Nombres constructibles à la règle et au compas

blogdemaths.wordpress.com

1 Points constructibles à la règle et au compas

Si M et N sont deux points distincts, on notera (MN) la droite passant par M et N et on notera $\mathscr{C}(M;N)$ le cercle de centre M passant par N.

Définition. *Un point P est constructible à la règle et au compas à partir d'un ensemble de points $\mathscr{E}$ s'il existe des points A, B, C et D de $\mathscr{E}$ tels que :*

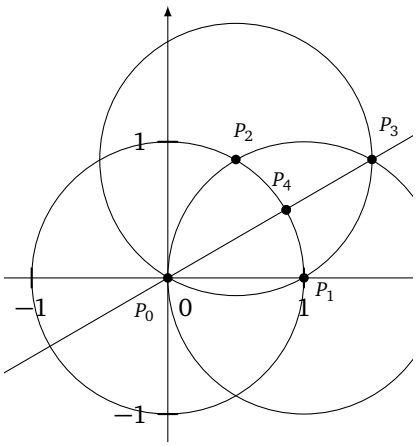
- *Soit P est l'intersection de la droite (AB) et de la droite (CD)*
- *Soit P est une intersection de la droite (AB) avec le cercle $\mathscr{C}(C;D)$*
- *Soit P est une intersection des cercles $\mathscr{C}(A;B)$ et $\mathscr{C}(C;D)$*

Dans le plan complexe, on note O le point d'affixe 0 et I le point d'affixe 1.

Définition. *On dit qu'un point P est constructible à la règle et au compas s'il existe une suite de points $P_0, P_1, \dots, P_n$ telle que :*

- $P_0 = O$
- $P_1 = I$
- *Pour tout $k \geqslant 2$, P_k est constructible à partir de l'ensemble $\{P_0, P_1, \dots, P_{k-1}\}$*

Par exemple, montrons que le point d'affixe $e^{i\pi/6}$ est constructible à la règle et au compas :



Voici les différentes étapes de construction :

1. P_0 est le point d'affixe 0 et P_1 est le point d'affixe 1
2. P_2 est une intersection du cercle $\mathscr{C}(P_0;P_1)$ avec le cercle $\mathscr{C}(P_1,P_0)$
3. P_3 est une intersection du cercle $\mathscr{C}(P_1;P_0)$ avec le cercle $\mathscr{C}(P_2,P_0)$
4. P_4 est l'intersection du cercle $\mathscr{C}(P_0;P_1)$ et de la droite (P_0P_3). Il s'agit du point d'affixe $e^{i\pi/6}$.

2 Condition nécessaire pour être constructible à la règle et au compas

Le théorème de Wantzel

Théorème. *Si un nombre complexe z est constructible alors il existe une suite croissante de corps $K_0 = \mathbb{Q} \subset K_1 \subset K_2 \subset \cdots \subset K_n$ telle que pour tout i, K_{i+1} est une extension de K_i de degré 2 et telle que $z \in K_n$.*

Ce théorème fut énoncé pour la première fois par Pierre-Laurent Wantzel en 1837. En fait, la réciproque de ce théorème est aussi vraie.

Quelques lemmes

Lemme (principal)**.** *Soit z un nombre complexe et $K \subset \mathbb{C}$ un corps. S'il existe un polynôme $P \in K[X]$ de degré 2 tel que $P(z) = 0$, alors $K(z)$ est un extension de K de degré 1 ou 2.*

La démonstration de ce lemme est donnée en annexe, avec quelques rappels sur les extensions quadratiques de corps.

Proposition. *(1) Soit M un point du plan d'affixe $z = x + iy$. On suppose M est le point d'intersection de deux droites (d) et (d') d'équations*

$$\begin{cases} \alpha x + \beta y + \gamma = 0 \\ \alpha' x + \beta' y + \gamma' = 0 \end{cases}$$

Si K est un corps contenant les coefficients α, β, γ et α', β', γ' alors $K(x)$ et $K(y)$ sont des extensions de K de degré 1. (Autrement dit, $K(x) = K(y) = K$).

