Contôle (Algèbre 6)

Il sera tenu compte, dans l'appréciation des copies, de la précision des raisonnements ainsi que la clarté de la rédaction.

LPEM

Corrigé :

بِسمِ اللّٰهِ الرَّحمٰنِ الرَّحِيمِ

وَ عـلَى اللَّـهِ فَليَتَوَكَّلِ المُتَوَكِّلـون

صـدق الله العظِيـم

Questions de Cours

Cours

Exercice 1

Soit G un groupe abélien d'ordre 35.

1. Les deux entiers 5 et 7 sont des diviseurs premiers de l'ordre de G, d'après le théorème de Cauchy, G admet un élément a d'ordre 7 et un élément b d'ordre 5.
On pose $H = \langle a \rangle$ et $K = \langle b \rangle$

2. H est un sous groupe engendré par un élément d'ordre 7 donc H est un sous groupe d'ordre 7. De même K est un sous groupe d'ordre 5.
Soit $f : K \times H \to G$ l'application définie par $f(x, y) = xy$

3. Soient $(x, y), (x', y') \in K \times H$. On a

$$f((x, y)(x', y')) = f(xx', yy') = xx'yy'$$

Or G est commutatif, on a donc $xx'yy' = xyx'y' = f(x, y)f(x', y')$. Autrement dit

$$f((x, y)(x', y')) = f(x, y)f(x', y')$$

L'application f est bien un morphisme de groupes.

4. Soit $(x, y) \in \ker f$. On a $f(x, y) = xy = e$, donc $x = y^{-1}$. On a $x \in K$ et K sous groupe d'ordre 5 donc $x^5 = e$. Par suite $e = x^5 = (y^5)^{-1}$, d'où $y^5 = e$.

5. Soit $(x, y) \in \ker f$. D'après le résultat de la question précédente, on a $y^5 = e$. D'autre part, d'après le théorème de Lagrange, $y^7 = e$. Puisque $5 \wedge 7 = 1$, le théorème de Bézout affirme qu'ils existent $u, v \in \mathbb{Z}$ tels que $1 = 5u + 7v$. Ainsi $y = y^{5u+7v} = (y^5)^u(y^7)^v = ee = e$. Par conséquent $x = y^{-1} = e$. D'où $(x, y) = (e, e)$. On en déduit que f est injectif.

6. Le morphisme $f : K \times H \to G$ est injectif et $|K \times H| = |H||K| = 35 = |G|$, donc f est bijectif. Par conséquent les deux groupes $K \times H$ et G sont isomorphes.

Exercice 2

Soit a un élément non nul de A. L'application $h : A \to A$ définie par $h(x) = ax$ est injectif, en effet si $h(x) = h(y)$ alors $ax = ay$ ou encore $a(x-y) = 0$, or a est non nul et A intègre, on a donc $x = y$. L'application h est injective et A finie donc h est bijective, en particulier surjective. il existe alors $b \in A$ tel que $h(b) = 1$ ou encore $ab = 1$. Ainsi a est inversible.

Remarque : On peut considérer l'application $f : \mathbb{N} \to A$ définie par $f(n) = a^n$. Puisque $\mathbb{N}$ est infini, cette application ne peut être injective. Donc il existe $n \neq m$ tel que $f(n) = f(m)$ autrement dit $a^n = a^m$. Si par exemple $n > m$, on obtient $a^m(1 - a^{n-m}) = 0$, de l'intégrité de A et le fait que $a \neq 0$, il vient que $1 - a^{n-m} = 0$ ou encore $1 = a^{n-m} = aa^{n-m-1}$ (notons que $n - m - 1 \geq 0$). Donc a est inversible.

PROBLÈME

Caractère d'un groupe

Soit G un groupe. Un caractère de G est un morphisme de groupes $G \to \mathbb{C}^*$ (le groupe $\mathbb{C}^*$ muni de la multiplication).

Première partie : Questions préliminaires

Soit $n \in \mathbb{N}^*$. On désigne par $\mathbb{U}_n$ l'ensemble des racines $n$ème de l'unité c'est-à-dire $\mathbb{U}_n = \{z \in \mathbb{C} \ / \ z^n = 1\}$. On pose $\omega = e^{\frac{2i\pi}{n}}$.

