

Devoir à la maison n°4 – À rendre le mardi 25 février 2020

Points rationnels sur des droites et des cercles rationnels

Dans toute la suite, le plan est muni d'un repère orthonormé $(O; \vec{i}, \vec{j})$.

On dit qu'un point $M(x_M; y_M)$ est rationnel si x_M et y_M sont deux nombres rationnels et que M est entier si x_M et y_M sont deux nombres entiers relatifs.

Partie A. — Droites rationnelles

Une droite rationnelle est une droite $\mathcal{D}$ ayant une équation de la forme $y = mx + p$ où m et p sont des nombres rationnels. Par exemple, $\mathcal{D} : y = \frac{1}{3}x + \frac{3}{4}$ est une droite rationnelle mais $\mathcal{D}' : y = \sqrt{2}x + 1$ n'est pas une droite rationnelle car $\sqrt{2} \notin \mathbb{Q}$.

1. Soit $\mathcal{D}$ une droite rationnelle dont le coefficient directeur est non nul et $M(x_M; y_M)$ un point de $\mathcal{D}$. Montrer que les trois assertions suivantes sont équivalentes :

(1) M est un point rationnel ; (2) $x_M \in \mathbb{Q}$; (3) $y_M \in \mathbb{Q}$.

On s'intéresse à présent aux points entiers appartenant à une droite rationnelle.

2. Un exemple

On considère la droite $\Delta : y = \frac{2}{3}x - \frac{4}{5}$.

a. Montrer que, pour tout $(u; v) \in \mathbb{Z}^2$, $10u - 15v$ est divisible par 5.

b. La droite Δ passe-t-elle par un point entier ?

3. Cas général

On considère une droite rationnelle $\mathcal{D} : y = mx + p$. On écrit $m = \frac{a}{b}$ et $p = \frac{c}{d}$ sous forme de fractions irréductibles.

a. On suppose que $M(x_M; y_M)$ est un point entier appartenant à $\mathcal{D}$.

Montrer que d divise bc et en déduire que d divise b .

b. Réciproquement, on suppose que d divise b .

Justifier qu'il existe trois entiers k , u et v tels que $au + kdv = 1$ et en déduire que $\mathcal{D}$ passe par un point entier.

c. Quelle propriété a-t-on démontrée dans les deux questions précédentes ?

Partie B. — Cercles rationnels

Un cercle rationnel est un cercle $\mathcal{C}$ ayant une équation de la forme $(x - x_0)^2 + (y - y_0)^2 = R^2$ où x_0 , y_0 et R^2 sont des nombres rationnels. Ainsi, $\mathcal{C} : (x - \frac{1}{2})^2 + (y - \frac{2}{3})^2 = \sqrt{2}^2$ est un cercle rationnel mais $\mathcal{C}' : (x - \sqrt{2})^2 + (y - \frac{2}{3})^2 = 2^2$ n'est pas un cercle rationnel.

1. Un résultat préliminaire

Dans toute la suite du devoir, on pourra utiliser le résultat suivant vu en exercice en cours : si a et b sont deux entiers non tous les deux nuls et si $d = \text{PGCD}(a, b)$ alors $\frac{a}{d}$ et $\frac{b}{d}$ sont deux entiers premiers entre eux.

a. Soit u et v deux entiers premiers entre eux.

Montrer que u^2 et v^2 sont premiers entre eux.

b. Soit a et b deux entiers non tous les deux nuls.

Déduire de la question précédente que si a^2 divise b^2 alors a divise b .

2. Points entiers non triviaux sur un cercle de rayon entier centré en O

Soit $n \in \mathbb{N}^*$. On considère le cercle $\mathcal{C}_n : x^2 + y^2 = n^2$. Le cercle $\mathcal{C}_n$ passe par les points entiers de coordonnées $(n; 0)$, $(-n; 0)$, $(0; n)$ et $(0; -n)$. Ces 4 points sont appelés les points entiers triviaux de $\mathcal{C}_n$. On s'intéresse dans la suite à l'existence de points entiers non triviaux sur le cercle $\mathcal{C}_n$.