Démonstration. Comme M appartient aux deux droites, les nombres réels x et y sont solutions du système :

$$\begin{cases} \alpha x + \beta y + \gamma = 0 \\ \alpha' x + \beta' y + \gamma' = 0 \end{cases}$$

La formule de Cramer nous dit alors que :

$$x = \frac{(-\gamma)\beta' - \beta(-\gamma')}{\alpha\beta' - \alpha'\beta} \text{ et } y = \frac{\alpha(-\gamma') - \alpha'(-\gamma')}{\alpha\beta' - \alpha'\beta}$$

c'est-à-dire :

$$x = \frac{\beta\gamma' - \gamma\beta'}{\alpha\beta' - \alpha'\beta} \text{ et } y = \frac{\alpha'\gamma' - \alpha\gamma'}{\alpha\beta' - \alpha'\beta}$$

Si K est un corps contenant α, β, γ et α', β', γ', alors le nombre $\dfrac{\beta\gamma' - \gamma\beta'}{\alpha\beta' - \alpha'\beta} \in K$. Ainsi, $x \in K$ donc, $K(x) = K$ (si $x \in K$, le corps engendré par x sur K est K lui-même). Autrement dit, $K(x)$ est de dimension 1 sur K. De même, on montre que $K(y)$ est de dimension 1 sur K. □

Proposition. *(2) Soit M un point du plan d'affixe $z = x + iy$. On suppose que M est le point d'intersection d'une droite (d) et d'un cercle $\mathscr{C}$ d'équations*

$$\begin{cases} \alpha x + \beta y + \gamma = 0 \\ (x-c)^2 + (y-d)^2 + e = 0 \end{cases}$$

Si K est un corps contenant les coefficients α, β, γ et c, d, e alors $K(x)$ et $K(y)$ sont des extensions de K de degré 1 ou 2.

Démonstration. Soit K un corps contenant les coefficients α, β, γ et c, d, e. Comme $\alpha x + \beta y + \gamma = 0$ est l'équation d'une droite, on a $\alpha \neq 0$ ou $\beta \neq 0$. On peut toujours supposer $\beta \neq 0$.

1er cas : $\alpha = 0$. Dans ce cas, l'équation de la droite est $\beta y + \gamma = 0$, ce qui entraîne que

$$\beta y + \gamma = 0 \iff y = \frac{-\gamma}{\beta} \in K$$

Comme $y \in K$, on a $K(y) = K$ et l'extension $K(y)$ est bien de degré 1 sur K. D'autre part, en remplaçant y par $\dfrac{-\gamma}{\beta}$ dans l'équation du cercle, on trouve

$$(x-c)^2 + \left(\frac{-\gamma}{\beta} - d\right)^2 + e = 0 \iff x^2 - 2cx + c^2 + \left(\frac{-\gamma}{\beta} - d\right)^2 + e = 0$$

et donc x est un racine du polynôme $P = X^2 - 2cX + c^2 + \left(\dfrac{-\gamma}{\beta} - d\right)^2 + e$ dont les coefficients sont dans K (donc $P \in K[X]$). Comme ce polynôme est de degré 2, on en déduit que $K(x)$ est un extension de K de degré 1 ou 2.

2ème cas : $\alpha \neq 0$. Comme le point M est sur la droite, on a

$$\alpha x + \beta y + \gamma = 0 \iff x = \frac{-\beta y - \gamma}{\alpha}$$

En remplaçant cette expression de x dans l'égalité $(x-c)^2 + (y-d)^2 + e = 0$, on obtient

$$\left(\frac{-\beta y - \gamma}{\alpha} - c\right)^2 + (y-d)^2 + e = 0$$

En développant cette expression, on trouve que y est racine du polynôme

$$P = AX^2 + BX + C$$

avec $A = \dfrac{\beta^2}{\alpha^2} + 1$, $B = \dfrac{2\beta(\alpha c + \gamma)}{\alpha^2} - 2d$ et $C = \dfrac{\gamma^2}{\alpha^2} + \dfrac{2\gamma c}{\alpha} + c^2 + d^2 + e$. Comme K est un corps contenant α, β, γ et c, d, e, il contient A, B et C. Ainsi, le polynôme P est un polynôme de K[X] de degré 2 annulant y. D'après le lemme principal, $K(y)$ est une extension de K de degré 1 ou 2. De plus,

$$\alpha x + \beta y + \gamma = 0 \iff x = \frac{-\beta y - \gamma}{\alpha} \in K(y)$$

