Enseignant au lycée de Bouxwiller, Edmond JUNG a eu cette année, pour la première fois, une Première L option math avec le nouveau programme, dont le chapitre « Nombres constructibles ». Et, dit-il, « *D'après les instructions du programme officiel, on a vite fait le tour de la question et, par conséquent, préparé le cours. Mais, lorsque le programme demande d'évoquer la quadrature du cercle, on aimerait bien savoir pourquoi elle est impossible !* ».

E. Jung a alors consulté divers ouvrages, dont le Birkhoff-MacLaine et des sites Internet(*) qui le renvoyaient à des ouvrages spécialisés ou se contentaient de généralités.

Ceux-ci se sont révélés difficiles – opinion partagée par ses collègues – mais E. Jung « voulait pourtant savoir ». La lettre qu'il nous a envoyée en proposant son article continue ainsi : « *En enseignant le chapitre en classe j'ai eu le pressentiment qu'il n'est qu'un cas particulier de la théorie des corps et qu'il est possible de démontrer les propriétés essentielles sans avoir recours à toute la théorie. C'est ce que je pense avoir fait. Alors, à qui s'adresse mon article ? À toute personne qui s'y intéresse, qui sait ce qu'est un ensemble fini, un corps et un sous-corps, et qui sait faire une démonstration par récurrence (ascendante et descendante).*
J'ai surtout écrit l'article pour moi, pour avoir des idées claires sur le sujet. »

La Commission du Bulletin a apprécié cette démarche et le texte qui en est résulté. Elle a pensé que tous deux pouvaient intéresser tous les collègues. D'où l'article qui suit, complété par nos soins d'une courte bibliographie, cette fois accessible à tous.

Nombres constructibles

(à la règle non graduée et au compas)

Edmond Jung(**)

I. Recherche des idées

Il s'agit de déterminer tous les réels que l'on peut obtenir, par construction à la règle non graduée et au compas, à partir d'un segment [OI] de longueur 1.

Pour cela on déterminera tous les points M_i du plan que l'on peut construire à la règle non graduée et au compas à partir des points O et I. Plus précisément, un **point** M_i sera dit **constructible** si je peux le construire à la règle non graduée et au compas à partir de deux points distants de 1 **et si** je connais parfaitement le point obtenu (je connais sa position ou ses coordonnées ou … si je peux le reconstruire).

L'abscisse de même que l'ordonnée de chaque point M_i constructible de la droite (OI) dans le repère (O ; I) sera un **réel constructible**.

Tout réel constructible positif sera un **nombre constructible**.

(*) NDLR : **Publimath** lui aurait fourni des ouvrages utiles parmi 12 analysés.

(**) 6 rue Belle-Vue, 67350 ENGWILLER. Mél : eddyjung@tele2.fr

On obtient un point constructible en utilisant la règle et le compas, donc en traçant des droites et des cercles.

Exemple 1 :

A et B sont deux points distants de 1. C_1 est un cercle de centre A et C_2 un cercle de centre B. Si les rayons de ces cercles sont quelconques mais suffisamment grands et pas trop, C_1 et C_2 se coupent en deux points M et N. M et N ont été construits à la règle et au compas, mais ils ne sont pas constructibles pour autant, puisqu'on ne connaît pas leur position exacte. Par contre, si on connaît les rayons des deux cercles, on connaît leur position exacte : on connaît par exemple leurs coordonnées dans un repère orthonormé (A ; B ; C).

Exemple 2 :

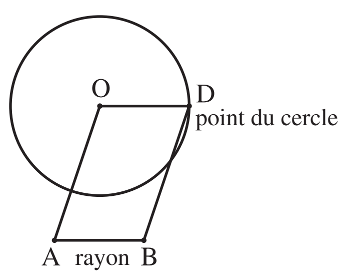
Reprenons l'exemple précédent en considérant deux cercles C_1 et C_2 de même rayon quelconque mais suffisamment grand et pas trop. (MN) coupe alors (AB) en P. P est constructible car on aurait pu choisir un rayon égal à 1.

On peut donc construire un point constructible en traçant des droites et des cercles arbitrairement, c'est-à-dire en traçant par exemple des cercles dont le centre ou (et) le rayon sont quelconques, mais sur l'exemple on peut aussi le construire avec un rayon constructible.

