Partiel du 16 octobre 2018

Exercice 1.
Quels sont les éléments d'ordre 3 du groupe $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$?

Éléments de correction de l'exercice 1.
On cherche $(\overline{x}, \overline{y}) \in (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$ tel que $3 = o(\overline{x}, \overline{y}) = \text{ppcm}(o(\overline{x}), o(\overline{y}))$, *i.e.* tel que
- $o(\overline{x}) = 1$ et $o(\overline{y}) = 3$;
- $o(\overline{x}) = 3$ et $o(\overline{y}) = 1$;
- $o(\overline{x}) = 3$ et $o(\overline{y}) = 3$.

Par ailleurs
- $o(\overline{x}) = 3$ si et seulement si $\overline{x} \in \{\overline{1}, \overline{2}\}$,
- $o(\overline{x}) = 1$ si et seulement si $\overline{x} = \overline{0}$,
- $o(\overline{y}) = 3$ si et seulement si $\overline{y} \in \{\overline{2}, \overline{4}\}$,
- $o(\overline{y}) = 1$ si et seulement si $\overline{y} = \overline{0}$.

Il en résulte que les éléments d'ordre 3 de $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ sont

$$(\overline{0}, \overline{2}), \qquad (\overline{0}, \overline{4}), \qquad (\overline{1}, \overline{0}), \qquad (\overline{2}, \overline{0}), \qquad (\overline{1}, \overline{2}), \qquad (\overline{1}, \overline{4}), \qquad (\overline{2}, \overline{2}), \qquad (\overline{2}, \overline{4}).$$

Exercice 2.
Étudier le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Éléments de correction de l'exercice 2.
La table de multiplication de $\mathrm{G} = \mathrm{Aut}\Big(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\Big) = \{e, a_1, a_2, a_3\}$ est :
- $\forall i \; e a_i = a_i$;
- $\forall\, i \; a_i^2 = e$;
- $\forall\, i \; \forall\, j \neq i \; a_i a_j = a_k$ où $k \neq i$, $k \neq j$, où $i, j, k \in \{1, 2, 3\}$.

Tout automorphisme f de G laisse fixe e. Il permute donc les autres éléments a_1, a_2 et a_3.

Réciproquement pour toute permutation f de ces trois éléments, en posant $f(e) = e$, on obtient une bijection de G sur G qui respecte la table de multiplication ci-dessus. C'est donc un automorphisme.

Ainsi Aut(G) est d'ordre $3! = 6$ et isomorphe au groupe $\mathcal{S}_3$ des permutations de $\{1, 2, 3\}$.

Exercice 3.
Montrer que les groupes $\mathbb{R}/\mathbb{Z}$ et $\mathcal{U} = \big\{z \in \mathbb{C} \,\big|\, |z| = 1\big\}$ sont isomorphes.

Éléments de correction de l'exercice 3.
Puisque $\mathbb{R}$ est abélien, le sous-groupe $\mathbb{Z}$ est distingué. Notons

$$p \colon \mathbb{R} \to \mathbb{R}/\mathbb{Z}, \qquad\qquad x \mapsto \overline{x}$$

le morphisme canonique.

L'application $f \colon \mathbb{R} \to \mathcal{U}$, $x \mapsto \exp(2\mathbf{i}\pi x)$ est un morphisme surjectif. De plus $\ker f = \{x \in \mathbb{R} \,|\, \exp(2\mathbf{i}\pi x) = 1\} = \mathbb{Z}$. Il existe donc un isomorphisme $\overline{f} \colon \mathbb{R}/\mathbb{Z} \to \mathcal{U}$ tel que $f = \overline{f} \circ p$.

Exercice 4.
Donner un exemple de groupe et de sous-groupes dont la réunion n'est pas un sous-groupe.

Éléments de correction de l'exercice 4. Dans $\mathbb{Z}$ la réunion des sous-groupes $2\mathbb{Z}$ et $3\mathbb{Z}$ n'est pas un groupe. En effet la somme $2 + 3 = 5$ d'un élément de $2\mathbb{Z}$ et d'un élément de $3\mathbb{Z}$ n'est ni multiple de 2, ni multiple de 3.

Exercice 5.

