CHAPITRE III

# Équations et racines

## III.1. Quadratiques et cubiques

**Équations quadratiques.** On dispose de *formules* pour la résolution des équations quadratiques (c'est à dire du second degré). En fait, la résolution de ces équations remonte à la Babylone antique, et est liée à divers problèmes de carrés.

Partons d'un problème simple (et classique) : trouver deux nombres connaissant leur somme et leur produit. On sait le résoudre a priori, en utilisant une des plus anciennes identités remarquable :

$$\left(\frac{x+y}{2}\right)^2 = \left(\frac{x-y}{2}\right)^2 + xy.$$

Connaissant la somme $S = x + y$ et le produit $P = xy$, on tire la différence $D = x - y$ par la formule

$$\frac{D}{2} = \sqrt{\left(\frac{S}{2}\right)^2 - P},$$

puis les valeurs de $x = \frac{S}{2} + \frac{D}{2}$ et $y = \frac{S}{2} - \frac{D}{2}$ soit

$$x = \frac{S}{2} + \sqrt{\left(\frac{S}{2}\right)^2 - P} \quad \text{et} \quad y = \frac{S}{2} + \sqrt{\left(\frac{S}{2}\right)^2 - P}. \tag{III.1.1}$$

Notons qu'il est tout aussi facile de trouver deux nombres connaissant leur *différence* et leur produit.

Soit maintenant une équation quadratique :

$$ax^2 + bx + c = 0. \tag{III.1.2}$$

On peut multiplier (plutôt que diviser) par $a$, on obtient

$$a^2x^2 + bax + ca = 0.$$

Posant $y = ax$, on se ramène alors à une équation du type

$$y^2 + by + ca = 0.$$

En fait dans l'Antiquité, on ne considère que des égalités entre nombres positifs. Donc par exemple, une équation du type "carré plus nombre égal *chose*" soit

$$y^2 + P = Sy. \tag{III.1.3}$$

On voit le lien avec le problème précédent : si $S = x + y$ est la somme de deux nombres, et $P = xy$ leur produit alors

$$Sy = xy + y^2 = P + y^2.$$

Trouver $x$ et $y$ dont on connaît la somme $S$ et le produit $P$ revient donc à résoudre l'équation III.1.3.

De nos jours (et de manière équivalente), on présente les racines de l'équation générale III.1.2 sous la forme

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

**Formules de Cardan.** Les racines d'une équation *cubique* (c'est à dire de degré 3) séxpriment de même par des formules publiées par Cardan en 1545 (dites *formules de Cardan*), découvertes plus tôt par Scipione Del Ferro puis par Tartaglia (qui les avait montrées à Cardan sous la condition de ne pas les divulguer!).

On cherche à résoudre l'équation

$$ax^3 + bx^2 + cx + d = 0.$$

On peut d'abord multiplier par $a^2$ et se ramener à l'équation

$$a^3x^3 + ba^2x^2 + ca^2x + da^2 = 0$$

puis noter que les deux premiers termes $a^3x^3 + ba^2x^2$ sont ceux du développement de $(ax + b/3)^3$. Si on fait le changement de variable $y = ax + b/3$ on obtient alors l'équation

$$y^3 + (ca - b^2/3)y + da^2 + 2b^3/27 - (abc)/3 = 0.$$

Si on sait résoudre cette équation en $y$ on sait alors résoudre l'équation initiale, en revenant à $x = y/a - b/3a$.

Tout revient donc à résoudre une équation sans terme carré, qu'on écrira sous *forme réduite*

$$y^3 - py - q = 0. \tag{III.1.4}$$

On cherche une solution sous la forme $y = u + v$. On doit alors avoir

$$(u + v)^3 - p(u + v) - q = 0. \tag{III.1.5}$$

Rappelant l'identité remarquable

$$(u + v)^3 = u^3 + 3u^2v + 3uv^2 + v^3 = u^3 + v^3 + 3uv(u + v)$$

et reportant dans l'équation III.1.5, on tire

$$u^3 + v^3 + (u + v)(3uv - p) - q = 0.$$

Mais alors il suffit que $u$ et $v$ vérifient les relations

$$\begin{cases} 3uv = p \\ \\ u^3 + v^3 = q \end{cases}$$

Soit encore

$$\begin{cases} u^3v^3 = (p/3)^3 \\ \\ u^3 + v^3 = q \end{cases}$$

On retrouve le problème classique de trouver deux nombres connaissant leur somme et leur produit! On pose

$$\Delta = \left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3$$

c'est le *discriminant* de l'équation. Des formules III.1.1 rappelées plus haut, on tire

$$u^3 = \frac{q}{2} + \sqrt{\Delta} \quad \text{et} \quad v^3 = \frac{q}{2} - \sqrt{\Delta}.$$

