Algèbre 2

Partiel du 10/11/2015

Calculatrices et documents non autorisés. Durée 2h

Exercice 1. (a) Déterminer tous les sous-groupes du groupe $\mathbb{U}_{42}$.

(b) Déterminer les générateurs du sous-groupe d'ordre 7 de $\mathbb{U}_{42}$.

(c) Résoudre dans $\mathbb{U}_{42}$ l'équation $x^7 = 1$.

Solution. Le groupe $\mathbb{U}_{42}$ est cyclique d''ordre 42 engendré par $\xi = e^{2i\pi/42} = e^{i\pi/21}$.
(a) Les sous-groupes de $\mathbb{U}_{42}$ sont donc en correspondance avec les diviseurs d de son ordre : 1, 2, 3, 6, 7, 12, 14, 21, 42. On note H_d le sous-groupe d'ordre d.

- $H_1 = \{1\}$.
- $H_2 = \langle \xi^{42/2} \rangle = \langle \xi^{21} \rangle = \langle e^{i\pi} \rangle = \{-1, 1\}$
- $H_3 = \langle \xi^{42/3} \rangle = \langle \xi^{14} \rangle = \langle e^{2i\pi/3} \rangle = \{1, j, j^2\}$.
- $H_6 = \langle \xi^{42/6} \rangle = \langle \xi^{7} \rangle = \langle e^{i\pi/3} \rangle$.
- $H_7 = \langle \xi^{42/7} \rangle = \langle \xi^{6} \rangle = \langle e^{2i\pi/7} \rangle$.
- $H_{12} = \langle \xi^{42/12} \rangle = \langle \xi^{7/3} \rangle = \langle e^{i\pi/6} \rangle$
- $H_{14} = \langle \xi^{42/14} \rangle = \langle \xi^{3} \rangle = \langle e^{i\pi/7} \rangle$
- $H_{42} = \mathbb{U}_{42}$.

(b) H_7 est un sous-groupe cyclique d'ordre 7 engendré par $a = e^{2i\pi/7}$. Il admet $\varphi(7) = 6$ générateurs qui sont $a, a^2, a^3, a^4, a^5, a^6$.

(c) L'ensemble $\{x \in \mathbb{U}_{42};\ x^7 = 1\}$ n'est autre que le sous-groupe H_6 de $\mathbb{U}_{42}$ d'ordre 6.

Exercice 2. Soit G un groupe d'ordre 21 qui agit sur un ensemble à 20 éléments. On suppose que G ne fixe aucun élément de E. Combien y a-t il d'orbites pour cette action?

Solution. Si $\mathcal{O}$ est une orbite de l'action de G sur E, alors $\mathbf{card}(\mathcal{O})$ divise $|G| = 21$. Donc $\mathbf{card}(\mathcal{O}) \in \{1, 3, 7, 21\}$. Comme G ne fixe aucun élément de E, $\mathbf{card}(\mathcal{O}) \neq 1$. Les orbites étant une partiction de E, donc $\mathbf{card}(\mathcal{O}) \neq 21$ (car $21 > 20$). Soit n le nombre d'orbites de cardinal 3 et m le nombre d'orbites de cardinal 7. On a alors (équation des classes) $3n + 7m = 20$. Modulo 3 cette équation est réduite à $m \equiv 2[3]$ et modulo 7 elle est réduite à $n \equiv 2[7]$. Donc les seuls valeurs possibles sont $n = 2$ et $m = 2$. Il y donc deux orbites à 3 éléments et deux orbites à 7 éléments.

Exercice 3. Soient H et N deux groupes, $\varphi, \psi : H \to Aut(N)$ deux morphismes de groupes.

(a) Rappeler la définition du produit semi-direct $N \rtimes_\varphi H$.

On se propose de trouver des conditions suffisantes pour que les groupes $N \rtimes_\varphi H$ et $N \rtimes_\psi H$ soient isomorphes.

(b) On suppose qu'il existe $\alpha \in Aut(H)$ tel que $\psi = \varphi \circ \alpha$. Montrer que $N \rtimes_\varphi H \simeq N \rtimes_\psi H$ (*penser à* $(n,h) \mapsto (n, \alpha(h))$).

