Devoir surveillé 3

▸ Exercice 1 : calcul intégral

1. En utilisant le changement de variable $x = \ln t$, déterminer la valeur de $I = \displaystyle\int_1^e \frac{\ln t}{(1+\ln t)^2}\,dt$.
2. Le but de cette question est de déterminer une primitive, sur $\mathbf{R}_+^*$, de la fonction $x \mapsto \dfrac{1}{\sqrt{x^2+1}}$.
   a. Soit $x \in \mathbf{R}_+^*$. À l'aide du changement de variable $u = \sqrt{1+t^2}$, montrer que
   $$\int_1^x \frac{dt}{t\sqrt{t^2+1}} = \ln\left(\sqrt{1+x^2}-1\right) - \ln(x) - \ln(\sqrt{2}-1).$$
   b. En déduire, en utilisant le changement de variable $u = \frac{1}{t}$, qu'une primitive de $t \mapsto \dfrac{1}{\sqrt{t^2+1}}$ est $x \mapsto \ln\left(x+\sqrt{x^2+1}\right)$.
3. **Deux applications de la question précédente** :
   a. Déterminer la valeur de $\displaystyle\int_1^2 \sqrt{t^2+1}\,dt$.
   b. Mettre sous forme canonique le polynôme $X^2-4X+13$, puis en utilisant un changement de variable affine bien choisi, déterminer une primitive de $x \mapsto \dfrac{x+1}{\sqrt{x^2-4x+13}}$.

▸ Exercice 2 : différence symétrique de deux ensembles

Soit E un ensemble. Pour tous $(A,B) \in \mathscr{P}(E)^2$, on appelle **différence symétrique de A et B**, et on note $A\Delta B$ la partie de E définie par $A\Delta B = (A \setminus B) \cup (B \setminus A) = (A \cap \overline{B}) \cup (B \cap \overline{A})$.
Notons qu'on a toujours $A\Delta B = B\Delta A$.

1. Pour $A \in \mathscr{P}(E)$, déterminer les ensembles : $A\Delta E$, $A\Delta A$, $A\Delta\emptyset$ et $A\Delta\overline{A}$.
2. Montrer que pour $(A,B) \in \mathscr{P}(E)^2$, $A\Delta B = (A \cup B) \setminus (A \cap B)$.
3. Soient A et B deux parties de E. Montrer que $\overline{A\Delta B} = \overline{A}\Delta B = A\Delta\overline{B}$. Que dire de $\overline{A}\Delta\overline{B}$?
4. **Associativité de Δ.** Soient A, B, C trois parties de E.
   a. Justifier que $(A\Delta B)\Delta C = \left((A\Delta B) \cap \overline{C}\right) \cup \left(\left(\overline{A}\Delta B\right) \cap C\right)$.
   b. En déduire que $(A\Delta B)\Delta C = \left(A \cap \overline{B} \cap \overline{C}\right) \cup \left(\overline{A} \cap B \cap \overline{C}\right) \cup \left(\overline{A} \cap \overline{B} \cap C\right) \cup (A \cap B \cap C)$.
   c. Sans nouveaux calculs, justifier alors que $(A\Delta B)\Delta C = A\Delta(B\Delta C)$.

   On dit alors que la différence symétrique est associative, et on note alors $A\Delta B\Delta C$ (sans parenthèses) l'ensemble $(A\Delta B)\Delta C = A\Delta(B\Delta C)$.
5. En effectuant le moins de calculs possibles, déterminer $A\Delta B\Delta A$, où A et B sont deux parties de E.
6. Soit $A \in \mathscr{P}(E)$. On note alors f_A l'application $f_A : \left|\begin{array}{ccc} \mathscr{P}(E) & \longrightarrow & \mathscr{P}(E) \\ B & \longmapsto & A\Delta B \end{array}\right.$.
   a. La proposition $\forall C \in \mathscr{P}(E), \exists B \in \mathscr{P}(E), f_A(B) = C$ est-elle vraie ? Justifier votre affirmation. *On pourra notamment utiliser le résultat de la question 5.*
   b. Montrer que f_A est injective, c'est-à-dire que $\forall (B,C) \in \mathscr{P}(E)^2,\ f_A(B) = f_A(C) \Rightarrow B = C$.
   c. Résoudre l'équation $A\Delta B = A$, d'inconnue $B \in \mathscr{P}(E)$.
7. Prouver que pour tout $(A,B) \in \mathscr{P}(E)^2$, on a $(A\Delta B = A \cap B) \Leftrightarrow (A = B = \emptyset)$.

▸ Problème : inversion circulaire et points rationnels sur un cercle

▸ Dans ce problème, le plan est muni d'un repère orthonormé $(O, \vec{i}, \vec{j})$.
▸ Pour $\omega \in \mathbf{C}$ et $r \in \mathbf{R}_+^*$, on note $\mathscr{C}_{\omega,r}$ le cercle de centre d'affixe ω et de rayon r.
▸ On identifiera un complexe z au point du plan d'affixe z, et donc on identifie une partie A du plan à l'ensemble des affixes des points de A. Par exemple, avec les notations ci-dessus, on a $\mathscr{C}_{\omega,r} = \{z \in \mathbf{C} \mid |z-\omega| = r\}$.
▸ On note f l'appplication (nommée *inversion circulaire*) définie sur $\mathbf{C}^*$ par $f : \left| \begin{array}{ccc} \mathbf{C}^* & \longrightarrow & \mathbf{C}^* \\ z & \longmapsto & \dfrac{1}{\overline{z}} \end{array} \right.$.
▸ Si A est une partie de $\mathbf{C}^*$, on note $f(A)$ la partie de $\mathbf{C}^*$ définie par $f(A) = \{f(z),\ z \in A\}$ ou encore, de manière équivalente $f(A) = \{y \in \mathbf{C}^* \mid \exists z \in A, y = f(z)\}$.

Partie I. Image d'un cercle par l'inversion

1. Prouver que pour tout $z \in \mathbf{C}^*$, $(f \circ f)(z) = z$.
2. Soit $A \subset \mathbf{C}^*$ une partie de $\mathbf{C}^*$, et soit $z \in \mathbf{C}^*$. Prouver soigneusement les équivalences suivantes :
   a. $z \in A \Leftrightarrow f(z) \in f(A)$ b. $z \in f(A) \Leftrightarrow f(z) \in A$.
3. Soit $\omega \in \mathbf{C}$, et $r \in \mathbf{R}_+$. Justifier que $\mathscr{C}_{\omega,r} = \left\{z \in \mathbf{C} \mid |z|^2 - \overline{\omega}z - \omega\overline{z} + |\omega|^2 - r^2 = 0\right\}$.
4. Soit $\omega \in \mathbf{C}$ et $r > 0$. Dans cette question, on pose $\mathscr{C} = \mathscr{C}_{\omega,r}$.
   a. Montrer que si $0 \notin \mathscr{C}$, alors $f(\mathscr{C})$ est le cercle de centre d'affixe $-\frac{\omega}{r^2-|\omega|^2}$ et de rayon $\frac{r}{|r^2-|\omega|^2|}$.
   b. Montrer que si $0 \in \mathscr{C}$, alors $f(\mathscr{C} \setminus \{0\})$ est une droite dont on précisera une équation.

