# Feuille de TD n° 12

*Endomorphismes orthogonaux de l'espace, Isométries, Anneaux prinipaux*

20 mai 2022

## *Pour commencer . . .*

**Exercice 1.**
$E$ est $\mathbb{R}^3$ ou un plan vectoriel de $\mathbb{R}^3$. Soit $u \in E$ un vecteur non nul, $\lambda \in \mathbb{R}$ un réel non nul, on considère l'application

$$f : \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & x + \lambda(u \cdot x)u \end{array}.$$

Déterminer une condition nécessaire et suffisante sur $\lambda$ et $u$ pour que $f$ soit un endomorphisme orthogonal de $E$. Caractériser alors $f$.

---

Supposons que $f$ est un endomorphisme orthogonal. On remarque que $f(u) = \left(1 + \lambda\|u\|^2\right) u$, or $f$ conserve les normes donc $\left|1 + \lambda\|u\|^2\right| = 1$. Si $1 + \lambda\|u\|^2 = 1$, on obtient $\lambda = 0$ ou $u = 0$, ce qui est exclu. Donc $1 + \lambda\|u\|^2 = -1$, ce qui donne $\lambda = -\dfrac{2}{\|u\|^2}$.

Réciproquement, on suppose que $\lambda = -\dfrac{2}{\|u\|^2}$, c'est-à-dire $f : x \longmapsto x - 2\dfrac{u \cdot x}{u \cdot u}u$. On a alors $f(u) = -u$ et pour tout vecteur $v$ orthogonal à $u$, $f(v) = v$. Il existe donc une base orthonormée $(u, v_1, v_2)$ dans laquelle la matrice de $f$ est $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Cette matrice est orthogonale donc $f$ est bien un endomorphisme orthogonal, c'est la réflexion d'axe $\mathbb{R}u$.

**Exercice 2.** Caractériser géométriquement les endomorphismes de $\mathbb{R}^3$ dont la matrice dans la base canonique est

$$A = \frac{1}{9}\begin{pmatrix} -8 & 4 & 1 \\ 4 & 7 & 4 \\ 1 & 4 & -8 \end{pmatrix} \quad \text{et} \quad B = \frac{1}{3}\begin{pmatrix} 2 & -1 & 2 \\ 2 & 2 & -1 \\ -1 & 2 & 2 \end{pmatrix}.$$

---

1. Soit $f$ l'endomorphisme tel que $\mathrm{Mat}_{\mathcal{C}}(f) = A$. On vérifie que $A \in \mathcal{O}_3(\mathbb{R})$, or la base canonique est orthonormée donc $f$ est un endomorphisme orthogonal. On remarque de plus que ${}^tA = A$, donc $A$ est une symétrie orthogonale. Il faut déterminer si c'est une symétrie par rapport à une droite ou un plan. Cherchons les vecteurs laissés fixes par $f$ :

$$A\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \iff \begin{cases} -8x + 4y + z &= x \\ 4x + 7y + 4z &= y \\ x + 4y - 8z &= z \end{cases} \iff \begin{cases} -17x + 4y + z &= 0 \\ 4x - 2y + 4z &= 0 \\ x + 4y - 17z &= 0 \end{cases}$$
$$\iff \begin{cases} -9x + 9z &= 0 \\ 2x - y + 2z &= 0 \\ 9x - 9z &= 0 \end{cases}$$
$$\iff \begin{cases} x &= z \\ y &= 4z \end{cases}.$$

On en déduit que $f$ est une symétrie orthogonale par rapport à la droite $\mathbb{R}\begin{pmatrix} 1 \\ 4 \\ 1 \end{pmatrix}$, ou dit autrement la rotation d'angle $\pi$ et d'axe $\mathbb{R}\begin{pmatrix} 1 \\ 4 \\ 1 \end{pmatrix}$.

