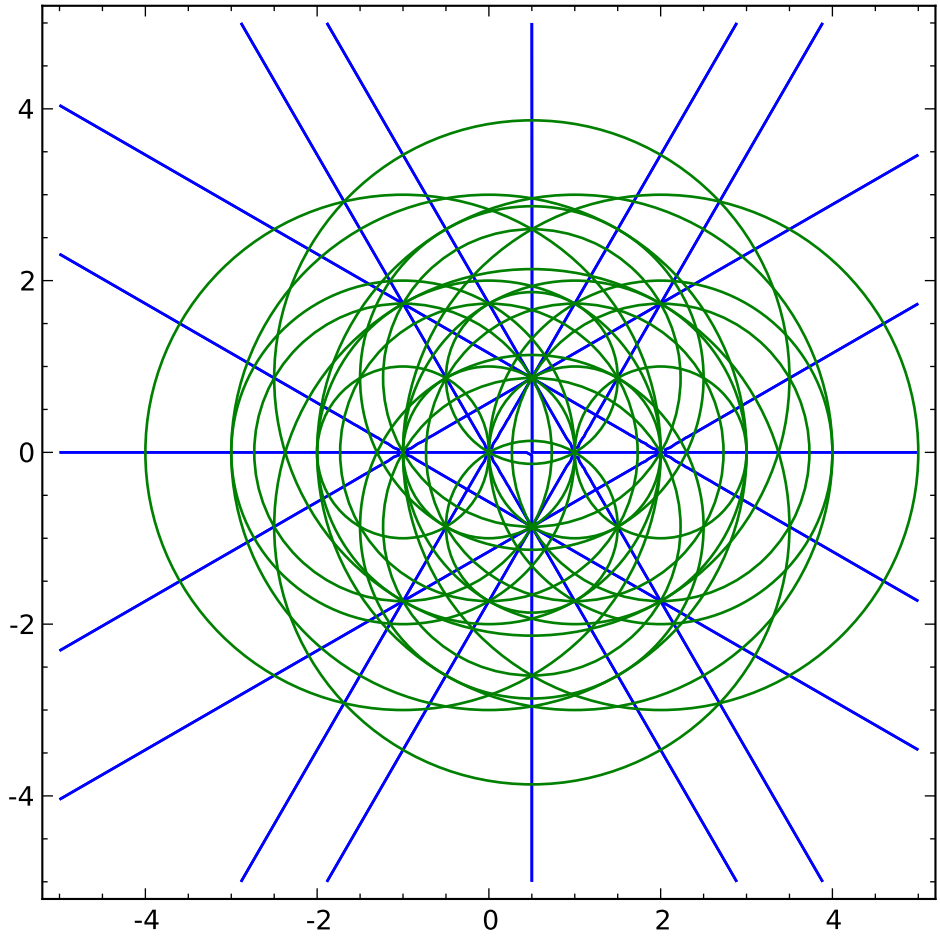

FIGURE 1 – l'ensemble P_2 est l'ensemble des intersections de droites et de cercles de ce dessin

Fiche IX : Construction à la règle et au compas

On définit par récurrence des parties du plan $\mathbb{R}^2$ identifié avec $\mathbb{C}$:

$P_0 := \{0, 1\}$ et P_n est l'ensemble des points obtenus comme l'intersection d'une droite joignant deux points de P_{n-1} avec une autre droite joignant deux points de P_{n-1} ou d'une droite joignant deux points de P_{n-1} avec un cercle centré en un point de P_{n-1} et de rayon la distance entre deux points de $n-1$ ou entre deux tels cercles. On s'autorise des cercles de centre 0 de sorte que $P_{n-1} \subseteq P_n$.

Par exemple :

On dira qu'un $z \in \mathbb{C}$ est *constructible à la règle*[†] *et au compas* ou *construc-*

†. *sous-entendu : non graduée*

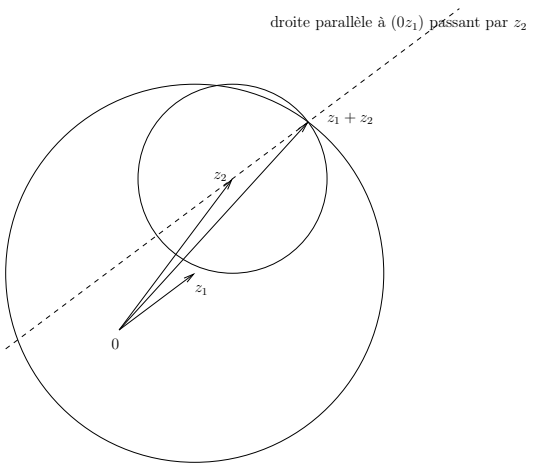

FIGURE 2 – somme

tible si $z \in \cup_{n\geq 0} P_n$. On dira qu'une droite joignant deux points constructible est constructible.