Nous allons donc supposer par la suite que tout point constructible s'obtient à partir de cercles et de droites parfaitement définis.

Pour tracer un cercle parfaitement défini, il faut placer les deux « pointes » du compas ; il faut donc connaître le centre et le rayon ou un point du cercle.

La figure ci-contre montre que si l'on connaît le centre et le rayon on connaît aussi un point constructible du cercle.



Donc, pour tracer un cercle parfaitement défini, il faut connaître le centre et un point du cercle.

Pour tracer une droite parfaitement définie à la règle non graduée, il faut connaître deux de ses points.

Ce qui nous amène à définir les notions suivantes.

II. Formalisation

Point constructible en une étape

Définition : Soit $E = \{M_i, i \text{ entier naturel}\}$ un ensemble fini ou infini de points du plan. Soit $C = \{C_{MN}, M \in E, N \in E\}$ l'ensemble des cercles de centre M passant par N, et $D = \{D_{MN}, M \in E, N \in E, M \neq N\}$ l'ensemble des droites (MN). On appelle **point constructible en une étape** à partir de E, tout point de E ou tout point d'intersection de deux éléments distincts de $C \cup D$.

Nous pouvons définir une suite (E_i) $(i \geq 1)$ de la façon suivante :

E_1 est un ensemble de points donné et E_{i+1} est l'ensemble des points constructibles en une étape à partir de E_i.

Point constructible

Définition : On appelle point constructible à partir de E_1, tout point de E_i, pour tout i.

Définition : On appelle point constructible du plan euclidien muni d'un repère orthonormé (O ; I ; J) tout point constructible à partir de $E_1 = \{O ; I\}$.

L'ensemble E des points constructibles du plan muni d'un repère orthonormé (O ; I ; J) est tel que $E = \bigcup_{i \in \mathbf{N}^*} E_i$.

Réel constructible

Propriété 1 : Le projeté orthogonal d'un point constructible sur un des axes de coordonnées est constructible (deux droites parallèles sont constructibles à la règle non graduée et au compas).

D'où la définition suivante :

Définition 1 : On appelle réel constructible toute abscisse ou toute ordonnée dans le repère (O ; I ; J) d'un point constructible.

Si M(a ; b) est un point constructible, alors a et b sont des réels constructibles.

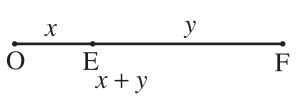
Définition : Appelons E l'ensemble des réels constructibles.

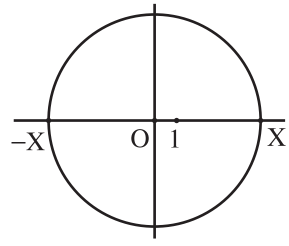
Propriété : Si A et B sont deux points constructibles, alors la distance AB est un réel constructible.

Faire la construction.

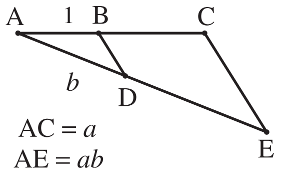
Propriétés : Recherchons quelques propriétés des réels constructibles.

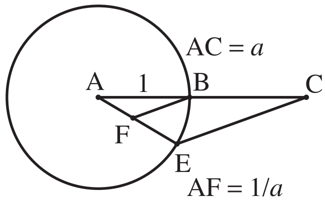
- 1 est constructible car I est donné.
- La somme de deux réels constructibles est constructible





- L'opposé d'un réel constructible est constructible
- Le produit de deux réels constructibles est constructible





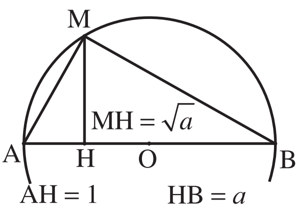
- L'inverse d'un réel constructible non nul est constructible.

- Le quotient d'un réel constructible par un réel constructible non nul est constructible.
- Le projeté orthogonal d'un point constructible sur un des axes de coordonnées est constructible.
- Un point est constructible si ses coordonnées le sont (un parallélogramme est constructible à la règle non graduée et au compas).
- On déduit l'équivalence suivante des deux propriétés précédentes :
  Pour tous réels a et b : M(a ; b) est un point constructible si et seulement si a et b sont des réels constructibles.

