École Normale Supérieure, Année 2019-2020

1^{e} année, Algèbre 1

Partiel : Correction

Exercice 1.

(a) Soit G un groupe d'ordre n tel que pour tout diviseur d de n il existe au plus un sous-groupe de G de cardinal d. Pour tout diviseur d de n on note $N(d)$ le nombre d'éléments d'ordre d dans G. On veut montrer que $N(n) \neq 0$. Pour d un diviseur de n donné, s'il existe un élément x d'ordre d dans G on a $N(d) = \varphi(d)$, la fonction indicatrice d'Euler. En effet, tout élément d'ordre d engendre *l'unique* sous-groupe cyclique d'ordre d de G et un tel groupe admet $\varphi(d)$ générateurs. En conclusion, pour d un diviseur de n on a soit $N(d) = \varphi(d)$, soit $N(d) = 0$. De plus, tout élément de G a un ordre qui divise l'ordre de G (Théorème de Lagrange). On en déduit que

$$\sum_{d|n} N(d) = n.$$

Mais on sait que $\sum_{d|n} \varphi(d) = n$. Or, $\sum_{d|n} N(d) \leqslant \sum_{d|n} \varphi(d)$ et donc pour tout diviseur d de n on a $N(d) = \varphi(d)$. On en déduit que $N(n) \neq 0$.

(b) Le groupe abélien $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ d'ordre 4 contient au moins un sous-groupe d'ordre 1, 2 et 4. Il contient en particulier 3 groupes d'ordre 2 qui sont $\langle(1,0)\rangle$, $\langle(0,1)\rangle$, $\langle(1,1)\rangle$. Mais il n'est pas cyclique car il ne contient pas d'élément d'ordre 4. On peut aussi considérer $\mathfrak{S}_3$ qui admet 3 sous-groupes d'ordre 2 et un sous-groupe d'ordre 3, mais qui n'est pas cyclique.

Exercice 2.

(a) Soit A une partie de $\mathbb{Z}/p^n m\mathbb{Z}$ de cardinal p^n fixe sous G. Soit $x_0 \in A$. Comme A est stable sous l'action de G, A contient l'orbite sous l'action de G de x_0, i.e. $G \cdot x_0 \subset A$. Par la simplification des égalités dans un groupe on a une bijection $G \cong G \cdot x_0$ et comme G est de cardinal p^n les cardinaux forcent $A = G \cdot x_0$. En tant qu'ensemble, l'orbite s'écrit $\{x_0 + x \ ; \ x \in G\}$, qui est par définition la classe de x_0 dans $\mathbb{Z}/p^n m\mathbb{Z}$ modulo G. Inversement, il est clair que toute classe modulo G est de cardinal p^n et est stable sous l'action de G puisque $\mathbb{Z}/p^n m\mathbb{Z}$ est abélien.

(b) On sait d'après le cours que $\mathrm{Card}(E) \equiv \mathrm{Card}(E^G) \mod p$. On a $\mathrm{Card}(E) = \binom{p^n m}{p^n}$. Par la question (a), les sous-ensembles de cardinal p^n stables par G sont précisément les classes de $\mathbb{Z}/p^n m\mathbb{Z}$ modulo G ; ainsi $\mathrm{Card}(E^G) = [\mathbb{Z}/p^n m\mathbb{Z} : G] = m$. La formule des classes donne alors

$$\binom{p^n m}{p^n} \equiv m \mod p.$$

Exercice 3.

Soit G un groupe de cardinal p^n tel que $Z(G)$ est au moins de cardinal p^{n-1}. Comme $Z(G)$ est un sous-groupe de G son cardinal divise celui de G donc $Z(G)$ est de cardinal p^{n-1} ou p^n. Supposons que $Z(G)$ est de cardinal p^{n-1}. Soit $x \in G$ tel que $x \notin Z(G)$. On pose $Z_G(x) = \{y \in G \mid yx = xy\}$ le centralisateur de x dans G. On vérifie facilement que c'est un sous-groupe de G et que $Z(G) \subset Z_G(x)$ et $x \in Z_G(x)$. Ainsi, $Z_G(x)$ contient strictement $Z(G)$ et donc est de cardinal $> p^{n-1}$. On en déduit que $Z_G(x) = G$, i.e. x commute à tout élément de G. Donc $x \in Z(G)$, ce qui est une contradiction. Ainsi, $Z(G)$ est de cardinal p^n et donc $G = Z(G)$, ce qui signifie que G est abélien.

Pour obtenir la contradiction on aurait aussi pu utiliser le fait suivant que l'on a vu dans le TD 1 (exercice 13) : si le quotient d'un groupe G par son centre est monogène alors le groupe est abélien. Comme ici $G/Z(G)$ est d'ordre p, ce quotient est cyclique et donc G est abélien.

Exercice 4.

