**Contrôle continu, mercredi 27 septembre, 10h15 - 12h15**

Documents et calculatrices non-autorisés. Les exercices sont indépendants.

Barème indicatif. Exercice 1 : 2 points, exercice 2 : 5 points, exercice 3 : 8 points, exercice 4 : 7 points.

## Exercice 1

Soient $n \in \mathbb{N}^*$ et $k$ dans $\mathbb{Z}$. On note $\overline{k}$ la classe de $k$ dans $\mathbb{Z}/n\mathbb{Z}$. Montrer que $\overline{k}$ est inversible pour la multiplication de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k$ est premier avec $n$.

## Exercice 2

On note $f$ l'application $z \mapsto |z|$ de $\mathbb{C}^*$ dans $\mathbb{R}_+^*$, et $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$.

1. Montrer que $f$ est un morphisme de groupes
2. Montrer que $\mathbb{U}$ est un sous-groupe de $\mathbb{C}^*$.
3. On note $p : \mathbb{C}^* \to \mathbb{C}^*/\mathbb{U}$ la projection canonique. Montrer l'existence et l'unicité d'une application $\overline{f}$ de l'ensemble quotient $\mathbb{C}^*/\mathbb{U}$ vers $\mathbb{R}_+^*$ telle que $f = \overline{f} \circ p$.
4. Montrer qu'on peut définir de façon cohérente une multiplication sur $\mathbb{C}^*/\mathbb{U}$ par $(z_1\mathbb{U})(z_2\mathbb{U}) = z_1 z_2 \mathbb{U}$.
5. Montrer que $\overline{f}$ est alors un isomorphisme de groupes.

## Exercice 3

Soit $G = \{a + b\sqrt{3} : (a, b) \in \mathbb{Z} \times \mathbb{Z}, a^2 - 3b^2 = 1\}$. On note $G_+ = G \cap \mathbb{R}_+^*$ et $g = 2 + \sqrt{3}$.

1. Montrer que $G$ et $G_+$ sont des sous-groupes de $(\mathbb{R}^*, \times)$.
2. Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ tel que $a^2 - 3b^2 = 1$. Montrer que $|a| > \sqrt{3}|b|$. En déduire que $a + b\sqrt{3} > 0$ si et seulement si $a > 0$.
3. Soit $x \in G_+$. D'après la question précédente, $x = a + b\sqrt{3}$ avec $(a, b) \in \mathbb{N}^* \times \mathbb{Z}$ tel que $a^2 - 3b^2 = 1$.
   (a) Si $b = 0$, que vaut $x$ ?
   (b) Montrer que si $b \geq 1$, alors $x \geq g$.
   (c) En déduire que si $b \leq -1$, alors $x \leq g^{-1}$.
4. En utilisant le fait que ln est un isomorphisme de $(\mathbb{R}_+^*, \times)$ vers $(\mathbb{R}, +)$, montrer que $G_+ = \{g^n : n \in \mathbb{Z}\}$ et que $G = \{\varepsilon g^n : \varepsilon \in \{-1, 1\},\ n \in \mathbb{Z}\}$.

## Exercice 4

Soit $G$ un groupe cyclique d'ordre $d$. Soit $a$ un générateur de $G$.

On note $\mathrm{End}(G)$ l'ensemble des endomorphismes du groupe $G$, c'est-à dire des morphismes de groupes de $G$ dans $G$.

On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes du groupe $G$, c'est-à dire des morphismes bijectifs de $G$ dans $G$.

Pour tout $k \in \mathbb{Z}$, on note $\rho_k$ l'application $x \mapsto x^k$ de $G$ dans $G$.

1. Soit $k \in \mathbb{Z}$. Montrer que $\rho_k \in \mathrm{End}(G)$.
2. Montrer que pour tout $k_1$ et $k_2$ dans $\mathbb{Z}$,
$$\rho_{k_1} = \rho_{k_2} \iff \rho_{k_1}(a) = \rho_{k_2}(a) \iff k_1 - k_2 \in d\mathbb{Z}.$$
3. Montrer que si $f \in \mathrm{End}(G)$, il existe $k \in \mathbb{Z}$ tel que $f = \rho_k$.
4. En déduire une bijection de $\mathbb{Z}/d\mathbb{Z}$ vers $\mathrm{End}(G)$.
5. Soit $k \in \mathbb{Z}$. Montrer que si $k$ et $d$ sont premiers entre eux, alors $\rho_k$ est bijectif.
6. En déduire une injection $\phi$ de $(\mathbb{Z}/d\mathbb{Z})^\times$ dans $\mathrm{Aut}(G)$
7. Montrer que $\phi$ est un isomorphisme de groupes.