D'où la formule qui donne la racine $y = u + v$ de l'équation cubique :

$$y = \sqrt[3]{\frac{q}{2} + \sqrt{\Delta}} + \sqrt[3]{\frac{q}{2} - \sqrt{\Delta}}.$$

Remarques III.1.1. 1) En général, il y trois racines cubiques dans le corps des complexes donc trois choix pour $u$ connaissant $u^3 = \frac{q}{2} + \sqrt{\Delta}$. Ayant choisi une racine cubique pour $u$, alors $v$ est uniquement déterminé puisque $u$ et $v$ sont liés par la relation $3uv = p$. Aux trois racines cubiques pour $u$ correspondent donc les trois racines (distinctes ou confondues) de l'équation de degré 3.
2) Une équation de degré 4 peut se ramener à une cubique ainsi que l'a montré Ludovico Ferrari, un disciple de Cardan. On dit que les équations de degré 2, 3 et 4 sont *résolubles par radicaux* : les racines s'expriment par des formules faisant intervenir des radicaux (racine carrées, cubiques ou quatrièmes). Paolo Ruffini en 1799, puis le norvégien Niels Abel et enfin le français Evariste Galois ont montré que de telles formules n'existaient pas pour les équations de degré 5 ou plus.

**Apparition des nombres complexes.** Cardan a noté que l'équation

$$x^3 = 15x + 4$$

avait la racine évidente $\alpha = 4$. Or les formules donnent

$$\begin{cases} u^3v^3 = (p/3)^3 = 125 \\ \\ u^3 + v^3 = 4 \end{cases}$$

soit $\Delta = \left(\frac{4}{2}\right)^2 - \left(\frac{15}{3}\right)^3 = -121$. Le calcul de $u^3$ et $v^3$ était donc réputé impossible. Notant que $121 = (11)^2$, on serait amené à écrire

$$u^3 = 2 + 11\sqrt{-1} \quad \text{et} \quad v^3 = 2 - 11\sqrt{-1}.$$

Cardan a alors introduit la notion de *nombre sophistique*. Si on pouvait calculer avec $\sqrt{-1}$ on retrouverait bien

$$\begin{cases} u^3v^3 = (2+11\sqrt{-1})(2-11\sqrt{-1}) = 4-(11\sqrt{-1})^2 = 4+121 = 125 \\ \\ u^3+v^3 = (2+11\sqrt{-1})+(2-11\sqrt{-1}) = 4 \end{cases}$$

Cette approche a été reprise par Rafaelle Bombelli (1526-1573) dans l'*Algebra*.

Ainsi il serait faux de dire que les nombres complexes ont été créés pour "inventer des racines imaginaires" : au contraire, ils sont apparus pour interpréter des formules devant conduire à des racines bien réelles.

## III.2. Coefficients et racines

On a vu le lien entre somme et produit des racines pour l'équation quadratique, il remonte à l'Antiquité. Cardan avait aussi noté certaines relations entre la somme des racines d'une cubique et ses coefficients ; des résultats dans le même sens furent obtenus par François Viète qui fut l'un des premiers à considérer les équations avec *paramètres*, c'est à dire dont les coefficients eux-mêmes sont des lettres et non des nombres. Les théorèmes généraux sont pour une grande part dus à Isaac Newton.

**Fonctions symétriques élémentaires des racines.**

Définition III.2.1. Soient $(x_1,\dots,x_n)$ $n$ éléments (distincts ou confondus) d'un corps $K$. On appelle *fonctions symétriques élémentaires* de ces éléments les expressions

$\sigma_1(x_1,\dots,x_n) = \sum_i x_i$, somme des $x_i$,
$\sigma_2(x_1,\dots,x_n) = \sum_{i<j} x_ix_j$, somme des produits deux à deux des $x_i$,
...
$\sigma_n(x_1,\dots,x_n) = \prod_i x_i$, produit des $x_i$.

Considérons maintenant les $n$ racines complexes (distinctes ou répétées chacune autant de fois que leur multiplicité) d'un polynôme de degré $n$.

