Corrigé du contrôle 3

Exercice 1 : racines carrées complexes

Déterminer de deux manières différentes les racines carrées du nombre complexe i : sous forme polaire et sous forme algébrique.

En déduire les valeurs de $\cos(\frac{\pi}{4})$ et $\sin(\frac{\pi}{4})$.

Commençons par déterminer les racines carrées de i sous forme polaire : $\mathrm{i} = 1 \cdot \mathrm{e}^{\mathrm{i}\frac{\pi}{2}}$, donc ses racines carrées sont $\pm \mathrm{e}^{\mathrm{i}\frac{\pi}{4}}$.

Sous forme algébrique, on cherche $\delta = x + \mathrm{i}y$ tel que $\delta^2 = \mathrm{i}$. On obtient le système $x^2 - y^2 = 0$ et $2xy = 1$ (on peut ajouter l'égalité des modules mais c'est ici inutile). On déduit de la première équation que $x = \pm y$. D'après la seconde équation x et y sont de même signe, donc $x = y$. Enfin, comme $2xy = 1$, on a $x^2 = \frac{1}{2}$. Finalement $x = y = \pm\frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}$. Les racines carrées de i sont donc $\frac{\sqrt{2}}{2} + \mathrm{i}\frac{\sqrt{2}}{2}$ et son opposé.

On peut identifier les racines que nous avons trouvé : $\mathrm{e}^{\mathrm{i}\frac{\pi}{4}} = \frac{\sqrt{2}}{2} + \mathrm{i}\frac{\sqrt{2}}{2}$. On en déduit

$$\cos(\tfrac{\pi}{4}) = \mathrm{e}^{\mathrm{i}\frac{\pi}{4}} \qquad \sin(\tfrac{\pi}{4}) = \mathrm{e}^{\mathrm{i}\frac{\pi}{4}}.$$

Exercice 2 : transformation géométrique

On considère la transformation géométrique suivante : partant d'un point du plan,

— on le translate du vecteur d'affixe $1 + i$;

— puis on le fait tourner d'un angle $\frac{\pi}{2}$ autour de l'origine ;

— enfin, on le translate du vecteur d'affixe -2.

1. Donner l'expression complexe de la fonction $f : \mathbf{C} \to \mathbf{C}$ correspondant à cette transformation.

   L'application complexe f est la composée de la translation $z \mapsto z + 1 + \mathrm{i}$, de la rotation $z \mapsto \mathrm{e}^{\mathrm{i}\frac{\pi}{2}} z = \mathrm{i}z$ et de la translation $z \mapsto z - 2$. Il s'agit de l'application définie par

   $$\forall z \in \mathbf{C}, \quad f(z) = \mathrm{i}(z + 1 + \mathrm{i}) - 2 = \mathrm{i}z - 3 + \mathrm{i}.$$

2. Déterminer les points fixes de f.

   Soit $z \in \mathbf{C}$. Alors

   $$f(z) = z \text{ ssi } \mathrm{i}z - 3 + \mathrm{i} = z \text{ ssi } z = \frac{-3 + \mathrm{i}}{1 - \mathrm{i}} = -2 - \mathrm{i}.$$

   f possède un seul point fixe : $z_0 = -2 - \mathrm{i}$.

3. En déduire que la transformation est une rotation dont on précisera le centre et l'angle.

L'application f représente la rotation de centre z_0 d'angle $\frac{\pi}{2}$. On peut le démontrer de deux manières : exprimons f en faisant apparaître z_0 :

$$f(z) = \mathrm{i}z - 3 + \mathrm{i} = \mathrm{i}(z + 2 + \mathrm{i}) - 2 - \mathrm{i} = \mathrm{e}^{\mathrm{i}\frac{\pi}{2}}(z - z_0) + z_0.$$

C'est bien l'expression de la rotation de centre z_0 d'angle $\frac{\pi}{2}$.

Deuxième preuve : les images des points $-2-\mathrm{i}$, -2 et $-\mathrm{i}$ par la rotation de centre $-2-\mathrm{i}$ d'angle $\frac{\pi}{2}$ sont les points $-2-\mathrm{i}$, $-3-\mathrm{i}$ et $-2+\mathrm{i}$. Or on peut calculer

$$f(-2-\mathrm{i}) = -2-\mathrm{i}, \quad f(-2) = -3-\mathrm{i}, \quad f(-\mathrm{i}) = -2+\mathrm{i}.$$

Ainsi, f coïncide avec la rotation pour ces trois points. Or une isométrie est parfaitement définie par les images de trois points non alignés. Donc f est bien cette rotation.