Partie II. Points rationnels des cercles

On note $\mathbf{Q}(i) = \{x + iy,\ (x,y) \in \mathbf{Q}^2\}$. Un point du plan est dit rationnel si son affixe est dans $\mathbf{Q}(i)$, c'est-à-dire si et seulement si son abscisse et son ordonnée sont des nombres rationnels.

5. Soit $z \in \mathbf{C}^*$. Prouver que $z \in \mathbf{Q}(i) \Leftrightarrow f(z) \in \mathbf{Q}(i)$.
6. Montrer qu'une droite qui contient au moins deux points rationnels en contient une infinité.
7. Soit $\mathscr{C}$ un cercle qui contient O ainsi qu'au moins deux autres points rationnels. En considérant $f(\mathscr{C} \setminus \{O\})$, prouver que $\mathscr{C}$ possède une infinité de points rationnels.
8. En déduire qu'un cercle qui contient trois points rationnels en possède une infinité.

Partie III. Une caractérisation des cercles qui possèdent une infinité de points rationnels.

Une similitude directe sera dite rationnelle si et seulement si elle est de la forme $z \mapsto az + b$, avec $a, b \in \mathbf{Q}(i)$.

9. a. Soient $a, b, c \in \mathbf{Q}$, avec $a \neq 0$. Montrer que si l'équation $ax^2 + bx + c = 0$ possède une solution dans $\mathbf{Q}$, alors toutes ses solutions complexes sont dans $\mathbf{Q}$.
   b. Soit $\mathscr{C}$ un cercle dont le centre est rationnel, et qui possède un point rationnel A.
   Soit également $\mathscr{D}$ une droite non verticale, de pente (c'est-à-dire de coefficient directeur) rationnelle.
   Montrer que si $\mathscr{D}$ passe par A, alors elle rencontre $\mathscr{C}$ en au plus un autre point, et que lorsque c'est le cas, ce point est rationnel.
10. Soit $s : \mathbf{C} \to \mathbf{C}$ une similitude directe rationnelle, et soit $z \in \mathbf{C}$. Prouver que $z \in \mathbf{Q}(i) \Leftrightarrow s(z) \in \mathbf{Q}(i)$.
11. Soit $\mathscr{C}$ un cercle qui contient trois points rationnels distincts A, B, C.
    a. Montrer qu'il existe une similitude directe rationnelle $s : \mathbf{C} \to \mathbf{C}$ telle que $s(\mathscr{C})$ soit un cercle $\mathscr{C}'$ passant par les deux points d'affixes 0 et 1, et contenant un troisième point rationnel.
    b. Prouver que le centre de $\mathscr{C}'$ est rationnel. Qu'en déduit-on au sujet du centre de $\mathscr{C}$?
12. Soit $\mathscr{C}$ un cercle de centre Ω. Montrer, à l'aide des questions 9 et 11 qu'il y a équivalence entre les deux propriétés suivantes :
    i) $\mathscr{C}$ contient une infinité de points rationnels
    ii) Ω est rationnel et $\mathscr{C}$ contient au moins un point rationnel.
13. **Question subsidiaire** : déduire de ce qui précède qu'il existe une infinité de triplets $(a, b, c) \in \mathbf{Z}^2$, avec a et b premiers entre eux et tels que $a^2 + b^2 = c^2$.

CORRECTION DU DEVOIR SURVEILLÉ 3

▸ Exercice 1 : calculs d'intégrales et de primitives

1. Réalisons le changement de variable $x = \ln(t)$, si bien que $dx = \dfrac{dt}{t}$. Alors

$$I = \int_1^e \frac{t\ln t}{(1+\ln t)^2}\frac{dt}{t} = \int_1^e \frac{e^{\ln t}\ln t}{(1+\ln t)}\frac{dt}{t} = \int_0^1 \frac{xe^x}{(1+x)^2}\,dx.$$

Réalisons alors une intégration par parties en posant $u(x) = xe^x$ et $v(x) = -\dfrac{1}{1+x}$, qui sont deux fonctions de classe $\mathscr{C}^1$ sur $[0,1]$, avec $u'(x) = xe^x + e^x = e^x(x+1)$ et $v'(x) = \dfrac{1}{(x+1)^2}$.
On a alors

$$I = \left[-\frac{xe^x}{x+1}\right]_0^1 + \int_0^1 \frac{e^x(x+1)}{x+1}\,dx = -\frac{e}{2} + [e^x]_0^1 = \boxed{\frac{e}{2} - 1.}$$

2.a. On a donc $du = \dfrac{t}{\sqrt{1+t^2}}\,dt$.
Notons qu'on a alors $u^2 = 1 + t^2$, et donc $t^2 = u^2 - 1$. Alors il vient

$$\begin{aligned}
\int_1^x \frac{dt}{t\sqrt{t^2+1}} &= \int_1^x \frac{1}{t^2}\frac{t\,dt}{\sqrt{t^2+1}} = \int_{\sqrt{2}}^{\sqrt{x^2+1}} \frac{du}{u^2-1} \\
&= \int_{\sqrt{2}}^{\sqrt{x^2+1}} \frac{du}{(u-1)(u+1)} \\
&= \int_{\sqrt{2}}^{\sqrt{x^2+1}} \frac{1}{2}\left(\frac{1}{u-1} - \frac{1}{u+1}\right) du \\
&= \frac{1}{2}\left[\ln\frac{u-1}{u+1}\right]_{\sqrt{2}}^{\sqrt{1+x^2}} \\
&= \frac{1}{2}\left(\ln\frac{\sqrt{1+x^2}-1}{\sqrt{1+x^2}+1} - \ln\frac{\sqrt{2}-1}{\sqrt{2}+1}\right) \\
&= \frac{1}{2}\ln\left(\frac{\left(\sqrt{1+x^2}-1\right)^2}{\left(\sqrt{x^2+1}-1\right)\left(\sqrt{x^2+1}+1\right)}\right) - \frac{1}{2}\ln\left(\frac{\left(\sqrt{2}-1\right)^2}{\sqrt{2}^2-1}\right) \\
&= \frac{1}{2}\ln\left(\frac{\left(\sqrt{1+x^2}-1\right)^2}{x^2}\right) - \frac{1}{2}\ln\left(\left(\sqrt{2}-1\right)^2\right) \\
&= \ln\left(\sqrt{1+x^2}-1\right) - \ln(x) - \ln\left(\sqrt{2}-1\right).
\end{aligned}$$

Danger !
$\frac{1}{u^2-1}$ n'a pas un dénominateur irréductible, et n'est pas un élément simple.

