Examen (seconde session) - *Algèbre 2*

20 Juin 2017 - durée de l'épreuve : 3h

Le sujet est constitué de 4 exercices indépendants. Vous pouvez les traiter dans l'ordre que vous choisirez. Les documents et les calculatrices sont interdits.

Exercice 1.

Soient G un groupe, H un sous-groupe distingué de G et K un sous-groupe de G.

(1) Montrer que $HK = KH$ et que KH est un sous-groupe de G.

(2) Montrer que H est un sous-groupe distingué de KH et que $K \cap H$ est un sous-groupe distingué dans K.

(3) On considère l'application $f : K \to KH/H$ qui à tout élément $k \in K$ associe $f(k) = \bar{k}$, où $\bar{k} = kH$ est la classe de k modulo le sous-groupe H.

(a) Montrer que f est un morphisme de groupe surjectif.

(b) Montrer que $\mathrm{Ker}(f) = K \cap H$.

(c) En déduire que les groupes KH/H et $K/(K \cap H)$ sont isomorphes.

Corrigé. *(1) Soit $a = hk \in HK$, alors $a = k(k^{-1}hk) \in KH$, car $k^{-1}hk \in H$, puisque H est distingué dans G. D'où $HK \subset KH$. L' inclusion $KH \subset HK$ se montre de la même façon.*
Montrons que KH est un sous-groupe de G.
– Soient $a_1 = k_1h_1 \in KH$ et $a_2 = k_2h_2 \in KH$ avec $k_i \in K$ et $h_i \in H$ pour $i = 1, 2$. Comme $h_1k_2 \in HK = KH$, il existe $h_3 \in H$ et $k_3 \in K$ tels que $h_1k_2 = k_3h_3$. Donc

$$a_1a_2 = (k_1h_1)(k_2h_2) = k_1(h_1k_2)h_2 = k_1(k_3h_3)h_2 = (k_1k_3)(h_3h_2) \in KH$$

Ainsi KH est stable par le produit.
– Soit $a = kh \in KH$ avec $k \in K$ et $h \in H$. On a

$$a^{-1} = (kh)^{-1} = h^{-1}k^{-1} = k^{-1}(kh^{-1}k^{-1}) \in KH$$

car $kh^{-1}k^{-1} \in H$, puisque H est distingué dans G. Ainsi KH est stable par passage à l'inverse.

(2) H est un sous-groupe de KH et H distingué dans G, donc H est distingué dans KH.

$K \cap H$ est un sous-groupe de H et H distingué dans G, donc $K \cap H$ est distingué dans G. Comme $K \cap H$ est un sous-groupe de K, il est distingué dans K.

(3) (a) Soient $k_1, k_2 \in K$. On a

$$f(k_1k_2) = (k_1k_2)H = (k_1H)(k_2H) = f(k_1)f(k_2)$$

donc f est un morphisme de groupes. De plus si $x \in KH/H$, alors il existe $a = kh \in KH$ tel que $x = aH = (kh)H = k(hH) = kH = f(k)$. D'où la surgectivité de f.

(b) Soit $k \in K$, On a

$$k \in \mathrm{Ker}(f) \iff f(k) = H \iff kH = H \iff k \in H$$

donc $k \in K \cap H$ et $\mathrm{Ker}(f) \subset K \cap H$. L'autre inclusion est évidente.

(c) D'après le théorème d'isomorphisme, $K/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)$, donc $K/(K \cap H) \simeq KH/H$

Exercice 2.

Un groupe G est dit *métacyclique* s'il existe un sous-groupe H de G cyclique, distingué dans G et tel que G/H est un groupe cyclique.

(1) Soit $G = \langle a \rangle$ un groupe cyclique (engendré par a) d'ordre n et H un sous-groupe de G.

(a) Dire pourquoi H est distingué dans G.
(b) Montrer que H est cyclique.
(c) Montrer que G/H est cyclique.
(d) Conclure.

(2) On considère dans cette question le groupe de permutations $\mathcal{S}_3$.
(a) Dire pourquoi $\mathcal{S}_3$ n'est pas cyclique.
(b) Montrer que $\mathcal{S}_3$ est métacyclique (ind. on prend $H = \langle\sigma\rangle$, où σ est un 3-cycle de $\mathcal{S}_3$).

(3) Soit G un groupe métacyclique, c-à-d. il existe un sous-groupe H de G cyclique, distingué dans G et tel que G/H est un groupe cyclique. Soit K un sous-groupe de G.
(a) Montrer que $K \cap H$ est un sous-groupe cyclique et distingué de K.
(b) Montrer que $K/(K \cap H)$ est un groupe cyclique (Ind. on peut utiliser (3) (c) Exercice 1).
(c) Conclure.

Corrigé. *(1) (a) $G = \langle a\rangle$ est cyclique, donc abélien. Par conséquent tout sous-groupe de G est distingué.*

(b) H est un sous-groupe de G donc son ordre divise n, l'ordre de G. Notons $d = |H|$ cet ordre. Comme $\langle a^{\frac{n}{d}}\rangle$ est un sous-groupe cyclique de G d'ordre d, donc par unicité (des sous-groupes d'ordre d), $H = \langle a^{\frac{n}{d}}\rangle$ et H est cyclique.

