I Construction géométrique de $\mathbb{C}$, géométrie élémentaire

Notation 1. Pour $u \in \mathbb{R}^2 \setminus \{0\}$, on note $\arg u$ l'angle orienté $((1,0), u)$

Déf. 2. On munit $\mathbb{R}^2$ de la loi de composition interne $\times : \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ suivante : pour $u, v \in \mathbb{R}^2$ on pose

$$u \times v = \|u\| \cdot \|v\| \cdot (\cos\theta, \sin\theta) \quad \text{où} \quad \theta = \arg(u) + \arg(v) \text{ si } u, v \neq 0, \; = 0 \text{ si } u = 0 \text{ ou } v = 0.$$

Ppté 3 On a :

(i) $\forall u, v \in \mathbb{R}^2$, $\|u \times v\| = \|u\| \cdot \|v\|$

(ii) $\forall u, v \in \mathbb{R}^2 \setminus \{0\}$, $\arg(u \times v) = \arg(u) + \arg(v)$

Th. 4 L'ensemble $(\mathbb{R}^2, +, \times)$ est un corps noté $\mathbb{C}$. On dispose d'une injection $\mathbb{R} \hookrightarrow \mathbb{C}$ donnée par $t \longmapsto t(1,0)$.

Not. 5 On note $(1,0) = 1$ $\quad (0,1) = i \quad u \times v = uv$ et $(t,0) = t$.
On note $\|u\| = |u|$. $\mathbb{C}$ est muni de la topologie induite par $|\cdot|$.

Th. 6 On définit un morphisme de groupes $:(\mathbb{C}, +) \longrightarrow (\mathbb{C}^*, \times)$ en posant $\exp(z) = \sum_{n \geq 0} \frac{z^n}{n!}$ pour $z \in \mathbb{C}$.

Prop. 7 Pour $\theta \in \mathbb{R}$, on a $e^{i\theta} = \cos\theta + i \sin\theta$.

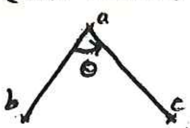
Cor. 8 Pour $\alpha, \beta \in \mathbb{R}$, on a :

(i) $\cos(\alpha + \beta) = \cos\alpha \cos\beta - \sin\alpha \sin\beta$

(ii) $\sin(\alpha + \beta) = \cos\alpha \sin\beta + \cos\beta \sin\alpha$

Cor. 9 Pour $\theta \in \mathbb{R}$ et $n \geq 0$, $\quad \cos(n\theta) + i\sin(n\theta) = (\cos\theta + i \sin\theta)^n$

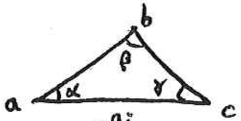
Th. 10 Soit $a, b, c \in \mathbb{C}$. Alors l'angle orienté $\theta = (b-a, c-a)$ est donné par $\theta = \arg \frac{c-a}{b-a}$



Cor. 11 Un polygône régulier à $n \geq 3$ cotés de centre 0 et ayant 1 pour sommet a exactement pour sommets $\mathbb{U}_n = \{\omega \in \mathbb{C} \mid \omega^n = 1\}$.

Cor. 12 Soit $a, b, c \in \mathbb{C}$ distincts et α, β, γ les angles du triangle abc comme ci-contre. Alors

$$\alpha + \beta + \gamma = \arg\left(\frac{b-a}{c-a} \, \frac{c-b}{a-b} \, \frac{a-c}{b-c}\right) = \pi \; [2\pi]$$



Cor. 13 On considère un polygône $a_1, \dots, a_n \in \mathbb{C}$ d'angles $\alpha_1, \dots, \alpha_n$. Alors $\alpha_1 + \dots + \alpha_n = 0 \; [\pi]$.

Th. 14 On dispose d'un "dictionnaire" qui permet de voir certaines transformations $\mathbb{R}^2 \to \mathbb{R}^2$ comme des transformations "algébriques" de $\mathbb{C}$.