Décomposition en éléments simples.

Rappel
Une fonction de la forme
$$x \mapsto \int_a^x f(t)\,dt$$
est une primitive de f par le théorème fondamental de l'analyse.

2.b. Notons que la question précédente nous dit notamment qu'une primitive de $x \mapsto \dfrac{1}{x\sqrt{1+x^2}}$ sur $\mathbf{R}_+^*$ est $x \mapsto \ln\left(\sqrt{x^2+1}-1\right) - \ln(x)$.
Dans cette question, nous cherchons plutôt à calculer $\displaystyle\int^x \frac{dt}{\sqrt{x^2+1}}$.
Posons alors $u = \frac{1}{t}$, si bien que $du = -\frac{1}{t^2}\,dt$. Alors

$$\begin{aligned}
\int^x \frac{dt}{\sqrt{t^2+1}} &= \int^x \frac{t^2}{\sqrt{t^2+1}}\frac{dt}{t^2} \\
&= -\int^{1/x} \frac{\frac{1}{u^2}}{\sqrt{\frac{1}{u^2}+1}}du
\end{aligned}$$

Intégrale «sans borne»
Rappelons que si vous n'êtes pas à l'aise avec la notation $\int^x$, il est toujours possible, pour trouver une primitive de f, de calculer $\int_a^x f(t)\,dt$, avec a fixé dans le domain de définition de f.

$$
\begin{aligned}
&= -\int^{1/x} \frac{1}{u\sqrt{u^2+1}} \\
&= -\ln\left(\sqrt{\frac{1}{x^2}+1}-1\right)+\ln\left(\frac{1}{x}\right) \\
&= \ln\left(\frac{1}{x\sqrt{\frac{1}{x^2}+1}-1}\right) \\
&= \ln\left(\frac{1}{\sqrt{x^2+1}-x}\right) \\
&= \ln\left(\frac{\sqrt{x^2+1}+x}{x^2+1-x^2}\right) =_b oxed\ln\left(\sqrt{x^2+1}+x\right).
\end{aligned}
$$

3. Deux applications de la question précédente

3.a. Procédons à une intégration par parties, en posant $u(t)=\sqrt{t^2+1}$ et $v(t)=t$, qui sont deux fonctions de classe $\mathscr{C}^1$ sur $[1,2]$, avec $u'(t)=\dfrac{t}{\sqrt{t^2+1}}$ et $v'(t)=1$. Il vient alors

$$
\begin{aligned}
\int_1^2 \sqrt{t^2+1}\,dt &= \left[t\sqrt{t^2+1}\right]_1^2 - \int_1^2 \frac{t^2}{\sqrt{t^2+1}}\,dt \\
&= 2\sqrt{5}-\sqrt{2}-\int_1^2 \frac{t^2+1-1}{\sqrt{t^2+1}}\,dt \\
&= 2\sqrt{5}-\sqrt{2}-\int_1^2 \sqrt{t^2+1}\,dt+\int_1^2 \frac{dt}{\sqrt{1+t^2}} \\
&= 2\sqrt{5}-\sqrt{2}+\left[\ln\left(\sqrt{t^2+1}+t\right)\right]_1^2-\int_1^2 \sqrt{t^2+1}\,dt.
\end{aligned}
$$

Si on note $I=\displaystyle\int_1^2 \sqrt{t^2+1}\,dt$ l'intégrale que l'on cherche à calculer, nous venons donc de prouver que

$$2I = 2\sqrt{5}-\sqrt{2}+\ln\left(2+\sqrt{5}\right)-\ln\left(1+\sqrt{2}\right).$$

Et donc $\boxed{I=\sqrt{5}+\frac{1}{2}\left(-\sqrt{2}+\ln\left(2+\sqrt{5}\right)-\ln\left(1+\sqrt{2}\right)\right).}$

3.b. On a $X^2-4X+13=(X-2)^2+9$. Et donc en particulier, pour $t\in\mathbf{R}$,

$$\frac{t+1}{\sqrt{t^2-4t+13}}=\frac{t+1}{\sqrt{(t-2)^2+3^2}}=\frac{t+1}{3\sqrt{\left(\frac{t-2}{3}\right)^2+1}}.$$

Donc un changement de variable tout indiqué est $u=\frac{t-2}{3}$. On a alors $t=3u+2$, et $du=\frac{dt}{3}$. Donc

$$
\begin{aligned}
\int^x \frac{t+1}{\sqrt{t^2-4t+13}}\,dt &= \int^x \frac{t+1}{\sqrt{\left(\frac{t-2}{3}\right)^2+1}}\frac{dt}{3} \\
&= \int^{\frac{x-2}{3}} \frac{3u+3}{\sqrt{u^2+1}}\,du \\
&= 3\int^{\frac{x-2}{3}} \frac{u\,du}{\sqrt{u^2+1}}+3\int^{\frac{x-2}{3}} \frac{du}{\sqrt{u^2+1}} \\
&= 3\left[\sqrt{u^2+1}\right]^{\frac{x-2}{3}}+3\left[\ln\left(\sqrt{u^2+1}+u\right)\right]^{\frac{x-2}{3}} \\
&= \boxed{\sqrt{x^2-4x+13}+3\ln\left(\frac{1}{3}\sqrt{x^2-4x+13}+\frac{x-2}{3}\right).}
\end{aligned}
$$

▸ Exercice 2 : différence symétrique de deux ensembles

1. On a

$$A\Delta E = (A \setminus E) \cup (E \setminus A) = \emptyset \cup \overline{A} = \overline{A}.$$
$$A\Delta A = (A \setminus A) \cup (A \setminus A) = \emptyset \cup \emptyset = \emptyset.$$
$$A\Delta\emptyset = (A \setminus \emptyset) \cup (\emptyset \setminus A) = A \cup \emptyset = A.$$
$$A\Delta\overline{A} = (A \setminus \overline{A}) \cup (\overline{A} \setminus A) = A \cup \overline{A} = E.$$