Soient G un groupe fini, H et K deux sous-groupes de G d'ordre h et k respectivement.
Si h et k sont premiers entre eux, que peut-on dire de $\mathrm{H} \cap \mathrm{K}$?

Éléments de correction de l'exercice 5.

$\mathrm{H} \cap \mathrm{K}$ est un sous-groupe de H et un sous-groupe de K. D'après le théorème de Lagrange l'ordre de $\mathrm{H} \cap \mathrm{K}$ divise h et divise k donc vaut 1. Autrement dit $\mathrm{H} \cap \mathrm{K} = \{e\}$.

Exercice 6.

Quel est le cardinal de $\mathrm{Aut}\Big(\mathbb{Z}/4\mathbb{Z}\Big)$? Et le cardinal de $(\mathbb{F}_4)^\times$?

Éléments de correction de l'exercice 6.

Le groupe $\mathrm{Aut}\Big(\mathbb{Z}/4\mathbb{Z}\Big)$ s'identifie à $\Big(\mathbb{Z}/4\mathbb{Z}\Big)^\times = \{\overline{1}, \overline{3}\}$, il est donc de cardinal 2.

$(\mathbb{F}_4)^\times$ est de cardinal 3 car tous les éléments non nuls sont inversibles dans un corps.

Exercice 7.

Dans les groupes suivants, donner un exemple d'élément d'ordre 4 s'il en existe, sinon donner un argument pour justifier qu'il n'y en a pas :

(a) le groupe linéaire $\mathrm{GL}_2(\mathbb{R})$;
(b) le groupe alterné $\mathcal{A}_8$;
(c) le groupe $\mathrm{Isom}^+(T) \subset \mathrm{SO}_3(\mathbb{R})$ des rotations de $\mathbb{R}^3$ préservant un tétraèdre régulier T ;
(d) un groupe d'ordre 16 quelconque (attention il s'agit de déterminer si *tout* sous-groupe d'ordre 16 admet un élément d'ordre 4).

Éléments de correction de l'exercice 7.

(a) La rotation d'angle $\pi/2$ est un exemple d'élément d'ordre 4 dans $\mathrm{GL}_2(\mathbb{R})$, sa matrice est $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
(b) $(1\,2\,3\,4)(5\,6)$ est un exemple d'élément d'ordre 4 dans $\mathcal{A}_8$.
(c) Le groupe $\mathrm{Isom}^+(T) \subset \mathrm{SO}_3(\mathbb{R})$ ne contient pas d'élément d'ordre 4. Il contient douze éléments dont huit d'ordre 3, trois d'ordre 2 et l'identité.
Autre justification possible : $\mathrm{Isom}^+(T) \subset \mathrm{SO}_3(\mathbb{R})$ est isomorphe à $\mathcal{A}_4$ et $\mathcal{A}_4$ ne contient pas d'élément d'ordre 4 (les 4-cycles ne sont pas de signature 1).
(d) Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un groupe d'ordre 16 qui contient le neutre d'ordre 1 et des éléments d'ordre 2.

Exercice 8.

On note $\mathbb{H}_8$ le sous-groupe de $\mathrm{GL}_2(\mathbb{C})$, appelé *groupe des quaternions* engendré par les trois matrices

$$I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad J = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix} \qquad K = \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix}$$

1. Calculer l'ordre de $\mathbb{H}_8$.
2. Exhiber les sous-groupes de $\mathbb{H}_8$.
3. Exhiber les sous-groupes distingués de $\mathbb{H}_8$.
4. Est-il isomorphe au groupe diédral D_8 ?

Éléments de correction de l'exercice 8.

1. On vérifie que

$$I^2 = J^2 = K^2 = -\mathrm{id} \qquad IJ = K.$$

Par conséquent le groupe des quaternions est

$$\mathbb{H}_8 = \{\mathrm{id}, -\mathrm{id}, I, -I, J, -J, K, -K\}.$$

En particulier il est d'ordre 8.

2. D'après le théorème de Lagrange les sous-groupes propres de $\mathbb{H}_8$ sont d'ordre 2 ou 4. Il y a un seul sous-groupe d'ordre 2 : $\langle -\mathrm{id} \rangle$ et trois sous-groupes d'ordre 4 : $\langle I \rangle$, $\langle J \rangle$, $\langle K \rangle$.

