Algèbre 2

Partiel du 09/11/2018 – Corrigé

Calculatrices et documents non autorisés. Durée 2h

Exercice 1(1) Déterminer tous les éléments d'ordre 9 du groupe $\mathbb{U}_{45}$.

(2) Déterminer tous les sous-groupes du groupe $\mathbb{Z}/8\mathbb{Z}$.

Corrigé. (1) Le groupe $\mathbb{U}_{45}$ est cyclique d'ordre 45 et engendré par $\xi = e^{2i\pi/45}$. Les éléments d'ordre 9 de $\mathbb{U}_{45}$ sont les générateurs du seul sous-groupe H_9 d'ordre 9. Il y en a $\varphi(9) = 3(3-1) = 6$. Ce sous-groupe peut être donné par $H_9 = \langle a \rangle$ où $a = \xi^{45/9} = e^{2i\pi/9}$. Un élément a^k $(0 \leq k \leq 8)$ est un générateur de H_9 si et seulement si $k \wedge 9 = 1$, c'est à dire $k = 1, 2, 4, 5, 7, 8$. Ainsi les éléments d'ordre 9 de $\mathbb{U}_{45}$ sont

$$a = e^{2i\pi/9}, a^2 = e^{4i\pi/9}, a^4 = e^{8i\pi/9}, a^5 = e^{10i\pi/9}, a^7 = e^{14i\pi/9}, a^8 = e^{16i\pi/9}.$$

(2) Le groupe $\mathbb{Z}/8\mathbb{Z}$ est cyclique d'ordre 8 et engendré par $\bar{1}$. Ses sous-groupes correspondent donc aux diviseurs de 8 : 1, 2, 4, 8.

$H_1 = \{\bar{0}\}$.

$H_2 = \langle \frac{8}{2}\bar{1} \rangle = \langle \bar{4} \rangle = \{\bar{0}, \bar{4}\} \simeq \mathbb{Z}/2\mathbb{Z}$

$H_4 = \langle \frac{8}{4}\bar{1} \rangle = \langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\} \simeq \mathbb{Z}/4\mathbb{Z}$

$H_8 = \mathbb{Z}/8\mathbb{Z}$.

Exercice 2 Soit G un groupe **non-abélien** d'ordre $8 = 2^3$.

(1) Montrer que G ne possède pas d'éléments d'ordre 8.

(2) Montrer que si G ne possède pas d'éléments d'ordre 4 alors G est abélien. En déduire qu'il existe un élément $a \in G$ d'ordre 4; on notera $H = \langle a \rangle$ le sous-groupe engendré par a.

(3) Calculer $[G : H]$. Montrer que que H est distingué dans G et qu'il existe $b \in G$, $b \notin H$ tel que $G = H \cup Hb$.

(4) Montrer que $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$.

(5) Montrer que $b^{-1}ab \in H$ et calculer l'ordre de $b^{-1}ab$. En déduire que $b^{-1}ab = a$ ou $b^{-1}ab = a^3$. (utiliser les propriétés des groupes cycliques).

(6) Montrer que si $b^{-1}ab = a$ alors G est abélien. En déduire que $b^{-1}ab = a^3$

(7) Montrer que $b^2 \in H$, $b^2 \neq a$ et $b^2 \neq a^3$. En déduire que $b^2 = e$ ou $b^2 = a^2$.

(8) On suppose que $b^2 = e$. Déterminer la table de G; on notera G_1 le groupe obtenu.

(9) On suppose que $b^2 = a^2$. Déterminer la table de G; on notera G_2 le groupe obtenu.

(10) Les groupes G_1 et G_2 sont-ils isomorphes? (observer les ordres des éléments de G_1 et G_2).

Corrigé. (1) Supposons que G admet un élément x d'ordre 8. Alors le sous-groupe $\langle x\rangle$ engendré par x serait un sous-groupe cyclique et donc abélien. Comme ce sous-groupe est d'ordre 8 et que G et lui même d'ordre 8, on déduit que $G = \langle x\rangle$, ce qui contredit le fait que G n'est pas abélien. Par conséquent, aucun élément de G n'est d'ordre 8.

(2) Supposons que G ne possède pas d'éléments d'ordre 4. Alors tout élément $x \in G$ est soit d'ordre 1, soit d'ordre 2. Il vérifie donc $x^2 = e$. Cette propriété est équivalente à $x^{-1} = x$ et entraine la commutativité de la loi du groupe G, ce qui contredit le fait que G est non abélien. On en déduit qu'il existe au moins un élément $a \in G$ d'ordre 4.