Théorème III.2.2. *Soit $f = a_nx^n + a_{n-1}x^{n-1} + \dots + a_0$ un polynôme complexe de degré $n$. Alors les fonctions symétriques élémentaires de ses racines sont liées aux coefficients par les relations :*

$$\sigma_1 = -\frac{a_{n-1}}{a_n}, \dots, \sigma_k = (-1)^k\frac{a_{n-k}}{a_n}, \dots, , \sigma_n = (-1)^n\frac{a_0}{a_n}.$$

*Démonstration.* Si les racines de $f$ sont $x_1,\dots,x_n$, on a

$$f = a_nx^n + a_{n-1}x^{n-1} + \dots + a_0 = a_n\prod_i(x-x_i).$$

Divisant par $a_n$ on se ramène à un polynôme unitaire

$$f = x^n + \frac{a_{n-1}}{a_n}x^{n-1} + \dots + \frac{a_0}{a_n} = \prod_i(x-x_i).$$

On peut alors développer le produit et identifier les coefficients et pour se convaincre des relations, raisonner par récurrence sur $n$.

— Pour $n = 2$, on a bien

$$(x - x_1)(x - x_2) = x^2 - (x_1 + x_2)x + x_1x_2.$$

— Notons $\sigma'_1, \ldots, \sigma'_{n-1}$ les fonctions symétriques élémentaires des $n-1$ premières racines $x_1, \ldots, x_{n-1}$. Par hypothèse de récurrence, on a

$$\prod_{i \leq n-1} (x - x_i) = x^{n-1} + \ldots + (-1)^{k-1}\sigma'_{k-1}x^{n-k} + (-1)^k\sigma'_k x^{n-k-1} + \ldots.$$

Multipliant $\prod_{i \leq n-1}(x - x_i)$ par $(x - x_n)$ on obtient un polynôme dont le terme de degré $n - k$ à pour coefficient

$$(-x_n)(-1)^{k-1}\sigma'_{k-1} + (-1)^k\sigma'_k = (-1)^k \left(x_n\sigma'_{k-1} + \sigma'_k\right).$$

Il reste à vérifier qu'on a bien

$$\sigma_k = x_n\sigma'_{k-1} + \sigma'_k.$$

En effet, $\sigma_k$ est la somme des produits $k$ à $k$ des racines, et donc des produits $k$ à $k$ des $n-1$ premières racines (de somme $\sigma'_k$) et des produits de $x_n$ avec les produits $k-1$ à $k-1$ des $n-1$ premières racines (de somme $\sigma'_{k-1}$). □

**Identités de Newton.** Les identités de Newton permettent de calculer par récurrence les sommes des puissances des racines. On note $S_k = \sum_i x_i^k$ la somme des puissances $k$-ièmes des racines. (On note en particulier qu'on a $S_0 = \sum_i x_i^0 = n$.)

THÉORÈME III.2.3. *Soit $f = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0$ un polynôme complexe de degré $n$. Alors, pour $k \leq n$, on a les relations*

$$a_nS_k + a_{n-1}S_{k-1} + \ldots + a_{n-k+1}S_1 + ka_{n-k} = 0$$

*et pour $k \geq n$, les relations*

$$a_nS_k + a_{n-1}S_{k-1} + \ldots + a_0S_{k-n} = 0.$$

*Démonstration.* 1) Pour $k \geq n$, il suffit de noter que pour toute racine $x_i$ on a

$$a_nx_i^n + a_{n-1}x_i^{n-1} + \ldots + a_0.$$

Multipliant par $x_i^{k-n}$, on obtient

$$a_nx_i^k + a_{n-1}x_i^{k-1} + \ldots + a_0x_i^{k-n}.$$

Ajoutant terme à terme les $n$ relations (pour chacune des racines), on obtient les relations de Newton.
2) Pour $k \leq n$, on exprime de deux manières différentes la dérivée $f'$ de $f$. On a d'abord

$$f' = na_nx^{n-1} + \ldots + (n-k)a_{n-k}x^{n-k-1} + \ldots. \tag{III.2.1}$$

Ensuite, écrivant $f = a_n\prod_i(x - x_i)$, on montre par récurrence sur $n$, en appliquant la formule de la dérivée d'un produit, qu'on a

$$f' = \sum_i f_i \quad \text{où} \quad f_i = \frac{f}{x - x_i}.$$

Comme $f(x_i) = 0$, on peut écrire, pour tout $i$

$$f_i = \frac{f(x) - f(x_i)}{x - x_i} = a_n \frac{x^n - x_i^n}{x - x_i} + a_{n-1} \frac{x^{n-1} - x_i^{n-1}}{x - x_i} + \ldots + a_1 \frac{x - x_i}{x - x_i}.$$