Ainsi, comme $x \in K(y)$, on en déduit que $K \subset K(x) \subset K(y)$ et donc l'extension $K(x)$ de K est elle aussi au plus de degré 2.

□

Proposition. *(3) Soit M un point du plan d'affixe $z = x + iy$. On suppose que M est le point d'intersection de deux cercles $\mathscr{C}$ et $\mathscr{C}'$ d'équations*

$$\begin{cases} (x-c)^2 + (y-d)^2 + e = 0 \\ (x-c')^2 + (y-d')^2 + e' = 0 \end{cases}$$

Si K est un corps contenant les coefficients c, d, e et c', d', e' alors $K(x)$ et $K(y)$ sont des extensions de K de degré 1 ou 2.

Démonstration. Soit K un corps contenant les coefficients c, d, e et c', d', e'. Le système d'équations peut se réécrire

$$\begin{cases} x^2 + y^2 - 2cx - 2dy + c^2 + d^2 + e = 0 \\ x^2 + y^2 - 2c'x - 2d'y + c'^2 + d'^2 + e' = 0 \end{cases}$$

En faisant la différence des ces deux équations de cercle, on obtient

$$-2(c-c')x - 2(d-d')y + c^2 - c'^2 + d^2 - d'^2 + e - e' = 0$$

Il s'agit de l'équation d'une droite à laquelle appartient le point M. Ainsi, en reprenant une des deux équations de départ, x et y vérifient le système d'équations :

$$\begin{cases} -2(c-c')x - 2(d-d')y + c^2 - c'^2 + d^2 - d'^2 + e - e' = 0 \\ (x-c')^2 + (y-d')^2 + e' = 0 \end{cases}$$

Nous sommes ainsi ramenés au cas de la proposition précédente puisqu'il s'agit de l'intersection d'une droite et d'un cercle et car le corps K contient bien encore tous les coefficients de ces deux équations ! □

Preuve du théorème de Wantzel

Soit z un nombre complexe constructible à la règle et au compas. Nous allons montrer par récurrence sur n que quelque soit la suite de complexes $z_0, z_1, \ldots, z_n$ tels que :

- $z_0 = 0$ et $z_1 = 1$.
- Pour tout i, z_{i+1} est constructible à partir de l'ensemble des nombres $\{z_0, z_1, \cdots, z_i\}$.
- $z_n = z$.

alors il existe une suite de corps $K_0 \subset K_1 \subset \cdots \subset K_j$ telle que K_j contient $z_0, z_1, \cdots, z_n$ ainsi que leurs parties réelles et imaginaires et telle que pour tout i, K_{i+1} est une extension de K_i de degré 2.

---

a) Si $n = 1$, on pose $K_0 = \mathbb{Q}$. Il est clair que $z_0 = 0$, $z_1 = z = 1$ et leurs parties réelles et imaginaires sont dans K_0.

b) Soit $n \geqslant 1$ un entier fixé et soit $z_0, z_1, \ldots, z_n, z_{n+1} = z$ une suite de complexes tels que :

- $z_0 = 0$ et $z_1 = 1$.
- Pour tout i, z_{i+1} est constructible à partir de l'ensemble des nombres $\{z_0, z_1, \cdots, z_i\}$.
- $z_{n+1} = z$.