2) Si z_1, z_2 $z_1 + z_2$ est constructible : en effet si on peut construire le cercle de centre z_1 et de rayon $|z_2|$ et le cercle de centre z_2 et de rayon $|z_1|$. Une des intersections de ces deux cercles est $z_1 + z_2$. Il est facile aussi de construire $z_1 + z_2$.

En particulier on peut construire la droite parallèle à la droite (Oz_1) passant par z_2. On en déduit que l'on peut construire la droite parallèle à une droite constructible passant par un point constructible. On en déduit grâce au théorème de Thalès que si $r_1, r_2 > 0$ sont des réels constructibles que $r_1 r_2$ et r_1/r_2 sont constructibles.

Si $z_1 = r_1 e^{it_1}, z_2 = r_2 e^{it_2}$ sont des complexes constructibles ($r_i > 0, t_i \in \mathbb{R}$), alors $r_1, r_2, r_1 r_2$ sont constructibles tout comme e^{it_1}, e^{it_2}. Il est facile de construire $\cos t_i, \sin t_i$, $i = 1, 2$ et donc :

$$\cos(t_1 + t_2) = \cos t_1 \cos t_2 - \sin t_1 \sin t_2$$

de là, il est facile de construire $e^{i(t_1+t_2)}$ et donc $z_1 z_2 = r_1 r_2 e^{i(t_1+t_2)}$. Le produit de deux nombres constructibles est donc constructible. De même le quotient de deux nombres constructibles est constructible. Donc l'ensemble $\mathscr{C}$ des nombres constructibles est un sous corps de $\mathbb{C}$.

3)

Le dessin 4 montre que la racine carrée d'un nombre réel constructible est constructible. Il est facile d'en déduire que les deux racines carrées d'un nombre complexe constructible sont constructibles. Donc $\mathscr{C}$ est stable par

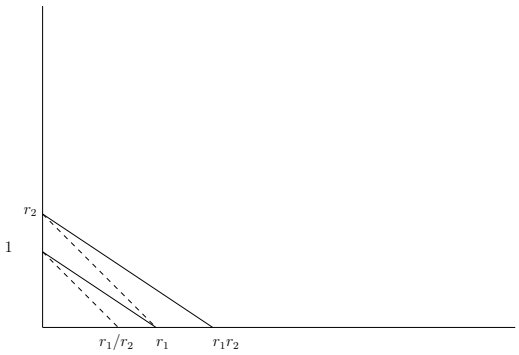

FIGURE 3 – produit

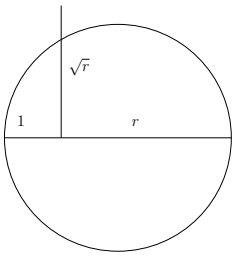

FIGURE 4 – racine carrée

$\sqrt{\ }$. Réciproquement, soit K un sous-corps de $\mathbb{C}$ tel que pour tout $z \in K$, les deux racines carrées de z sont dans K.

Comme K est un corps de caractéristique nulle, K contient $\mathbb{Q}$. Comme K est stable par la racine carrée, K contient aussi $\pm i = \sqrt{-1}$. Montrons que K contient P_n pour tout n, par récurrence. Pour $n = 0$, c'est évident. Supposons $P_n \subseteq K$.

Soient D, D' deux droites construites en joignant deux points de P_n et C, C' deux cercles centrés en des points de P_n et de rayons r, r' deux distances entre deux points de P_n. Nous allons montrer que les intersections

$$D \cap D' \, , \, D \cap C \, , \, C \cap C'$$

sont dans K. Comme tous les points de P_{n+1} s'obtiennent ainsi, on aura montré que $P_{n+1} \subseteq K$.

Il est facile de voir que chaque P_n est symétrique par rapport à l'axe des abscisses ($= \mathbb{R}$). Donc si $z = x + iy \in P_n \subseteq K$, $\overline{z} \in P_n \subseteq K$. Donc $x = \frac{z+\overline{z}}{2}$ et $y = \frac{z-\overline{z}}{2i} \in K$.