2. Soit $g$ l'endomorphisme tel que $\mathrm{Mat}_{\mathcal{C}}(g) = B$. Notons $C_1$, $C_2$ et $C_3$ les colonnes de $B$, on vérifie que $\|C_1\| = \|C_2\| = 1$, $C_1 \cdot C_2 = 0$ et $C_1 \wedge C_2 = C_3$. Ainsi, $(C_1, C_2, C_3)$ est une BON directe de $\mathbb{R}^3$. $g$ transforme une BON directe (la base canonique) en une BON directe, donc $g$ est un endomorphisme orthogonal direct, c'est-à-dire une rotation.
On commence par déterminer l'axe, en résolvant $B\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$, et on trouve $\mathbb{R}u$ où $u = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$.
Ensuite, on détermine l'angle $\theta$ à un signe près : on a $1 + 2\cos\theta = \mathrm{Tr}(B) = 2$, donc $\theta = \pm\frac{\pi}{3}$.
Il reste à déterminer dans quel sens on tourne. On oriente $\mathbb{R}u$ et donc le plan orthogonal $(\mathbb{R}u)^\perp$ par le vecteur $u$. Soit $v = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$, $v$ est orthogonal à $u$. On a alors $f(v) = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$ et donc $v \wedge f(v) = u$. On en déduit que $\sin\theta$ est positif, c'est-à-dire $\theta = \frac{\pi}{3}$.

**Exercice 3.** On considère le plan affine $\mathcal{E} = \mathbb{R}^2$ muni du repère orthonormé canonique $(O, \overrightarrow{e_1}, \overrightarrow{e_2})$ et on note $E = \mathbb{R}^2$ sa direction. Soit $f$ :

$$\begin{array}{ccc}\mathcal{E} & \longrightarrow & \mathcal{E} \\ \begin{pmatrix}x\\y\end{pmatrix} & \longmapsto & \begin{pmatrix}-y+2\\x\end{pmatrix}\end{array}.$$

1. Déterminer la partie linéaire $\overrightarrow{f}$ de $f$.
2. Montrer que $f$ est une isométrie de $\mathcal{E}$.
3. Caractériser $\overrightarrow{f}$.
4. Déterminer l'ensemble des points fixes de $f$.

---

1. Puisqu'on peut choisir n'importe quel point de référence pour $\overrightarrow{f}$, on choisit $O$. Si $\overrightarrow{u} \in E$, $\overrightarrow{f}(\overrightarrow{u}) = \overrightarrow{f(O)f(O+\overrightarrow{u})}$. Or $f(O)$ est le point de coordonnées $(2,0)$ et si $\overrightarrow{u}$ a pour coordonnées $(x,y)$ dans $(\overrightarrow{e_1},\overrightarrow{e_2})$, alors $f(O+\overrightarrow{u})$ est le point de coordonnées $(-y+2,x)$. Donc $\overrightarrow{f(O)f(O+\overrightarrow{u})}$ est le vecteur de coordonnées $(-y,x)$. Ainsi $\overrightarrow{f}$ : $\begin{array}{ccc}E & \longrightarrow & E \\ \begin{pmatrix}x\\y\end{pmatrix} & \longmapsto & \begin{pmatrix}-y\\x\end{pmatrix}\end{array}$.

   *Il faut retenir en fait que si $f$ est défini par $f : \begin{pmatrix}x\\y\end{pmatrix} \longmapsto A\begin{pmatrix}x\\y\end{pmatrix} + \begin{pmatrix}a\\b\end{pmatrix}$, alors $\overrightarrow{f}$ est simplement donné par $\overrightarrow{f} : \begin{pmatrix}x\\y\end{pmatrix} \longmapsto A\begin{pmatrix}x\\y\end{pmatrix}$.*
2. La partie linéaire $\overrightarrow{f}$ est un endomorphisme orthogonal car sa matrice dans la base canonique est $\begin{pmatrix}0 & -1\\1 & 0\end{pmatrix} \in \mathcal{O}_2(\mathbb{R})$. Donc $f$ est une isométrie.
3. $\overrightarrow{f}$ est la rotation vectorielle d'angle $\frac{\pi}{2}$.
4. On résout
$$f\left(\begin{pmatrix}x\\y\end{pmatrix}\right) = \begin{pmatrix}x\\y\end{pmatrix} \iff \left\{\begin{array}{rcl} -y+2 &=& x \\ x &=& y\end{array}\right. \iff \left\{\begin{array}{rcl} x &=& 1 \\ y &=& 1\end{array}\right. .$$
   Ainsi $f$ a unique point fixe $A$, de coordonnées $(1,1)$.
   *On voit donc que $f$ est la rotation de centre $A$ et d'angle $\theta$.*

## ■ *Pour aller plus loin . . .*

**Exercice 4.** On considère l'espace vectoriel orienté $\mathbb{R}^3$.

1. Soit $r$ une rotation (d'angle non nul) et $D$ une droite vectorielle telle que $r(D) = D$. Montrer que soit $D$ est l'axe de $r$, soit $r$ est une rotation d'angle $\pi$ et $D$ est orthogonale à l'axe de $r$.
2. Soit $r_1$ et $r_2$ deux rotations (vectorielles, d'angles non nuls) de $\mathbb{R}^3$. On note $D_1$ l'axe de $r_1$ et $D_2$ l'axe de $r_2$. Montrer que $r_1(D_2) = D_2$ et $r_2(D_1) = D_1$.
3. À quelle condition $r_1$ et $r_2$ commutent-elles ?

