Quelques notes sur des choses qu'on n'a pas eu le temps de voir.

Groupe fini dont tous les éléments (excepté le neutre) sont d'ordre 2. La deuxième question du premier exercice demandait de prouver l'existence d'un élément d'ordre p dans tout groupe G d'ordre $2p$, avec $p \geqslant 3$ premier. On montrait alors que, vu le théorème de Lagrange, tout élément différent du neutre est d'ordre 2, p ou $2p$. S'il existe un élément d'ordre p, on n'a plus rien à faire, s'il existe un élément d'ordre $2p$, son carré est d'ordre p en vertu de la première question, et sinon tous les éléments (excepté le neutre) sont d'ordre 2, ce qui n'est pas possible en vertu du lemme suivant.

Lemme. *Soit G un groupe fini tel que $x^2 = e$ pour tout $x \in G$. Alors G est un groupe abélien de cardinal 2^m avec $m \in \mathbf{N}$.*

Preuve Le caractère abélien est facile à montrer. Pour le cardinal de G, nous donnons deux idées de preuve.

1. On munit G d'une structure d'espace vectoriel sur le corps $\mathbb{F}_2$. On pourra prendre une notation additive pour la loi du groupe G pour ne pas s'embrouiller.

   On définit alors la loi de composition externe par $1 \cdot x = x$ et $0 \cdot x = e$ pour tout $x \in G$, et on vérifie ainsi que $(G, +, \cdot)$ est bien un $\mathbb{F}_2$-ev. Les vérifications faites, on conclut que, comme G est de dimension finie car fini, G est isomorphe à $\mathbb{F}_2^m$ (avec $m = \dim G$) en tant que qu'espace vectoriel et est ainsi de cardinal 2^m.

2. On raisonne par récurrence sur $\operatorname{Card} G$. On prend H un sous-groupe de G différent de G de cardinal maximal. H vérifie les hypothèses du théorème et est de cardinal strictement plus petit que celui de G, donc par hypothèse de récurrence, H est de cardinal une puissance de 2. On prend alors $a \in G \backslash H$, et on montre que $H \cup aH$ est un sous-groupe de G. Ayant $H \cap aH = \varnothing$, on conclut que $H \cup aH = G$ et que, en passant au cardinal, le cardinal de G est bien une puissance de 2.

□

Sous-groupes d'un groupe cyclique. Pour l'exercice 3, une manière de faire demande de savoir décrire les sous-groupes d'un groupe cyclique. On exhibe ici une manière assez simple de les trouver.

Lemme. *Soit $f : G \to G'$ un morphisme de groupes. Notons $\mathcal{A}$ l'ensemble des sous-groupes de G contenant $\ker f$, et $\mathcal{B}$ l'ensemble des sous-groupes de G' inclus dans $\operatorname{im} f$. Alors $F : H \in \mathcal{A} \mapsto f(H) \in \mathcal{B}$ est une bijection.*

Proposition. *Soit G un groupe cyclique d'ordre n et g un générateur de G. L'application $d \mapsto \langle g^d \rangle$ définit une bijection entre les diviseurs positifs de n et l'ensemble des sous-groupes de G.*

Preuve Remarquer que $n\mathbf{Z} \subseteq d\mathbf{Z} \iff d|n$ et appliquer le lemme précédent au morphisme $f : m \in \mathbf{Z} \mapsto g^m \in G$ de noyau $n\mathbf{Z}$. On remarquera, en vertu de la question 1 du premier exercice, que si d divise n, g^d est d'ordre n/d, et donc $\langle g^d \rangle$ est un groupe cyclique d'ordre n/d. □

Porisme. *Pour $n \geqslant 1$, on a*

$$\sum_{d|n} \varphi(d) = n$$

Preuve Soit G un groupe cyclique d'ordre n. Si $d|n$, alors $x \in G$ est d'ordre d si et seulement s'il génère un sous-groupe d'ordre d, mais d'après la proposition précédente, les sous-groupes de G sont uniquement déterminés par leur ordre, donc les éléments d'ordre d dans G sont les générateurs d'un même groupe cyclique d'ordre d, ils sont donc au nombre de $\varphi(d)$. En partitionnant G selon l'ordre de ses éléments, on obtient que

$$n = \sum_{d|n} \varphi(d)$$

□