Appliquant les identités remarquables

$$x^k - x_i^k = (x - x_i)(x^{k-1} + x_i x^{k-2} + \ldots + x_i^{k-1})$$

on obtient

$$f_i = a_n x^{n-1} + \ldots + [a_n x_i^k + a_{n-1} x_i^{k-1} + \ldots + a_{n-k}] x^{n-k-1} + \ldots.$$

Ajoutant entre-eux tous les $f_i$, on arrive à

$$f' = n a_n x^{n-1} + \ldots + [a_n S_k + a_{n-1} S_{k-1} + \ldots + n a_{n-k}] x^{n-k-1} + \ldots. \quad \text{(III.2.2)}$$

Identifiant les coefficients de degré $n-k-1$ entre III.2.1 et III.2.2, on obtient

$$(n - k) a_{n-k} = a_n S_k + a_{n-1} S_{k-1} + \ldots + n a_{n-k}$$

dont on tire les relations de Newton. □

**Coefficients entiers, solutions entières.**

PROPOSITION III.2.4. *Soit $f = x^n + a_{n-1} x^{n-1} + \ldots + a_0$, un polynôme unitaire à coefficients entiers. Si $f$ admet une racine rationnelle $\alpha$, alors $\alpha$ est un entier et il divise le terme constant $a_0$.*

*Démonstration.* Soit $\alpha = a/b$ une racine rationnelle qu'on peut supposer sous forme irréductible (et de dénominateur positif). On a

$$f(\alpha) = (a/b)^n + a_{n-1}(a/b)^{n-1} + \ldots + a_0 = 0$$

multipliant par $b^n$ on tire

$$a^n = -b\big(a_{n-1} a^{n-1} + \ldots + a_0 b^{n-1}\big).$$

Tout facteur premier $p$ de $b$ divise $a^n$ donc divise aussi $a$. Ayant supposé la fraction sous forme irréductible, $b$ n'admet aucun tel facteur $p$. Autrement dit, $b = 1$ et $\alpha = a$ est un entier (relatif). Par ailleurs on peut aussi écrire

$$a_0 = -a\big(a^{n-1} + a_{n-1} a^{n-2} + \ldots + a_1\big)$$

donc $\alpha = a$ divise $a_0$. □

EXEMPLE III.2.5. Le polynôme $f = x^3 - 2$ n'admet aucune racine rationnelle. En effet une telle racine serait un entier diviseur de 2. Il suffit de vérifier que $1, -1, 2, -2$ ne sont pas racines de $f$. Comme il est de degré 3, ce polynôme est donc irréductible sur $\mathbb{Q}$ [Proposition II.2.3].

## III.3. La règle et le compas

**Constructions géométriques.** Avec une règle et un compas, on peut réaliser des constructions géométriques. On connaît les plus classiques : médiatrice d'un segment, bissectrice d'un angle, parallèle à une droite, etc. on peut aussi citer la construction du pentagone régulier (dont on dit que les pythagoriciens avaient fait leur emblème).

Trois problèmes fameux ont été posés dès l'Antiquité :

— *La trisection de l'angle* : donné un angle $\theta$, le partager en trois angles égaux (chacun de valeur $\theta/3$).

— *La duplication du cube* : donné un cube, construire un segment qui soit le côté du cube de volume double (de même que le carré construit sur la diagonale d'un carré a une surface double que le carré donné).

— *La quadrature du cercle* : donné un cercle, construire un carré de même surface que le disque ainsi considéré.

Pour résoudre certains de ces problèmes, les grecs ont parfois utilisé d'autres outils que la règle (la droite) et le compas (le cercle). Ainsi, au IV$^{ème}$ siècle avant Jésus Christ, Menechme avait déjà montré comment réaliser la duplication du cube par intersection de deux coniques : à l'intersection d'une parabole (d'équation $y = x^2$) et d'une hyperbole (d'équation $y = 2/x$) est le point $A$ d'abcisse $\sqrt[3]{2}$. Cette approche a été systématiquement développée par le mathématicien et poète Omar Khayyam au XII$^{ème}$ siècle pour la résolution des équations cubiques.

Néanmoins, on cherche ici à déterminer quels problèmes ont une solution à la règle et au compas seuls : partant d'un ensemble de points qui définissent la figure initiale, on ne s'autorise qu'à joindre deux de ces points par une droite ou à tracer un cercle de centre un point donné et passant par un autre de ces points. L'intersection de deux droites, de deux cercles ou d'un cercle et d'une droite est alors un point obtenu par construction à la règle et au compas. Ce nouveau point peut ensuite être utilisé dans une étape suivante, selon les mêmes principes.