---

1. Soit $r$ une rotation d'axe $\mathbb{R}u$, avec $u$ unitaire, et d'angle $\theta \in ]0, 2\pi[$ lorsque $\mathbb{R}u$ est orienté par $u$. Soit $D$ une droite vectorielle telle que $r(D) = D$. On définit $v$ unitaire tel que $D = \mathbb{R}v$. Alors puisque $r$ conserve les normes, $r(D) = D$ si et seulement si $r(v) = \pm v$. Complétons $u$ en une base orthonormée directe $(u, e_1', e_2')$, on note $v = v_1 u + v'$, avec $v' = v_1' e_1' + v_2' e_2'$. La matrice de $r$ dans cette base est alors $\begin{pmatrix}1 & 0 & 0\\0 & \cos\theta & -\sin\theta\\0 & \sin\theta & \cos\theta\end{pmatrix}$.
   - On a
   $$r(v) = v \iff r(v') = v' \iff \left\{\begin{array}{rcl} (\cos\theta - 1)v_1' - \sin\theta v_2' &=& 0 \\ \sin\theta v_1' + (\cos\theta - 1)v_2' &=& 0\end{array}\right. \iff v' = 0,$$
   car le déterminant de ce système est non nul (l'angle $\theta$ est supposé non nul). Donc $r(v) = v$ si et seulement si $v$ est colinéaire à $u$, c'est-à-dire si et seulement si $D$ est l'axe de $r$.
   - On a
   $$r(v) = -v \iff \left\{\begin{array}{rcl} v_1 &=& 0 \\ r(v') &=& -v'\end{array}\right. \iff \left\{\begin{array}{rcl} v_1 &=& 0 \\ (\cos\theta + 1)v_1' - \sin\theta v_2' &=& 0 \\ \sin\theta v_1' + (\cos\theta + 1)v_2' &=& 0\end{array}\right. .$$
   Or le déterminant de ce système est $2(1+\cos\theta)$. Donc si $\theta \neq \pi$, $r(v) = -v$ si et seulement si $v_1 = 0$ et $v' = 0$, ce qui donne $v = 0$ : exclu. On doit donc avoir $\theta = \pi$ et dans ce cas, $r(v) = -v$ si et seulement si $v_1 = 0$, c'est-à-dire si et seulement si $v$ est orthogonal à $u$.

   On a donc prouvé le résultat.
2. Il faut remarquer ici que l'axe d'une rotation $r$ d'angle non nul est égal à $\mathrm{Ker}\,(r - \mathrm{Id})$, c'est-à-dire l'ensemble des vecteurs fixes par $r$. Montrons alors le résultat : soit $x \in D_1$, on a $r_2(x) = r_2(r_1(x)) = r_1(r_2(x))$, donc $r_2(x)$ est fixe par $r_1$. On obtient ainsi $r_2(D_1) \subset D_1$, et l'égalité vient de la bijectivité de $r_2$. L'égalité $r_1(D_2) = D_2$
3. Supposons tout d'abord que $r_1 \circ r_2 = r_2 \circ r_1$. On a alors $r_1(D_2) = D_2$, donc d'après la première question, $D_2 = D_1$ ou $r_1$ est une rotation d'angle $\pi$ avec $D_2$ orthogonale à $D_1$. De même, $r_2(D_1) = D_1$ donc $D_1 = D_2$ ou $r_2$ est une rotation d'angle $\pi$ avec $D_1$ orthogonale à $D_2$. Finalement on obtient : $D_1 = D_2$ ou $r_1$ et $r_2$ sont des rotations d'angle $\pi$ d'axes orthogonaux.
   Réciproquement, deux rotations de même axe commutent. Maintenant, si $r_1$ et $r_2$ sont deux rotations d'angle $\pi$ et d'axes $D_1$ et $D_2$ orthogonaux, on définit deux vecteurs unitaires $u_1$ et $u_2$ tels que $D_1 = \mathbb{R}u_1$ et $D_2 = \mathbb{R}u_2$. On choisit un vecteur $v$ unitaire tel que $\mathcal{B} = (u_1, u_2, v)$ soit une BON. Dans cette base, on a
   $$\mathrm{Mat}_{\mathcal{B}}(r_1) = \begin{pmatrix}1 & 0 & 0\\0 & -1 & 0\\0 & 0 & -1\end{pmatrix} \quad \text{et} \quad \mathrm{Mat}_{\mathcal{B}}(r_2) = \begin{pmatrix}-1 & 0 & 0\\0 & 1 & 0\\0 & 0 & -1\end{pmatrix}.$$