Un corrigé

Exercice 1 : 2 points

Soit $k \in \mathbb{Z}$. Par définition de la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ et le théorème de Bezout,

$$\begin{aligned}
\overline{k} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z} &\iff \exists \ell \in \mathbb{Z}, \overline{k} \times \overline{\ell} = \overline{1} \\
&\iff \exists \ell \in \mathbb{Z}, \overline{k\ell} = \overline{1} \\
&\iff \exists \ell \in \mathbb{Z}, k\ell \equiv 1 \quad [n] \\
&\iff \exists \ell \in \mathbb{Z},\ \exists m \in \mathbb{Z},\ k\ell + nm = 1 \\
&\iff k \wedge n = 1.
\end{aligned}$$

Exercice 2 : 0,5+0,5+1,5+1+2=5,5 points

1. Pour tous $z_1$ et $z_2$ dans $\mathbb{C}$, $f(z_1 z_2) = |z_1 \times z_2| = |z_1| \times |z_2| = f(z_1) \times f(z_2)$. Comme $(\mathbb{C}^*, \times)$ et $(\mathbb{R}_+^*, \times)$ sont des groupes, $f$ est un morphisme de groupes
2. Par définition, $\mathbb{U} = \mathrm{Ker} f$. Donc $\mathbb{U}$ est un sous-groupe de $\mathbb{C}^*$.
3. Si $\overline{f}$ est une application de $\mathbb{C}^*/\mathbb{U}$ dans $\mathbb{R}_+^*$ telle que $f = \overline{f} \circ p$, l'image par $\overline{f}$ de toute classe $z\mathbb{U} \in \mathbb{C}^*/\mathbb{U}$ est imposée par l'égalité $\overline{f}(z\mathbb{U}) = \overline{f}(p(z)) = f(z)$, ce qui montre l'unicité.

   Pour montrer l'existence, on vérifie que pour tout $z \in \mathbb{C}^*$, $f(z)$ ne dépend que de la classe de $z$ dans $\mathbb{C}^*/\mathbb{U}$. En effet, si $z'$ est un élément de la même classe que $z$ (autrement dit $z' \in z\mathbb{U}$), alors $z^{-1}z' \in \mathbb{U}$, donc $f(z)^{-1} f(z') = f(z^{-1}z') = 1$, d'où $f(z') = f(z)$. Ainsi, l'égalité $\overline{f}(z\mathbb{U}) = f(z)$ définit de façon cohérente une application $\overline{f}$ de $\mathbb{C}^*/\mathbb{U}$ vers $\mathbb{R}_+^*$, et par construction, $f = \overline{f} \circ p$.
4. Soient $z_1, z_2, z_1', z_2'$ dans $\mathbb{C}^*$ tels que $z_1\mathbb{U} = z_1'\mathbb{U}$ et $z_2\mathbb{U} = z_2'\mathbb{U}$. Alors

   $$(z_1 z_2)^{-1}(z_1' z_2') = (z_1^{-1} z_1')(z_2^{-1} z_2') \in \mathbb{U},$$

   donc $(z_1 z_2)\mathbb{U} = (z_1' z_2')\mathbb{U}$. On peut donc définir de façon cohérente une multiplication sur $\mathbb{C}^*/\mathbb{U}$ par $(z_1\mathbb{U})(z_2\mathbb{U}) = (z_1 z_2)\mathbb{U}$.
5. Par construction, la multiplication sur $\mathbb{C}^*/\mathbb{U}$ est interne et $p$ est un morphisme surjectif de $\mathbb{C}^*$ dans $\mathbb{C}^*/\mathbb{U}$. À l'aide de ce morphisme, on vérifie que la multiplication sur $\mathbb{C}^*/\mathbb{U}$ est associative, que $1\mathbb{U}$ est élément neutre et que tout élément $z\mathbb{U} \in \mathbb{C}^*/\mathbb{U}$ a pour inverse $z^{-1}\mathbb{U}$. Ainsi, $\mathbb{C}^*/\mathbb{U}$ est un groupe.
   Pour tous $z_1\mathbb{U}$ et $z_2\mathbb{U}$ dans $\mathbb{C}^*/\mathbb{U}$,

