Devoir maison
Entiers quadratiques – Construction à la règle et au compas

Exercice 1. Le but de cet exercice est de déterminer quels entiers $n \in \mathbb{N}$ sont sommes de deux carrés : $n = a^2 + b^2$ avec $a, b \in \mathbb{N}$. On pose $\Sigma = \{n \in \mathbb{N} \,|\, n = a^2 + b^2;\ a, b \in \mathbb{N}\}$.

a. Parmi les entiers de 1 jusque 12 lesquels sont dans Σ.

L'idée est que si $n = a^2 + b^2$ alors $n = (a + ib)(a - ib)$ dans $\mathbb{C}$ et que cette relation à lieu, en fait, dans

$$\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \,|\, a, b \in \mathbb{Z}\}.$$

b. Montrer que si $n \in \mathbb{N}$ est congrue à 3 modulo 4 on a $n \notin \Sigma$.

c. Montrer que $\mathbb{Z}[i]$ est un sous-anneau intègre de $\mathbb{C}$.

On introduit des applications σ et N en posant

$$\begin{array}{rcl} \sigma : \mathbb{Z}[i] & \to & \mathbb{Z}[i] \\ z = a + ib & \mapsto & \overline{z} = a - ib \end{array} \qquad \begin{array}{rcl} N : \mathbb{Z}[i] & \to & \mathbb{N} \\ z = a + ib & \mapsto & z\overline{z} = a^2 - b^2 \end{array}$$

d. Montrer que $z \in \mathbb{Z}[i]$ est inversible si et seulement si $N(z) = 1$ puis déterminer le groupe des inversibles de $\mathbb{Z}[i]$.

e. Montrer que Σ est stable par multiplication. En déduire que l'étude de Σ se ramène à l'étude des nombres premiers de $\mathbb{N}$ qui sont dans Σ.

f. Montrer que pour tout x et y de $\mathbb{Z}[i] \setminus \{0\}$, il existe q et r dans $\mathbb{Z}[i]$ tel qu'on ait $x = yq + r$ avec $N(r) < N(y)$. En déduire que $\mathbb{Z}[i]$ est principal.

Soit $p \in \mathbb{N}$ un nombre premier.

g. Montrer qu'on a $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.

h. Montrer que p n'est pas irréductible dans $\mathbb{Z}[i]$ si et seulement si $\mathbb{Z}[i]/(p)$ est non intègre.

i. Montrer que $\mathbb{Z}[i]$ est isomorphe à $\mathbb{Z}[X]/(X^2 + 1)$.

j. Soit φ l'application de $\mathbb{Z}[i]$ dans $\mathbb{F}_p[X]/(X^2 + 1)$ définie par $\varphi(a + ib) = \overline{\overline{a} + X\overline{b}}$. Montrer que φ est un morphisme surjectif et déterminer son noyau. En déduire l'isomorphisme

$$\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2 + 1).$$

k. En déduire que $p \in \Sigma$ si et seulement si $-1 \in (\mathbb{F}_p^*)^2$.

On a déjà vu (au TD 1) que x est un carré dans $\mathbb{F}_p$ si et seulement si $x^{\frac{p-1}{2}} = 1$.

l. Montrer que -1 est un carré dans $\mathbb{F}_p$ si et seulement si $p = 2$ ou $p \equiv 1 \mod 4$.

m. Conclure.

Exercice 2. On se place dans un plan euclidien $\mathcal{P}$ muni d'un repère orthonormé (O, I, J) qu'on identifie avec le plan complexe $\mathbb{C}$. Soit $\mathcal{E}$ un ensemble de points. On dit qu'un point M est *constructible* à partir de $\mathcal{E}$, si M peut être obtenu comme

– l'intersection de deux droites (AB) et (CD) avec $A, B, C, D \in \mathcal{E}$,

– l'intersection d'une droite(AB) et d'un cercle de centre C et de rayon DE avec $A, B, C, D, E \in \mathcal{E}$,

– l'intersection d'un cercle de centre A et de rayon BC et d'un cercle de centre D et de rayon EF avec $A, B, C, D, E, F \in \mathcal{E}$.

Nous dirons qu'un réel x est *construit* dans $\mathcal{E}$ s'il est l'abscisse d'un point de E. De même nous dirons qu'un complexe z est *construit* à partir de $\mathcal{E}$ s'il est l'affixe d'un point de E.