Ces deux matrices commutent donc $r_1$ et $r_2$ commutent.
On a donc prouvé que deux rotations de l'espace (différentes de l'identité) commutent si et seulement si elles ont le même axe ou si ce sont des rotations d'angle $\pi$ dont les axes sont orthogonaux.

## *Un peu d'Algèbre . . .*

**Exercice 5.** 1. Soit $A$ un anneau commutatif et intègre.
On suppose que $A$ possède au au moins un élément irréductible.
Montrer que l'anneau $A$ a une infinité d'éléments.

2. Montrer que $B = \{\frac{p}{3^q},\ p \in \mathbb{Z}, q \in \mathbb{N}\}$ est un anneau commutatif, intègre.
3. Déterminer $B^\times$.
4. Montrer que tout $x = \frac{p}{3^q} \in B$ est associé à un entier $n$ non divisible par 3.
5. Montrer que les éléments irréductibles de $B$, à association près, sont les nombres premiers de $\mathbb{Z}$ sauf 3.
On pourra traiter séparément les cas $n$ non premier et $n$ premier.
6. Trouver un anneau commutatif intègre $C$ qui ne possède qu'un nombre fini d'éléments irréductibles.
On pourra chercher un anneau similaire à $B$.

---

1. Soit $p \in A$ irréductible.
On sait d'après le cours que $p$ n'est pas inversible.
Pour $1 \leq n < m$, montrons que $p^n \neq p^m$. Cela montrera que $A$ contient une infinité d'éléments.
Supposons par l'absurde que $p^n = p^m$.
On a donc $p^n = p^n p^{m-n}$.
Comme $A$ est un anneau intègre, en factorisant par $p^n$ on obtient $1 = p^{m-n}$.
Comme $m - n > 0$, on a $1 = p^{m-n} = pp^{m-n-1}$. Donc, $p$ est un élément inversible.
Contradiction.
Donc, on a $p^n \neq p^m$, ce qui conclut la question.
2. $B$ est un sous-ensemble de $\mathbb{Q}$. Il contient 1, et pour $x, y \in B$ on a $x - y \in B$ et $xy \in B$.
C'est donc un sous-anneau de $\mathbb{Q}$, donc un anneau.
3. Soient $x, y \in B$. On a $x = \frac{p}{3^q}$, $y = \frac{p'}{3^{q'}}$.
Alors, on a $xy = 1$ ssi $pp' = 3^{q+q'}$ ssi ($p = 3^a$ et $p' = 3^{q+q'-a}$) ou ($p = -3^a$ et $p' = -3^{q+q'-a}$).
Cela montre que les seuls éléments inversibles de $B$ sont de la forme $3^n$, $n \in \mathbb{Z}$ ou $-3^n$, $n \in \mathbb{Z}$.
Ainsi, $B^\times = \{\pm 3^n,\ n \in \mathbb{Z}\}$.
4. Soit $x \in B$. On a $x = \frac{p}{3^q}$. D'après la question précédente, $x$ est associé à $3^q x = p$.
Donc, les éléments irréductibles de $B$ sont, à association près, des entiers.
De même, pour $n \in \mathbb{Z}$ non-nul, on écrit $n = 3^a.b$ avec $pgcd(3, b) = 1$.
Alors $n$ est associé à $3^{-a}n = b$.
Donc, les éléments irréductibles de $B$ sont, à association près, des entiers non divisibles par 3.
5. Soit $n \in \mathbb{Z}$ non-nul, non divisible par 3, et irréductible dans $B$.
• Si $n$ n'est pas premier, alors $n = mk$ avec $m, k \in \mathbb{Z}$ différents de $1, -1$.
Comme $n$ n'est pas divisible par 3, $m$ et $k$ ne sont pas divisibles par 3.
Donc, $m$ et $k$ ne sont pas inversibles dans $B$. Cela implique que $n$ n'est pas irréductible dans $B$. • Si $n$ est premier, soient $x, y \in B$ tels que $n = xy$.
Pour $x = \frac{p}{3^q}$, $y = \frac{p'}{3^{q'}}$, on a alors $3^{q+q'}n = pp'$.
Comme $n$ est premier, on a alors $n \mid p$ ou $n \mid p'$. Supposons que $n \mid p$.
Cela donne $p = n.k$, donc $x = n\frac{k}{3^q}$.
D'où, $n = n\frac{k}{3^q}\frac{p'}{3^{q'}}$.
Comme $B$ est intègre, cela donne $1 = \frac{k}{3^q}\frac{p'}{3^{q'}}$.
Ainsi, $y = \frac{p'}{3^{q'}}$ sont inversibles.
Donc, si $n = xy$ avec $x, y \in B$, on a $y$ inversible ou $x$ inversible.
Cela montre que $n$ est irréductible dans $B$.
6. On pose $C = \{\frac{p}{q}$ tels que $p \in \mathbb{Z}, q \in \mathbb{N}^*$ et $2 \not| q\}$.
On montre alors que $C$ est un sous-anneau de $\mathbb{Q}$.
Dans ce sous-anneau, tous les nombres $\frac{p}{q}$ avec $2 \not| p$ sont inversibles.
Ainsi, à association près, les seuls nombre non-inversibles sont les $2^n$, $n \geq 1$ (Si $x = \frac{p}{q}$ n'est pas inversible, on a forcément $p = 2^n p'$ avec $n > 0$, et alors $x$ est associé à $x\frac{q}{p'} = 2^n$).
Cela montre que le seul élément irréductible de $C$, à association près, est 2.