Le sous-corps de R des réels constructibles

L'ensemble des réels constructibles E muni de l'addition et de la multiplication des réels est donc un sous-corps de **R**.

La racine carrée de tout réel constructible est constructible.



Conséquence 1 : E vérifie les conditions suivantes :
1) E est un sous-corps de **R**.
2) Pour tout $x \in \mathbf{R}^+$, $x \in \mathrm{E} \Rightarrow \sqrt{x} \in \mathrm{E}$.

III. But et exemples

Le but des démonstrations qui suivent est de montrer que :

Résultat 1 : L'ensemble des nombres constructibles est le plus petit sous-ensemble E de **R** qui vérifie les conditions suivantes :
1) E est un sous-corps de **R**.
2) Pour tout $x \in \mathbf{R}^+$, $x \in \mathrm{E} \Rightarrow \sqrt{x} \in \mathrm{E}$.

Résultat 2 : Tout réel constructible est racine d'un polynôme irréductible[(1)] de degré 2^p à coefficients dans **Q**.

Faisons une petite récréation

Cherchons le plus petit sous-corps K de **R**. Tout sous-corps de **R** contient 0 et 1. On a : $1 \in$ K, donc $1 + 1 = 2 \in$ K, donc $2 + 1 = 3 \in$ K, donc, … , donc $238\,596\,478\,123\,659\,874 \in$ K, donc $-3 \in$ K, donc $\frac{1}{-3} \in$ K, donc $\frac{1}{-3} \times 2 \in$ K, donc … On se rend compte que tout rationnel est élément de K et comme **Q** est un corps, le plus petit sous-corps de **R** est **Q**. Cela nous donne une idée, mais n'est pas une démonstration.

On constate aussi que tout rationnel a est racine d'un polynôme P irréductible de degré 1 à coefficients dans **Q** : $\mathrm{P}(x) = x - a$. On dit que a est de degré 1 sur **Q**.

(1) Irréductible : premier au sens de la division des polynômes.

Élargissons :

Soit maintenant le plus petit sous-corps de **R** qui contient **Q** et 2. Notons-le **Q**(2). **Q** contient déjà 2. En « combinant » 2 de toutes les façons possibles avec tous les éléments de **Q**, nous n'arriverons pas à « sortir » de **Q**. On « voit » donc que **Q**(2) = **Q**.

Élargissons vraiment :

Examinons $\mathbf{Q}\left(\sqrt{2}\right)$, le plus petit sous-corps de **R** qui contient **Q** et $\sqrt{2}$. Comme chacun sait, $\sqrt{2}$ n'appartient pas à **Q**. $\mathbf{Q}\left(\sqrt{2}\right)$ contient donc 0 ; 1 ; 2 ; 568 942 ; $\frac{-49}{27}$; mais aussi $\sqrt{2}$; $87\sqrt{2}+\frac{473}{289}$ et même $\left(\frac{37\sqrt{2}-\frac{38}{15}}{253-13\sqrt{2}}\right)\Big/\left(\frac{\frac{43}{18}+17\sqrt{2}}{3\sqrt{2}+11}\right)$ et … ainsi de suite ! Mais rassurez-vous, on arrive facilement à démontrer que tout élément de $\mathbf{Q}\left(\sqrt{2}\right)$ peut s'écrire de façon unique sous la forme $a+b\sqrt{2}$ avec a et b rationnels.

Certains éléments de $\mathbf{Q}\left(\sqrt{2}\right)$, les rationnels, sont racines d'un polynôme de degré 1 alors que $\sqrt{2}$ est racine d'un polynôme P irréductible de degré 2 à coefficients dans **Q** : $P(x) = x^2 - 2$. $\sqrt{2}$ est de degré 2 sur **Q**.

$2\sqrt{2}+3$ est également de degré 2 sur **Q**. Déterminer le polynôme P correspondant ! Plus généralement on peut montrer que tout élément de $\mathbf{Q}\left(\sqrt{2}\right)$ qui n'est pas rationnel est de degré 2 sur **Q**.