Soient $z = x + iy \neq z' = x' + iy' \in P_n$ avec $x, x', y, y' \in \mathbb{R}$. On obtient facilement une équation de la droite (zz') :

$$aX + bY + c = 0$$

avec $a, b, c \in \mathbb{Q}(x, x', y, y') \subseteq K$.

En particulier, si $z, z', w, w' \in P_n \subseteq K$ sont tels que $D = (zz'), D' = (ww')$ alors on peut trouver deux équations :

$$aX + bY + c = 0 \; ; \; a'X + b'Y + c' = 0$$

pour les droites (zz') et (ww') avec $a, b, c, a', b', c' \in K$. L'intersection de ces deux droites a pour coordonnées :

$$\begin{pmatrix} a & b \\ a' & b' \end{pmatrix}^{-1} \begin{pmatrix} -c \\ -c' \end{pmatrix} \in K^2 \; .$$

Une équation de C est de la forme :

$$(X - x_0)^2 + (Y - y_0)^2 = r^2$$

avec $x_0, y_0, r^2 \in K$.

Le point $z = x + iy \in C \cap D$ $(x, y \in \mathbb{R})$ si et seulement si :

$$\begin{cases} (x - x_0)^2 + (y - y_0)^2 = r^2 \\ ax + by + c = 0 \end{cases}$$

Par exemple si $b \neq 0$, tout revient à résoudre une équation de degré 2 en x :

$$(x - x_0)^2 + (-c/b - a/b\, x - y_0)^2 = r^2$$

dont le discriminant Δ est dans K. On trouve $\sqrt{\Delta} \in K$ et donc on trouve $x \in K$ et $y = -c/b - a/b\, x \in K$.

Pour $C \cap C'$:

On résout un système de la forme :

$$\begin{cases} (x - x_0)^2 + (y - y_0)^2 = r^2 & (L1) \\ (x - x_0')^2 + (y - y_0')^2 = r'^2 & (L2) \end{cases}$$

où $x_0', y_0', r'^2 \in K$.

Ce système équivaut à :

$$\begin{cases} (x - x_0)^2 + (y - y_0)^2 = r^2 & (L1) \\ x(2(x_0 - x_0')) + y(2(y_0 - y_0')) = r'^2 - r^2 & (L2 - L1) \end{cases}$$

et on est ramené à déterminer l'intersection d'un cercle et d'une droite. On trouve encore des solutions à coefficients dans K.

4) Si $K_i \subseteq K_{i+1}$ est une extension quadratique, alors $K_{i+1} = K_i(x)$ pour un certain $x \in K_{i+1}$. Soit $X^2 + aX + b$ le polynôme minimal de x sur K_i. On a $a, b \in K_i$ et $x = \frac{-a \pm \sqrt{\Delta}}{2}$ où $\Delta = a^2 - 4b \in K_i$. Donc $K_{i+1} = K_i(\sqrt{\Delta})$ pour un certain $\Delta \in K_i$. On en déduit que si $\mathbb{Q} = K_0 \subseteq ... \subseteq K_n$ est une suite d'extensions quadratiques et si $x \in K_n$, alors $x \in \mathscr{C}$ car le corps $\mathscr{C}$ contient $\mathbb{Q}$ et est stable par les racines carrées.

Réciproquement, on montre par récurrence sur n que si $x \in \mathbb{Q}(i)(P_n)$, alors il existe une suite d'extensions quadratiques :

$$\mathbb{Q} = K_0 \subseteq ... \subseteq K_N$$

telles que $x \in K_N$. C'est évident si $n = 0$ car $\mathbb{Q}(i)(P_0) = \mathbb{Q}(i)$. Supposons que c'est vrai pour n. On a vu au 3) que x est algébrique de degré ≤ 2 sur $\mathbb{Q}(i)(P_n)$. D'après le théorème de l'élément primitif, on a :

$$\mathbb{Q}(i)(P_n) = \mathbb{Q}(y)$$

pour un certain $y \in \mathbb{Q}(i)(P_n)$. Mais par hypothèse de récurrence, on peut trouver :

$$\mathbb{Q} = K_0 \subseteq ... \subseteq K_N$$

une suite d'extensions quadratiques telles que $y \in K_N$. Il suffit alors de poser $K_{N+1} := K_N$ si $x \in \mathbb{Q}(i)(P_n) = K_N$ et $K_{N+1} := K_N(x)$ si $x \notin \mathbb{Q}(i)(P_n) = K_N$.

Soit :

$$\mathbb{Q} = K_0 \subseteq ... \subseteq K_N$$

une suite d'extensions quadratiques. Alors $[K_N : \mathbb{Q}] = 2^N$.