(3) Soit $H = \langle a\rangle = \{e, a, a^2, a^3\}$ le sous-groupe de G engendré par a.
D'après le théorème de Lagrane $[G : H] = \frac{|G|}{|H|} = \frac{8}{4} = 2$, donc H est un sous-groupe d'indice 2 dans G, il est donc distingué dans G. D'autre part, l'ensemble quotient $H\backslash G$ (des classes à droite) est de cardinal 2. Il contient donc deux éléments, la classe $\bar{a} = Ha = H$ (car $a \in H$) et la classe $\bar{b} = Hb$ d'un élément $b \in G$ n'appartenant pas à H (les classes d'équivalences sont ou bien égales ou bien disjointes). Comme les classes d'équivalences de G forment une partition de G, on a alors $G = H \cup Hb$.
(4) De la question précédente on déduit que G est une réunion disjointe de $H = \{e, a, a^2, a^3\}$ et $Hb = \{b, ab, a^2b, a^3b\}$, donc le groupe $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$.

(5) Si $b^{-1}ab \in Hb$, alors $b^{-1}a \in H$ et par suite $b \in H$ ce qui est absurde. On en déduit que $b^{-1}ab \in H$. Or $o(b^{-1}ab) = o(a) = 4$ et H est un groupe cyclique d'ordre 4. Donc $b^{-1}ab$ est un générateur de H. Mais H admet $\varphi(4) = 2$ générateurs, qui sont a et a^3. On en déduit que $b^{-1}ab = a$ ou $b^{-1}ab = a^3$.

(6) Supposons que $b^{-1}ab = a$, alors $ab = ba$ et donc G est abélien, ce qui contredit la première l'hypothèse de l'exercice. On en déduit que $b^{-1}ab = a^3$.

(7) On a $b^2 \in G$ et G est réunion disjointe de H et Hb. Si $b^2 \in Hb$, alors forcément $b \in H$ ce qui est absurde. On en déduit que $b^2 \in H$.
– Si $b^2 = a$, alors $ab = b^3 = ba$ ce qui entraine que G est abélien.
– Si $b^2 = a^3$, alors $b^2 = b^{-1}ab$ et $b^2 = a$. On se ramène alors au cas précédent.
Par conséquent, $b^2 = e$ ou $b^2 = a^2$.

(8) On suppose $b^2 = e$, alors dans ce cas on notera $G = G_1$. Sa table du groupe est

$\times$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

On peut remarquer que le groupe G_1 ci-dessus admet cinq éléments d'ordre 2 (tous les éléments de Hb et a^2) et deux éléments d'ordre 4 (a et a^3). G_1 est un **groupe diédral**.

(9) On suppose $b^2 = a^2$, alors dans ce cas on notera $G = G_2$. Sa table du groupe

est

$\times$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	e	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	e
a^2b	a^2b	ab	b	a^3b	e	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	e	a^3	a^2

.

On peut remarquer que le groupe G_2 ci-dessus admet six éléments d'ordre 4, un élément d'ordre 2 (qui est a^2). G_2 est appelé **groupe quaternionique**.

(10) Un isomorphisme de groupes conserve les ordres des éléments. Comme il n y'a pas autant d'éléments d'ordre 2 (ou d'ordre 4) dans les groupes G_1 et G_2, alors ces deux groupes ne peuvent pas être isomorphes.

Exercice 3

Lemme 1. Si G est un groupe fini et si H et K sont deux sous-groupes distingués de G tels que $H \cap K = \{e\}$ et $|G| = |H| \times |K|$, alors $G \simeq H \times K$.

Soit $p \geq 2$ un nombre premier.

(1) Soit G groupe fini d'ordre p^2 (donc abélien).

(a) Montrer que si G possède un élément d'ordre p^2, alors $G \simeq \mathbb{Z}/p^2\mathbb{Z}$.

(b) Montrer que si G ne possède aucun élément d'ordre p^2, alors $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. (On pourra considérer les deux sous-groupes $\langle x \rangle$, et $\langle y \rangle$ où $x \in G$, $x \neq e$ et $y \in G$, $y \notin \langle x \rangle$ et penser au Lemme 1).

(2) Soit G un groupe **abélien** d'ordre p^3.

(a) Montrer que si G possède un élément d'ordre p^3, alors $G \simeq \mathbb{Z}/p^3\mathbb{Z}$.

(b) Montrer que si tous les éléments de $G \setminus \{e\}$ sont d'ordre p, alors $G \simeq (\mathbb{Z}/p\mathbb{Z})^3$ (on pourra utiliser à deux reprises le Lemme 1).

On suppose que G ne possède pas d'éléments d'ordre p^3, mais au moins un éléments x d'ordre p^2. Soit $H = \langle x \rangle$ le sous-groupe engendré par x.

(c) On suppose qu'en dehors de H tous les éléments de G sont d'ordre p^2. Montrer que G contient $p^3 - p$ éléments d'ordre p^2 (utiliser les propriétés des groupes cycliques). En déduire que G contient $p - 1$ éléments d'ordre p.