(a) Soit $d \geqslant 1$ un entier. On montre que $\overline{1/d}$ est d'ordre d. On a $d \cdot \overline{1/d} = \overline{0}$. Soit k un entier tel que $k < d$ et supposons que $k \cdot \overline{1/d} = \overline{0}$. Alors $k/d \in \mathbb{Z}$, i.e. d divise k, ce qui est absurde. On sait qu'un élément d'ordre d engendre un sous-groupe de cardinal d, donc G_d est de cardinal d.

(b) On sait que pour tout entier $d \geqslant 1$, $G_d \subset \mathbb{Q}/\mathbb{Z}$. Ainsi $\bigcup_{d \geqslant 1} G_d \subset \mathbb{Q}/\mathbb{Z}$. Soit $\frac{a}{d} \in \mathbb{Q}$, alors $\overline{a/d} \in G_d$. Ainsi tout élément de $\mathbb{Q}/\mathbb{Z}$ appartient à un G_d et donc

$$\bigcup_{d \geqslant 1} G_d = \mathbb{Q}/\mathbb{Z}.$$

(c) Soit $\delta, d \geqslant 1$ deux entiers. Supposons que $d|\delta$. Soit k un entier tel que $\delta = dk$. Alors $k \cdot \overline{1/\delta} = \overline{1/d}$ et donc le groupe engendré par $\overline{1/\delta}$ contient $\overline{1/d}$. Ainsi on a $G_d \subset G_\delta$. Inversement, supposons que $G_d \subset G_\delta$. Alors l'ordre de G_d divise l'ordre de G_δ, donc par la question (a) d divise δ.

(d) On va montrer que $\overline{1/d} \in G$ car alors G contient le sous-groupe engendré par $\overline{1/d}$ qui est G_d. Par le théorème de Bezout on fixe $u, v \in \mathbb{Z}$ tel que $ua + vd = 1$. On divise alors par d et comme $v \in \mathbb{Z}$ on obtient dans $\mathbb{Q}/\mathbb{Z}$:

$$u \cdot \overline{\frac{a}{d}} = \overline{\frac{1}{d}}.$$

Comme $\overline{a/d} \in G$ le membre de gauche est dans G, donc $\overline{1/d} \in G$.

(e) Soit n l'ordre de G. Alors par le théorème de Lagrange, pour tout $x \in G$ on a $n \cdot x = 0$. Montrons que $G = G_n$. Remarquons que $\mathrm{Card}(G) = \mathrm{Card}(G_n)$ d'après la question (a) donc il suffit de montrer que $G \subset G_n$. Soit $x = \overline{a/d} \in G$ pour $a \in \mathbb{Z}$ et $d \geqslant 1$ premiers entre eux. Alors comme $n \cdot x = 0$, $na \in d\mathbb{Z}$. Ainsi $d|na$ et donc $d|n$ puisqu'on a supposé a et d premiers entre eux. Soit $k \geqslant 1$ tel que $kd = n$. On a alors dans $\mathbb{Q}/\mathbb{Z}$

$$\overline{\frac{a}{d}} = \overline{\frac{ak}{n}} \in G_n.$$

Ainsi $x \in G_n$ et donc $G \subset G_n$. Une autre preuve possible consiste à remarquer que les dénominateurs de G sont en nombres finis, donc si on note d' le produit de ces dénominateurs $G \subset G_{d'}$. Mais $G_{d'}$ est cyclique d'ordre d' donc G est un sous-groupe cyclique engendré par un élément a/d avec a et $d \geqslant 1$ premiers entre eux. On déduit que $G = G_d$ par la question précédente.

(f) Soit $m_d \colon \mathbb{Q} \to \mathbb{Q}$ le morphisme $x \mapsto dx$, de multiplication par d (c'est bien un morphisme car $\mathbb{Q}$ est abélien). Le morphisme m_d est surjectif et injectif. Composé avec la projection (surjective) modulo $\mathbb{Z}$, on obtient un morphisme surjectif $\overline{m_d} \colon \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ donné par $x \to d \cdot \overline{x}$. Par la propriété universelle du quotient on en déduit un isomorphisme $\mathbb{Q}/\ker(m_d) \cong \mathbb{Q}/\mathbb{Z}$. On a

$$\ker(\overline{m_d}) = m_d^{-1}(\mathbb{Z}) = \frac{1}{d} \cdot \mathbb{Z} \subset \mathbb{Q},$$

donc $\ker(\overline{m_d})$ est le sous-groupe de $\mathbb{Q}$ engendré par $\frac{1}{d}$ et donc par définition, sa classe modulo $\mathbb{Z}$ est $\ker(\overline{m_d})/\mathbb{Z} = G_d$. Ainsi la relation du biquotient donne

$$\mathbb{Q}/\ker(\overline{m_d}) \cong (\mathbb{Q}/\mathbb{Z})/(\ker(\overline{m_d})/\mathbb{Z}) \cong (\mathbb{Q}/\mathbb{Z})/G_d,$$

et l'isomorphisme obtenu par la propriété universelle nous donne finalement $(\mathbb{Q}/\mathbb{Z})/G_d \cong \mathbb{Q}/\mathbb{Z}$. On aurait aussi pu montrer directement que la multiplication par d sur $\mathbb{Q}/\mathbb{Z}$ est surjective et que son noyau est G_d.

