Université Joseph Fourier 3 Septembre 2014
Mathématiques

Préparation à l'agrégation, stage
Groupes

I. Vrai ou Faux?

On désigne par G un groupe et par x, y des éléments de G.
Répondre par Vrai ou Faux aux assertions suivantes (justifiez). Dans le cas d'une assertion fausse, étudier si l'assertion devient vraie en ajoutant une certaine hypothèse.

1.1 Si x et y sont d'ordre fini,

a) leur produit l'est aussi.

b) le sous–groupe $< x, y >$ est fini.

1.2 Si x, y sont d'ordre fini et commutent,

a) l'ordre de leur produit xy est majoré, resp. s'exprime par une certaine expression (laquelle?) en fonction des ordres de x et de y.

b) l'ordre du groupe $< x, y >$ est majoré, resp. s'exprime par une certaine expression (laquelle?) en fonction des ordres de x et de y.

c) G contient un élément d'ordre $ppcm(x, y)$.

1.3 Soit p un nombre premier. Tout x d'ordre fini s'écrit de manière unique comme produit $x = su = us$, où $s, u \in G$, l'ordre de s est premier à p et celui de u est une puissance de p.

1.4 Si H est un sous–groupe d'indice fini n de G, on a $x^n \in H$.

1.5 Soit H un sous–groupe distingué de G. On note $\bar{x}$ l'image canonique de x dans G/H et on suppose que $\bar{x}$ est d'ordre fini m.

a) Il existe x' d'ordre m dans G tel que $\bar{x'} = \bar{x}$.

b) Si on suppose que m est premier avec l'ordre fini de H, alors x est aussi d'ordre m.

1.6 Si G est abélien fini de cardinal $p^a m$ où p est premier et ne divise pas m, il existe un unique sous–groupe H de G d'ordre p^a. De plus H contient tous les p–éléments de G. (NB: peut se justifier sans thm de Sylow ni thm de structure, en utilisant 1.3 et le thm de Cauchy 3.2).

1.7 a) Si $|G| = 15$, alors G est abélien.

b) Si $|G| = 15$, alors G est cyclique.

1.8 Si G est cyclique, tous ses sous-groupes sont cycliques.

1.9 Si $\mathbb{F}_q$ est un corps fini de cardinal impair, et $G = \mathbb{F}_q^*$, alors

a) x est un carré dans G si et seulement si $x^{(q-1)/2} = 1$. Sinon, on a $x^{(q-1)/2} = -1$.

b) Le produit de deux "non carrés" de G est un carré.

II. Groupes cycliques, exercices

2.1 Si l'élément g du groupe G est d'ordre n et $k \in \mathbb{Z}$, quel est l'ordre de g^k?

2.2 Trouver tous les générateurs du groupe $\mathbb{F}_{13}^*$. (On rappelle que si p est premier, $\mathbb{F}_p$ est le corps $\mathbb{Z}/p\mathbb{Z}$.)

2.3 On suppose que $G =< g >$ est d'ordre n et que $k \in \mathbb{Z}$.
a) Quel est le sous–groupe $N_k = \{x \in G \,|\, x^k = 1\}$?
b) Déterminer tous les sous–groupes de G.
c) Quel est le nombre d'éléments d'ordre d (où $d|n$) dans G?
d) Quel est le sous–groupe G^k image du morphisme $x \mapsto x^k$ de G dans G?
e) CARRÉS ET CUBES On prend $G = \mathbb{F}_q^*$ avec q impair. Donner deux descriptions du sous–groupe G^2, et son ordre. Étudier de même le sous–groupe G^3 (deux cas). Application: $\bar{2}$ est-il un carré (resp. un cube) dans $\mathbb{F}_{19}^*$? (répondre sans énumérer les carrés resp. cubes).
f) Pour $a \in G$, résoudre l'équation $x^k = a$ dans G (indication: écrire $a = g^s$, $0 \le s \le n-1$).

2.4 Résoudre dans $\mathbb{Z}/60\mathbb{Z}$: $24\bar{k} = \bar{0}$.

2.5 Résoudre dans $\mathbb{F}_{19}^*$:
a) $x^{25} = \bar{3}$ **b)** $x^{10} = \bar{7}$ **c)** $x^{15} = \overline{13}$. **d)** $x^{15} = \overline{12}$.