Élargissons toujours :

Examinons $\mathbf{Q}\left(\sqrt{2};\sqrt{3}\right)$ qui est le plus petit sous-corps de **R** qui contient **Q,** $\sqrt{2}$ et $\sqrt{3}$ ou encore le plus petit sous-corps de **R** qui contient $\mathbf{Q}\left(\sqrt{2}\right)$ et $\sqrt{3}$ ou encore le plus petit sous-corps de **R** qui contient $\mathbf{Q}\left(\sqrt{3}\right)$ et $\sqrt{2}$.

Quelques éléments de $\mathbf{Q}\left(\sqrt{2};\sqrt{3}\right)$: $\frac{-78}{17}$; $7-4\sqrt{2}-3{,}5\sqrt{3}$; $2{,}7\sqrt{6}$.

On peut montrer que tout élément de $\mathbf{Q}\left(\sqrt{2};\sqrt{3}\right)$ peut s'écrire de façon unique sous la forme $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ avec a, b, c et d rationnels.

Les rationnels de $\mathbf{Q}\left(\sqrt{2};\sqrt{3}\right)$ sont de degré 1 sur **Q**, certains éléments comme $\sqrt{2}$, $\sqrt{3}$ et $\sqrt{6}$ sont de degré 2 sur **Q**. Mais quel est le degré de $\sqrt{2}+\sqrt{3}$?

$\sqrt{2}+\sqrt{3}$ est racine de $x-\left(\sqrt{2}+\sqrt{3}\right)$, polynôme du **premier degré à coefficients dans** $\mathbf{Q}\left(\sqrt{2};\sqrt{3}\right)$.

$$\left(\sqrt{2}+\sqrt{3}\right)^2=5+2\sqrt{2}\sqrt{3}$$

$$\left(\sqrt{2}+\sqrt{3}\right)^2-2\sqrt{2}\left(\sqrt{3}+\sqrt{2}\right)+2\sqrt{2}\sqrt{2}-5=0$$

$$\left(\sqrt{2}+\sqrt{3}\right)^2-2\sqrt{2}\left(\sqrt{3}+\sqrt{2}\right)-1=0$$

$\sqrt{2}+\sqrt{3}$ est donc racine de $x^2-2\sqrt{2}x-1$, polynôme du second degré à coefficients dans $\mathbf{Q}\left(\sqrt{2}\right)$.

$$x^2-2\sqrt{2}x-1=x^2-1-2\sqrt{2}x$$

et

$$\left[\left(x^2-1\right)-2\sqrt{2}x\right]\left[\left(x^2-1\right)+2\sqrt{2}x\right]=\left(x^2-1\right)^2-8x^2.$$

Ce dernier polynôme est du quatrième degré à coefficients dans **Q**. Ses racines sont $\sqrt{2}+\sqrt{3}$, $\sqrt{2}-\sqrt{3}$, $-\sqrt{2}-\sqrt{3}$ et $-\sqrt{2}+\sqrt{3}$. En multipliant deux des quatre monômes suivants :

$$x-\left(\sqrt{2}+\sqrt{3}\right),\ x-\left(\sqrt{2}-\sqrt{3}\right),\ x-\left(-\sqrt{2}-\sqrt{3}\right)\ \text{et}\ x-\left(-\sqrt{2}+\sqrt{3}\right)$$

entre eux de toutes les façons possibles, on n'obtient pas de polynôme à coefficients dans **Q**. Essayez !

$\left(x^2-1\right)^2-8x^2$ est donc irréductible sur **Q** et $\sqrt{2}+\sqrt{3}$ est de degré 4 sur **Q**.

Et plus on élargit, plus cela se complique !

IV. Démonstrations

Les démonstrations des résultats 1 et 2 cités dans le début du paragraphe III « Buts et exemples » se trouvent dans divers ouvrages d'algèbre de niveau maîtrise, mais, comme je ne suis pas un algébriste confirmé, j'ai rédigé une démonstration accessible à toute personne qui a passé son baccalauréat, qui sait faire un raisonnement par récurrence et qui connaît les propriétés de base des corps et des sous-corps.

Les démonstrations sont assez longues et je vais me contenter de vous en décrire les grandes lignes.