2. Une preuve par double inclusion est possible. Mais préférons le calcul suivant :

$$\begin{aligned}
A\Delta B &= (A \setminus B) \cup (B \setminus A) = (A \cap \overline{B}) \cup (B \cap \overline{A}) \\
&= \Big((A \cap \overline{B}) \cup B\Big) \cap \Big((A \cap \overline{B}) \cup \overline{A}\Big) && \text{Distributivité.} \\
&= \left((A \cup B) \cap \underbrace{\Big(\overline{B} \cup B\Big)}_{=E}\right) \cap \left(\underbrace{\Big(A \cup \overline{A}\Big)}_{=E} \cap \Big(\overline{B} \cup \overline{A}\Big)\right) && \text{Re-distributivité.} \\
&= (A \cup B) \cap \Big(\overline{A} \cup \overline{B}\Big) \\
&= (A \cup B) \cap \Big(\overline{A \cap B}\Big) = \boxed{(A \cup B) \setminus (A \cap B).}
\end{aligned}$$

3. On a, en utilisant la question précédente,

$$\begin{aligned}
\overline{A\Delta B} &= \overline{(A \cup B) \cap \Big(\overline{A \cap B}\Big)} \\
&= \Big(\overline{A \cup B}\Big) \cup \overline{\overline{(A \cap B)}} && \text{Loi de De Morgan.} \\
&= (\overline{A} \cap \overline{B}) \cup (A \cap B) \\
&= \Big(\overline{A} \cup (A \cap B)\Big) \cap \Big(\overline{B} \cup (A \cap B)\Big) \\
&= \left(\underbrace{\Big(\overline{A} \cup A\Big)}_{=E} \cap \Big(\overline{A} \cup B\Big)\right) \cap \left(\Big(\overline{B} \cup A\Big) \cap \underbrace{\Big(\overline{B} \cup B\Big)}_{=E}\right) \\
&= \Big(\overline{A} \cup B\Big) \cap \Big(\overline{B} \cup A\Big) \\
&= \Big(\overline{A} \cup B\Big) \cap \Big(\overline{A} \cap B\Big) \\
&= \Big(\overline{A} \cup B\Big) \setminus (\overline{A} \cap B) = \boxed{\overline{A}\Delta B.}
\end{aligned}$$

Et pour la seconde égalité, notons qu'on a toujours[1] $A\Delta B = B\Delta A$ et donc

$$A\Delta\overline{B} = \overline{B}\Delta A = \overline{B\Delta A} = \overline{A\Delta B}.$$

On a alors $\overline{A}\Delta\overline{B} = \overline{A\Delta\overline{B}} = A\Delta\overline{\overline{B}} = \boxed{A\Delta B.}$

[1] On dit que Δ est **commutative**.

4. **Associativité de Δ.**

4.a. On a $(A\Delta B)\Delta C = \Big((A\Delta B) \cap \overline{C}\Big) \cup \Big(\overline{A\Delta B} \cap C\Big) = \boxed{\Big((A\Delta B) \cap \overline{C}\Big) \cup \Big((\overline{A} \cap B) \cap C\Big).}$

4.b. Reprenons l'expression de la question précédente :

$$\begin{aligned}
(A\Delta B)\Delta C &= \Big(\Big((A \cap \overline{B}) \cup (\overline{A} \cap B)\Big) \cap \overline{C}\Big) \cup \Big(\Big((\overline{A} \cap \overline{B}) \cup (A \cap B)\Big) \cap C\Big) \\
&= \Big(A \cap \overline{B} \cap \overline{C}\Big) \cup \Big(\overline{A} \cap B \cap \overline{C}\Big) \cup \Big(\overline{A} \cap \overline{B} \cap C\Big) \cup (A \cap B \cap C)\,.
\end{aligned}$$

4.c. Remarquons que $A\Delta(B\Delta C) = (B\Delta C)\Delta A = (C\Delta B)\Delta A$.
Et donc en reprenant le calcul précédent, et échangeant A et C, il vient

$$A\Delta(B\Delta C) = \Big(C \cap \overline{B} \cap \overline{A}\Big) \cup \Big(\overline{C} \cap B \cap \overline{A}\Big) \cup \Big(\overline{C} \cap \overline{B} \cap A\Big) \cup (C \cap B \cap A) = \boxed{(A\Delta B)\Delta C.}$$

5. On a $A\Delta B\Delta A = A\Delta(B\Delta A) = A\Delta(A\Delta B) = (A\Delta A)\Delta B = \emptyset\Delta B = \boxed{B.}$

6.a. La question précédente prouve que pour tout $C \in \mathscr{P}(E)$, $A\Delta(C\Delta A) = C \Leftrightarrow f_A(C\Delta A) = C$.
Donc pour $C \in \mathscr{P}(E)$ fixé, C possède bien un[2] antécédent B par f_A, à savoir $C\Delta A = A\Delta C$.

[2] Au moins.

6.b. Soient B et C soient deux parties de E telles que $f_A(B) = f_A(C) \Leftrightarrow A\Delta B = A\Delta C$.
Alors $A\Delta(A\Delta B) = A\Delta(A\Delta C)$, soit encore $A\Delta B\Delta A = A\Delta C\Delta A$.
Et donc par la question 5, $B = C$.

6.c. Nous savons que $B = \emptyset$ est une solution puisque $f_A(\emptyset) = A\Delta\emptyset = A$.
Mais la question 6.b nous dit qu'une solution, si elle est existe est unique.
En effet, si B est une solution, alors $f_A(B) = A = f_A(\emptyset)$, et donc $B = \emptyset$.
Et donc $\boxed{\text{l'unique solution de } A\Delta B = A \text{ est } B = \emptyset.}$

> **Remarque**
> La question 7.b prouve que tout élément de $\mathscr{P}(E)$ possède au plus un antécédent par f_A, quand la question 7.a prouve que tout élément possède au moins un antécédent par f_A.
> Et donc tout élément de $\mathscr{P}(E)$ possède un unique antécédent par f_A, on dira plus tard que f_A est bijective.
> Mieux, la preuve de la question 6.a nous donne l'unique antécédent de B par f_A : c'est $A\Delta B$.

7. Il est évident que si $A = B = \emptyset$, alors $A \cap B = \emptyset$ et $A\Delta B = \emptyset$, donc $A\Delta B = A \cap B$.