Transformation de $\mathbb{R}^2$	Translation de vecteur $a \in \mathbb{R}^2$	$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$	$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$
$z \longmapsto$	$z + a$	$e^{i\theta} z$	λz	$\bar{z}$	$\frac{1}{2}(z + \bar{z})$	$\frac{1}{2}(z - \bar{z})$

En particulier, les similitudes de $\mathbb{R}^2$ sont exactement les fonctions affines de $\mathbb{C}$ en z ou $\bar{z}$.

Déf. 15 On dit d'une application $f : \mathbb{R}^2 \to \mathbb{R}^2$ qu'elle est holomorphe si elle est différentiable et si sa différentielle est, en chaque point, une similitude directe.

Th. 16 Une application $f : \mathbb{C} \to \mathbb{C}$ est holomorphe si et seulement si elle est $\mathbb{C}$-dérivable en chaque point de $\mathbb{C}$: pour tout $z \in \mathbb{C}$ la limite $\frac{1}{h}(f(z+h) - f(z))$ existe pour $h \in \mathbb{C}^*$, $h \to 0$.

Prop. 17 Soit $f : \mathbb{C} \to \mathbb{C}$. Les propositions suivantes sont équivalentes :
(i) L'application f est holomorphe sur $\mathbb{C}$.
(ii) L'application f est différentiable sur $\mathbb{C}$ et $\partial_x f + i \partial_y f = 0$.

Hors sujet ?

Prop. 18 On dispose des isomorphismes de groupes suivants :

$$\begin{aligned} \mathbb{U} &\longrightarrow SO(2) \\ \omega &\longmapsto (z \mapsto \omega z) \end{aligned} \qquad O(2) \simeq \mathbb{U} \rtimes_{\alpha} \{z, \bar{z}\} \quad \text{où } \alpha(\bar{z})(\omega) = \bar{\omega} \text{ pour } \omega \in \mathbb{U}.$$

Cor. 19 Soit $n \geq 3$ et soit D_n le groupe des isométries du polygône à n cotés $P_n = \{\exp(\frac{2ik\pi}{n}), k \in \mathbb{Z}\}$. Alors $D_n \overset{\phi}{\simeq} \langle r, s \mid r^n = 1, s^2 = 1, srs = r^{-1} \rangle$ où l'isomorphisme ϕ vérifie $\phi(r) = (z \mapsto \exp(\frac{2i\pi}{n}) z)$ et $\phi(s) = (z \mapsto \bar{z})$.

Cor. 20 Un sous-groupe fini $G \subset O(2)$ est soit isomorphe à un $\mathbb{Z}/n\mathbb{Z}$ $(n \geq 1)$ soit à un D_n $(n \geq 3)$.

Th. 21 Notons $\langle \cdot, \cdot \rangle$ le produit scalaire usuel sur $\mathbb{R}^2$ et $\det$ le déterminant par rapport à la base canonique. Alors :

$$\forall a, b \in \mathbb{R}^2 = \mathbb{C}, \quad \langle a | b \rangle = \mathrm{Re}(\bar{a} b) \qquad \det(a, b) = \mathrm{Im}(\bar{a}, b).$$

Cor. 22 Pour $a, b \in \mathbb{C}$, $\quad |a+b|^2 + |a-b|^2 = 2(|a|^2 + |b|^2)$.

Cor. 23 On considère une courbe C^1 $\gamma : [0, 2\pi] \longrightarrow \mathbb{R}^2$ fermée délimitant une aire $\mathcal{A}$. Alors $\mathcal{A} \leq 4\pi (\mathrm{long}(\gamma))^2$.

II Sphère de Riemann (Annexe 1)

Déf. 24 On nomme sphère de Riemann l'espace topologique $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ dont les ouverts sont les ouverts de $\mathbb{C}$ et les ensembles $E \cup \{\infty\}$ où $E \subset \mathbb{C}$ et $\mathbb{C} \setminus E$ est un compact de $\mathbb{C}$.