Comme en particulier z_n est constructible à partir de l'ensemble $\{z_0, z_1, \cdots, z_{n-1}\}$, l'hypothèse de récurrence nous dit qu'il existe une suite de corps $K_0 \subset K_1 \subset \cdots \subset K_j$ telle que K_j contient $z_0, z_1, \cdots, z_n$ ainsi que leurs parties réelles et imaginaires et telle que pour tout i, K_{i+1} est une extension de K_i de degré 2.
Notons $z = x + iy$. Commme $z = z_{n+1}$ est constructible à partir de l'ensemble $\{z_0, z_1, \cdots, z_n\}$, il y a trois cas possibles :

— soit c'est l'intersection de deux droites passant par des points z_i. Comme les coefficients des équations cartésiennes de ces droites s'expriment à partir des parties réelles et imaginaires de z_i, ces coefficients sont dans K_j. Nous avons alors vu dans la propriété (1) que $K_j(x)$ et $K_j(y)$ sont des extensions de K_j de degré 1.
— soit c'est l'intersection de deux cercles définis par des points z_i. Comme les coefficients des équations de ces cercles s'expriment à partir des coordonnées des z_i (parties réelles et imaginaires), nous savons via la propriété (2) que $K_j(x)$ et $K_j(y)$ sont des extensions de K_j de degré 1 ou 2.
— soit c'est l'intersection d'une droite et d'un cercle définis par des points z_i. Nous savons grâce à la propriété (3) que $K(x)$ et $K(y)$ sont des extensions de K_j de degré 1 ou 2.

Dans tous les cas, nous avons $K_j \subset K_j(x)$ qui est une extension de degré 1 ou 2. De même, $K_j \subset K_j(y)$ est de degré 1 ou 2 et on sait alors que y est racine d'un polynôme $P \in K_j[X]$ de degré 2. En particulier, comme $K_j \subset K_j(x)$, le polynôme P est aussi un polynôme de degré 2 de $K_j(x)[X]$. Ainsi, $K_j(x)(y) = K_j(x,y)$ est une extension de $K_j(x)$ de degré 1 ou 2. Un argument similaire montre que $K_j(x,y) \subset K_j(x,y)(i) = K_j(x,y,i)$ est une extension de degré 1 ou 2 (en effet, i est racine de $P = X^2 + 1 \in \mathbb{Q}[X]$ qui peut être vu comme un polynôme de $K_j(x,y)$ car $\mathbb{Q} \subset K_j(x,y)$).
Ainsi, nous avons trouvé une suite de corps

$$K_0 \subset K_1 \subset \cdots \subset K_j \subset K_{j+1} \subset K_{j+2} \subset K_{j+3}$$

avec $K_{j+1} = K_j(x)$, $K_{j+2} = K_j(x,y)$ et $K_{j+3} = K_j(x,y,i)$. De plus, $z_{n+1} = z = x + iy$ (ainsi que sa partie réelle et sa partie imaginaire) est bien contenu dans K_{j+3}.
Enfin, quitte à extraire une sous-suite, on peut toujours supposer chacune des extensions intermédiaires de degré 2 (si l'une est de degré 1, c'est que les deux corps sont égaux). CQFD.

3 Condition suffisante pour ne pas être constructible

Lemme. *Soit $K \subset L$ une extension de degré 2. Si $P \in K[X]$ est un polynôme de degré 3 qui possède une racine dans L alors il possède aussi une racine dans K.*

Démonstration. Comme L est une extension de degré 2 de K, on sait qu'il existe un nombre z tel que $L = K(z) = \{a + bz \mid a, b \in K\}$. (voir en annexe pour une démonstration de ce résultat).
Si w est une racine de P dans $K(z)$ alors $w = a + bz$ avec $a, b \in K$.