Inversement, supposons que A et B soient deux parties de E telles que $A\Delta B = A \cap B$.
Par la question 2, on a toujours $(A\Delta B) \cap (A \cap B) = \emptyset$.
Mais si ces deux ensembles sont égaux, leur intersection est $A\Delta B$, de sorte que $A\Delta B = \emptyset$. Et donc $A \cap B$ est également vide.
Or

$$(A\Delta B) \cup (A \cap B) = \underbrace{\left((A \cup B) \cap (\overline{A \cap B})\right)}_{=A\cup B} \cup (A \cap B)$$
$$= ((A \cup B) \cup (A \cap B)) \cap \underbrace{\left(\overline{A \cap B} \cup (A \cap B)\right)}_{=E} = A \cup B.$$

Donc $A \cup B = (A\Delta B) \cup (A \cap B) = \emptyset$.
Et donc $A \subset A \cup B = \emptyset$, de sorte que $A \subset A \cup B = \emptyset$, et donc $A = \emptyset$, et de même $B = \emptyset$.
Donc $\boxed{A = B = \emptyset.}$

Une solution plus «pédestre» est possible[3] : supposons par l'absurde que $A \neq \emptyset$. Alors il existe $x \in A$.
▶ Si $x \in B$, alors $x \in A \cap B$, et donc $x \in A\Delta B$. Mais ceci est absurde puisque $x \in A$ **et** $x \in B$, donc x n'est ni dans $A \setminus B$ ni dans $B \setminus A$, donc pas dans leur union $A\Delta B$.
▶ Si $x \notin B$, alors $x \notin A \cap B$. Mais $x \in A$ **et** $x \notin B$, de sorte que $x \in A\Delta B = A \cap B$. Là encore, c'est absurde, et on en déduit donc que A est vide.
Et le même raisonnement prouverait que B est également vide.

[3] Et finalement plus rapide.

▸ Problème : inversion circulaire et points rationnels des cercles

Partie I. Image d'un cercle par l'inversion

1. Soit $z \in \mathbf{C}^*$. Alors $(f \circ f)(z) = \dfrac{1}{f(z)} = \frac{1}{\frac{1}{z}} = \boxed{z.}$

2. Si $z \in A$, alors par définition[4] $f(z) \in f(A)$.
Inversement, si $f(z) \in f(A)$, alors il existe $y \in A$ tel que $f(z) = f(y)$.
Mais alors en appliquant f aux deux membres, il vient $f(f(z)) = f(f(y))$, soit encore $z = y$. Et par conséquent, $z \in A$.
Ceci prouve donc que $\boxed{z \in A \Leftrightarrow f(z) \in f(A).}$

[4] L'ensemble $f(A)$ est formé des éléments de $\mathbf{C}^*$ qui ont au moins un antécédent par f dans A. C'est évidemment le cas de $f(z)$ dont z est un antécédent.

En particulier, si on applique ceci à $f(z)$, il vient $f(z) \in A \Leftrightarrow f(f(z)) \in f(A)$.
Or $f(f(z)) = z$, si bien que $\boxed{f(z) \in A \Leftrightarrow z \in f(A).}$

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

$$|z-\omega|^2 = (z-\omega)\overline{(z-\omega)} = (z-\omega)(\overline{z}-\overline{\omega}) = z\overline{z} - \overline{\omega}z - \omega\overline{z} + \omega\overline{\omega} = |z|^2 - \overline{\omega}z - \omega\overline{z} + |\omega|^2.$$

Et donc

$$z \in \mathscr{C}_{\omega,r} \Leftrightarrow |z-\omega| = r \Leftrightarrow |z-\omega|^2 = r^2 \Leftrightarrow |z|^2 - \overline{\omega}z - \omega\overline{z} + |\omega|^2 - r^2 = 0.$$

Et puisqu'on a raisonné par équivalence, on a donc

$$\mathscr{C}_{\omega,r} = \left\{z \in \mathbf{C} \mid |z|^2 - \overline{\omega}z - \omega\overline{z} + |\omega|^2 - r^2 = 0\right\}.$$

> **Rappel**
> Deux ensembles A et B sont égaux si et seulement si pour tout z,
> $$z \in A \Leftrightarrow z \in B.$$

4.a. Notons que puisque $0 \notin \mathscr{C}$, alors $|0-\omega| \neq r$, soit encore $|\omega|^2 \neq r^2$. Soit $z \in \mathbf{C}^*$. Alors par la question 2, $z \in f(\mathscr{C})$ si et seulement si $f(z) \in \mathscr{C}$.
Soit si et seulement si $\left|\frac{1}{\overline{z}}\right|^2 - \overline{\omega}\frac{1}{\overline{z}} - \omega\frac{1}{z} + |\omega|^2 - r^2 = 0 \quad (\star)$.
D'autre part, z appartient au cercle $\mathscr{C}'$ de centre d'affixe $-\dfrac{\omega}{r^2-|\omega|^2}$ et de rayon $\dfrac{r}{|r^2-|\omega|^2|}$ si et seulement si $|z|^2 + \dfrac{\overline{\omega}}{r^2-|\omega|^2}z + \dfrac{\omega}{r^2-|\omega|^2}\overline{z} + \underbrace{\dfrac{|\omega|^2}{(r^2-|\omega|^2)^2} - \dfrac{r^2}{(r^2-|\omega|^2)^2}}_{=\frac{1}{|\omega|^2-r^2}} = 0.$
Mais en multipliant $(\star)$ par $z\overline{z} = |\overline{z}|^2$, on a $f(z) \in \mathscr{C}$ si et seulement si

$$1 - \overline{\omega}z - \omega\overline{z} + \left(|\omega|^2 - r^2\right)|z|^2 = 0.$$

Soit si et seulement si[5] $|z|^2 + \dfrac{\overline{\omega}}{|r^2-\omega|^2}z + \dfrac{\omega}{r^2-|\omega|^2}\overline{z} + \dfrac{1}{|\omega|^2-r^2} = 0.$
Et donc $z \in f(\mathscr{C}) \Leftrightarrow z \in \mathscr{C}'$, si bien que $f(\mathscr{C}) = \mathscr{C}'$, comme demandé.

[5] En divisant la relation précédente par $|\omega|^2 - r^2$.

4.b. Si $0 \in \mathscr{C}$, alors $|0-\omega| = r \Leftrightarrow |\omega| = r \Leftrightarrow |\omega|^2 = r^2$.
Et donc pour $z \in \mathbf{C}^*$, on a $z \in f(\mathscr{C} \setminus \{0\}) \Leftrightarrow f(z) \in \mathscr{C} \setminus \{0\}$, soit encore si et seulement si

$$\left|\frac{1}{\overline{z}}\right|^2 - \frac{\overline{\omega}}{z} - \frac{\omega}{z} = 0.$$

Après multiplication par $|z|^2 = z\overline{z}$, c'est le cas si et seulement si $1 - \overline{\omega}z - \omega\overline{z} = 0$.
Soit si et seulement si $2\,\mathrm{Re}\,(\overline{\omega}z) = \overline{\omega}z + \omega\overline{z} = 1$.
Notons alors z sous forme algébrique : $z = x + iy$, avec $x, y \in \mathbf{R}$, et de même, $\omega = \omega_1 + i\omega_2$, avec $\omega_1, \omega_2 \in \mathbf{R}$.
Alors $\mathrm{Re}\,(\overline{\omega}z) = \mathrm{Re}\,((\omega_1 - i\omega_2)(x+iy)) = x\omega_1 + y\omega_2$.
Et donc $z \in f(\mathscr{C} \setminus \{0\}) \Leftrightarrow \omega_1 x + \omega_2 y = 1$.
Il s'agit bien là de l'équation d'une droite du plan.