Prop. 25 On définit un homéomorphisme $\phi : \mathbb{S}^2 \longrightarrow \hat{\mathbb{C}}$ en posant, pour $(u, v, w) \in \mathbb{S}^2 \subset \mathbb{R}^3$, $\phi(u, v, w) = {}^{u+iv}/_{1-w}$ si $w \neq 1$ et $\phi(u, v, w) = \infty$ sinon.

Application 26: $\hat{\mathbb{C}}$ est compact. Les seules fonctions méromorphes sur $\hat{\mathbb{C}}$ (c'est-à-dire qui soient méromorphes sur $\mathbb{C}$ et se prolongent par continuité en $\{\infty\}$) sont les fractions rationnelles.

déf et prop 27: Les automorphismes de $\hat{\mathbb{C}}$ sont les homographies définies par $z \in \hat{\mathbb{C}} \to \frac{az+b}{cz+d}$ où $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C})$

Rq 28: il est engendré par $z \to \frac{1}{z}$ et les similitudes.
Pour présenter les propriétés liées aux homographies nous définissons la droite projective $P^1(\mathbb{C})$ dont la sphère de Riemann est une représentation.

déf 29: Pour E un $\mathbb{K}$-ev de dimension $n+1$, on définit la relation d'équivalence, pour $x, y \in E \setminus \{0\}$, $x \mathcal{R} y$ ssi il existe $\lambda \in \mathbb{K}^*$ tq $x = \lambda y$
on note alors $P(E) := \frac{E \setminus \{0\}}{\sim}$ munie de la topologie quotient l'espace projectif. On note $p : E \setminus \{0\} \to P(E)$ la projection et $C\ell(y)$ la classe d'équivalence de (x, y)

Ex : $P^1(\mathbb{C})$ est la droite projective du plan complexe $\mathbb{C}$.

Prop 30: dans un repère cartésien $(z_1, \dots, z_{n+1})$, l'hyperplan affine $z = 1$ est homéomorphe à $P(E) \setminus P(F)$ où F est l'hyperplan vectoriel $z = 0$
En particulier, $\mathbb{C} \simeq P^1(\mathbb{C}) \setminus \{\infty\}$

déf 31: $PGL(E)$ est l'ensemble des applications f de $P(E)$ dans lui-même telles qu'il existe $\tilde{f} \in GL(E)$ tq $f \circ p = p \circ \tilde{f}$.
En particulier $PGL(E)$ est isomorphe à $\frac{GL(E)}{\{\lambda Id, \lambda \in \mathbb{K}^*\}}$

$$\begin{array}{ccc} E \setminus \{0\} & \xrightarrow{\tilde{f}} & E \setminus \{0\} \\ p \downarrow & & \downarrow p \\ P(E) & \xrightarrow{f} & P(E) \end{array}$$

application 32: on peut décrire explicitement $PGL(\mathbb{C}^2)$, ce sont les applications
$(1, z) \to [1, \frac{az+b}{cz+d}]$
$(0, 1) \to [1, \frac{a}{c}]$
on obtient un homéomorphisme entre $P^1(\mathbb{C})$ et $\hat{\mathbb{C}}$.

déf 33: un vecteur $(m_0, \dots, m_{n+1})$ forme un repère projectif de $P(E)$ si $(m_1, \dots, m_n)$ est l'image par p d'une base $(e_1, \dots, e_{n+1})$ et $m_0 = p(e_1 + \dots + e_{n+1})$

Rq 34: l'image de trois vecteurs (a, b, c) non colinéaires (deux à deux) forment un repère projectif de $P^1(\mathbb{C})$

Prop 35: étant donné deux repères projectifs (a, b, c) et (u, v, w) de $P^1(\mathbb{C})$, il existe une unique homographie qui envoie (a, b, c) sur (u, v, w)

déf 36: le birapport noté $[a, b, c, d]$ est l'image de d par l'unique homographie qui envoie $\begin{cases} a \to 0 \\ b \to 1 \\ c \to \infty \end{cases}$ (dans $P^1(\mathbb{C})$)

Rq 37: on peut explicitement calculer le birapport $[a, b, c, d] = \frac{d-b}{d-a} \times \frac{c-a}{c-b}$

Prop 38: quatre points de $\mathbb{C}$ sont alignés ou cocycliques (appartiennent au même cercle) ssi leur birapport est réel.