1. Il suffit de montrer que $\mathbb{U}_n$ est un sous groupe de $\mathbb{C}^*$. Clairement $1 \in \mathbb{U}_n$. Si $z, z' \in U_n$ alors $(zz'^{-1}) = z^n(z'^n)^{-1} = 1$. Donc $zz'^{-1} \in \mathbb{U}_n$.

2. On a $\omega \neq 1$, donc $\displaystyle\sum_{k=0}^{n-1} \omega^k = \frac{1-\omega^n}{1-\omega} = 0$ car $\omega^n = 1$.

3. Chaque élément de $\mathbb{U}_n$ est de la forme $e^{\frac{2ik\pi}{n}} = \omega^k$ où $k \in \mathbb{Z}$, donc $\mathbb{U}_n = \{\omega^k \ / \ k \in \mathbb{Z}\} = \langle\omega\rangle$. De plus $\omega^n = 1$, donc $\mathbb{U}_n$ est un groupe monogène fini, par conséquent cyclique.
Soit $f : \mathbb{Z} \to \mathbb{U}_n$ l'application définie par $f(k) = \omega^k$.

4. Pour $k, l \in \mathbb{Z}$, on a
$$f(k+l) = \omega^{k+l} = \omega^k\omega^l = f(k)f(l)$$
Donc f est un morphisme de groupes.

5. Chaque élément de $\mathbb{U}_n$ est de la forme $\omega^k = f(k)$, donc f est surjective. D'après le théorème d'isomorphisme $\mathbb{Z}/\ker f$ est isomorphe à $\mathbb{U}_n$. Il suffit maintenant de démontrer que $\ker f = n\mathbb{Z}$. Si $d \in n\mathbb{Z}$ alors $d = nl$ avec $l \in \mathbb{Z}$, et donc $f(d) = \omega^{nl} = (\omega^n)^l = 1$, par suite $n\mathbb{Z} \subseteq \ker f$. Réciproquement, soit $d \in \ker f$, en effectuant la division euclidienne de d par n, ils existe $(l, r) \in \mathbb{Z} \times \mathbb{N}$ tels que $d = nl + r$ et $0 \leq r < n$. On a $1 = \omega^d = \omega^{nl}\omega^r$, donc $\omega^r = 1$ avec $0 \leq r < n$. Donc $r = 0$ ou encore $d = nl \in n\mathbb{Z}$.

Deuxième partie : Caractère d'un groupe abélien fini

Dans cette partie G est un groupe abélien fini d'ordre $n \geq 2$ et $g : G \to \mathbb{C}^*$ un caractère de G.

6. Par récurrence sur k : Pour $k = 0$, on a $g(x^0) = g(e) = 1 = (g(x))^0$.
Soit $k \in \mathbb{N}$, et supposons que $g(x^k) = g(x)^k$. On a $g(x^{k+1}) = g(x^k x) = g(x^k)g(x) = (g(x))^k g(x) = (g(x))^{k+1}$.

7. On a $(g(x))^n = g(x^n)$, d'après le théorème le Lagrange, $x^n = e$, d'où $(g(x))^n = g(e) = 1$, par conséquent $g(x) \in \mathbb{U}_n$.

8. On a $|g(x)|^n = |g(x)^n| = 1$, donc $|g(x)| = 1$. De plus on a $g(x)g(x^{-1}) = g(xx^{-1}) = g(e) = 1$ et $g(x)\overline{g(x)} = |g(x)|^2 = 1$, donc $g(x)g(x^{-1}) = g(x)\overline{g(x)}$, par suite $g(x^{-1}) = \overline{g(x)}$, en effet $g(x) \in \mathbb{C}^*$ donc il est non nul.
On suppose dans la suite de cette partie qu'il existe $x_0 \in G$ tel que $g(x_0) \neq 1$.

9. Clairement $\{x_0x \ / \ x \in G\} \subseteq G$, et si $y \in G$ alors $y = x_0(x_0^{-1}x)$, donc $G = \{x_0x \ / x \in G\}$.