Considérons maintenant l'application $\phi : G \to G$ tel que $g \mapsto \phi(g) = g^p$. Vérifier que ϕ est un morphisme de groupes, déterminer l'image des éléments d'ordre p^2 puis compter le nombre d'antécédents d'un élément de l'image de ϕ d'ordre p. Aboutir à une contradiction.

(d) En déduire qu'il existe un élément $y \in G$, $y \notin H$ d'ordre p et que $G \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (on pourra utiliser le Lemme 1).

(3) Déterminer, à isomorphisme près, tous les groupes d'ordre 8 (utiliser les conclusions des exercices 2 et 3).

Corrigé. Montrons le Lemme 1. Considérons le morphisme canonique $G \to G/H \times G/K$. Son noyau est $H \cap K = \{e\}$, donc c'est une injection. Comme $\mathrm{card}(G/H \times G/K) = \mathrm{card}(G/H) \times \mathrm{card}(G/K) = \mathrm{card}(K) \times \mathrm{card}(H) = \mathrm{card}(G)$, le

morphisme considéré est bijectif. D'où $G \simeq G/H \times G/K$.
Pour répondre à la question, il suffit donc de vérifier que $G/H \simeq K$ et $G/K \simeq H$. Pour cela soit la projection canonique $q : G \to G/K$ et considérons $q_{|H} : H \to G/K$ sa restriction à H. Son noyau est $H \cap K = \{e\}$, c'est donc une injection et par égalité des cardinaux c'est une bijection, donc $G/K \simeq H$. On montre de même que $G/H \simeq K$. D'où $G \simeq H \times K$.

(1) (a) Soit G un groupe d'ordre p^2. Donc G est abélien.

Si G possède un élément x d'ordre p^2, alors G est cyclique et isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$.

(b) Supposons que G ne possède aucun élément d'ordre p^2. Soit $x \in G$ un élément différent de e, alors x est d'ordre p et engendre un sous-groupe $\langle x \rangle$ d'ordre p isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Soit $y \in G$ tel que $y \notin \langle x \rangle$. Cet élément est aussi d'ordre p et engendre un sous-groupe cyclique $\langle y \rangle$ d'ordre p isomorphe à $\mathbb{Z}/p\mathbb{Z}$. De plus $\langle x \rangle \cap \langle y \rangle = \{e\}$. On peut donc appliquer la question (1) (car dans un groupe abélien tout sous-groupe est distingué), d'où $G \simeq \langle x \rangle \times \langle y \rangle \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

(2) Soit G un groupe d'ordre p^3.

(a) Si G possède un élément x d'ordre p^3, alors G est cyclique et isomorphe à $\mathbb{Z}/p^3\mathbb{Z}$.

(b) Supposons que tous les éléments non triviaux de G sont d'ordre p, alors G possède un sous-groupe d'ordre p^2 isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$: il suffit de prendre le sous-groupe K engendré par un élément non trivial x et par $y \notin \langle x \rangle$.
Soit $z \in G$ tel que $z \notin K$. Alors z est d'ordre p et $K \cap \langle z \rangle = \{e\}$ et on peut encore une fois appliquer la question (1), d'où $G \simeq K \cap \langle z \rangle \simeq (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \times \mathbb{Z}/p\mathbb{Z} = (\mathbb{Z}/p\mathbb{Z})^3$.

On suppose que G ne possède pas d'éléments d'ordre p^3, mais au moins un éléments x d'ordre p^2. Soit $H = \langle x \rangle$ le sous-groupe engendré par x. Donc $H \simeq \mathbb{Z}/p^2\mathbb{Z}$.

(c) On suppose qu'en dehors de H tous les éléments de G sont d'ordre p^2.
Comme H est cyclique d'ordre p^2, alors il contient $\varphi(p^2) = p(p-1)$ générateurs, et donc $p(p-1)$ élément d'ordre p^2. On en déduit que le nombre d'éléments de G d'ordre p^2 est $p^3 - p^2 + p(p-1) = p^3 - p$. Par conséquent G contient $p-1$ éléments d'ordre p. Mais l'application $\psi : a \mapsto a^p$ est un morphisme de G dans G car G est abélien, et envoie les éléments d'ordre p^2 sur les éléments d'ordre p. Ainsi un élément d'ordre p doit avoir $\frac{p^3-p}{p-1} = p(p+1)$ antécédents par ψ. Mais tous les éléments de l'image de ψ ont le même nombre d'antécédents, qui est égal au cardinal du noyau de ψ, qui ici est p. d'où une contradiction.
On en déduit qu'il existe $y \in G$ tel que $y \notin H$ d'ordre p.

(d) Une fois encore on conclut en utilisant la question (1), d'où $G \simeq H \times \langle y \rangle \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

(3) Soit G un groupe d'ordre 8. Si G est abélien, alors (d'après Exercice 3) il est isomorphe à l'un des groupes $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^3$. Si G n'est pas abélien, alors G est isomorphe à l'un des groupes G_1 ou G_2.