   $$\overline{f}\big((z_1\mathbb{U})(z_2\mathbb{U})\big) = \overline{f}\big((z_1 z_2)\mathbb{U}\big) = f(z_1 z_2) = f(z_1) f(z_2) = \overline{f}(z_1\mathbb{U})\overline{f}(z_2\mathbb{U}),$$

   et

   $$\begin{aligned}
   \overline{f}(z_1\mathbb{U}) = \overline{f}(z_2\mathbb{U}) \iff f(z_1) = f(z_2) \iff 1 = f(z_1^{-1}z_2) &\iff z_1^{-1}z_2 \in \mathbb{U} \\
   &\iff z_1\mathbb{U} = z_2\mathbb{U}.
   \end{aligned}$$

   Donc $\overline{f}$ est un morphisme injectif de groupes. Mais $f$ est surjectif car pour tout $r \in \mathbb{R}_+^*$, $r = f(r) = \overline{f}(r\mathbb{U})$. Ainsi, $\overline{f}$ est un isomorphisme de groupes.

Exercice 3 : 3,5+1+1,5+2=8 points.

1. Comme $1 = 1 + 0\sqrt{3}$, $(1,0) \in \mathbb{Z} \times \mathbb{Z}$ et $1^2 - 3 \times 0^2 = 1$, on a $1 \in G$.
   Soit $x \in G$. Alors on peut écrire $x = a + b\sqrt{3}$ avec $(a,b) \in \mathbb{Z}^2$ tel que $a^2 - 3b^2 = 1$. Comme $-b \in \mathbb{Z}$ et $a^2 - 3(-b)^2 = 1$, le réel $x' = a + (-b)\sqrt{3}$ est aussi dans $G$ et vérifie $xx' = a^2 - 3b^2 = 1$. Donc $x$ est inversible dans $G$ et en particulier $x \neq 0$, ce qui montre l'inclusion $G \subset \mathbb{R}^*$.
   Soit $y \in G$. Alors $y = c + d\sqrt{3}$ avec $(c,d) \in \mathbb{Z}^2$ tel que $c^2 - 3d^2 = 1$. Donc

   $$xy = (a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}$$

   Or $(ac + 3bd, ad + bc) \in \mathbb{Z}^2$ et

   $$\begin{aligned}(ac + 3bd)^2 - 3(ad + bc)^2 &= a^2c^2 + 6abcd + 9b^2d^2 - 3a^2d^2 - 6abcd - 9b^2c^2 \\ &= (a^2 - 3b^2)(c^2 - 3d^2) = 1.\end{aligned}$$

   Donc $xy \in G$.
   Ainsi, $G$ est un sous-groupe de $(\mathbb{R}^*, \times)$, donc $G_+ = G \cap \mathbb{R}_+^*$ aussi, comme intersection de sous-groupes de $(\mathbb{R}^*, \times)$.
2. Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ tel que $a^2 - 3b^2 = 1$. Alors $a^2 = 3b^2 + 1 > 3b^2$, donc $|a| > \sqrt{3}|b|$, donc $a$ et $a + b\sqrt{3}$ sont non nuls et de même signe. En particulier, $a + b\sqrt{3} > 0$ si et seulement si $a > 0$.
3. Soit $x \in G_+$. D'après la question précédente, $x = a + b\sqrt{3}$ avec $(a,b) \in \mathbb{N}^* \times \mathbb{Z}$ tel que $a^2 - 3b^2 = 1$.
   (a) Si $b = 0$, alors $a^2 = 1$, donc $a = 1$ (puisque $a \in \mathbb{N}^*$) donc $x = 1$.
   (b) Montrer que si $b \geq 1$, alors $a^2 = 3b^2 + 1 \geq 4$, donc $a \geq 2$ (puisque $a \in \mathbb{N}^*$). Ainsi, $x \geq 2 + \sqrt{3} = g$.
   (c) Si $b \leq -1$, on peut appliquer ce qui précède à $x^{-1} = a + (-b)\sqrt{3}$. Comme $x^{-1} \geq g > 0$, on a $x \leq g^{-1}$.
4. Comme $\ln G_+$ est un sous-groupe de $(\mathbb{R}_+^*, \times)$ et ln est un isomorphisme de $(\mathbb{R}_+^*, \times)$ vers $(\mathbb{R}, +)$, $\ln G_+$ est un sous-groupe de $(\mathbb{R}, +)$.
   Mais $g \in G_+$, donc d'après la question précédente, $g = \min(G_+ \cap ]1, +\infty[)$, donc $\ln g = \min(\ln G_+ \cap \mathbb{R}_+^*)$. Ainsi, $\ln G_+ = (\ln g)\mathbb{Z}$, donc $G_+ = g^{\mathbb{Z}} = \{g^n : n \in \mathbb{Z}\}$.
   On vérifie que si $x \in G$, alors $-x \in G$ ; mais comme $x \neq 0$, soit $x$ soit $-x$ est dans $G_+$. Ainsi, $G = G_+ \cup (-G_+) = \{\varepsilon g^n : \varepsilon \in \{-1, 1\},\ n \in \mathbb{Z}\}$.