2.6 Dans $\mathbb{Z}/18\mathbb{Z}$, déterminer le sous–groupe engendré par $\{\,\bar{6}, \overline{14}\,\}$ puis l'intersection des sous–groupes $< \bar{6} >$ et $< \overline{14} >$.

2.7 En dénombrant les éléments d'ordre donné dans $\mathbb{Z}/n\mathbb{Z}$, montrer la formule $n = \sum_{d|n} \varphi(d)$.
Soit G un groupe d'ordre n qui pour tout d contient au plus un sous–groupe d'ordre d. Montrer que G est cyclique.
Application: tout sous–groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

2.8 Expliciter un isomorphisme de groupes ET son inverse entre les groupes $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/12\mathbb{Z}$.
À quelle condition sur (m, n) le groupe produit $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est–il cyclique?

2.9 Pour $n \in \mathbb{N}^*$, on note $\mathbb{U}_n$ le sous–groupe (cyclique!) des racines n-ièmes de l'unité dans $\mathbb{C}^*$. Soient m, n dans $\mathbb{N}^*$, de *ppcm* N.
a) Identifier le groupe $\mathbb{U}_n \cap \mathbb{U}_m$. Montrer que le sous–groupe $\mathbb{U}_n \cdot \mathbb{U}_m =$

$< \mathbb{U}_n, \mathbb{U}_m >$ est égal à $\mathbb{U}_N$.
b) On suppose n et m premiers entre eux. Montrer que tout générateur de $\mathbb{U}_{nm}$ s'écrit de manière unique comme produit d'un générateur de $\mathbb{U}_n$ et d'un générateur de $\mathbb{U}_m$. Qu'en déduisez–vous pour la fonction d'Euler φ?

III. Ordre d'un élément, exercices

3.1 Si p, q sont premiers et q divise $2^p - 1$, alors $q \equiv 1 \pmod{2p}$ (introduire un groupe convenable). Montrer que le nombre de Mersenne $2^{23} - 1$ n'est pas premier.

3.2 Prouver le théorème de Cauchy pour les groupes abéliens finis: si p premier divise l'ordre du groupe G, alors G possède un élément d'ordre p (on pourra raisonner par récurrence sur $|G|$).

3.3 a) Soit G un groupe abélien fini. Si n est l'ordre maximal d'un élément de G, montrer que l'ordre de tout élément de G divise n (*cf.* 1.2 c)); n est dit *l'exposant* de G (ppcm des ordres). Que se passe-t-il si $G = \mathfrak{S}_3$?

b) Soit $H =< y >$, où $y \in G$ est d'ordre n. Établir 1.5 a) dans ce cas. En déduire une preuve par récurrence de l'existence d'un isomorphisme de G avec un produit de groupes cycliques de cardinaux $(a_i)_{1 \leq i \leq r}$, avec $a_i | a_{i+1}$ pour tout i et $a_r = n$.

*****

Compléments autour de 1.1b):

- Voici un groupe *infini* d'isométries du plan affine euclidien qui est engendré par deux éléments d'ordre 3 dont le produit est aussi d'ordre 3: partant d'un triangle équilatéral ABC, on note α (resp. β, γ) la rotation d'angle $2\pi/3$ de centre A (resp. B, resp. C). Alors on vérifie que $\alpha \circ \beta \circ \gamma = id_{\mathbb{R}^2}$, alors que $\beta \circ \alpha \circ \gamma$ est une translation (laquelle?), d'ordre infini. Le groupe G engendré par α et β convient donc (c'est le groupe des isométries positives qui conservent un pavage hexagonal).

- Le *problème de Burnside*, problème majeur en théorie des groupes, soulevé en 1902, demande si tout groupe de type fini dont tout élément est d'ordre fini est fini. Pour les sous–groupes de $\mathrm{GL}_n(\mathbb{C})$, c'est un théorème de Schur (1911) (et pour l'agrégation, vous verrez probablement le cas où ce sous–groupe est supposé d'exposant fini, résolu par Burnside). Mais l'énoncé général est faux, cela même en se limitant aux groupes d'exposant fini (Adian et Novikov, 1968).