10. Notons d'abord que si $x \neq x'$ alors $x_0x \neq x_0x'$ donc les éléments x_0x avec $x \in G$ sont deux à deux distincts. On a donc

$$\sum_{x\in G} g(x) = \sum_{x\in G} g(x_0x) = \sum_{x\in G} g(x_0)g(x) = g(x_0)\left(\sum_{x\in G} g(x)\right)$$

11. D'après le résultat de la question précédente, on a $(g(x_0)-1)\left(\sum_{x\in G} g(x)\right) = 0$, or $g(x_0) \neq 1$, on a donc $\sum_{x\in G} g(x) = 0$.

Troisième partie : Groupe dual

On note $\widehat{G}$ l'ensemble de tout les caractères de G. Pour $g, g' \in \hat{G}$, on note gg' l'application de $G \to \mathbb{C}^*$ définie, pour tout $x \in G$, par $(gg')(x) = g(x)g'(x)$.

12. Soit $x, y \in G$, on a

$$(gg')(xy) = g(xy)g'(xy) = g(x)g(y)g'(x)g'(y) = g(x)g'(x)g(y)g'(y) = (gg')(x)(gg')(y)$$

Donc gg' est un morphisme de groupes, autrement dit $gg' \in \widehat{G}$.

13. D'après le résultat de la question précédente, la multiplication est une loi interne sur $\widehat{G}$. L'associativité est immédiate (c'est une conséquence de l'associativité de la multiplication dans $\mathbb{C}^*$). L'application constante égale à 1 est un élément de $\widehat{G}$ c'est-à-dire un morphisme de groupes (c'est le neutre de $\widehat{G}$). Soit $g \in \widehat{G}$ et posons $h = \frac{1}{f}$ (c'est l'inverse de f), on a

$$h(xy) = \frac{1}{f(xy)} = \frac{1}{f(x)f(y)} = \frac{1}{f(x)}\frac{1}{f(y)} = h(x)h(y)$$

autrement dit h est un morphisme de groupes. De plus on a $fh = 1$, ainsi tout élément de $\widehat{G}$ est inversible.
Remarque : Une autre méthode consiste à démontrer que $\widehat{G}$ est un sous groupe du groupe formé par toutes les applications de G à valeurs dans $\mathbb{C}^*$.

14. On considère l'application $\varphi : \widehat{G} \to \mathbb{U}_n$ définie par $\varphi(g) = g(\overline{1})$. Cette application est bien définie car d'après le résultat de la question 7., on a $g(\overline{1}) \in \mathbb{U}_n$. Pour $g, g' \in \widehat{G}$, on a

$$\varphi(gg') = (gg')(\overline{1}) = g(\overline{1})g'(\overline{1}) = \varphi(g)\varphi(g')$$

Donc φ est un morphisme de groupes.
Soit $g \in \ker\varphi$, autrement dit $\varphi(g) = 1$. On a par définition $g(\overline{1}) = 1$. Pour $0 \leq k \leq n-1$, on a

$$g(\overline{k}) = g(k\overline{1}) = (g(\overline{1}))^k = 1$$

Donc g est le neutre de $\widehat{G}$, par conséquent φ est injectif.
Soit $z \in \mathbb{U}_n$ et $g : G = \mathbb{Z}/n\mathbb{Z} \to \mathbb{U}_n$ l'application définie par $g(\overline{k}) = z^k$. L'application g est bien

définie, car si $\overline{k} = \overline{k'}$ alors $k - k' = nd$ où $d \in \mathbb{Z}$ ou encore $k = k' + nd$. Donc $z^k = z^{k'} z^{nd} = z^{k'}$ (notons que $z^n = 1$ puisque $z \in \mathbb{U}_n$). De plus pour $\overline{k}, \overline{l} \in G$, on a

$$g(\overline{k} + \overline{l}) = g(\overline{k+l}) = z^{k+l} = z^k z^l = g(\overline{k})g(\overline{l})$$

g est donc un morphisme de groupe c'est-à-dire élément de $\widehat{G}$. Finalement on a $\varphi(g) = g(\overline{1}) = z$. On en déduit que φ est surjective, donc un isomorphisme. Les deux groupes $\widehat{G}$ et $\mathbb{U}_n$ sont isomorphes. On combine avec le résultat de la question 5, on obtient le résultat voulu.