(g) Par définition,

$$\Gamma_p = \bigcup_{n \geqslant 1} G_{p^n},$$

qui est une union croissante d'après la question (c). C'est donc bien un sous-groupe de $\mathbb{Q}/\mathbb{Z}$. En effet il contient 0 et si $x, y \in \Gamma_p$, il existe $n \geqslant 1$ tel que $x, y \in G_{p^n}$, donc $-x$ et $x + y$ sont dans G_{p^n} et a fortiori dans Γ_{p^n}. De plus, d'après la question (a), $\mathrm{Card}(G_{p^n}) = p^n$ donc Γ_p contient des sous-groupes de taille arbitrairement grand et donc Γ_p est infini.

(h) On montre que les éléments de Γ_p sont tous d'ordre une puissance de p. Par ce qui précède, si $x \in \Gamma_p$ alors il existe $n \geqslant 1$ tel que $x \in G_{p^n}$ donc $p^n \cdot x = 0$. Ainsi l'ordre de x divise p^n et donc c'est une puissance de p.
Inversement, soit $x = \overline{b/d} \in \mathbb{Q}/\mathbb{Z}$ tel qu'il existe $n \geqslant 1$ tel que $p^n \cdot x = 0$. Alors il existe $a \in \mathbb{Z}$ tel que $p^n b = ad$. On en déduit que
$$\overline{\frac{b}{d}} = \overline{\frac{a}{p^n}} \in G_{p^n}.$$
Ainsi on a montré que $x \in G_{p^n}$ donc a fortiori $x \in \Gamma_p$.

(i) On note P l'ensemble des nombres premiers. Pour tout $p \in P$ on a un sous-groupe $\Gamma_p \subset \mathbb{Q}/\mathbb{Z}$, on en déduit l'inclusion
$$\Gamma = \sum_{p \in P} \Gamma_p \subset \mathbb{Q}/\mathbb{Z}.$$
Montrons que la somme est exhaustive. Soit $x = \overline{a/b} \in \mathbb{Q}/\mathbb{Z}$, montrons que $x \in \Gamma$. Soit $b = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la décomposition en nombres premiers de b. Pour tout i tel que $1 \leqslant i \leqslant r$ on pose $q_i = b/p^{\alpha_i}$. Alors les q_i sont premiers dans leurs ensemble donc par le théorème de Bézout il existe $a_1, \ldots, a_r \in \mathbb{Z}$ tel que $\sum_{i=1}^r a_i q_i = 1$. On multiplie cette relation par a/b et on prend sa classe modulo $\mathbb{Z}$ pour obtenir
$$x = \sum_{i=1}^{r} \overline{\frac{aa_i}{p^{\alpha_i}}} \in \Gamma.$$
Montrons que la somme est directe. Soit $p_1, \ldots, p_r \in P$ une famille distinctes de nombres premiers. Soit pour tout i tel que $1 \leqslant i \leqslant r$ un élément $x_i \in \Gamma_{p_i}$; alors d'après la question précédente il existe $\nu_i \in \mathbb{N}$ tel que x_i est d'ordre p^{ν_i}. On pose, comme précédemment, $q_i = \prod_{j \neq i} p^{\nu_j}$, qui sont premiers dans leurs ensemble. Supposons que $\sum_{j=1}^r x_{p_j} = 0$. Alors, soit i tel que $1 \leqslant i \leqslant r$, on a
$$0 = q_i \sum_{j=1}^{r} x_{p_j} = q_i x_{p_i}.$$
Donc l'ordre de x_{p_i} divise le pgcd de q_i et $p_i^{\nu_i}$ qui est 1. Donc pour tout indice i on a $x_{p_i} = 0$, ce qui montre que la somme est directe.
On aurait aussi pu raisonner en utilisant le lemme chinois qui donne que pour tout entier $d \geqslant 1$
$$G_d = \bigoplus_{p \mid d} (\Gamma_p \cap G_d) = \bigoplus_{p \in P} (\Gamma_p \cap G_d). \tag{1}$$
Il suffit alors de justifier la suite d'égalités suivantes, en remarquant qu'on peut écrire l'union de la question (b) comme une union croissante :
$$\mathbb{Q}/\mathbb{Z} = \bigcup_{d \geqslant 1} G_d = \bigcup_{d \geqslant 1} \bigoplus_{p \in P} (\Gamma_p \cap G_d) = \bigoplus_{p \in P} (\Gamma_p \cap \bigcup_{d \geqslant 1} G_d) = \bigoplus_{p \in P} \Gamma_p.$$
Attention à ne pas croire qu'on peut toujours échanger une union et une somme directe...