3. Tous les sous-groupes de $\mathbb{H}_8$ sont distingués.
4. Le groupe diédral D_8 compte 5 éléments d'ordre 2 donc n'est pas isomorphe à $\mathbb{H}_8$ qui n'en compte qu'un.

Exercice 9.

(1) Soit G un groupe abélien. Soient a et b deux éléments de G d'ordres finis premiers entre eux. Montrer que ordre(ab) = ordre(a)ordre(b).

(2) Soit G un groupe abélien fini et soit m le maximum parmi les ordres des éléments de G, m est appelé l'exposant de G. Montrer que l'ordre de tout élément de G divise m.

(3) Soit $\Bbbk$ un corps et $\mathrm{G} \subset \Bbbk^*$ un sous-groupe fini du groupe multiplicatif $\Bbbk^*$. Montrer que G est cyclique. [Indication : on peut considérer les racines du polynôme $X^m - 1 \in \Bbbk[X]$ où m est l'exposant de G.]

(4) Qu'en déduire pour le groupe $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ avec p premier ? Qu'en déduire pour le groupe $\mathbb{C}^*$?

Éléments de correction de l'exercice 9.

(1) Posons m = ordre de a et n = ordre de b. On a $(ab)^{mn} = (a^m)^n(b^n)^m = 1$ donc mn est un multiple de d = ordre de (ab).
Par ailleurs on a $(ab)^d = 1$. Alors $a^d = b^{-d}$ sont de même ordre p divisant à la fois m et n (car $a^d \in \langle a\rangle$ et $b^{-d} \in \langle b\rangle$), donc $p = 1$. Autrement dit $a^d = b^{-d} = 1$ (dans un groupe le neutre est l'unique élément d'ordre 1). Ainsi d est un multiple commun de m et n donc un multiple de ppcm(m,n)= mn. Il en résulte que $d = mn$.

(2) Soit $x \in \mathrm{G}$ réalisant l'ordre maximal m. Raisonnons par l'absurde : supposons qu'il existe $y \in \mathrm{G}$ dont l'ordre q ne divise pas m. Il existe alors un premier p et des entiers $b > a$ tels que

$$m = p^a m' \qquad\qquad q = p^b q'$$

avec m', n' premiers avec p. D'après (1) l'ordre de $y^{q'}x^{p^a}$ est $p^b m' > m$: contradiction.

(3) D'après (2) tous les éléments de G sont des racines de $X^m - 1$. Or un polynôme de degré m sur un corps a au plus m racines et les m éléments du groupe $\langle x\rangle$ engendré par x fournissent déjà m racines. Il s'en suit que $\mathrm{G} = \langle x\rangle$. En particulier G est cyclique.

(4) Pour tout premier p le groupe $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ est cyclique.
Tout sous-groupe fini de $\mathbb{C}^*$ est un groupe cyclique engendré par une racine de l'unité.

Exercice 10.

(1) Soient $n \geq 1$ et k deux entiers. Montrer l'équivalence des assertions suivantes :
(i) $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ engendre $\mathbb{Z}/n\mathbb{Z}$;
(ii) n et k sont premiers entre eux ;
(iii) $\overline{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

(2) Montrer que $\big(\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ\big) \simeq \big((\mathbb{Z}/n\mathbb{Z})^*, \times\big)$.

Éléments de correction de l'exercice 10.

(1) Soient $n \geq 1$ et k deux entiers. Montrons que $(i) \Longleftrightarrow (iii)$. Si $\overline{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ alors il existe $a \geq 1$ tel que

$$\underbrace{\overline{k} + \overline{k} + \ldots + \overline{k}}_{a \text{ fois}} = \overline{1}$$

et donc $\overline{a}$ est l'inverse de $\overline{k}$ modulo n.
Réciproquement si $\overline{k}$ est inversible modulo n on peut choisir d'écrire l'inverse sous la forme $\overline{a}$ avec $a \geq 1$.