(c) On suppose qu'il existe $u \in Aut(N)$ tel que

$$\forall h \in H, \quad \varphi(h) = u \circ \psi(h) \circ u^{-1}$$

Montrer que $N \rtimes_\varphi H \simeq N \rtimes_\psi H$ (*penser à* $(n,h) \mapsto (u(n), h)$).

Solution. (a) La loi du produit semi-direct $N \rtimes_\varphi H$ est donnée par

$$(n,h)(n',h') = (n\varphi(h)(n'), hh'), \ \ \forall (n,h),(n,h') \in N \rtimes_\varphi H$$

(b) Considérons l'application

$$\begin{array}{rccc} f: & N \rtimes_\psi H & \to & N \rtimes_\varphi H \\ & (n,h) & \mapsto & (n, \alpha(h)) \end{array}$$

et montrons qu'il s'agit d'un ismomorphisme de groupes.

Soient $(n,h),(n,h') \in N \rtimes_\psi H$. On a d'une part

$$f((n,h)(n',h')) = f(n\psi(h)(n'), hh') = (n\psi(h)(n'), \alpha(hh')).$$

D'autre part

$$\begin{aligned} f(n,h)f(n',h') &= (n,\alpha(h))(n',\alpha(h')) \\ &= (n\varphi(\alpha(h))(n'), \alpha(h)\alpha(h')) \\ &= (n(\varphi\circ\alpha)(h)(n'), \alpha(hh')), \text{ car } \alpha \in Aut(H) \\ &= (n\psi(h)(n'), \alpha(hh')), \text{ car } \psi = \varphi \circ \alpha \end{aligned}$$

Ainsi $f((n,h)(n',h')) = f(n,h)f(n',h')$ et f est un morphisme de groupes. On vérifie facilement que f est bijective, de bijection réciproque l'application

$$\begin{array}{ccc} N \rtimes_\varphi H & \to & N \rtimes_\psi H \\ (n,h) & \mapsto & (n, \alpha^{-1}(h)) \end{array}$$

(c) Considérons l'application

$$\begin{array}{rccc} f: & N \rtimes_\psi H & \to & N \rtimes_\varphi H \\ & (n,h) & \mapsto & (u(n), h). \end{array}$$

et montrons qu'il s'agit d'un ismomorphisme de groupes.

Soient $(n,h),(n,h') \in N \rtimes_\psi H$. On a d'une part

$$f((n,h)(n',h')) = f(n\psi(h)(n'), hh') = (u(n\psi(h)(n')), hh').$$

D'autre part

$$\begin{aligned}
f(n,h)f(n',h') &= (u(n),h)(u(n'),h') \\
&= (u(n)\varphi(h)(u(n')),hh') \\
&= (u(n)(\varphi(h)\circ u)(n'),hh') \\
&= (u(n)(u\circ\psi(h))(n'),hh'),\ \text{car } \varphi(h)=u\circ\psi(h)\circ u^{-1} \\
&= (u(n\psi(h)(n')),hh'),\ \text{car } u\in Aut(N)
\end{aligned}$$

Ainsi $f((n,h)(n',h')) = f(n,h)f(n',h')$ et f est un morphisme de groupes. On vérifie facilement que f est bijective, de bijection réciproque l'application

$$\begin{array}{ccc}
N\rtimes_\varphi H & \to & N\rtimes_\psi H \\
(n,h) & \mapsto & (u^{-1}(n),h).
\end{array}$$

Exercice 4. Soit G un groupe abélien d'élément neutre 0. Soit H un sous-groupe de G. On dit que H est *dense* dans G si, pour tout sous-groupe **non nul** K de G, on a $H\cap K\neq\{0\}$.

(a) Déterminer tous les sous-groupes denses dans $\mathbb{Z}$.

(b) Soit H un sous-groupe dense dans G. Montrer que :

(i) Tout élément d'ordre un nombre premier de G appartient H.

(ii) Pour tout $x\in G$, il existe un entier $n\in\mathbb{N}^*$ tel que $nx\in H$.

(c) Réciproquement, montrer que, si H est un sous-groupe de G vérifiant les conditions (i) et (ii) ci-dessus, alors H est dense dans G.