Application 39: Toute homographie de $\mathbb{C}$ transforme un cercle ou une droite en un cercle ou une droite.

prop 40: Si $f \in PGL(\mathbb{C})$ alors f conserve le birapport, c'est-à-dire

$$[f(a), f(b), f(c), f(d)] = [a, b, c, d]$$

Déf Une inversion envoie l'intérieur d'un cercle sur l'extérieur et vice-versa.

Déf: Une inversion est la composée d'une homographie et d'une réflexion: $\frac{1}{\bar{z}}$ par ex.

déf 41 le groupe circulaire est le groupe engendré par les homographies et la symétrie $z \to \bar{z}$ qui définissent ainsi des transformations sur $\hat{\mathbb{C}}$.

prop 42: le groupe circulaire est engendré par les inversions et les réflexions.

Thm 43: les transformations qui préservent l'ensemble des cercles et droites de $\mathbb{R}^2$ sont les éléments du groupe cyclique.

déf 44: le demi plan de Poincaré est l'ensemble $H = \{z \in \mathbb{C}, Im(z) > 0\} \cup \{\infty\}$
On appelle droites hyperboliques les demi droites de la forme $(a + i\mathbb{R}_+^*)$ pour $a \in \mathbb{R}$ et les demi cercles de centre réels. On note $\mathcal{D}_H$ l'ensemble de ces éléments

prop 45 les homographies de la forme $z \to \frac{az+b}{cz+d}$ avec $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$ et $\det = (ad - bc) > 0$

agissent transitivement sur $\mathcal{H}$ et sur $\mathcal{D}_H$

III Constructions à la règle et au compas (Annexe 2)

Déf. 46 Un nombre $z \in \mathbb{C}$ est dit constructible en une étape à partir d'un ensemble E si l'une des conditions suivantes est vérifiée :

(i) $\exists\, a,b,c \in E$, $a',b',c' \in E$ $\mid$ $|z-a| = |b-c|$ et $|z-a'| = |b'-c'|$

(ii) $\exists\, a,b,c \in E$, $d,e \in E$, $\lambda \in \mathbb{R}$ $\mid$ $|z-a| = |b-c|$ et $z = d + \lambda(e-d)$

(iii) $\exists\, d,e \in E$, $\lambda \in \mathbb{R}$, $d',e' \in E$, $\lambda' \in \mathbb{R}$ $\mid$ $z = d + \lambda(e-d)$ et $z = d' + \mu(e-d)$

En d'autres termes, z est intersection de deux droites ou deux cercles ou une droite et un cercle construits sur E.

Déf. 47 Un nombre $z \in \mathbb{C}$ est constructible s'il est constructible à partir de $\mathbb{Q}$ en un nombre fini d'étapes.

Ex. 48 Un nombre $z \in \mathbb{C}$ est constructible si et seulement si $\mathrm{Re}\, z$ et $\mathrm{Im}\, z$ le sont également.

Prop. 49 Si $z, \omega \in \mathbb{C}$ sont constructibles et $\omega \neq 0$ alors $z+\omega$, z/ω le sont également. Si $x \in \mathbb{R}_+ \subset \mathbb{C}$ est constructible, $\sqrt{x}$ l'est également.

Cor. 50 L'ensemble des nombres constructibles est un sous-corps de $\mathbb{C}$.

Th. 51 (Wantzel) Un nombre $z \in \mathbb{C}$ est constructible si et seulement si il existe une tour d'extensions $K_0 = \mathbb{Q} \subset K_1 \subset K_2 \subset \cdots \subset K_n$ telles que $2 = [K_{i+1} : K_i]$ pour $i+1 \leq n$ et $z \in K_n$.

Cor. 52 (Pentagône) Le pentagône régulier $\overbrace{\text{de centre}}^{\text{à 5 cotés}}$ 0 et ayant 1 pour sommet est constructible (i.e. chacun de ses sommets le sont).