1) Tout ensemble E est fini (dans le but d'indexer les éléments et de faire des démonstrations par récurrence).
2) On classe les réels constructibles d'après l'ordre chronologique de leur construction (ou presque) : par exemple $r_0 = 0$, $r_1 = 1$, r_2, r_3, … ; puis on étudie successivement **Q**, $\mathbf{Q}(r_2)$, $\mathbf{Q}(r_2, r_3)$, $\mathbf{Q}(r_2, r_3, r_4)$, …, $\mathbf{Q}(r_2, r_3, r_4, r_5, \dots, r_i)$.
3) On montre que tout élément de $\mathbf{Q}(\mathrm{E}_{i+1})$ est de degré 1 ou 2 dans $\mathbf{Q}(\mathrm{E}_i)$ d'où le résultat 1.
4) On montre que tout élément de $\mathbf{Q}(r_2, r_3, r_4, r_5, \dots, r_{i+1})$ est de degré 1 ou 2 dans $\mathbf{Q}(r_2, r_3, r_4, r_5, \dots, r_i)$.
5) On montre que, s'il existe un réel p tel que a est de degré p dans $\mathbf{Q}(r_2, r_3, r_4, r_5, \dots, r_{i+1})$, alors il existe un réel q tel que a est de degré q dans $\mathbf{Q}(r_2, r_3, r_4, r_5, \dots, r_i)$.
6) On montre le théorème suivant par récurrence :

Théorème : Pour tout réel constructible a, il existe un entier naturel p tel que a est racine d'un polynôme unitaire et irréductible de degré 2^p à coefficients dans **Q**.

La réciproque du théorème est fausse.

Conséquences :

1) Toute racine d'un polynôme irréductible de degré différent de 2^p n'est pas constructible.

2) Tout nombre constructible est algébrique (racine d'un polynôme à coefficients dans **Q**).
La réciproque est fausse.

3) Les trois problèmes classiques de l'antiquité :

a) **La duplication du cube**.
Question : Est-il possible de construire, à partir d'un segment de longueur 1, le côté d'un cube de volume 2 ?

Réponse : Le côté du cube mesure $\sqrt[3]{2}$. Or $\sqrt[3]{2}$ est racine du polynôme $x^3 - 2$ irréductible dans **Q** qui est de degré 3. $\sqrt[3]{2}$ n'est pas constructible.

b) **La quadrature du cercle**.
Question : Est-il possible de construire, à partir d'un carré (de côté 1) un cercle qui a la même aire que le carré ?
Réponse :
L'aire du carré est 1, celle du disque également. Le rayon r du disque est tel que $\pi r^2 = 1$. Donc $r = \sqrt{\frac{1}{\pi}}$. Si r est constructible, alors $\frac{1}{\pi}$ et π sont constructibles. Or π n'est pas algébrique (il est transcendant). Donc π n'est pas constructible et r non plus.

c) **La trisection de l'angle.**
Question : Est-il possible de partager un angle en trois angles égaux ?

Réponse :

On peut facilement partager un angle droit en trois angles de $\frac{\pi}{6}$.

Soit α un angle. On peut construire l'angle α si et seulement si $\cos\alpha$ est constructible (nous avons défini le réel constructible, pas l'angle constructible !).

On a pour tout réel x : $\cos 3x = 4\cos^3 x - 3\cos x$ ou encore :

$$4\cos^3(\alpha/3) - 3\cos(\alpha/3) - \cos\alpha = 0.$$

$\cos(\alpha/3)$ est donc racine du polynôme $P(x) = 4x^3 - 3x - \cos\alpha$. Il est de degré 3.

Tout dépend donc de α. Si P est irréductible sur **Q**, la trisection de α est impossible.

Si $\alpha = \frac{\pi}{2}$, par exemple, $\cos\alpha = 0$ et $P(x) = x(4x^2 - 3)$ donc $\cos(\alpha/3)$ est racine de $Q(x) = x$ ou de $Q'(x) = 4x^2 - 3$ ($\cos\frac{\pi}{6}$ est racine de Q') qui sont irréductibles de degré 2^n. On sait que la trisection de $\frac{\pi}{2}$ est possible.

Bibliographie :

J.-C. Carréga. *Théorie des corps : la règle et le compas*, Réédition Hermann 2001.

J.-M. Arnaudiès et J.-P. Delezoïde. *Constructions géométriques par intersections de coniques*. Bulletin APMEP n° 446, p. 367-382 et n° 447, p. 505-516,