**Exercice 6.** On étudie $\mathbb{Z}[i] = \{a + ib,\ a, b \in \mathbb{Z}\}$.

1. Montrer que $(\mathbb{Z}[i], +, \times)$ est un sous-anneau de $\mathbb{C}$.
2. Quelles sont ses propriétés ? (commutatif ? intègre ?)
3. Soit $z = x + iy \in \mathbb{Z}[i]$.
En utilisant la fonction $|z|^2 = z\overline{z}$, Montrer que l'on a $z \in \mathbb{Z}[i]^\times$ ssi $|z| = 1$.
4. En déduire que $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.
5. Soit $z \in \mathbb{Z}[i]$ tel que $|z|^2 = p$, avec $p$ premier.
Montrer que $z$ est irréductible dans $\mathbb{Z}[i]$.
6. Soit $q$ un nombre premier, tel que $q \equiv 3 \mathrm{mod}\ (4)$. On veut montrer que $q$ est irréductible dans $\mathbb{Z}[i]$.

(a) Supposons par l'absurde que $q$ est réductible dans $\mathbb{Z}[i]$.
On écrit alors $q = zz'$, avec $z, z'$ qui ne sont pas inversibles.
Combien vaut $|z|^2$ ? Et $|z'|^2$ ?

(b) Montrer que pour $z = x + iy$, on a $x, y \neq 0$.
On pourra démontrer cela par l'absurde.

(c) Trouver une relation entre $arg(z)$ et $arg(z')$.

(d) Montrer que $z' = \overline{z}$.

(e) En déduire que $q$ est la somme de deux carrés.
Conclure.

7. On admet que l'anneau $\mathbb{Z}[i]$ est principal. (On démontre cela en prouvant qu'il existe une division euclidienne sur $\mathbb{Z}[i]$.)
Dire si les éléments $1 + 2i$, 5, 13, $3 + 4i$, sont irréductibles dans $\mathbb{Z}[i]$.
Si non, donner leur factorisation en produit d'éléments irréductibles.