Exercice 4 : 0,5+1,5+1+1,5+1+1+1,5=8 points

1. Soit $k \in \mathbb{Z}$. Pour tout $x$ et $y$ dans $G$, $\rho_k(xy) = (xy)^k = x^k y^k = \rho_k(x)\rho_k(y)$ car $G$ est cyclique donc abélien. Donc $\rho_k$ est un morphisme de groupes.
2. Soient $k_1$ et $k_2$ dans $\mathbb{Z}$. Comme $G = \{a^\ell : \ell \in \mathbb{Z}\}$, et comme $a$ est d'ordre $d$,

$$\begin{aligned}
\rho_{k_1} = \rho_{k_2} &\iff \forall \ell \in \mathbb{Z}, \rho_{k_1}(a^\ell) = \rho_{k_2}(a^\ell) \\
&\iff \forall \ell \in \mathbb{Z}, \rho_{k_1}(a)^\ell = \rho_{k_2}(a)^\ell \\
&\iff \rho_{k_1}(a) = \rho_{k_2}(a) \\
&\iff a^{k_1} = a^{k_2} \\
&\iff a^{k_1-k_2} = 1_G \\
&\iff k_1 - k_2 \in d\mathbb{Z}.
\end{aligned}$$

3. Soit $f \in \mathrm{End}(G)$. Comme $f(a) \in G$, on peut trouver $k \in \mathbb{Z}$ tel que $f(a) = a^k$. Pour tout $x \in G$, il existe $\ell \in \mathbb{Z}$ tel que $x = a^\ell$, et pour un tel $\ell$, on a

$$f(x) = f(a^\ell) = f(a)^\ell = (a^k)^\ell = a^{k\ell} = (a^\ell)^k = x^k.$$

   Donc $f = \rho_k$.
4. Soit $\Phi : \mathbb{Z} \to \mathrm{End}(G)$ l'application qui à un entier $k$ associe l'endomorphisme $\rho_k$. On a vu que pour tout $k_1$ et $k_2$ dans $\mathbb{Z}$, $\Phi(k_1) = \Phi(k_2) \iff k_1 - k_2 \in d\mathbb{Z}$. Comme pour tout $k \in \mathbb{Z}$, $\Phi(k) = \rho_k$ ne dépend que de la classe de $k$ dans $\mathbb{Z}/d\mathbb{Z}$, on définit de façon cohérente une application $\overline{\Phi}$ de $\mathbb{Z}/d\mathbb{Z}$ dans $\mathrm{End}(G)$ en posant $\overline{\Phi}(\overline{k}) = \Phi(k) = \rho_k$ pour tout $k \in \mathbb{Z}$.
   $\overline{\Phi}$ est injective car pour tous $k_1$ et $k_2$ dans $\mathbb{Z}$, $\overline{\Phi}(\overline{k_1}) = \overline{\Phi}(\overline{k_2}) \iff \overline{k_1} = \overline{k_2}$.
   Enfin, la question précédente montre que $\overline{\Phi}$ est surjective.
5. Si $k \wedge d = 1$, le théorème de Bezout fournit $(u, v) \in \mathbb{Z}^2$ tel que $ku + dv = 1$. Soit $x \in G$. Comme l'ordre de $x$ dans $G$ divise $d$ (d'après le théorème de Lagrange) donc $dv$, on a $x^{dv} = 1$ et $x = x^{ku} = (x^k)^u = (x^u)^k$. Ainsi $\rho_k$ est bijectif, de bijection réciproque $\rho_u$.
6. Soit $\overline{k} \in (\mathbb{Z}/d\mathbb{Z})^\times$. Alors $k \wedge d = 1$ donc $\overline{\Phi}(\overline{k}) = \Phi(k) = \rho_k \in \mathrm{Aut}(G)$. Donc la bijection $\overline{\Phi}$ induit une injection $\phi$ de $(\mathbb{Z}/d\mathbb{Z})^\times$ dans $\mathrm{Aut}(G)$.
7. $\phi$ est un morphisme de groupes car pour tout $\overline{k}$ et $\overline{\ell}$ dans $(\mathbb{Z}/d\mathbb{Z})^\times$,