- Si $b = 0$ alors $w = a \in K$ et il n'y a rien à prouver.
- Sinon, rappelons que le conjugué d'un nombre $u = a + bz \in K(z)$ est le nombre $\overline{u} = a - bz$. Les propriétés sur la somme et le produit de deux conjugués (voir annexe) montrent que

$$P(w) = 0 \iff \overline{P(w)} = \overline{0} \iff P(\overline{w}) = 0$$

Ainsi, le conjugué $\overline{w}$ est une autre racine de P (en effet, $b \neq 0 \Rightarrow w \neq \overline{w}$). Puisque P est de degré 3 et qu'il possède déjà deux racines, il se factorise alors sous la forme suivante :

$$P = \lambda(X - w)(X - \overline{w})(X - r)$$

où $\lambda \in K$ (car c'est le coefficient dominant de P) et où r est une troisième racine de P. Mais, on sait que la somme des racines d'un polynôme de degré 3 est égale à l'opposé du coefficient de X^2 divisé par le coefficient dominant λ, d'où

$$w + \overline{w} + r \in K$$

Or, $w + \overline{w} = (a + bz) + (a - bz) = 2a \in K$. Ainsi, $2a + r \in K \Rightarrow r \in K$. Le polynôme P possède donc bien un racine dans K.

□

Voici une condition suffisante pour qu'un nombre complexe ne soit pas constructible à la règle et au compas :

Théorème. *Soit $P \in \mathbb{Q}[X]$ un polynôme à coefficients rationnels de degré 3 dont les racines (complexes) ne sont pas des nombres rationnels. Alors, les racines de ce polynôme ne sont pas constructibles à la règle et au compas.*

Démonstration. Soit α une racine de ce polynôme P. Supposons par l'absurde que α soit constructible à la règle et au compas. D'après le théorème de Wantzel, il existe une suite de corps $K_0 = \mathbb{Q} \subset K_1 \subset K_2 \subset \cdots \subset K_n$

telle que pour tout i, K_{i+1} est une extension de K_i de degré 2 et telle que $\alpha \in K_n$. Comme $\mathbb{Q} \subset K_{n-1}$, le polynôme P est un polynôme de degré 3 de $K_{n-1}[X]$ qui possède une racine dans une extension K_n de K_{n-1} de degré 2. On en déduit d'après le lemme précédent que P possède une racine β dans K_{n-1}. Mais, le polynôme P est aussi un polynôme de $K_{n-2}[X]$ qui possède une racine β dans le corps K_{n-1} qui est une extension de degré 2 de K_{n-2}. Il possède donc une racine γ dans K_{n-2}. Et ainsi de suite, on montre que, nécessairement, P possède une racine dans $K_0 = \mathbb{Q}$, ce qui contredit le fait que P n'a pas de racine rationnelle. □

Rappels sur les extensions quadratiques

Quelques définitions

Définition. *Soit K et L deux corps tels que $K \subset L$. On dit que L est une extension de K de degré n si L est un espace vectoriel de dimension n sur K.*
Si L est une extension de degré 2 de K, on dit que L est une extension quadratique de K.

Définition. *Soit z un nombre complexe et $K \subset \mathbb{C}$ un corps. On note $K(z)$ le plus petit sous-corps de $\mathbb{C}$ contenant K et z.*

Caractérisation des extensions quadratiques

Proposition. *Si L est une extention de degré 2 de K, alors il existe $z \in L$ racine d'un polynôme $P \in K[X]$ de degré 2 tel que $L = K(z)$ et $z^2 \in K$. De plus,*

$$L = K(z) = \{a + bz \mid a, b \in K\}$$

et tout élément de L s'écrit de manière unique sous la forme $a + bz$ $(a, b \in K)$.

Démonstration. Par hypothèse, L est une extension de degré 2, c'est-à-dire un K-espace vectoriel de degré 2. Comme la famille constituée du nombre 1 est libre, on peut la compléter en une base, c'est-à-dire qu'il existe $w \in L$ tel que $(1, w)$ est une base de L. On peut alors décomposer l'élément $w^2 \in L$ dans cette base sous la forme $w^2 = b \cdot z + c \cdot 1$ (avec $b, c \in K$). Ainsi, le nombre w vérifie l'équation du second degré

$$w^2 - bw - c = 0$$

En faisant apparaître la forme canonique de cette équation, on trouve :

$$\left(w - \frac{b}{2}\right)^2 - \left(\frac{b}{2}\right)^2 - c = 0 \iff \left(\frac{2w - b}{2}\right)^2 = \frac{b^2 + 4c}{4}$$
$$\iff (2w - b)^2 = b^2 + 4c$$