Soit $\sigma : K_N \to \mathbb{C}$ un morphisme de corps. Soit $x \in K_N$ tel que $K_N = K_{N-1}(x)$. Par récurrence, on suppose $\sigma(K_{N-1}) \subseteq K_{N-1}$ alors, comme K_N/K_{N-1} est de degré 2 c'est une extension normale donc il existe un automorphisme $\widetilde{\sigma}$ de K_N qui prolonge $\sigma\big|_{K_{N-1}}$. On a alors $\tau := \sigma\widetilde{\sigma}^{-1}$ qui est l'identité sur K_{N-1}. Donc comme K_N/K_{N-1} est normale, on a :

$$\sigma(K_N) = \tau(K_N) \subseteq K_N \ .$$

Réciproquement, si $K/\mathbb{Q}$ est une extension normale (donc galoisienne car on est en caractéristique nulle) de degré 2^N, alors le groupe de Galois $G := \mathrm{Gal}(K/\mathbb{Q})$ est d'ordre 2^N.

Montrons par récurrence sur N qu'il existe une suite de sous-groupes :

$$1 = G_0 \subseteq G_1 \subseteq ... \subseteq G_N = G$$

tels que $|G_i/G_{i-1}| = 2$.

On aura alors une suite d'extensions quadratiques :

$$\mathbb{Q} = K^G = K_0 \subseteq ... \subseteq K^{G_0} = K \ .$$

Soit Z le centre de G. Le centre Z est non trivial en effet, notons $O_1, ..., O_r$ les orbites de G pour l'action de G sur lui-même par conjugaison.

Supposons que O_1 est l'orbite du neutre : e. On a $|O_1| = 1$. De plus $|G| = |O_1| + ... + |O_r| = 1 + ...|O_r| = 2^N$. Il existe $i > 1$ tel que $|O_i|$ est impair. Or $|O_i|$ divise 2^N donc $|O_i| = 1$. Donc l'élément non $g \in O_i$ est dans le centre de G (et $g \neq e$).

Par hypothèse de récurrence, on a une suite :

$$1 = \overline{G_0} \subseteq \overline{G_1} \subseteq ... \subseteq \overline{G_l} = G/Z$$

de sous-groupes d'indice 2.

On pose alors $G_i := \pi^{-1}\overline{G_i}$ où $\pi : G \to G/Z$ est la surjection canonique. On a :

$$Z = G_0 \subseteq ... \subseteq G_l = G$$

et $G_i/G_{i-1} \simeq \overline{G_i}/\overline{G_{i-1}} \simeq \mathbb{Z}/2\mathbb{Z}$.

Or Z est abélien d'ordre une puissance de 2. On en déduit facilement par (récurrence) qu'il existe une suite de sous-groupes

$$1 \subseteq Z_1 \subseteq ... \subseteq Z_k = Z$$

telle que Z_i/Z_{i-1} est d'ordre 2 pour tout i. D'où une suite :

$$1 \subseteq Z_1 \subseteq Z_2 \subseteq ... \subseteq Z \subseteq G_1 \subseteq ... \subseteq G_l = G \ .$$

6) Soit ζ une racine primitive $n-$ième de l'unité. L'extension $\mathbb{Q}(\zeta)$ est normale et de degré $\varphi(n)$. Donc ζ est constructible si et seulement si $\varphi(n)$ est une puissance de 2.

Or, si $n = 2^a p_1^{k_1}...p_r^{k_r}$ avec $a, r \geq 0, k_1, ..., k_r > 0$ et $p_1 < ... < p_r$ des nombres premiers impairs, alors :

$$\varphi(n) = 2^{a-1} p_1^{k_1-1}(p_1 - 1)...(p_r - 1) \ .$$

Donc $\varphi(n)$ est une puissance de 2 si et seulement si tous les p_i sont de la forme $2^{m_i} + 1$.

Si $p = 2^m + 1$ est premier alors m est une puissance de 2. En effet, sinon, $m = xl$ avec $l \geq 3$ impair et on a :

$$p = 2^{xl} + 1 = (2^x + 1)(2^{x(l-1)} - 2^{x(l-2)} + ... + 1)$$

absurdo car p est premier.

Les nombres premiers de la forme $F_m := 2^{2^m} + 1$ sont appelés les *nombres premiers de Fermat.*

$$F_1, F_2, F_3, F_4$$

sont premiers mais non $F_5, F_6, ...$ C'est une question ouverte de savoir s'il en existe d'autres.