**Usage de coordonnées et nombres constructibles.** René Descartes, dans le célèbre *Discours de la Méthode*, ramène les problèmes géométriques de construction à la détermination des nombres qui peuvent mesurer les "lignes" construites (par *ligne* il désigne ce qu'on appelle aujourd'hui un segment de droite). Il explique comment, à partir de segments de longueur $\alpha$ et $\beta$, on peut (facilement) construire à la règle et au compas des segments de longueur $\alpha + \beta, \alpha - \beta, \alpha\beta, \alpha/\beta$. Il explique aussi comment passer de $x$ à $\sqrt{x}$.

En fait, partant d'un segment $OA$ de longueur unité, on peut mener la droite portant $O$ et $A$ et construire la perpendiculaire en $O$, autrement dit, on peut considérer un système d'axes orthonormé.

LEMME III.3.1. *A partir d'un système orthonormé, on peut construire le point $B$ de coordonnées $(x, y)$ à la règle et au compas si et seulement si on peut construire des segments de longueurs $|x|$ et $|y|$.*

*Démonstration.* Ayant $B$ on peut construire ses projections $H$ et $Q$ sur les axes et les segments $OH$ et $OK$ sont respectivement de longueur $|x|$ et $|y|$. Inversement, on peut reporter les grandeurs $|x|$ et $|y|$ sur les axes, donc obtenir $H$ et $Q$ et construire $B$ (à l'intersection de perpendiculaires à chacun des axes). □

DÉFINITION III.3.2. On dit qu'un nombre réel $x$ est *constructible* si, étant donné un système orthonormé (son origine, ses axes et l'unité), on peut construire un point à la règle et au compas dont $x$ est une coordonnée.

Il résulte des travaux de Descartes que les nombres constructibles forment une partie de $\mathbb{R}$ qui est fermée pour les quatre opérations arithmétiques (somme, différence, produit, quotient). On dit qu'ils forment un *corps*. En outre ce corps est fermé pour la racine carrée : si $x$ est constructible, $\sqrt{x}$ l'est aussi. En particulier, se donnant l'unité, on obtient tous les entiers, mais aussi tous les rationnels et aussi les racines carrées de rationnels, et ainsi de suite, on peut ajouter, multiplier, diviser et prendre des racines carrées de nombres constructibles pour en obtenir de nouveaux. Par exemple $\sqrt{\frac{1}{2} + \sqrt{3}}$ est constructible.

**Corps quadratiques, extensions quadratiques.** Étendant la notion aux complexes, on dit qu'une partie $K$ de $\mathbb{C}$ est un *sous-corps* de $\mathbb{C}$ si elle est fermée pour les quatre opérations arithmétiques : si $\alpha$ et $\beta$ sont dans $K$, alors $\alpha+\beta, \alpha-\beta, \alpha\beta$ sont dans $K$ ainsi que $\alpha/\beta$ pour $\beta \neq 0$. On en connaît déjà trois exemples : la partie formée par l'ensemble $\mathbb{Q}$ des rationnels, la partie formée par l'ensemble $\mathbb{R}$ des réels ainsi que $\mathbb{C}$ lui-même (la partie toute entière).

On peut obtenir d'autres sous-corps par "adjonction" d'une racine carrée. Si $d$ est un complexe, il résulte du théorème de d'Alembert [Théorème II.4.1] que l'équation $x^2 = d$ a toujours au moins une racine dans $\mathbb{C}$. Notant $\sqrt{d}$ une racine, on dit que c'est une *racine carrée de $d$*.

PROPOSITION III.3.3. *Soient $K$ un sous corps de $\mathbb{C}, d \in K$ et $\sqrt{d}$ une racine carrée de $d$ dans $\mathbb{C}$. La partie $L$ de $\mathbb{C}$ définie par*

$$L = \{\alpha + \beta\sqrt{d} \mid \alpha \in K, \beta \in K\}$$

*est un sous corps de $\mathbb{C}$ contenant $K$ et $\sqrt{d}$.*

*Démonstration.* — $L$ contient $K$ : pour $x \in K$, on a $x = \alpha + \beta\sqrt{d}$ en prenant $\alpha = x$ et $\beta = 0$.
— $L$ contient $\sqrt{d}$ : on a $\sqrt{d} = \alpha + \beta\sqrt{d}$ en prenant $\alpha = 0$ et $\beta = 1$.
— Si $\sqrt{d}$ est dans $K$, autrement dit si $d$ est un carré dans $K$, alors $L = K$ et $L$ est bien un sous corps de $\mathbb{C}$ contenant $K$.