Cor. 53 (Duplication du cube) Le nombre $\sqrt[3]{2}$ n'est pas constructible.

Cor. 54 (Trissection de l'angle) Soit $\alpha \in [0, 2\pi]$. Le nombre $\cos(\alpha/3)$ est constructible (resp. constructible à partir de $\mathbb{Q}(\cos\alpha)$) si et seulement si $4X^3 - 3X - \cos(\alpha)$ n'est pas irréductible dans $\mathbb{Q}[X]$ (resp. $\mathbb{Q}(\cos\alpha)[X]$).

Ex. 55 Le polygône régulier à 9 cotés de centre 0 et ayant 1 pour sommet n'est pas constructible.

Th. 56 (Constructibilité ou non des polygones réguliers)

(i) Soit $m,n \geq 1$ avec $m \wedge n = 1$. Alors $\cos(2\pi/mn)$ est constructible si et seulement si $\cos(2\pi/m)$ et $\cos(2\pi/n)$ le sont.

(ii) Soit $p \geq 3$ premier et $\alpha \geq 1$. Le nombre $\cos(2\pi/p^\alpha)$ est constructible si et seulement si $\alpha = 1$ et $p = 1 + 2^{2^n}$ pour un certain $n \in \mathbb{N}$.

Ex. 57 Le nombre $\cos\left(\frac{2\pi}{17}\right)$ est constructible.

IV Quaternions

hors sujet ?

Déf. 58 On note $\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ et $\mathbb{H} = \mathrm{Vect}_{\mathbb{R}} \{\mathbb{1}, I, J, K\} \subset M_2(\mathbb{C})$. C'est une sous-algèbre de $M_2(\mathbb{C})$ dont le seul élément non inversible est 0. On la nomme algèbre des quaternions.

Prop. 59 On a $IJK = -\mathbb{1} = I^2 = J^2 = K^2$. En particulier, on dispose d'une injection $\mathcal{J} : \mathbb{C} \hookrightarrow \mathbb{H}$ en posant $\mathcal{J}(x+iy) = x\mathbb{1} + Iy$. On notera donc $\mathbb{1} = 1$, $I = i$, $J = j$ et $K = k$.

Déf. 60 Pour $z = a + ib + jc + kd \in \mathbb{H}$, on pose :

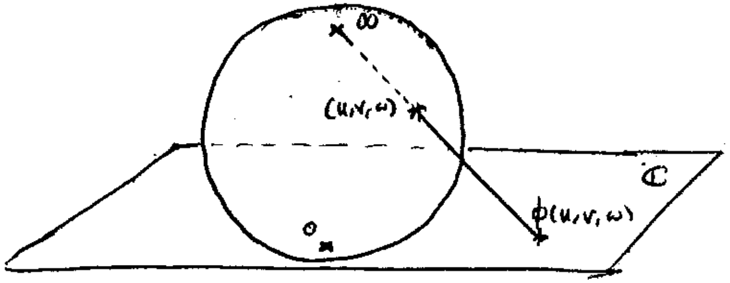
(i) $\bar{z} = a - ib - jc - kd$ (transconjuguée de $z \in M_2(\mathbb{C})$)

(ii) $N(z) = z\bar{z} =$ (déterminant de $z \in M_2(\mathbb{C})$)

Cela permet en particulier de munir $\mathbb{S}^3 = \{z \in \mathbb{H} \mid N(z) = 1\}$ d'une structure de groupe.

Th. 61 On pose $\mathbb{H}_p = \mathrm{Vect}_{\mathbb{R}} \{i, j, k\} \equiv \mathbb{R}^3$. Alors le groupe $\mathbb{H}^\times$ agit sur $\mathbb{H}_p$ par conjugaison, ce qui se traduit en une action sur $\mathbb{R}^3$ par $SO(3)$. Le noyau de cette action est $\mathbb{R}^\times$ de sorte que : $SO(3) \simeq \mathbb{H}^\times / \mathbb{R}^\times$.