Montrons que $(ii) \Longleftrightarrow (iii)$.
L'égalité $\overline{a}\overline{k} = \overline{1}$ équivaut à l'existence d'un $u \in \mathbb{Z}$ tel que $ak + un = 1$. Par Bezout ceci équivaut à k et n premiers entre eux.

(2) Montrons que $\big(\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ\big) \simeq \big((\mathbb{Z}/n\mathbb{Z})^*, \times\big)$.
Puisque $\mathbb{Z}/n\mathbb{Z}$ est cyclique, un morphisme φ est entièrement déterminé par l'image d'un générateur, donc en particulier par l'image de $\overline{1}$.

φ est un automorphisme si et seulement $\varphi(\overline{1})$ est aussi un générateur de $\mathbb{Z}/n\mathbb{Z}$.
Par la question précédente on associe donc à chaque $\varphi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ un élément inversible $\overline{a} = \varphi(\overline{1}) \in (\mathbb{Z}/n\mathbb{Z})^*$.
Montrons qu'en fait φ est l'homothétie de rapport $\overline{a}$. On peut supposer $g \geq 1$. Pour tout $0 \leq x \leq n-1$ on écrit

$$\varphi(\overline{x}) = \varphi(\underbrace{\overline{1}+\overline{1}+\ldots+\overline{1}}_{x \text{ fois}}) = \underbrace{\varphi(\overline{1})+\varphi(\overline{1})+\ldots+\varphi(\overline{1})}_{x \text{ fois}} = \underbrace{\overline{a}+\overline{a}+\ldots+\overline{a}}_{x \text{ fois}} = \overline{ax}.$$

Ceci implique que la bijection

$$\varphi\colon \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^*, \qquad \overline{1} \mapsto \varphi(\overline{1})$$

est un morphisme de groupes donc un isomorphisme.

Exercice 11.

Montrer que le sous-groupe Int(G) des automorphismes intérieurs de G est un sous-groupe distingué du groupe Aut(G) et que $\mathrm{Int(G)} \simeq \mathrm{G}/Z(\mathrm{G})$ où $Z(\mathrm{G})$ est le centre de G.

Éléments de correction de l'exercice 11.

Soit φ l'automorphisme intérieur associé à la conjugaison par $y \in \mathrm{G}$:

$$\forall\, x \in \mathrm{G} \qquad \varphi(x) = yxy^{-1}.$$

Soit ψ un élément de Aut(G). On a pour tout $x \in \mathrm{G}$

$$\psi\varphi\psi^{-1}(x) = \psi(y\psi^{-1}(x)y^{-1}) = \psi(y)x\psi(y)^{-1}.$$

Ainsi $\psi\circ\varphi\circ\psi^{-1}$ est encore un automorphisme intérieur associé à la conjugaison par $\psi(y)$. Par conséquent Int(G) est distingué dans Aut(G).

D'autre part, via l'action par conjugaison de G sur lui-même on obtient un morphisme surjectif de G vers Int(G), dont le noyau est le centre de G. On conclut par le théorème d'isomorphisme que $\mathrm{Int(G)} \simeq \mathrm{G}/Z(\mathrm{G})$.

Exercice 12.

Soit G un groupe abélien infini. Montrer que l'ensemble T des éléments d'ordre fini de G est un sous-groupe de G.

Si $\mathrm{T} = \{e\}$, on dit que G est sans torsion.

Montrer que G/T est sans torsion.

Éléments de correction de l'exercice 12.

Puisque $o(e) = 1$, on a $e \in \mathrm{T}$. Soient x, $y \in \mathrm{T}$ d'ordres k, $m \in \mathbb{N}^*$. On a $(xy)^{km} = (x^k)^m(y^m)^k = e$ donc $xy \in \mathrm{T}$. Comme $o(x) = o(x^{-1})$, on a $x^{-1} \in \mathrm{T}$. Ainsi T est un sous-groupe de G.

Considérons l'application canonique $\varphi\colon \mathrm{G} \to \mathrm{G/T}$. Soit $a \in \mathrm{G/T}$ d'ordre fini $s \in \mathbb{N}^*$. Il existe $x \in \mathrm{G}$ tel que $a = \varphi(x)$. On a

$$\varphi(x^s) = a^s = e$$

donc $x^s \in \mathrm{T} = \ker\varphi$. Il existe donc $r \in \mathbb{N}^*$ tel que $x^{sr} = (x^s)^r = e$ ce qui prouve que $x \in \mathrm{T}$ et donc que $a = \varphi(x) = e$. Par suite G/T est sans torsion.