— Si $\sqrt{d}$ n'est pas dans $K$, il faut vérifier que $L$ est fermé pour les quatre opérations arithmétiques. Par exemple que l'inverse d'un élément non nul de $L$ est dans $L$. C'est clair s'il s'agit d'un élément de $K$, considérons donc l'inverse de $\alpha + \beta\sqrt{d}$ où $\beta \neq 0$. On a

$$\frac{1}{\alpha + \beta\sqrt{d}} = \frac{\alpha - \beta\sqrt{d}}{\alpha^2 - d\beta^2} = \alpha_1 + \beta_1\sqrt{d}$$

où $\alpha_1 = \frac{\alpha}{\alpha^2 - d\beta^2}$ et $\beta_1 = \frac{-\beta}{\alpha^2 - d\beta^2}$ sont bien dans $K$ si toutefois ces expressions ont un sens, c'est à dire si le dénominateur $\alpha^2 - d\beta^2$ n'est pas nul. Mais c'est le cas, sinon $\alpha^2 = d\beta^2$ et $d = \left(\frac{\alpha}{\beta}\right)^2$ serait un carré dans $K$. □

Définitions III.3.4. Soient $K$ un sous corps de $\mathbb{C}, d$ un élément de $K$ qui n'est pas un carré dans $K$ et $\sqrt{d}$ une racine carrée de $d$ dans $\mathbb{C}$. On note $K[\sqrt{d}]$ le sous corps de $\mathbb{C}$ défini par

$$K[\sqrt{d}] = \{\alpha + \beta\sqrt{d} \mid \alpha \in K, \beta \in K\}.$$

On dit que $K[\sqrt{d}]$ est une *extension quadratique de* $K$. On dit en particulier qu'une extension quadratique de $\mathbb{Q}$ est un *corps quadratique*.

Exemples III.3.5. Il est d'usage de noter $i$ (plutôt que $\sqrt{-1}$) une racine carrée de $(-1)$ dans $\mathbb{C}$. Le corps $\mathbb{C}$ des complexes n'est rien d'autre que l'extension quadratique $\mathbb{R}[i]$ des réels :

$$\mathbb{C} = \mathbb{R}[i] = \{\alpha + i\beta \mid \alpha \in \mathbb{R}, \beta \in \mathbb{R}\}.$$

On peut de même considérer le corps quadratique $\mathbb{Q}[i]$ :

$$\mathbb{Q}[i] = \{\alpha + i\beta \mid \alpha \in \mathbb{Q}, \beta \in \mathbb{Q}\}.$$

On a aussi le corps quadratique $\mathbb{Q}[\sqrt{2}]$ :

$$\mathbb{Q}[\sqrt{2}] = \{\alpha + \beta\sqrt{2} \mid \alpha \in \mathbb{Q}, \beta \in \mathbb{Q}\}.$$

**Suite d'extensions quadratiques.** On a vu que les rationnels sont des nombres constructibles. La racine carrée d'un nombre rationnel est constructible, donc les éléments un corps quadratique réel (contenu dans $\mathbb{R}$) sont constructibles. Plus généralement, comme la racine carrée d'un nombre constructible est constructible, si on a une suite de sous-corps de $\mathbb{R}$

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n$$

tels que chacun est une extension quadratique du précédent, alors les éléments de $K_n$ sont constructibles. En fait, il s'agit d'une caractérisation des nombres constructibles :

Théorème III.3.6. *Un nombre $x$ est constructible si et seulement si il existe une suite de sous-corps de $\mathbb{R}$ :*

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n$$

*tels que chacun est une extension quadratique du précédent et $x \in K_n$.*

*Démonstration.* S'il existe une telle suite, on a vu que les éléments de $K_n$ sont constructibles, il nous reste à montrer que si $x$ est constructible alors il existe une telle suite. La figure dont on part est formée de l'origine $O$ et du point $A$ d'abcisse 1 sur l'axe des $x$. Leurs coordonnées sont des éléments de $\mathbb{Q}$ (en fait, 0 et 1). Supposons, par récurrence, qu'après un certain nombre de constructions (intersections de droites et de cercles), tous les points qu'on a obtenu ont leur coordonnées dans un corps $K = K_{n-1}$ obtenu par $n-1$ extensions quadratiques successives. Faisons une nouvelle construction, à partir de ces points, en distinguant les cas :