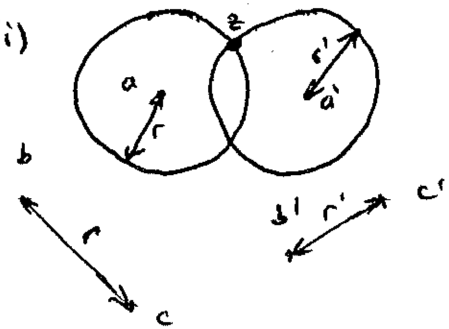
Annexe 1 : Sphère de Riemann



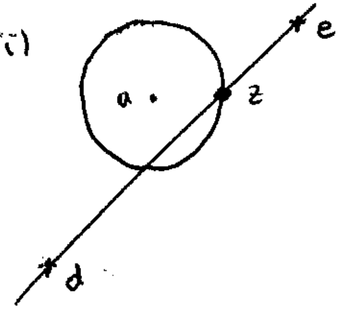
Annexe 2

(46) $a, b, c, d, e, \; a', b', c', d', e' \in E$.

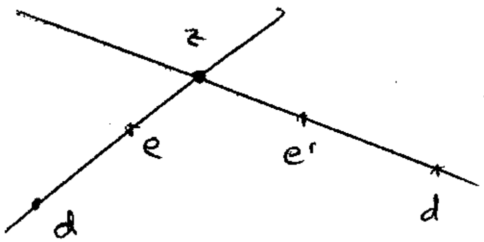
(i)



(ii)

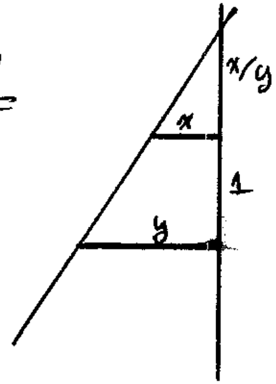


(iii)

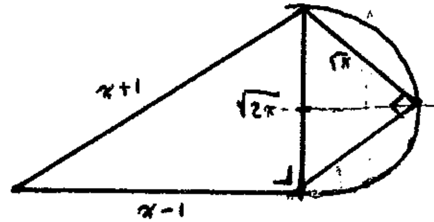


(49) $x, y \in \mathbb{R}_+ \quad y \neq 0$

x/y



$\sqrt{x}$ $\quad x \geq 1$



$T : \mathbb{C} \to \mathbb{C}$, $z \mapsto (1+i)z - i$ est une similitude de centre 1 et de rapport $(1+i)$ [rapport $\sqrt{2}$ et d'angle $\frac{\pi}{4}$].

$a, b, c \in \mathbb{C}$ de même module. Affixe de h l'orthocentre ? $\to a + b + c =: h$. [Qh 21 : $\mathrm{Re}\left((a+b+c-a)\overline{(b-c)}\right) = 0$]

l'isobaricentre ? $\to \frac{1}{3}(a+b+c)$

↳ ainsi orthocentre, isobaricentre et centre du cercle circonscrit sont alignés !

Th 61 : un isomorphisme pour SO_4 ?

Polygones réguliers constructibles [1]

Leçons : 102, 121, 125, 182, 183

[MerCdG], théorème 318

Théorème (*Gauss-Wantzel*)

Soit p un nombre premier impair, $\alpha \in \mathbb{N}^*$.
Alors l'angle $\widehat{\frac{2\pi}{p^\alpha}}$ est constructible $\Leftrightarrow$ $\alpha = 1$ et p est un nombre premier de Fermat (c'est-à-dire que p est un nombre premier qui s'écrit sous la forme $1 + 2^{2^\beta}$, où $\beta \in \mathbb{N}$).

Démonstration :

$\Rightarrow$ On pose $q = p^\alpha$ et $\omega = \exp\left(\frac{2i\pi}{q}\right)$.

