Université Joseph Fourier — **Agrégation de Mathématiques**
Stage d'Autrans — **17 septembre 2013**

Constructions à la règle et au compas

Le but de la théorie, convertie ici sous forme de suite d'exercices, est de déterminer précisément quelles sont les constructions planes possibles à la règle et au compas.

Première partie : constructions élémentaires

Dans un plan affine euclidien orienté $\mathcal{P}$ (la feuille de papier !), on se donne un nombre fini de points A_0, A_1, ... , A_n. On choisit le point $O = A_0$ comme origine, A_0A_1 comme unité de longueur, et enfin on fixe un repère orthonormé direct $(O, \overrightarrow{u}, \overrightarrow{v})$ tel que $\overrightarrow{u} = \overrightarrow{A_0A_1}$. Ceci permet d'identifier $\mathcal{P}$ au plan complexe $\mathbb{C}$, quitte à faire une rotation de la feuille de papier. On note

$$a_0 = 0, \quad a_1 = 1, \quad a_j \in \mathbb{C}, \quad 2 \leq j \leq n$$

les affixes des points A_j (on s'intéresse particulièrement au cas $n = 1$, ce qui veut dire alors qu'il n'y a pas de complexes a_j, $j \geq 2$).

On dit qu'un point $M \in \mathcal{P}$, resp. son affixe $z \in \mathbb{C}$, est "contructible" (sous-entendu à la règle et au compas) à partir des points donnés A_j si on peut l'obtenir par une construction finie de droites, de cercles et de leurs intersections mutuelles, une droite étant déterminée par deux points donnés ou déjà construits, et un cercle par son centre et un point de la circonférence, supposés également donnés ou déjà construits. Dans la suite on cherche à déterminer des conditions nécessaires et suffisantes pour qu'un complexe $z \in \mathbb{C}$ soit constructible.

1) Si z et z' sont des complexes constructibles, montrer que $z+z'$ est constructible. (ne pas oublier que z et z' peuvent éventuellement correspondre à des points M, M' tels que O, M, M' soient alignés !)

2) Si z est constructible, montrer que $-z$, $\overline{z}$ et $|z|$ sont constructibles.

3) Si $x > 0$ est un réel constructible, montrer que $1/x$ et $\sqrt{x}$ sont constructibles.

4) Si x, y sont des réels constructibles, montrer que xy est constructible.

5) Si z et z' sont constructibles, montrer que zz' est constructible, et que si $z \neq 0$ est constructible, alors $1/z$ l'est.

6) Montrer que l'ensemble K des nombres constructibles est un corps, que celui-ci contient le corps k engendré par les $(a_j)_{j\geq 2}$ et leurs conjugués, noté

$$k = \mathbb{Q}(a_2, \ldots, a_n, \overline{a_2}, \ldots, \overline{a_n}) \qquad \text{(si } n = 1\text{, on a simplement } k = \mathbb{Q}\text{)},$$

et enfin que K est stable par conjugaison complexe.

7) Si z est constructible, montrer que les deux racines carrées complexes de z sont constructibles. En déduire que K contient toute solution complexe des équations du second degré $az^2 + bc + c = 0$ à coefficients $a, b, c \in K$.

8) A l'aide de ce qui précède, prouver "algébriquement" la constructibilité du pentagone régulier de centre O donné, ayant un sommet A_1 donné. [On pourra observer que les racines 5-ièmes de l'unité autres que 1 sont solutions de l'équation du 4e degré $z^4 + z^3 + z^2 + z + 1 = 0$, et que celle-ci se ramène à une résolution d'équations du second degré en posant $w = z + 1/z$. En déduire au passage les valeurs de $\cos(2\pi/5)$ et $\sin(2\pi/5)$.]

Deuxième partie : extensions de corps

On rappelle que si $K \subset L$ est un sous-corps du corps $(L, +, \times)$ (désormais, on omettra les lois pour simplifier les notations), alors L est un espace vectoriel sur K. On appelle *degré* de L sur K, noté $[L : K]$ la dimension de L comme espace vectoriel sur K. On dit que L est une *extension finie* de L si cette dimension est finie.

9) Soit $K \subset L \subset E$ des extensions successives de corps. Si $(\alpha_i)_{i\in I}$ est une base de L sur K et $(\beta_j)_{j\in J}$ une base de E sur L, montrer que $(\alpha_i\beta_j)_{(i,j)\in I\times J}$ est une base de E sur K. En déduire la relation qui existe entre les degrés $[E : K]$ et $[E : L]$, $[L : K]$.

10) On suppose que $L = K(\alpha)$ où α est la racine d'un polynôme irréductible de degré d à coefficient dans K. Montrer que l'anneau $K[\alpha]$ coïncide avec le corps $K(\alpha)$ et que $(1, \alpha, ..., \alpha^{d-1})$ est une base de $K(\alpha)$ sur K. Que vaut le degré $[K(\alpha) : K]$?

11) Si $K \subset L$ est une extension de degré 2, montrer que $L = K(\alpha)$ où α est solution d'une équation irréductible du second degré à coefficients dans K.

12) On reprend ici les notations de la première partie. Montrer que $z \in \mathbb{C}$ est constructible (i.e. $z \in K$) si et seulement si il existe une suite finie d'extensions successives K_j de degré 2 telle que

$$k = K_0 \subset K_1 \subset \ldots \subset K_N$$

avec $z \in K_N$. [Indication: le calcul d'intersections de droites et de cercles se ramène toujours à des équations du second degré au plus.]

13) En considérant le corps $k(z) \subset K_N$, en déduire que tout nombre complexe z constructible est racine d'un polynôme irréductible sur k dont le degré est une puissance de 2.

14) Montrer que la construction de l'heptagone régulier se ramène à la résolution d'une équation du troisième degré qui est irréductible sur $\mathbb{Q}$ (poser $w = z + 1/z$ avec $z = e^{2i\pi/7}$). En déduire que l'heptagone régulier n'est pas constructible à la règle et au compas.

15) Soit $\zeta_n = e^{2\pi i/n}$, $n \geq 3$. On note $n = p_1^{m_1} \ldots p_s^{m_s}$. On peut démontrer que

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \prod_{1\leq j\leq s} p_j^{m_j-1}(p_j - 1) \qquad \text{“fonction indicatrice d'Euler”.}$$

En déduire que si le polygône régulier à n côtés est constructible, alors n est de la forme

$$(*) \qquad n = 2^m p_1 \ldots p_s$$

où les p_j sont des “nombres premiers de Fermat” distincts. Rappelons qu'un nombre premier p est dit de Fermat si est de la forme $p = 2^k + 1$ et dans ce cas k est nécessairement une puissance de 2, soit $k = 2^n$; on note ainsi $F_n = 2^{2^n} + 1$; les seuls nombres premiers de Fermat connus sont

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537.$$

(Tous les F_n, $5 \leq n \leq 32$ sont composés. À ce jour, on ignore la nature de F_{33}...)

16) Apprendre les rudiments de la théorie de Galois, démontrer la valeur de $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ énoncée à la question précédente, et montrer que la condition $(*)$ donnée sur n est nécessaire et suffisante pour avoir la constructibilité (ainsi le polygône régulier à 17 côtés ou à 257 côtés est constructible à la règle et au compas !) : c'est le théorème de Gauss-Wantzel.