(c) Il suffit de voir que $G/H = \langle\bar{a}\rangle$ où $\bar{a} = aH$. En effet, $\langle\bar{a}\rangle \subset G/H$. Inversement, soit $\bar{x} = xH \in G/H$. Comme $x \in G$ et $G = \langle a\rangle$, il existe $m \in \mathbb{Z}$ tel que $x = a^m$, d'où $\bar{x} = \overline{a^m} = \bar{a}^m \in \langle\bar{a}\rangle$, donc $G/H \subset \langle\bar{a}\rangle$.

(d) Tout groupe cyclique est métacyclique.

(2) (a) Puisque $\mathcal{S}_3$ n'est pas abélien, il n'est pas cyclique.

(b) Soit σ un 3-cycle de $\mathcal{S}_3$ et $H = \langle\sigma\rangle$, il est donc d'ordre 3. Le sous-groupe H est distingué dans $\mathcal{S}_3$, car il est d'indice $[\mathcal{S}_3 : H] = \frac{6}{3} = 2$. Comme le groupe quotient $\mathcal{S}_3/H$ est d'ordre 2, il est cyclique. Ainsi $\mathcal{S}_3$ est métacyclique. (3)(a) $K \cap H$ est un sous-groupe de K. montrons qu'il est distingué dans K. Soit $k \in K$ et soit $x \in K \cap H$. On a $kxk^{-1} \in H$, car H est distingué dans G. et on a aussi $kxk^{-1} \in K$, car $x \in K$, d'où $kxk^{-1} \in K \cap H$.

D'autre part, puisque H est cyclique et que $K \cap H$ est un sous-groupe de K, alors $K \cap H$ est cyclique (d'après (1)(b)).

(b) D'après (3)(c) Exercice 1, le groupe $K/K \cap H$ est isomorphe au groupe KH/H. Comme KH/H est un sous-groupe de G/H et que G/H est cyclique, alors KH/H est cyclique. Par isomorphisme $K/K \cap H$ est cyclique.

(c) K est métacyclique : tout sous-groupe d'un groupe métacyclique est métacyclique.

Exercice 3.
Déterminer, à isomorphisme près, tous les groupes abéliens d'ordre 360.
Corrigé. *Soit G un groupe abélien d'ordre $360 = 2^3 \times 3^2 \times 5$. On a*

$$\begin{aligned} 8 &= 2^3 = 2^2 \times 2 = 2 \times 2 \times 2 \\ 9 &= 3^2 = 3 \times 3 \\ 5 &= 5, \end{aligned}$$

puis la liste des invariants

$$\begin{aligned} 360 &= (2^3) \times (3^2) \times (5) = 2^3 \times 3^2 \times 5 = 360 \to \boxed{360} \\ 360 &= (2^2 \times 2) \times (3^2) \times (5) = (2^2 \times 3^2 \times 5) \times (2) = 180 \times 2 \to \boxed{(2, 180)} \\ 360 &= (2 \times 2 \times 2) \times (3^2) \times (5) = (2 \times 3^2 \times 5) \times (2) \times (2) = 90 \times 2 \times 2 \to \boxed{(2, 2, 90)} \\ 360 &= (2^3) \times (3 \times 3) \times (5) = (2^3 \times 3 \times 5) \times (3) = 120 \times 3 \to \boxed{(3, 120)} \\ 360 &= (2^2 \times 2) \times (3 \times 3) \times (5) = (2^2 \times 3 \times 5) \times (2 \times 3) = 60 \times 6 \to \boxed{(6, 60)} \\ 360 &= (2 \times 2 \times 2) \times (3 \times 3) \times (5) = (2 \times 3 \times 5) \times (2 \times 3) \times (2) = 30 \times 6 \times 2 \to \boxed{(2, 6, 30)} \end{aligned}$$

D'où la liste des invariants

$$(360), (2, 180), (2, 2, 90), (3, 120), (6, 60), (2, 6, 30).$$

Donc à isomorphisme près, les groupes abéliens d'ordre 360 sont

$$\begin{array}{l} \mathbb{Z}/360\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z} \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z} \\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}. \end{array}$$

Exercice 4.

Soit G un groupe d'ordre 35 opérant sur un ensemble E de cardinal 19. On suppose que G ne fixe aucun élément de E. Combien y a-t-il d'ordres pour cette action?

Corrigé. *On suppose* $|G| = 35$ *et* $\mathbf{card}(E) = 19$. *Une orbite quelconque* $\mathcal{O}$ *a pour cardinal 1 ou 5 ou 7 ou 35. Une telle orbite ne peut avoir 35 comme cardinal (car* $35 > 19$*) et ne peut pas avoir un seul point (car* G *ne fixe aucun élément de* E*). Soit et* a *le nombre d'orbites à 5 d'éléments et* b *le nombre d'orbites à 7 d'éléments. Alors (équation des classes)* $5a + 7b = 19$. *La seule possibilité est* $b = 2$ *et* $a = 1$. *Il y a donc une seule orbite à 5 éléments et 2 orbites à 7 éléments.*

Exercice 5.