Exercice 3 : racines cubiques dans un groupe

1. **Résultats théoriques**

   (a) Soit $(G, *)$ un groupe commutatif et soit f l'application définie de G vers G par
   $$f(x) = x^3 = x * x * x.$$
   Démontrer que f est un morphisme de groupe.

   Soient x et y dans G. Alors
   $$f(xy) = (xy)^3 = xyxyxy.$$
   Or G est supposé commutatif, donc
   $$f(xy) = xxxyyy = x^3y^3 = f(x)f(y).$$
   f est bien un endomorphisme de groupe.

   (b) Soient $(G, *)$ et $(F, \times)$ des groupes, $g : G \to F$ un morphisme de groupes et H un sous-groupe de F.
   Démontrer que l'image réciproque $g^{-1}(H) = \{x \in G \mid g(x) \in H\}$ est un sous-groupe de $(G, *)$.

   Soient x et x' dans $g^{-1}(H)$. Donc $g(x) \in H$ et $g(y) \in H$. Or H est un sous-groupe, donc par stabilité, $g(x)\times g(y) \in H$. Or g est un morphisme, donc $g(x)\times g(y) = g(x*y)$. Ainsi $g(x * y) \in H$, donc $x * y \in g^{-1}(H)$. $g^{-1}(H)$ est stable par la loi $*$.
   Soit e_G l'élément neutre de G. Comme g est un morphisme, $g(e_G) = e_F$. Or H est un sous-groupe de F, donc il contient e_F. Donc $g(e_G) \in H$ et ainsi $e_G \in g^{-1}(H)$.
   Soit $x \in g^{-1}(H)$. Alors $g(x) \in H$. Or H est un sous-groupe, donc $g(x)^{-1}$ appartient aussi à H. Mais g est un morphisme, donc $g(x)^{-1} = g(x^{-1})$. Donc $g(x^{-1}) \in H$ et ainsi $x^{-1} \in g^{-1}(H)$: $g^{-1}(H)$ est stable par inversion.
   Nous avons bien démontré que $g^{-1}(H)$ est un sous-groupe de G.

2. **Exemples**
   Dans chacun des exemples qui suivent, on considère un certain groupe $(G, *)$ et on s'intéresse à l'application $f : G \to G$ définie par $f(x) = x^3$.

   (a) **Dans** $(\mathbf{C}^*, \times)$

   i. Montrer que tout nombre complexe admet au moins une racine cubique dans $\mathbf{C}$.

   Disons déjà que 0 admet une racine cubique : 0. Soit $z \in \mathbf{C}^*$. Alors il admet une forme polaire : $z = re^{i\theta}$ avec $r \in \mathbf{R}_+^*$ et $\theta \in \mathbf{R}$. Posons $z' = \sqrt[3]{r}e^{i\frac{\theta}{3}}$. Alors $z'^3 = z$. Donc z admet bien une racine cubique.

   ii. Donner le noyau de l'application $f : z \mapsto z^3$.

   Soit $z \in \mathbf{C}^*$. Alors $z \in Ker(f)$ ssi $f(z) = 1$ ssi $z^3 = 1$: les éléments du noyau sont les racines cubiques de 1. Donc
   $$Ker(f) = \{e^{i\frac{2k\pi}{3}} \ ; \ k = 0, 1, 2\}.$$

iii. Déterminer $f^{-1}(\mathbf{R}_+^*)$ et le représenter. Est-ce un sous-groupe de $(\mathbf{C}^*, \times)$?

$f^{-1}(\mathbf{R}_+^*)$ est l'ensemble des nombres complexes z tels que $z^3 \in \mathbf{R}_+^*$. C'est l'ensemble des racines cubiques de tous les nombres réels strictement positifs :

$$f^{-1}(\mathbf{R}_+^*) = \{r\mathrm{e}^{\mathrm{i}\frac{2k\pi}{3}} \ ; \ r > 0, \ k = 0, 1, 2\}.$$

Graphiquement, cet ensemble est l'union de trois demi-droites :

(b) **Dans** $((\mathbf{Z}/p\mathbf{Z})^*, \times)$

On considère un nombre premier p de la forme $p = 3q + 2$ avec $q \in \mathbf{N}$.

i. Soit $\bar{x} \in (\mathbf{Z}/p\mathbf{Z})^*$. Montrer que si $\bar{x}^3 = \bar{1}$, alors $\bar{x} = \bar{1}$.
Indication : utiliser le petit théorème de Fermat.