$$\phi(\overline{k}) \circ \phi(\overline{k}) = \Phi(k) \circ \Phi(\ell) = \rho_k \circ \rho_\ell = \rho_{k\ell} = \Phi(k\ell) = \phi(\overline{k\ell}) = \phi(\overline{k\ell}).$$

   L'injectivité de $\phi$ est déjà vue. La surjectivité de $\phi$ découle de celle de $\overline{\Phi}$ et de l'implication $\rho_k$ bijectif $\implies k \wedge d = 1$. Cette dernière implication en remarquant par exemple que si $k \wedge d > 1$, alors le noyau de $\rho_k$ n'est pas réduit à $\{1_G\}$ : en effet, l'entier $d' = d/(k \wedge d)$ est un diviseur strict de $d$ donc $a^{d'} \neq 1_G$, mais $\rho_k(a^{d'}) = a^{kd'} = 1_G$ car $kd' = dk/(k \wedge d)$ est un multiple de $d$.

Remarques sur les copies

Exercice 1 : raisonner par équivalences et penser aux quantificateurs.

Exercice 2 :

1. Fait par presque tous. Les propriétés du module sont supposées connues.
2. Presque personne n'a pensé à dire que $\mathbb{U} = \mathrm{Ker} f$.
3. Quelle que soit la méthode employée, il faut à un moment ou un autre démontrer l'équivalence $|z_1| = |z_2| \iff z_1\mathbb{U} = z_2\mathbb{U}$, ou bien utiliser le fait que $\mathbb{U}$ est le noyau de $f$. Beaucoup de copies oublient ce point essentiel.
   Beaucoup parlent de classe d'équivalence sans préciser la relation d'équivalence considérée. Il y en a deux naturelles ici : celle associée à $f$ et celle associée au sous-groupe $\mathbb{U}$. Le fait que ce soit la même relation demande une vérification !
   Pour montrer qu'on peut définir de façon cohérente $\overline{f}$ en vérifiant que $f(z)$ ne dépend que de la classe de $z$, il ne faut pas utiliser $\overline{f}$ dans la preuve !
4. De même, pour montrer qu'on peut définir de façon cohérente une multiplication sur $\mathbb{C}^*/\mathbb{U}$ en vérifiant que la classe de $z_1 z_2$ ne dépend que des classes de $z_1$ et $z_2$, il ne faut pas faire comme si la multiplication était déjà définie !
5. Penser à montrer que $\mathbb{C}^*/\mathbb{U}$ est un groupe, cela n'a pas encore été vu en cours.

Exercice 3 :

1. Dans la preuve du fait que $G$ contient 1, est stable par produit et par passage à l'inverse, il faut faire apparaître des coefficients $a$ et $b$ entiers tels que $a^2 - 3b^2 = 1$.
2. Beaucoup d'arguments inutilement compliqués, voire faux.
3. Beaucoup d'inégalités fausses.
4. Rarement fait.

Exercice 4 :

1. L'égalité $(xy)^k = x^k y^k$ est vraie parce que $x$ et $y$ commutent (pourquoi ?).
2. Pour justifier l'équivalence $a^{k_1 - k_2} = 1_G \iff d | k_1 - k_2$, dire explicitement que $a$ est d'ordre $d$.
3. Il s'agit de trouver $k \in \mathbb{Z}$ tel que pour tout $x \in G$, $f(x) = x^k$. En particulier, $k$ est indépendent de $x$.
4. Beaucoup introduisent des bijections réciproques $\overline{k} \mapsto \rho_k$ et $\rho_k \mapsto \overline{k}$ sans se préoccuper de savoir si les applications sont bien définies.
5. Souvent mal fait.
6. Au lieu de recommencer le travail, il suffit de restreindre la bijection de la question 4 à $(\mathbb{Z}/d\mathbb{Z})^\times$ au départ et à $\mathrm{Aut}(G)$ à l'arrivée, grâce au résultat de la question 5.
7. Rarement fait.