On considère l'ensemble $\mathbb{Z}[\sqrt{-7}] = \{a + ib\sqrt{7};\ \ a, b \in \mathbb{Z}\}$.

(1) Montrer que $\mathbb{Z}[\sqrt{-7}]$ est un sous-anneau de $\mathbb{C}$.

On note $(\mathbb{Z}[\sqrt{-7}])^*$ le groupe des éléments inversibles de $\mathbb{Z}[\sqrt{-7}]$.

(2) On pose pour tout $z \in \mathbb{Z}[\sqrt{-7}]$, $\theta(z) = z\bar{z} = |z|^2$.

Montrer que $(\mathbb{Z}[\sqrt{-7}])^* = \{z \in \mathbb{Z}[\sqrt{-7}];\ \theta(x) = 1\}$, déterminer alors $(\mathbb{Z}[\sqrt{-7}])^*$.

(3) Montrer que 2, $1 + i\sqrt{7}$ et $1 - i\sqrt{7}$ sont irréductibles dans $\mathbb{Z}[\sqrt{-7}]$.

(4) Montrer que 2 n'est associé ni à $1 + i\sqrt{7}$ ni à $1 - i\sqrt{7}$ dans l'anneau $\mathbb{Z}[\sqrt{-7}]$.

(5) Montrer que 8 admet dans $\mathbb{Z}[\sqrt{-7}]$ deux décompositions en facteurs irréductibles. En déduire que l'anneau $\mathbb{Z}[\sqrt{-7}]$ n'est pas factoriel.

Corrigé. *(1) Il est facile de montrer que* $\mathbb{Z}[\sqrt{-7}]$ *est un sous-anneau de* $\mathbb{C}$.

(2) Soit $z \in (\mathbb{Z}[\sqrt{-7}])^\star$, *alors il existe* $w \in \mathbb{Z}[\sqrt{-7}]$ *tel que* $zw = 1$. *Donc* $\theta(z)\theta(w) = \theta(zw) = 1$. *De cette égalité entre entiers naturels on déduit que* $\theta(z) = 1$. *Réciproquement, soit* $z \in \mathbb{Z}[\sqrt{-7}]$ *tel que* $\theta(z) = 1$ *c'est-à-dire* $z\bar{z} = 1$. *Puisque l'anneau est stable par la conjugaison complexe,* $\bar{z} \in \mathbb{Z}[\sqrt{-7}]$ *et donc* z *est inversible d'inverse* $\bar{z}$.

Soit $z = a + ib\sqrt{7} \in \mathbb{Z}[\sqrt{-7}]$. *Alors*

$$z \in (\mathbb{Z}[\sqrt{-7}])^\star \iff a^2 + 7b^2 = 1 \iff b = 0, a = \pm 1$$

On en déduit que $(\mathbb{Z}[\sqrt{-7}])^\star = \{\pm 1\}$.

(3) $2 \notin (\mathbb{Z}[\sqrt{-7}])^\star$. *De plus, si* $2 = zw$ *avec* $z, w \in \mathbb{Z}[\sqrt{-7}]$, *alors nécessairement* $4 = \theta(z)\theta(w)$ *(avec* $\theta(z), \theta(w) \in \mathbb{N}$*). Or si* $\theta(z) = \theta(w) = 2$, *alors on aurait* $a^2 + 7b^2 = 2$ *(si par exemple* $z = a + ib\sqrt{7}$*). Mais dans cette égalité, nécessairement* $b = 0$ *(car sinon* $a^2 + 7b^2 \geq 7$*), donc* $a^2 = 2$ *ce qui est impossible dans* $\mathbb{Z}$. *On en déduit que* $\theta(z) = 1$ *et* $\theta(w) = 4$ *ou inversement. Ce qui veut dire* $z \in (\mathbb{Z}[\sqrt{-7}])^\star$ *ou* $w \in (\mathbb{Z}[\sqrt{-7}])^\star$. *Par conséquent 2 est irréductible dans* $\mathbb{Z}[\sqrt{-7}]$.

On montre de même que $1 \pm i\sqrt{7}$ *sont irréductibles dans* $\mathbb{Z}[\sqrt{-7}]$.

(4) Les éléments inversibles étant ± 1, *l'élément 2 n'est associé ni à* $1 + i\sqrt{7}$ *ni à* $1 - i\sqrt{7}$.

(5) On a $8 = 2^3$ *et* $8 = (1 + i\sqrt{7})(1 - i\sqrt{7})$. *Donc dans* $\mathbb{Z}[\sqrt{-7}]$ *l'élément 8 admet deux décompositions en produit de facteurs irréductibles et 2 n'est associé ni à* $1 + i\sqrt{7}$ *ni à* $1 - i\sqrt{7}$. *Donc l'anneau* $\mathbb{Z}[\sqrt{-7}]$ *n'est pas factoriel.*

Barême indicatif : Exercice 1 (**7pt**), Exercice 2 (**7pt**), Exercice 3 (**4pt**), Exercice 4 (**7pt**).