> **Remarque**
> Notons que cette droite ne passe pas par l'origine.

Partie II. Points rationnels des cercles

5. Si $z \in \mathbf{Q}(i)$, notons $z = x + iy$, avec $x, y \in \mathbf{Q}$ non tous deux[6] nuls.
Alors $f(z) = \dfrac{1}{x-iy} = \dfrac{x+iy}{x^2+y^2} = \dfrac{x}{x^2+y^2} + i\dfrac{y}{x^2+y^2} \in \mathbf{Q}(i)$.
Et inversement, si $f(z) \in \mathbf{Q}(i)$, alors $z = f(f(z)) \in \mathbf{Q}(i)$.
Donc on a bien $\boxed{z \in \mathbf{Q}(i) \Leftrightarrow f(z) \in \mathbf{Q}(i).}$

[6] L'un des deux peut être nul, mais pas les deux à la fois.

6. Soit $\mathscr{D}$ une droite du plan, et supposons qu'elle contienne deux points rationnels A et B, de coordonnées (x_A, y_A) et (x_B, y_B).
Si $x_A = x_B$, alors $\mathscr{D}$ est verticale, d'équation $x = x_A$.
Et particulier, pour tout $r \in \mathbf{Q}$, le point de coordonnées (x_A, r) appartient à $\mathscr{D}$, et puisque $x_A \in \mathbf{Q}$, $\mathscr{D}$ contient une infinité de points rationnels.
Si $x_A \neq x_B$, alors une équation de $\mathscr{D}$ est $y = \dfrac{y_B - y_A}{x_B - x_A}(x - x_A) + y_A$.
Puisque A et B sont rationnels, $\dfrac{y_B - y_A}{x_B - x_A} \in \mathbf{Q}$, et donc une équation de $\mathscr{D}$ est de la forme $y = mx + p$, avec $m, p \in \mathbf{Q}$.
Et par conséquent, pour tout $r \in \mathbf{Q}$, le point de coordonnées $(r, mr + p)$ est un point rationnel, qui appartient à $\mathscr{D}$.
Donc $\boxed{\mathscr{D} \text{ possède une infinité de points rationnels.}}$

7. Soit $\mathscr{C}$ un cercle qui contient O et deux autres points rationnels A et B.
Alors $\mathscr{D} = f(\mathscr{C} \setminus \{0\})$ est une droite, qui contient au moins les deux points rationnels[7] $f(A)$ et $f(B)$.
Donc par la question précédente, $f(\mathscr{C} \setminus \{0\})$ contient une infinité de points rationnels.
Mais, toujours d'après la seconde équivalence de la question 2 pour $z \in \mathscr{D} = f(\mathscr{C} \setminus \{0\})$, on

[7] La question 5 nous garantit que l'image d'un point rationnel par f est un point rationnel.

a $f(z) \in \mathscr{C} \setminus \{0\}$. Puisque l'image par f d'un point rationnel est encore un point rationnel, pour $z \in \mathscr{D} \cap \mathbf{Q}(i)$, $f(z) \in \mathscr{C} \cap \mathbf{Q}(i)$.
Donc puisque $\mathscr{D} \cap \mathbf{Q}(i)$ est infini, il en est de même de $\mathscr{C} \cap \mathbf{Q}(i)$.
Donc $\boxed{\mathscr{C} \text{ contient une infinité de points rationnels.}}$

Remarque
Il est bon de noter que f ne prend jamais deux fois la même valeur. Donc des points distincts de $\mathscr{D} \cap \mathbf{Q}(i)$ sont envoyés par f sur des points distincts de $\mathscr{C} \cap \mathbf{Q}(i)$. C'est cela qui garantit que même application de f, on a bien une infinité de points.

8. Soit $\mathscr{C}$ un cercle de centre d'affixe ω et de rayon $r > 0$ ne passant par O et possédant trois points rationnels A, B, C, d'affixes respectives a, b, c.
Notons $\mathscr{C}'$ le cercle de centre d'affixe $\omega - a$ et de rayon r.
Alors $\mathscr{C}'$ contient O (car $|0 - (\omega - a)| = |a - \omega| = r$), et contient au moins deux autres points rationnels, à savoir $b - a$ et $c - a$.

Remarque
$\mathscr{C}'$ n'est rien d'autre que l'image de $\mathscr{C}$ par la translation de vecteur $-a$. En effet, celle-ci préserve les distances (car son «coefficient directeur» (en tant que fonction affine de $\mathbf{C}$ dans $\mathbf{C}$) vaut 1), donc envoie les cercles sur des cercles de même rayon. Elle envoie ω sur $\omega - a$, et elle envoie A sur O.

Donc par ce qui précède, $\mathscr{C}'$ contient une infinité de points rationnels.
Mais si z est un point rationnel de $\mathscr{C}'$, alors $z + a$ est un point rationnel de $\mathscr{C}$. En effet, si $|z - (\omega - a)| = r$, alors $|(z + a) - \omega| = r$, et si $z \in \mathbf{Q}(i)$, puisque $a \in \mathbf{Q}(i)$, $z + a \in \mathbf{Q}(i)$.
Et donc $\mathscr{C}'$ contenant une infinité de points rationnels, il en est de même de $\mathscr{C}$.

Partie III. Une caractérisation des cercles qui possèdent une infinité de points rationnels

9.a. Notons z_1, z_2 les solutions complexes (éventuellement confondues) de $ax^2 + bx + c = 0$.
Quitte à échanger z_1 et z_2, on peut supposer que $z_1 \in \mathbf{Q}$. Alors par les relations entre racines et coefficients, $z_1 + z_2 = -\dfrac{b}{a} \in \mathbf{Q}$. Et donc $z_2 = -\dfrac{b}{a} - z_1 \in \mathbf{Q}$.
Donc $\boxed{\text{toutes les solutions complexes de } ax^2 + bx + c = 0 \text{ sont rationnelles.}}$

Remarque : il aurait été possible de revenir à la forme de z_1, z_2 en fonction du discriminant Δ, et de prouver que celui-ci est tel que $\sqrt{\Delta} \in \mathbf{Q}$. Mais l'argument ci-dessus nous évite des calculs, et pourra se généraliser plus tard (lorsque nous aurons des relations racines-coefficients pour les polynômes de degré plus grand que 2) pour prouver par exemple que si un polynôme de degré 3, à coefficients dans $\mathbf{Q}$, possède deux racines rationnelles, alors la troisième racine (si elle existe) est également rationnelle.