Exercice 5.

(a) Vu dans le TD : soit G un groupe dont tous les éléments sont d'ordre 2. Alors pour tout $x \in G$ on a $x = x^{-1}$. Or pour $x, y \in G$ on a $(xy)^{-1} = y^{-1}x^{-1}$. Ainsi
$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx,$$
donc G est commutatif.

(b) Vu dans le TD : soit H un sous-groupe d'indice 2 de G. Soit $g \in G$ tel que $g \notin H$, alors les décomposition en classes à gauche et à droite donnent
$$G = H \cup gH \text{ et } G = H \cup Hg,$$
donc $gH = Hg$ et ainsi H est distingué.

(c) On utilise le théorème de classification des groupes abéliens. Les facteurs invariants de G sont soit 8, soit $2, 4$, soit $2, 2, 2$ et donc les groupes abéliens d'ordre 8 sont

$$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^3.$$

(d) Le groupe diédral D_4 est engendré par un élément r d'ordre 4 et un élément s d'ordre 2 tel que $srs = r^{-1}$. Ainsi $D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$ et donc il y a 5 éléments d'ordre 2 qui sont r^2, s, sr, sr^2, sr^3.

(e) On pose $H = Q_8$ le groupe des quaternions, on a $H = \{1, -1, i, -i, j, -j, k, -k\}$ où $\pm i, \pm j, \pm k$ sont des éléments d'ordre 4. Il y a donc un unique élément d'ordre 2 qui est -1 et donc H ne peut pas être isomorphe au groupe diédral qui admet 5 éléments d'ordre 2.

(f)(f1) Supposons que G n'a pas d'élément d'ordre 4. Rappelons que l'ordre des éléments de G divise son cardinal, donc G admet des éléments d'ordre 2 ou 8. S'il contient un élément d'ordre 8 il est cyclique ce qui n'est pas possible puisqu'il est supposé non abélien. Ainsi tout élément est d'ordre 2 ce qui n'est pas possible non plus puisque ceci impliquerait qu'il est abélien par la question (a). Ainsi G contient un élément i d'ordre 4 qu'on fixe dans la suite.

(f2) L'élément d'ordre 4 engendre un sous-groupe $I \subset G$ isomorphe à $\mathbb{Z}/4\mathbb{Z}$ (car cyclique d'ordre 4) qui est alors d'indice 2. Par la question (b) il est distingué et le quotient est d'ordre 2 donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$. On obtient une suite exacte courte

$$0 \to \mathbb{Z}/4\mathbb{Z} \to G \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

Cette suite exacte est scindée : soit $s \in G$ un élément d'ordre 2 différent de i^2, qui existe par hypothèse. Alors on pose la section $\phi\colon \mathbb{Z}/2\mathbb{Z} \to G$ qui envoie 1 sur s. Pour montrer que c'est une section il suffit de montrer que s n'est pas dans le noyau de la surjection $G \to \mathbb{Z}/2\mathbb{Z}$ i.e. qu'il n'est pas dans I. Mais le seul élément d'ordre 2 de I est i^2 et on a supposé que $s \neq i^2$. Ainsi s n'est pas envoyé sur 0 par cette surjection et ne peut donc être envoyé que sur 1. Comme la suite exacte est scindée on en déduit que G est un produit semi-direct i.e. $G \cong \mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ où $\varphi\colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. Or comme G est supposé non abélien, φ est non trivial, mais il existe un unique morphisme non nul $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ et donc un unique produit semi-direct non trivial $\mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$.

Le groupe diédral est un groupe non-abélien d'ordre 8, il contient l'élément r d'ordre 4 et l'élement s d'ordre 2 qui est tel que $r^2 \neq s$. Il vérifie les hypothèses de ce qu'on vient de montrer, donc $D_4 \cong \mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z} \cong G$.

(f3) Dans ce cas on note toujours I le sous-groupe engendré par i. Par hypothèse, il n'existe pas d'élément d'ordre 2 qui n'appartient pas à I, donc il existe un élément $j \in G$ d'ordre 4. De plus ij n'est pas dans $\langle i \rangle$ ni dans $\langle j \rangle$, donc il est d'ordre 4. On a de plus $j^2 = (ij)^2 = i^2$, l'unique élément d'ordre 2. Les éléments de G sont alors $1, i, i^2, i^3, j, j^3, ij, (ij)^3$ et si on explicite la table de multiplication, on se rend compte qu'on obtient bien H, le groupe des quaternions.