdot x = x\}$.

(a) Vérifiez que X est stable sous l'action de G.

(b) Montrer que tout élément non trivial g de G fixe exactement deux points de X.

(c) On rappelle que $G\backslash X$ désigne l'ensemble des orbites de X sous G. Dans chaque $\omega \in G\backslash X$ on choisit un élément x_ω. Montrez à l'aide de la formule de Burnside (qui n'a pas été vue en cours mais figure dans le poly, lemme 4.4.4, et a été étudiée en TD) que

$$2 - \frac{2}{|G|} = \sum_{\omega \in G\backslash X} \left(1 - \frac{1}{|\mathrm{Stab}(x_\omega)|}\right).$$

(d) En déduire que X se décompose en 2 ou 3 orbites.

(e) Conclure dans le cas où X se décompose en 2 orbites que G est un groupe cyclique.

(f) Supposons que X se décompose en 3 orbites. On notera les cardinaux des stabilisateurs de ces orbites p_1, p_2, p_3, la numérotation étant choisie de sorte que $p_1 \leqslant p_2 \leqslant p_3$. Montrez qu'il existe un entier r tel que $|G| = 2r$ et

$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} = 1 + \frac{1}{r}.$$

En déduire que $(p_1, p_2, p_3, |G|) = (2, 2, r, 2r)$ ou $(2, 3, 3, 12)$ ou $(2, 3, 4, 24)$ ou $(2, 3, 5, 60)$.

(f1) Si $(p_1, p_2, p_3, |G|) = (2, 2, r, 2r)$ montrez que G est isomorphe au groupe diédral D_r.

(f2) Si $(p_1, p_2, p_3, |G|) = (2, 3, 3, 12)$ montrez que G est isomorphe à $\mathfrak{A}_4$.

(f3) Si $(p_1, p_2, p_3, |G|) = (2, 3, 4, 24)$ montrez que G est isomorphe à $\mathfrak{S}_4$.

(f4) Si $(p_1, p_2, p_3, |G|) = (2, 3, 5, 60)$ montrez que G est isomorphe à $\mathfrak{A}_5$.

(g) Question plus culturelle et informelle (on ne demande pas un traitement rigoureux). Dans chacun des cas ci-dessus, quelle est à votre avis l'allure de l'ensemble X ?

Exercice 2. Soit G un groupe fini simple. On suppose que tous les sous-groupes *stricts* de G sont abéliens, et l'on se propose de montrer que G est cyclique d'ordre premier. Un sous-groupe strict de G est dit *maximal* s'il est maximal en tant que sous-groupe strict de G.

(a) Supposons que $\{e\}$ est un sous-groupe strict maximal de G. Montrez que G est cyclique d'ordre premier.

(b) On suppose à partir de maintenant que $\{e\}$ n'est pas un sous-groupe strict maximal de G, et l'on souhaite aboutir à une contradiction. Soient A et B deux sous-groupes stricts maximaux de G et soit H leur intersection. Si $A \neq B$, montrez que le normalisateur de H dans G est égal à G tout entier, et conclure que H est trivial.

(c) Soit M un sous-groupe strict maximal de G dont on note m le cardinal. Montrez que M est son propre normalisateur. Soit E la réunion de tous les conjugués de M. En utilisant la question (b) calculez le cardinal de E.

(d) Montrez qu'il existe un sous-groupe strict maximal M' de G non contenu dans E ; soit E' la réunion des conjugués de M'. Montrez que l'inersection $E' \cap E$ est réduite à $\{e\}$; aboutir à une contradiction par un argument de cardinal.

Exercice 3. On se propose dans cet exercice de déterminer les entiers $n > 0$ tels que tout groupe de cardinal n soit cyclique.

(a) *Questions préliminaires.*

(a1) Montrez que si Γ est un groupe abélien fini dont le cardinal est de la forme $p_1 \dots p_r$ où les p_i sont des nombres premiers deux à deux distincts alors Γ est cyclique.

(a2) Donnez une condition nécessaire et suffisante sur la décomposition d'un entier non nul n en produit de facteurs premiers pour que n soit premier à son indicateur d'Euler $\Phi(n)$. Si elle est satisfaite, montrez que d est premier à $\Phi(d')$ pour tout couple (d, d') de diviseurs de n.

(b) Soit n un entier tel que $\mathrm{PGCD}(n, \Phi(n)) = 1$ et soit G un groupe de cardinal n. On se propose de montrer que G est cyclique. On raisonne par récurrence sur n. Le cas $n = 1$ est trivial, on suppose donc $n > 1$ et le résultat vrai pour les entiers $< n$.

(b1) Montrez à l'aide de l'exercice 2 que G est ou bien cyclique d'ordre premier, ou bien non simple. On se place désormais sous cette dernière hypothèse.

(b2) Soit H un sous-groupe distingué strict et non trivial de G. Montrez que $H \subset \mathrm{Z}(G)$. *Indication* : considérer le morphisme $G \to \mathrm{Aut}(H)$ induit par la conjugaison ; utiliser l'hypothèse de récurrence.

(b3) En utilisant encore l'hypothèse de récurrence, montrer que G est abélien, puis cyclique.

(c) Soit ℓ un entier > 0 tel que $\mathrm{PGCD}(\ell, \Phi(\ell)) \neq 1$. Montrez qu'il existe un groupe non cyclique de cardinal ℓ.