Exercice 13. Soient $p < q$ deux nombres premiers tels que p divise $q-1$. Donner un exemple de groupe non-abélien G d'ordre pq constitué de matrices triangulaires dans $\mathrm{GL}_2\big(\mathbb{Z}/q\mathbb{Z}\big)$.

Éléments de correction de l'exercice 13. Soient $p < q$ deux nombres premiers tels que p divise $q-1$. On a : $\mathbb{F}_q^*$ est cyclique d'ordre $q-1$. Soit a un générateur de $\mathbb{F}_q^*$. Posons $\mathrm{H} = \langle a^k\rangle$ où k est tel que $kp = q-1$. Alors

$$\left\{ \begin{pmatrix} b & c \\ 0 & b \end{pmatrix} \mid b \in \mathrm{H},\, c \in \mathbb{F}_q \right\}$$

est un groupe d'ordre pq.

Exercice 14. Soient G un groupe et H un sous-groupe de G.

(a) Montrer qu'en posant $g \cdot a\mathrm{H} = (ga)\mathrm{H}$, où a, $g \in \mathrm{G}$, on définit une action de G sur l'ensemble G/H des classes à gauche modulo H.

(b) Montrer que cette action est transitive.
Déterminer le stabilisateur de aH.

(c) On suppose G fini. Calculer le cardinal d'une orbite et retrouver un théorème classique.

Éléments de correction de l'exercice 14.

(a) Posons $X = G/H$. Soient g dans G et x dans X. Désignons par a, a' deux représentants de la classe à gauche x. On a $a\mathrm{H} = a'\mathrm{H} = x$ ou encore $a^{-1}a' \in \mathrm{H}$. Or

$$(ga)^{-1}ga' = a^{-1}g^{-1}ga' = a^{-1}a' \in \mathrm{H}$$

donc $ga\mathrm{H} = ga'\mathrm{H}$.
Si on remplace a par un autre représentant a' de la classe $x = a\mathrm{H}$, alors $ga'\mathrm{H} = ga\mathrm{H}$. La formule a donc bien un sens et définit une application de $\mathrm{G} \times X \to X$.
C'est bien une action de G sur X puisque

- $\forall\, x = a\mathrm{H} \in X$ $e \cdot x = ea\mathrm{H} = a\mathrm{H} = x$,
- $\forall\, x = a\mathrm{H} \in X$, $\forall\, g \in \mathrm{G}$, $\forall\, g' \in \mathrm{G}$,

$$g \cdot (g' \cdot x) = g \cdot (g'a\mathrm{H}) = g(g'a)\mathrm{H} = (gg')a\mathrm{H} = gg' \cdot x$$

(b) Pour tous $x = a\mathrm{H} \in X$ et $y = b\mathrm{H} \in X$ il existe $g \in \mathrm{G}$ tel que $g \cdot x = y$ (prendre $g = ba^{-1}$). Il existe donc une seule orbite, égale à X.
Le stabilisateur de $x = a\mathrm{H}$ est $a\mathrm{H}a^{-1}$ car :

$$g \in \mathrm{G}_x \iff ga\mathrm{H} = a\mathrm{H} \iff a^{-1}ga\mathrm{H} = \mathrm{H} \iff a^{-1}ga \in \mathrm{H} \iff g \in a\mathrm{H}a^{-1}.$$

(c) Comme $\mathrm{G}_x = a\mathrm{H}a^{-1} = \mathrm{Ad}_a(\mathrm{H}) \simeq \mathrm{H}$, on retrouve le théorème de Lagrange

$$[\mathrm{G} : \mathrm{H}] = \mathrm{card}(G/H) = \mathrm{card}(\mathrm{orb}(x)) = \frac{[\mathrm{G} : 1]}{[\mathrm{G}_x : 1]} = \frac{[\mathrm{G} : 1]}{[\mathrm{H} : 1]}.$$