1) Intersection de deux droites. Joignant deux points $A_1$ et $A_1'$ de coordonnées respectives $(a_1, b_1)$ et $(a_1', b_1')$, on considère une droite d'équation

$$(x - a_1)(b_1' - b_1) - (y - b_1)(a_1' - a_1) = 0.$$

De même la droite joignant $A_2$ et $A_2'$ de coordonnées $(a_2, b_2)$ et $(a_2', b_2')$ a pour équation

$$(x - a_2)(b_2' - b_2) - (y - b_2)(a_2' - a_2) = 0.$$

Par hypothèse les coordonnées des points donnés sont dans $K_{n-1}$. Trouver les coordonnées de l'intersection de ces droites revient donc à résoudre un système d'équations linéaires à coefficients dans $K_{n-1}$ de la forme

$$\begin{cases} \alpha_1 x + \beta_1 y = \gamma_1 \\ \\ \alpha_2 x + \beta_2 y = \gamma_2 \end{cases}$$

Les solutions s'obtiennent par des opérations arithmétiques élémentaires sur les coefficients, elles sont donc encore dans $K = K_{n-1}$.

2) Intersection d'une droite et d'un cercle. Supposons construits le point $\Omega$ de coordonnées $(p, q)$, ainsi qu'un segment de longueur $r$. Par hypothèse de récurrence, $p, q$ et $r$ sont dans $K$. Le cercle de centre $\Omega$ et de rayon $r$ a pour équation

$$(x - p)^2 + (y - q)^2 - r^2 = 0.$$

Trouver les coordonnées de l'intersection de ce cercle et d'une droite passant par deux points déjà construits, c'est résoudre un système de la forme

$$\begin{cases} \alpha x + \beta y = \gamma \\ \\ x^2 + y^2 + \alpha' x + \beta' y + \gamma' = 0 \end{cases}$$

Éliminant $y$, on arrive à une équation quadratique $ax^2 + bx + c = 0$ où $a, b$ et $c$ sont dans $K$, car ils s'obtiennent par des opérations arithmétiques élémentaires sur les coefficients des équations de la droite et du cercle. Dire que la droite coupe le cercle, c'est dire que cette équation a des solutions réelles, donc que son discriminant $\Delta = b^2 - 4ac$ est positif. Les solutions de l'équation, à savoir $\frac{-b \pm \sqrt{\Delta}}{2a}$ appartiennent alors à l'extension quadratique $K_n = K[\sqrt{\Delta}]$ de $K = K_{n-1}$.

3) Intersection de deux cercles. Cette fois on doit résoudre le système

$$\begin{cases} x^2+y^2+\alpha x+\beta y+\gamma=0 \\ \\ x^2+y^2+\alpha' x+\beta' y+\gamma'=0 \end{cases}$$

Soustrayant les deux équations, on se ramène au problème de l'intersection d'un cercle et de la droite d'équation

$$(\alpha-\alpha')x+(\beta-\beta')y+(\gamma-\gamma')=0.$$

□

**Constructions impossibles.**

PROPOSITION III.3.7. *Si $x$ est un nombre constructible et racine d'une équation cubique à coefficients rationnels, alors cette équation admet au moins une racine rationnelle.*

*Démonstration.* On raisonne sur une équation cubique réduite, c'est à dire qu'on suppose $x$ racine d'un polynôme $f$ de la forme

$$f=x^3-px-q.$$

D'après le théorème III.3.6, comme $x$ est constructible, il existe une suite de sous-corps de $\mathbb{R}$ :

$$\mathbb{Q}=K_0\subset K_1\subset\ldots\subset K_n$$

tels que chacun est une extension quadratique du précédent et $x\in K_n$. On montre que $f$ admet au moins une racine dans $K_{n-1}$. On montrerait de même que $f$ admet une racine dans $K_{n-2}$ et ainsi de suite, jusqu'à $K_0=\mathbb{Q}$. Pour simplifier, on note $K=K_{n-1}$. Alors $K_n=K[\sqrt{d}]$ où $d\in K$ n'est pas un carré dans $K$ et $x=\alpha+\beta\sqrt{d}$, avec $\alpha,\beta$ dans $K$.
— Si $\beta=0$, alors la racine $x=\alpha$ est elle même dans $K$.
— Si $\beta\neq 0$, montrons que $y=\alpha-\beta\sqrt{d}$ est une autre racine de l'équation. Comme $x$ est racine de $f$ on a