D'après le petit théorème de Fermat dans $(\mathbf{Z}/p\mathbf{Z})^*$, $\bar{x}^{p-1} = \bar{1}$. Or $p = 3q+2$, donc $\bar{x}^{3q+1} = (\bar{x}^3)^q \bar{x} = \bar{1}$. Si on suppose $\bar{x}^3 = \bar{1}$, alors on obtient $\bar{x} = \bar{1}$.

ii. En déduire que $f : \bar{x} \mapsto \bar{x}^3$ est injectif.

Déterminons le noyau de f. Soit $\bar{x} \in (\mathbf{Z}/p\mathbf{Z})^*$. D'après ce qui précède, $\bar{x} \in \mathrm{K}er(f)$ ssi $\bar{x}^3 = \bar{1}$ ssi $\bar{x} = \bar{1}$. Le noyau de f ne contient donc que $\bar{1}$. Cela signifie que f est injectif.

iii. En déduire finalement que f est bijectif et donc que tout élément de $(\mathbf{Z}/p\mathbf{Z})^*$ admet une unique racine cubique dans $(\mathbf{Z}/p\mathbf{Z})^*$.

f est une application injective de $(\mathbf{Z}/p\mathbf{Z})^*$ vers $(\mathbf{Z}/p\mathbf{Z})^*$. Les ensembles de départ et d'arrivée ont le même nombre d'éléments $p - 1$. Donc si f est injectif, il est automatiquement surjectif. Donc f est un morphisme bijectif.
Cela signifie que tout élément de $(\mathbf{Z}/p\mathbf{Z})^*$ admet un antécédent par f : autrement dit, tout élément de $(\mathbf{Z}/p\mathbf{Z})^*$ admet une racine cubique dans $(\mathbf{Z}/p\mathbf{Z})^*$.

iv. Exemple : dans $(\mathbf{Z}/11\mathbf{Z})^*$, calculer $\bar{2}^{12}$ et en déduire la racine cubique de $\bar{4}$.

On peut calculer rapidement $\bar{2}^{12}$. Dans $(\mathbf{Z}/11\mathbf{Z})^*$, $\bar{2}^{10} = \bar{1}$. Donc $\bar{2}^{11} = \bar{2}$ et $\bar{2}^{12} = \bar{4}$. Comme $(\bar{2}^4)^3 = \bar{2}^{12}$, on en déduit que $\bar{2}^4$ est une racine cubique de $\bar{4}$. Et on peut vérifier que $\bar{2}^4 = \bar{5}$.

(c) **Dans** $(\mathfrak{S}_4, \circ)$

i. On considère les permutations $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ et $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$.
Calculer $\tau = \sigma_1\sigma_2, \ \ \sigma_1^3, \ \ \sigma_2^3$ et τ^3.
Que peut-on dire de l'application $f : \sigma \mapsto \sigma^3$?

On obtient $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = \tau_{12}.$, $\sigma_1^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$, $\sigma_2^3 = \mathrm{i}d$ et $\tau^3 = \tau$.
On remarque que $\sigma_1^3 \sigma_2^3 \neq \tau^3$, donc $f(\sigma_1)f(\sigma_2) \neq f(\sigma_1\sigma_2)$: f n'est pas un morphisme de groupes. Cela ne contredit pas le résultat de la question 1 car le groupe $\mathfrak{S}_4$ n'est pas un groupe commutatif.

ii. Calculer σ_1^9 et en déduire une racine cubique de la permutation σ_1.

On obtient $\sigma_1^9 = (\sigma_1^3)^3 = \sigma_1$. On en déduit que σ_1^3 est une racine cubique de σ_1.

iii. Montrer que la permutation σ_2 n'admet pas de racine cubique.
Indication : montrer que s'il existait une racine cubique, elle serait d'ordre 9 et aboutir à une contradiction.

Supposons qu'il existe une permutation σ telle que $\sigma^3 = \sigma_2$. Alors $\sigma^9 = \sigma_2^3 = \mathrm{i}d$. On en déduit que l'ordre de σ est un diviseur de 9. Or $\sigma^3 \neq \mathrm{i}d$ et on ne peut pas non plus avoir $\sigma = \mathrm{i}d$. Donc σ n'est ni d'ordre 3, ni d'ordre 1, donc σ est d'ordre 9. Mais l'ordre d'un élément doit diviser le cardinal du groupe. Comme $\mathfrak{S}_4$ est de cardinal 24, il n'est pas divisible par 9 et on obtient une contradiction. Donc σ_2 ne possède pas de racine cubique.