Supposons que $M(x_M; y_M)$ soit un point entier sur $\mathcal{C}_n$ avec $x_M \neq 0$ et $y_M \neq 0$.

On note $d = \text{PGCD}(x_M, y_M)$.

a. Justifier qu'on peut toujours se ramener au cas où $x_M > 0$ et $y_M > 0$.

b. Montrer que d divise n .

On pose $a = \frac{x_M}{d}$, $b = \frac{y_M}{d}$ et $c = \frac{n}{d}$. Ainsi, a , b et c sont des entiers strictement positifs tels que $a^2 + b^2 = c^2$.

c. Justifier qu'au moins un des deux nombres a ou b est impair puis, en raisonnant modulo 8, montrer que a et b n'ont pas la même parité.

Dans la suite, on fait l'hypothèse que b est pair. On pose $u = \frac{b}{2}$, $s = \frac{c+a}{2}$ et $t = \frac{c-a}{2}$.

d. Justifier que u , s et t sont des entiers strictement positifs.

e. En considérant $s - t$ et $s + t$, montrer que s et t sont premiers entre eux.

f. Soit $\frac{p}{q}$ l'écriture sous forme de fraction irréductible du rationnel $\frac{u}{t}$.

Montrer que $n = d(p^2 + q^2)$.

g. Réciproquement, soit $d \in \mathbb{N}^*$, p et q deux entiers premiers entre eux tels que $p > q > 0$ et $n = d(p^2 + q^2)$. Montrer que $M(d(p^2 - q^2); 2dpq)$ est un point entier non trivial appartenant à $\mathcal{C}_n$.

h. Le cercle $\mathcal{C}_7$ passe-t-il par des points entiers non triviaux? Et le cercle $\mathcal{C}_{10}$?

3. Points rationnels sur un cercle centré en O et dont le rayon est la racine carrée d'un entier (facultatif)

Soit $n \in \mathbb{N}^*$ et $\mathcal{C}_n : x^2 + y^2 = n$. On va montrer que si $\mathcal{C}_n$ passe par un point rationnel alors il passe par un point entier.

Pour cela, on raisonne par l'absurde en supposant qu'il existe un point rationnel $M(x_M; y_M)$ appartenant à $\mathcal{C}_n$ mais qu'aucun point de $\mathcal{C}_n$ n'est entier. Notons $\mathcal{E}$ l'ensemble des coordonnées des points rationnels de $\mathcal{C}_n$. Si $(x; y) \in \mathcal{E}$, on note c le plus petit dénominateur commun entre x et y . Ainsi, $c \in \mathbb{N}^*$ et il existe deux entiers a et b tels que $x = \frac{a}{c}$ et $y = \frac{b}{c}$.

Enfin, l'ensemble des valeurs prises par c lorsque $(x; y)$ parcourt $\mathcal{E}$ est une partie non vide de $\mathbb{N}^*$: elle admet donc un plus petit élément que nous notons m . Comme aucun point de $\mathcal{C}_n$ n'est entier, $m \geq 2$. Considérons un couple $(x; y) \in \mathcal{E}$ tel qu'il existe deux entiers a et b tels que $x = \frac{a}{m}$ et $y = \frac{b}{m}$ et notons M le point de coordonnées $(x; y)$.

On note u l'entier le plus proche de x , v l'entier le plus proche de y et N le point de coordonnées $(u; v)$. Enfin, on pose $d = MN$.

a. Montrer que $0 < d^2 \leq \frac{1}{2}$.

b. Montrer qu'il existe un entier $m' > 0$ tel que $d^2 = \frac{m'}{m}$ et en déduire que $m' < m$.

c. Montrer que la droite (MN) coupe le cercle $\mathcal{C}_n$ en deux points : le point M et un autre point que l'on note P .

d. Montrer que les coordonnées de P sont de la forme $\frac{c}{m'}$ et $\frac{d}{m'}$ avec $c \in \mathbb{Z}$ et $d \in \mathbb{Z}$.

e. Conclure.