On dit qu'un réel x (resp un complexe z) est *constructible* s'il existe une suite d'ensemble

$$\{0, I, J\} = \mathcal{E}_0 \subseteq \mathcal{E}_1 \subseteq ... \subseteq \mathcal{E}_n$$

telle que x (resp z) soit construit dans $\mathcal{E}_n$ et telle que pour $i = 1, ..., n-1$ on ait $\mathcal{E}_{i+1} = \mathcal{E}_i \cup \{M_{i+1}\}$ avec M_{i+1} constructible à partir de $\mathcal{E}_i$.

a. Soient x et y deux nombres réels constructibles.

i. Montrer que $-x$ est constructible.

ii. Montrer que $x + y$ est constructible.

iii. Montrer que $x \times y$ est constructible.

iv. Montrer que pour $x \neq 0$ le nombre $\frac{1}{x}$ est constructible.

v. Montrer que si $x > 0$ alors $\sqrt{x}$ est constructible.

On note $\mathcal{C}_\mathbb{R}$ (resp $\mathcal{C}_\mathbb{C}$) l'ensemble des nombres réels (resp. complexes) constructibles.

b. Montrer que $\mathcal{C}_\mathbb{R}$ est un corps et qu'on a $\mathbb{Q} \subseteq \mathcal{C}_\mathbb{R}$.

c. Soit $\mathcal{E}$ un ensemble de point et $M = (x_M, y_M)$ un point constructible à partir de $\mathcal{E}$. On note $X_\mathcal{E}$ l'ensemble des abscisses des point de $\mathcal{E}$. On pose $K = \mathbb{Q}(X_\mathcal{E})$ et $L = K(x_M)$.

i. Montrer que tout élément de L est constructible, *i.e.*, $L \subseteq \mathcal{C}_\mathbb{R}$.

ii. Montrer qu'on a soit $L = K$ soit il existe $\alpha \in K$ tel que $L = K(\sqrt{\alpha})$.

iii. Quelle(s) valeur(s) peut prendre $[L : K]$?

d. Montrer qu'un nombre réel x est constructible seulement si le degré de $\mathbb{Q}(x)/\mathbb{Q}$ est une puissance de 2.

e. En déduire que parmi les nombres réels seuls les algébriques sont constructibles.

f. Parmi les réels $\frac{1+\sqrt{5}}{2}$, $\sqrt[3]{2}$, $\sqrt{2+\sqrt{3}}$, π, lesquels sont constructibles ? Justifier vos réponses.

g. Soit α un réel tel que $\mathbb{Q}(\alpha)/\mathbb{Q}$ soit une extension galoisienne. On suppose de plus que son groupe de Galois $G = \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ est 2-résoluble. Montrer que α est constructible.

h. Soit $\zeta_n = e^{\frac{2i\pi}{n}}$ une racine primitive n-ème de l'unité. On pose $x_n = \mathrm{Re}(\zeta_n)$, $y_n = \mathrm{Im}(\zeta_n)$ et $K_n = \mathbb{Q}(x_n)$

i. Montrer que K_n est une sous-extension de $\mathbb{Q}(\zeta_n)$ contenant $\mathbb{Q}$.

ii. Déterminer $\alpha \in \mathbb{Q}(\zeta_n)$ tel que $\mathbb{Q}(\zeta_n) = K_n(\alpha)$.

iii. En déduire que $\mathbb{Q}(\zeta_n)$ est une extension quadratique de K_n.

iv. Après avoir remarqué que l'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est galoisienne, montrer que l'extension $K_n/\mathbb{Q}$ est galoisienne.

i. On dit que le polygone régulier P_n à n côtés est constructible si le complexe ζ_n l'est.

i. Montrer que le polygone P_n est constructible si et seulement si x_n l'est.

ii. Montrer que le groupe de Galois $\mathrm{Gal}(K_n, \mathbb{Q})$ est 2-résoluble si et seulement si $\varphi(n)$ est une puissance de 2.

iii. En déduire que P_n est constructible si et seulement si $\varphi(n)$ est une puissance de 2.

j. Nous cherchons à déterminer les entiers naturels n tels que $\varphi(n)$ soit une puissance de 2.

i. Soit n et m deux entiers premiers entre eux. Montrer que $\varphi(nm)$ est une puissance de 2 si et seulement si $\varphi(n)$ et $\varphi(m)$ le sont.

ii. Soit $k \in \mathbb{N}$, montrer que $\varphi(2^k)$ est un puissance de 2.

iii. Soit p un premier $\neq 2$ et k un entier. Montrer que $\varphi(p^k)$ est une puissance de 2 si et seulement si $k = 1$ et p est un premier de Fermat (p est un premiers de Fermat si $p-1$ est une puissance de 2. A ce jour, les seuls premier de Femat connus sont $3, 5, 17, 257$ et 65537).

iv. En déduite les valeurs de $n \in \mathbb{N}$ tel que P_n soit constructible à la règle et au compas.