9.b. Supposons donc que $\mathscr{D}$ possède une équation de la forme $y = ax + b$, avec $a \in \mathbf{Q}^*$.
En particulier, si on note (x_A, y_A) les coordonnées de A, $y_A = ax_A + b$, si bien que $b = y_A - ax_A \in \mathbf{Q}$.
Les points de $\mathscr{D}$ ont donc pour coordonnées $(x, ax + b)$, avec $x \in \mathbf{R}$.
Un tel point est dans $\mathscr{C} \cap \mathscr{D}$ si et seulement si

$$(x - x_\Omega)^2 + (ax + b - y_\Omega)^2 = r^2$$

Détails
On a supposé $x_A, y_A \in \mathbf{Q}$ car A est rationnel et $a \in \mathbf{Q}$ par hypothèse.

où $\Omega = (x_\Omega, y_\Omega)$ est le centre de $\mathscr{C}$ et r son rayon.
Soit encore si et seulement si $(a^2 + 1)x^2 - (2x_\Omega + 2a(b - y_\Omega))x + x_\Omega^2 + (b - y_\Omega)^2 = r^2 \quad (E)$.
Puisque $A \in \mathscr{C}$, et que A et Ω sont rationnels, $r^2 = (x_A - x_\Omega)^2 + (y_A - y_\Omega)^2 \in \mathbf{Q}$.
Et donc l'équation (E) est de degré 2, à coefficients rationnels.
Elle possède une solution rationnelle x_A, et donc possède au plus une autre solution x_B, qui est aussi rationnelle.
Et donc $\mathscr{C} \cap \mathscr{D}$ est soit réduit à $\{A\}$ (dans le cas où x_A est la seule solution de (E)), soit égal à $\{A, B\}$ où B est le point de coordoonées $(x_B, ax_B + b)$, qui est un point rationnel.

10. Soit $s : z \mapsto az + b$ une similitude directe rationnelle, avec $a, b \in \mathbf{Q}(i)$ et $a \neq 0$.
En utilisant la forme algébrique, il est facile de constater[8] que pour $z, z' \in \mathbf{Q}(i)$, on a $z + z' \in \mathbf{Q}(i)$, $zz' \in \mathbf{Q}(i)$, et si $z' \neq 0$, alors $\frac{z}{z'} \in \mathbf{Q}(i)$.
Donc en particulier, si $z \in \mathbf{Q}(i)$, alors $s(z) = az + b \in \mathbf{Q}(i)$.
Et inversement, si $f(z) \in \mathbf{Q}(i)$, alors $z = \dfrac{f(z) - b}{a} \in \mathbf{Q}(i)$.
Donc par double implication, $\boxed{z \in \mathbf{Q}(i) \Leftrightarrow s(z) \in \mathbf{Q}(i).}$

[8] Car la somme, le produit, le quotient de deux rationnels est un rationnel.

Remarque
Nous dirons plus tard que $\mathbf{Q}(i)$ est un **corps**.

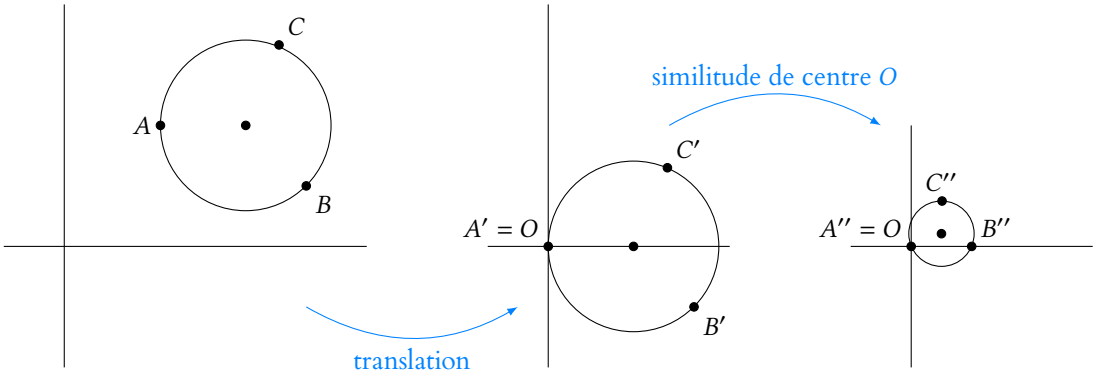
11.a. Commençons par remarquer que si s est une similitude directe de la forme $z \mapsto az + b$, et si $\mathscr{C}$ est le cercle de centre d'affixe ω et de rayon r, alors $f(\mathscr{C})$ est le cercle de centre $s(\omega)$ et de rayon $|a|r$.
En effet, on a

$$z \in \mathscr{C} \Leftrightarrow |z - \omega| = r \Leftrightarrow \left|\frac{az + b}{a} - \frac{b}{a} - \omega\right| = r \Leftrightarrow |az + b - (a\omega + b)| = r|a|$$

donc si et seulement si $s(z)$ appartient au cercle de centre $a\omega + b = s(\omega)$ et de rayon $|a|r$.
Ainsi, quelle que soit la similitude directe s choisie, $s(\mathscr{C})$ sera un cercle.

Notons z_A, z_B, z_C les affixes de A, B, C.
Nous pourrions chercher $a, b \in \mathbf{Q}(i)$ tels que $az_A + b = 0$ et $az_B + b = 1$, ce qui nous conduit à la résolution d'un système, qui possède bien une unique solution dans $\mathbf{C}^2$, qui est de plus dans $\mathbf{Q}(i)^2$.

Mais plus géométriquement, la translation de vecteur $-z_A$ envoie A sur O et B sur le point d'affixe $z_B - z_A$.
Si on compose par la similitude directe $z \mapsto \dfrac{1}{z_B - z_A} z$, qui laisse O fixe et envoie le point d'affixe $z_B - z_A$ sur le point d'affixe 1, on obtient bien une similitude directe rationnelle car composée de deux similitudes rationnelles, qui envoie $\mathscr{C}$ sur un cercle qui contient O (image de A), 1 (image de B) et un troisième point rationnel, qui est l'image de C.



Autrement dit, la similitude directe $s : z \mapsto \dfrac{1}{z_B - z_A}(z - z_A)$ envoie z_A sur 0, z_B sur 1.
Puisqu'elle est rationnelle[9], elle envoie le point rationnel C sur un point rationnel, dont l'affixe n'est ni 0 ni 1 (puisque c'est $\dfrac{z_C - z_A}{z_B - z_A}$).

[9] Car z_A, z_B sont dans $\mathbf{Q}(i)$

Géométriquement

Ce centre est sur la médiatrice du segment joignant les points d'affixes 0 et 1.
Cette médiatrice est clairement la droite d'équation $x = \frac{1}{2}$.