On pose alors $z = 2w - b$. Comme $z^2 = b^2 + 4c$ alors $z^2 \in K$. De plus, la famille $(1, z)$ est aussi une base de L. Pour le voir, comme L est un espace vectoriel de dimension 2, il suffit de montrer que cette famille est libre. Mais pour tous $\lambda, \mu \in K$,

$$\lambda \cdot 1 + \mu z = 0 \Rightarrow \lambda + \mu(2w - b) = 0 \Rightarrow (\lambda - b\mu) \cdot 1 + 2\mu w = 0$$

Comme la famille $(1, w)$ est libre, cela entraîne en particulier que $2\mu = 0$ donc $\mu = 0$ et que $\lambda - b\mu = 0$ c'est-à-dire $\lambda = 0$. Ainsi, la famille $(1, z)$ est libre et est donc une base de L. Cela montre que $L = \{a + bz \mid a, b \in K\}$.
Il reste à voir que $L = K(z)$. D'une part, comme L contient K et z, il contient $K(z)$ (qui est, par définition, le plus petit corps contenant K et z). D'autre part, si on prend un élément $\ell \in L$, il peut se décomposer de manière unique dans la base $(1, z)$ sous la forme $\ell = a + bz$ avec $a, b \in K$. Comme $K(z)$ est un corps contenant K, il contient alors a et b, et comme il contient z, il contient $a + bz$ (stabilité par somme et produit). Ainsi, $\forall \ell \in L, \ell \in K(z)$ ce qui prouve que $L \subset K(z)$ et donc $L = K(z)$. □

Proposition. *Soit z un nombre complexe et $K \subset C$ un corps. S'il existe un polynôme $P \in K[X]$ de degré 2 tel que $P(z) = 0$, alors $K(z)$ est une extension de K de degré 1 ou 2.*

Démonstration. Si $z \in K$, alors $K(z) = K$ et donc $K(z)$ est une extension de K de degré 1. On peut donc supposer $z \notin K$ dans la suite. Par hypothèse, z est racine d'un polynôme du second degré $P = \alpha z^2 + \beta z + \gamma$ dans K. Remarquons que ce polynôme est nécessairement irréductible dans $K[X]$. En effet, si ce n'était pas le cas, il serait divisible par un polynôme de $K[X]$ de degré 1 et donc il posséderait une racine $z' \in K$. Ainsi, on aurait la somme des racines serait $z + z' = -\beta$ ce qui donnerait $z = -\beta - z' \in K$ ce qui n'est pas le cas.

A présent, définissons l'ensemble $A = \{a + bz \mid a, b \in K\}$ Nous allons montrer que :

1. A est un anneau inclus dans $K(z)$;
2. A est en plus un corps.

Comme $K(z)$ est le plus petit sous-corps contenant K et z, cela voudra dire que $K(z) \subset A$ et donc $K(z) = A$.

Montrons que A est un sous-anneau de $\mathbb{C}$:

— Il est clair que $1 \in A$.

— On a : $(a + bz) + (c + dz) = (a + c) + (b + d)z$ donc A est stable par somme.

— Enfin, Si $a + bz$ et $c + dz$ sont deux éléments de A, alors

$$(a + bz)(c + dz) = ac + (ad + bc)z + bdz^2$$

Or, $\alpha z^2 + \beta z + \gamma = 0$ donc $z^2 = Bz + C$ avec $B = -\beta/\alpha \in K$ et $C = -\gamma/\alpha \in K$. Ainsi,

$$(a + bz)(c + dz) = ac + bdC + (ad + bc + bdB)z \in A$$

L'ensemble A est donc stable par produit. C'est donc bien un sous-anneau de $\mathbb{C}$.