---

1. Cela a été traité en cours, il faut vérifier que $\mathbb{Z}[i]$ contient 1, et que pour $z, z' \in \mathbb{Z}[i]$ on a $z - z'$ et $zz'$ dans $\mathbb{Z}[i]$.
2. Cet anneau est commutatif et intègre, comme sous-anneau d'un anneau commutatif intègre.
3. Soit $z = x + iy \in \mathbb{Z}[i]$. Si $|z| = 1$ alors $z\overline{z} = |z|^2 = 1$. Comme $\overline{z} = x - iy \in \mathbb{Z}[i]$, $z$ est bien inversible dans $\mathbb{Z}[i]$.
Réciproquement, soit $z \in \mathbb{Z}[i]^\times$. On a $z' = x' + iy'$ tel que $zz' = 1$. Alors, $1 = |zz'|^2 = |z|^2|z'|^2 = (x^2 + y^2)(x'^2 + y'^2)$.
Comme $x, y, x', y'$ sont des entiers, $|z|^2$ et $|z'|^2$ sont des entiers.
Comme cet entiers divisent 1 et sont positifs, on a donc $|z|^2 = 1$, d'où $|z| = 1$.
4. On a $x^2 + y^2 = 1$ avec $x, y \in \mathbb{Z}$ si et seulement si ($x = \pm 1$ et $y = 0$) ou ($x = 0$ et $y = \pm 1$).
Cela donne les 4 éléments de $\mathbb{Z}[i]$, $1, -1, i, -i$.
5. Soient $a, b \in \mathbb{Z}[i]$ tels que $z = ab$.
Alors, on a $p = |z|^2 = |ab|^2 = |a|^2|b|^2$.
Comme $p$ est un nombre premier et $|a|^2, |b|^2$ sont entiers positifs, on a donc ($|a|^2 = 1$ et $|b|^2 = p$) ou ($|a|^2 = p$ et $|b|^2 = 1$).
Ainsi, on a $a$ inversible ou $b$ inversible, d'après la question précédente.
Cela prouve que $z$ est un élément irréductible de $\mathbb{Z}[i]$.
6. (a) On a $q^2 = |zz'|^2 = |z|^2|z'|^2$.
Comme $q$ est premier, on en déduit donc que $|z|^2 = 1, q, q^2$.
Comme $z$ et $z'$ ne sont pas inversibles, on a $|z| \neq 1$ et $|z'| \neq 1$, d'après une question précédente.
Donc, le seul cas possible est $|z|^2 = |z'|^2 = q$.

(b) Pour $z = x + iy$.
Si $y = 0$, on a $z = x$. On a ainsi $q = xz'$.
Cela implique que $z'$ est un nombre réel, donc un entier naturel. Ainsi, $x \mid q$ avec $x$ entier. Cela donne $x = \pm 1$ ou $x = \pm q$.
Cela donne $x^2 = 1$ ou $x^2 = q^2$.
Mais on a obtenu $|z|^2 = |x|^2 = q$ à la question précédente. Contradiction.
Si $x = 0$, on a $z = iy$. On a ainsi $q = y(iz')$.
Cela implique que $iz'$ est un nombre réel, donc un entier naturel. Ainsi, $y \mid q$ avec $y$ entier. Cela donne $y = \pm 1$ ou $y = \pm q$.
Cela donne $y^2 = 1$ ou $y^2 = q^2$.
Mais on a obtenu $|z|^2 = |y|^2 = q$ à la question précédente. Contradiction.

(c) Comme $zz'$ est un nombre réel positif, on a $arg(z') = -arg(z)$.

(d) Ainsi, pour $z = Re^{it}$, on a $R = \sqrt{q}$.
Pour $z' = R'e^{it'}$, on a $R' = R = \sqrt{q}$ et $t' = -t$, donc $z' = Re^{-it} = \overline{z}$.

(e) Pour $z = x + iy$, avec les questions précédentes on a $x, y \neq 0$ et $x^2 + y^2 = |z|^2 = z\overline{z} = zz' = q$.
Donc, $q$ est la somme de deux carrés.

(f) Or, modulo 4 cela est impossible. La somme de deux carrés est congue à 0,1, ou 2, mais pas à 3.
On obtient donc une contradiction. Le nombre $q$ est donc irréductible dans $\mathbb{Z}[i]$.

7. On a $5 = 4 + 1 = (1 + 2i)(1 - 2i)$, donc 5 est réductible.
On a $|1 + 2i|^2 = 1 + 4 = 5$, donc $1 + 2i$ est irréductible. Cela donne la décomposition en facteurs irréductibles de 5.
On a $13 = 4 + 9 = (2 + 3i)(2 - 3i)$, donc 13 est réductible. Les nombres $2 + 3i$ et $2 - 3i$ sont irréductibles dans $\mathbb{Z}[i]$ car leur norme au carré est un nombre premier.
On a $3^2 + 4^2 = 9 + 16 = 25$. Donc, $(3 + 4i)(3 - 4i) = 5x5 = (1 + 2i)^2(1 - 2i)^2$.
L'élément irréductible $1 + 2i$ divise donc $3 + 4i$ ou $3 - 4i$, d'après le théorème d'Euclide.
Ce nombre n'est donc pas irréductible dans $\mathbb{Z}[i]$.
On a $(1 + 2i)^2 = -3 + 4i$, donc $3 + 4i = (-i)(1 + 2i)(1 + 2i) = (2 - i)(1 + 2i)$.