11.b. Le centre Ω' de $\mathscr{C}'$, d'affixe $\omega' = x + iy$, vérifie $|0 - \omega'| = |1 - \omega'|$.
Donc $x^2 + y^2 = (1-x)^2 + y^2 \Leftrightarrow x^2 + y^2 = 1 - 2x + x^2 + y^2 \Leftrightarrow 1 - 2x = 0 \Leftrightarrow x = \frac{1}{2}$.
De plus, $|z_{C'} - \omega'| = |\omega'|$, et donc

$$\left(x_{C'} - \frac{1}{2}\right)^2 + (y_{C'} - y)^2 = \frac{1}{2^2} + y^2 \Leftrightarrow x_{C'}^2 - x_{C'} + y_{C'}^2 - 2yy_{C'} = 0.$$

Cette équation[10] d'inconnue y possède une unique solution, et puisque $x_{C'}$ et $y_{C'}$ sont rationnels, cette solution l'est aussi.
Donc Ω' est un point rationnel.

[10] De degré 1

Puisque $\omega' = s(\omega) \in \mathbf{Q}(i)$, par la question 10, $\omega \in \mathbf{Q}(i)$.
Donc $\boxed{\Omega \text{ est un point rationnel.}}$

12. Si $\mathscr{C}$ contient une infinité de points rationnels, alors il en contient au moins trois. Et donc par la question 11, son centre est rationnel.
Et donc $\mathscr{C}$ vérifie la propriété ii).

Inversement, si $\mathscr{C}$ possède un centre rationnel et au moins un point rationnel A.
Alors par la question 9, pour tout rationnel a, la droite $\mathscr{D}_a$ d'équation $y = ax + b$, qui passe par A coupe $\mathscr{C}$ en un autre point rationnel, sauf dans le cas où où $\mathscr{C} \cap \mathscr{D}_a = \{A\}$.
Ceci ne se produira que si l'équation (E) de la question 11.b possède un discriminant nul.
Or ce discriminant est un polynôme de degré au plus 2 en a, donc il s'annule au plus deux fois.
Donc il existe une infinité de valeurs de a pour lesquelles $\mathscr{D}_a \cap \mathscr{C}$ contient deux points rationnels. Pour un tel a, notons B_a le point de $\mathscr{D}_a \cap \mathscr{C}$ distinct de A.
Ces points sont deux à deux distincts puisque si $B_a = B_{a'}$, alors les droites $\mathscr{D}_a$ et $\mathscr{D}_{a'}$ passent toutes les deux par A et par B_a, donc ont même équation, et donc même pente.
Ainsi, $\boxed{\text{il existe une infinité de points rationnels sur } \mathscr{C}.}$

Remarque

Avec un peu plus de courage, on prouverait qu'en fait il s'agit d'un polynôme de degré 1 en a, qui s'annule donc une seule fois. C'est le cas lorsque a est la pente de la tangente à $\mathscr{C}$ en le point A, qui est la seule droite qui passe par A et qui ne rencontre qu'une seule fois $\mathscr{C}$.

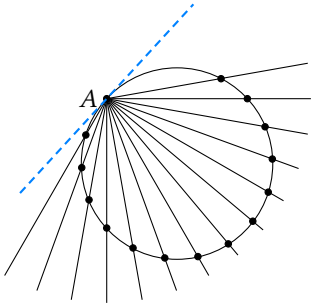


FIGURE 0.1 – Une machine à fabriquer des points rationnels : l'intersection avec des droites de pente rationnelle passant par un point rationnel.
Seule la tangente au cercle en ce point (en pointillés) ne donne pas de nouveau point rationnel.

13. Notons que $a^2+b^2=c^2 \Leftrightarrow \left(\frac{a}{c}\right)^2+\left(\frac{b}{c}\right)^2=1$.

C'est le cas si et seulement si $\left(\frac{a}{c},\frac{b}{c}\right)$ appartient au cercle trigonométrique.

Or le cercle trigonométrique possède une infinité de points rationnels, puisque son centre O est rationnel et que $(1,0)$ en est un point rationnel.

Et si $\left(\frac{p_1}{q_1},\frac{p_2}{q_2}\right)$ est un point rationnel du cercle trigonométrique, on a alors $p_1^2q_2^2+p_2^2q_1^2=q_1^2q_2^2$.
Notons alors d le pgcd de p_1q_2 et de p_2q_1, de sorte qu'il existe deux entiers a et b, premiers entre eux, tels que $p_1q_2=da$ et $p_2q_1=db$.
Alors $a^2+b^2=\left(\frac{q_1q_2}{d}\right)^2$.
Puisque a et b sont entiers, $\left(\frac{q_1q_2}{d}\right)^2$ est entier.
Or si un rationnel r possède un carré entier, c'est nécessairement un entier.
En effet, si on note $r=\frac{p}{q}$ avec p,q premiers entre eux, alors $\frac{p^2}{q^2}$ est entier, donc q^2 divise p^2.
Donc q divise p^2.
Or q est premier avec p, donc par le lemme de Gauss, q divise p.
Donc q divise p et q, il divise leur pgcd qui vaut 1. Donc $q=1$, si bien que $\frac{q_1q_2}{d}$, est un entier c, et on a alors $a^2+b^2=c^2$, avec a et b premiers entre eux.
Autrement dit, à tout point rationnel du cercle trigonométrique correspond un triplet $(a,b,c)\in\mathbf{Z}^3$ tel que a et b soient premiers entre eux et tel que $a^2+b^2=c^2$.

Gauss
Rappelons que le lemme de Gauss dit que si a divise bc et que a est premier avec b, alors a divise c.

Reste à vérifier que deux points rationnels distincts donnent deux triplets distincts
Avec les notations précédentes, on a $\frac{a}{c}=\frac{\frac{p_1q_2}{d}}{\frac{q_1q_2}{d}}=\frac{p_1}{q_1}$, et de même $\frac{b}{c}=\frac{p_2}{q_2}$, donc le triplet (a,b,c) construit détermine de manière unique le point rationnel de départ, si bien qu'il existe une infinité de triplets $(a,b,c)\in\mathbf{Z}^3$ avec a et b premiers entre eux et $a^2+b^2=c^2$.

Commentaire *: les tirplets que nous venons de construire s'appelent les triplets pythagoriciens primitifs. Il est en fait possible, avec un peu d'arithmétique, de décrire explicitement tous les tels triplets.*
Tout triplet $(a,b,c)\in\mathbf{Z}^3$ tel que $a^2+b^2=c^2$ est de la forme (ma',mb',mc'), avec $m\in\mathbf{Z}$ et (a',b',c') triplet pythagoricien primitif.

Subtilité.
À ce stade, il se pourrait encore que tous les points rationnels donnent le même triplet, ce qui ne nous permettrait donc pas d'en déduire l'existence d'une infinité de tels triplets.