(d) On note $\pi(G)$ l'ensemble des éléments d'ordre premier de G et $d(G)$ le sous-groupe de G engendré par $\pi(G)$. Montrer que, si G est fini, alors $d(G)$ est dense dans G.

(e) Déterminer $d(G)$ pour $G=\mathbb{Z}/8\mathbb{Z}$ et $G=\mathbb{Z}/15\mathbb{Z}$.

Solution. Si H est un sous-groupe desne dans G avec $G\neq\{0\}$, alors $H=H\cap G\neq\{0\}$.

(a) Les seuls sous-groupes de $\mathbb{Z}$ sont ceux de la forme $n\mathbb{Z}$ avec $n\in\mathbb{N}$. Soit H un sous-groupe non nul dense de $\mathbb{Z}$, alors $H=n\mathbb{Z}$ avec $n\in\mathbb{N}^*$.

(b) Soit H un sous-groupe dense de G.

(i) Soit $x\in G$ d'ordre p, un nombre premier. Alors $K=\langle x\rangle$ est un sous-groupe d'ordre p et $H\cap K$ est un sous-groupe non nul de K.. L'ordre de $H\cap K$ divise l'ordre de K et n'est pas égal à 1, c'est donc p et $K\cap H=K$. Donc $x\in K\cap H\subset H$.

(ii) Soit $x\in G$ et posons $K=\langle x\rangle=\{ma;\ m\in\mathbb{Z}\}=\{0,nx,-nx;\ n\in\mathbb{N}^*\}$. Par hypothèse $\{0\}\subsetneq H\cap K$. Donc il existe $n\in\mathbb{N}^*$ tel que $nx\in K\cap H\subset H$ ou $-nx\in K\cap H\subset H$. Comme H est stable par passage à l'opposé, il contient nx.

(c) Soit H un sous-groupe de G vérifiant (i) et (ii).

Soit K un sous-groupe de G, $K\neq\{0\}$. On choisit $x\in K$, $x\neq 0$. D'après (ii), il existe $n\in\mathbb{N}^*$ tels que $nx\in H$, donc $nx\in H\cap K$.

- 1er cas : $nx\neq 0$, alors $H\cap K\neq\{0\}$.

- 2eme cas : $nx = 0$, alors x est d'ordre fini $q \geq 2$. Si p est un diviseur premier de q on peut écrire $q = pr$. Le plus petit entier $m \geq 1$ tel que $mrx = 0$ est p. Donc rx est d'ordre p. D'après (i) on a $rx \in H$, donc $0 \neq rx \in H \cap K$ et $H \cap K \neq \{0\}$.

Par conséquent H est dense dans G.

(d) Par définition $d(G)$ vérifie (i). Si $x \in G$, il est d'ordre fini divisant l'ordre de G, donc il existe $n \in \mathbb{N}^*$ tel que $nx = 0 \in d(G)$. Ainsi (ii) est aussi vérifiée et $d(G)$ est dense dans G.

(e) Dans $\mathbb{Z}/8\mathbb{Z}$, $\bar{0}$ est d'ordre 1, $\bar{1}, \bar{3}, \bar{5}$ et $\bar{7}$ sont d'ordre 8, $\bar{2}$ et $\bar{6}$ sont d'ordre 4 et seul $\bar{4}$ est d'ordre 2 (premier). Donc $d(\mathbb{Z}/8\mathbb{Z}) = \langle \bar{4} \rangle = \{\bar{0}, \bar{4}\} = 4\mathbb{Z}/8\mathbb{Z}$.

Dans $\mathbb{Z}/8\mathbb{Z}$, $\bar{3}$ est d'ordre 5 et $\bar{5}$ est d'ordre 3. Donc $d(\mathbb{Z}/15\mathbb{Z})$ contient un élément d'ordre 3 et un élément d'ordre 5; son ordre est donc multiple de 15. Comme c'est un sous-groupe de $\mathbb{Z}/15\mathbb{Z}$ qui est d'ordre 15, il lui est égal, $d(\mathbb{Z}/15\mathbb{Z}) = \mathbb{Z}/15\mathbb{Z}$.