Maintenant qu'on a vu que A est un anneau, nous allons montrer que tout élément $a+bz \neq 0$ de cet anneau est inversible. Pour cela, on considère le polynôme $Q = a + bX$. Il s'agit d'un polynôme de $K[X]$ de degré 1 et comme P (le polynôme de degré 2 qui annule z) est irréductible, alors Q et P sont premiers entre eux. D'après le théorème de Bézout, il existe deux polynômes $U, V \in K[X]$ tels que

$$UP + VQ = 1$$

En évaluant cette égalité pour $X = z$, on trouve $U(z)\times 0 + V(z)\times(a+bz) = 1$ et donc $\dfrac{1}{a+bz} = V(z)$. Or, si on effectue la division euclidienne de V par P alors on peut trouver deux polynômes R et S tels que

$$V = PR + S \text{ avec } \deg(S) < \deg(P)$$

Comme S est de degré strictement inférieur à 2, il est de la forme $S = c + dX$. Ainsi,

$$V(z) = P(z) \times R(z) + S(z) = 0 \times R(z) + c + dz = c + dz \in A$$

On en déduit que le nombre complexe $\dfrac{1}{a+bz} = c + dz$ est dans A. Tout élément de A est donc inversible et donc A est bien un corps. Ainsi, $K(z) = A = \{a + bz \mid a, b \in K\}$. Pour finir, nous allons montrer que $K(z)$ est un K-espace vectoriel de dimension 2 en montrant que la famille $(1, z)$ est une base de $K(z)$.
Tout d'abord, il est clair que cette famille est génératrice car $K(z) = A$. D'autre part, considérons une relation de la forme

$$\lambda \cdot 1 + \mu z = 0 \text{ avec } \lambda, \mu \in K$$

Si on avait $\mu \neq 0$, alors on aurait $z = -\dfrac{\lambda}{\mu}$ et donc z appartiendrait à K, ce qui n'est pas le cas. Ainsi, $\mu = 0$ et donc $\lambda \cdot 1 + 0 = 0$ ce qui entraîne que $\lambda = 0$. La famille $(1, z)$ est donc libre.

□

Conjugué dans une extension quadratique

Définition. *Si $K(z)$ est une extension quadratique de K , le conjugué de $a + bz \in K(z)$ est défini comme étant le nombre*

$$\overline{a+bz} := a - bz$$

En particulier, le conjugué d'un nombre dans K est lui-même.

Proposition. *Soit K un corps, soit $z \in \mathbb{C}$ tel que $K(z)$ soit une extension quadratique. Pour tout $a, b, c, d \in K$,*

- $\overline{(a+bz)+(c+dz)} = \overline{a+bz} + \overline{c+dz}$
- $\overline{(a+bz)(c+dz)} = \overline{a+bz} \times \overline{c+dz}$

Démonstration.

1. D'une part,

$$\overline{(a+bz)+(c+dz)} = \overline{(a+c)+(b+d)z} = (a+c)-(b+d)z$$

   D'autre part, $\overline{a+bz}+\overline{c+dz} = a-bz+c-dz = (a+c)-(b+d)z$ ce qui prouve l'assertion.

2. Rappelons que dans une extension quadratique $K(z)$, on a $z^2 \in K$. Ainsi,

   $$(a+bz)(c+dz) = ac+adz+bcz+bdz^2 = (ac+bdz^2)+(ad+bd)z$$

   Comme $bdz^2 \in K$, on a donc

   $$\begin{aligned}\overline{(a+bz)(c+dz)} = \overline{(ac+bdz^2)+(ad+bd)z} \\ = (ac+bdz^2)-(ad+bd)z\end{aligned}$$

   D'autre part,

   $$\begin{aligned}\overline{a+bz}\times\overline{c+dz} &= (a-bz)(c-dz) \\ &= ac-adz-bcz+bdz^2(ac+bdz^2)-(ad+bd)z\end{aligned}$$

   d'où l'égalité.

□