$$f(x)=(\alpha+\beta\sqrt{d})^3-p(\alpha+\beta\sqrt{d})-q=\alpha_1+\beta_1\sqrt{d}=0$$

où $\alpha_1=\alpha^3+3d\alpha\beta^2-p\alpha-q$, et $\beta_1=3\alpha^2\beta+d\beta^3-p\beta$ sont dans $K$. En fait $\beta_1=0$. Sinon $\alpha_1+\beta_1\sqrt{d}=0$ et $\sqrt{d}=\frac{-\alpha_1}{\beta_1}$, soit $d=\left(\frac{\alpha_1}{\beta_1}\right)^2$ et $d$ serait un carré dans $K$. Mais alors on a aussi $\alpha_1=0$ (puisque $\alpha_1+\beta_1\sqrt{d}=0$). On peut donc conclure qu'on a

$$f(y)=(\alpha-\beta\sqrt{d})^3-p(\alpha-\beta\sqrt{d})-q=\alpha_1-\beta_1\sqrt{d}=0.$$

Par ailleurs, comme le polynôme $f$ n'a pas de terme de degré 2, la somme de ses racines est nulle [Théorème III.2.2]. Dans $\mathbb{C}$, le polynôme $f$ admet trois racines : $x,y$ et une troisième racine $z$. Pour finir, on peut voir que cette troisième racine est en fait dans le corps $K$, en effet

$$z=-(x+y)=-\big((\alpha+\beta\sqrt{d})+(\alpha-\beta\sqrt{d})\big)=-2\alpha.$$

□

On peut maintenant conclure à l'impossibilité des constructions fameuses de l'Antiquité :

— *La trisection de l'angle* : il est par exemple impossible de réaliser la trisection des angles d'un triangle équilatéral. Donné un segment $OA$ de longueur unité, on sait construire un triangle équilatéral de côté $OA$, ce qui revient, étant donné le cercle trigonométrique (de centre 0 de rayon 1), à construire la droite qui fait avec l'axe des $x$ l'angle $\frac{\pi}{3}$. Réaliser la trisection reviendrait à construire la droite qui fait avec l'axe des $x$ l'angle $\frac{\pi}{9}$. Les coordonnées du point correspondant sur le cercle, soient $\cos(\frac{\pi}{9}), \sin(\frac{\pi}{9})$, seraient alors des nombres constructibles. On rappelle la relation

$$\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta).$$

Comme $\cos(\frac{\pi}{3}) = \frac{1}{2}$, on voit que $\cos(\frac{\pi}{9})$ est racine de l'équation cubique

$$8x^3 - 6x - 1 = 0.$$

Posons $\xi = 2\cos(\frac{\pi}{9}), \xi$ est racine du polynôme

$$f = x^3 - 3x - 1.$$

Si $\xi$ était constructible, $f$ devrait avoir une racine rationnelle, mais il résulte de la proposition III.2.4 que ce n'est pas le cas (il suffit de vérifier que ni 1 ni $-1$ ne sont racines de $f$).

— *La duplication du cube* : si la duplication du cube était possible, le nombre $\sqrt[3]{2}$ serait constructible. Le polynôme $x^3 - 2$ devrait alors avoir une racine rationnelle. On a vu que ce n'était pas le cas [Exemple III.2.5].

— *La quadrature du cercle* : C'est à Pierre-Laurent Wantzel qu'on doit d'avoir montré l'impossibilité de la trisection de l'angle et de la duplication du cube dans la "Recherche sur les moyens de reconnaître si un problème de géométrie peut se résoudre à la règle et au compas" publiée en 1837. L'impossibilité de la quadrature du cercle est plus difficile. Donné un cercle de rayon 1, il faut construire un carré de même aire donc de côté $\sqrt{\pi}$. Cela revient à dire que $\sqrt{\pi}$ est un nombre constructible. Si c'était le cas, $\pi$ serait également constructible. Johann Heinrich Lambert (1728-1777), collègue d'Euler et Lagrange à l'académie des sciences de Berlin, avait montré que $\pi$ n'est pas un nombre rationnel, ni la racine carrée d'un nombre rationnel. En fait $\pi$ n'est pas d'avantage une racine carrée de racine carrée ni une racine cubique, ni même la racine d'aucune équation algébrique à coefficients rationnels, on dit que c'est un *nombre transcendant*. Ce résultat à été établi par Ferdinand von Lindemann (1852-1939) en 1882. On peut en déduire que $\pi$ n'est pas constructible et mettre ainsi fin à une quête de près de 25 siècles!