On suppose que l'angle $\widehat{\frac{2\pi}{q}}$ est constructible, id est, que $\cos\left(\frac{2\pi}{q}\right)$ est un nombre constructible.
Alors, par le théorème de Wantzel [2], on obtient : $\left[\mathbb{Q}\left(\cos\frac{2\pi}{q}\right) : \mathbb{Q}\right] = 2^m$, où $m \in \mathbb{N}$.
Aussi, le polynôme cyclotomique Φ_q étant le polynôme minimal de ω, on a :

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg \Phi_q = \varphi(q) = p^{\alpha-1}(p-1).$$

Comme $\omega^2 - 2\omega\cos\frac{2\pi}{q} + 1 = 0$, on a $\cos\frac{2\pi}{q} \in \mathbb{Q}(\omega)$ et même $\left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\frac{2\pi}{q}\right)\right] = 2$.
Par multiplicativité du degré, on obtient $2^{m+1} = p^{\alpha-1}(p-1)$.
Comme p est impair, il vient $\alpha = 1$, puis $p = 1 + 2^{m+1}$; montrons que $m+1$ est une puissance de 2.
On écrit alors $m + 1 = \lambda 2^\beta$, avec $\beta \in \mathbb{N}$ et $\lambda \in \mathbb{N}^*$ impair ; on a alors $p = 1 + \left(2^{2^\beta}\right)^\lambda$.
Or, λ étant impair, on a dans $\mathbb{Z}[X]$: $1 + X \mid 1 + X^\lambda$ et donc $1 + 2^{2^\beta} \mid p$ et donc, comme p est premier, on en déduit $\lambda = 1$.
Donc p est un nombre premier de Fermat.

$\Leftarrow$ On note $n = 2^\beta$, de sorte que $p = 1 + 2^n$, et $\zeta = \exp\left(\frac{2i\pi}{p}\right)$.
On a : $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \Phi_p = \varphi(p) = p - 1$.

1. On peut ajouter quelques résultats autour de ce développement pour détailler son utilité.

Lemme

- Les angles de la forme $\widehat{\frac{2\pi}{2^\alpha}}$ sont constructibles, où $\alpha \in \mathbb{N}^*$.
- Soient $m, n \in \mathbb{N}^*$, avec $m \wedge n = 1$,
  Alors l'angle $\widehat{\frac{2\pi}{mn}}$ est constructible $\Leftrightarrow$ $\widehat{\frac{2\pi}{m}}$ et $\widehat{\frac{2\pi}{n}}$ le sont.

En conséquence, les polygones réguliers constructibles sont ceux qui possèdent $2^{\alpha_2} \prod_{p \in \mathcal{F}} p^{\alpha_p}$ côtés, où $\mathcal{F}$ est l'ensemble des nombres premiers de Fermat, et où les α_i sont des entiers naturels.

En effet :
- C'est immédiat, puisque par récurrence, il suffit de savoir tracer des bissectrices à la règle et au compas.
- $\Leftarrow$ Il est facile de construire le multiple d'un nombre constructible (en reportant avec le compas le bon nombre de fois la corde formée par l'angle sur le cercle unité).

  $\Rightarrow$ Par Bézout, $\exists \lambda, \mu \in \mathbb{Z}, \lambda m + \mu n = 1$; dès lors $\widehat{\frac{2\pi}{mn}} = \lambda\widehat{\frac{2\pi}{m}} + \mu\widehat{\frac{2\pi}{n}}$.
  Et on construit sans peine la somme de deux angles constructibles en traçant des représentants de ces angles avec un côté adjacent.

2. Le théorème de Pierre-Laurent Wantzel, énoncé en 1837, donne une condition nécessaire et suffisante pour qu'un nombre soit constructible à la règle et au compas : il faut et il suffit que ce nombre appartienne à une extension de $\mathbb{Q}$ qui soit le terme d'une suite d'extensions quadratiques.

On note $G = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta))$; et si $g \in G$, alors g fixe $\mathbb{Q}$ et est entièrement déterminé par $g(\zeta)$.
g étant un morphisme d'anneaux, on a : $0 = g(0) = g\left(\Phi_p(\zeta)\right) = \Phi_p(g(\zeta))$.
Donc $g(\zeta)$ est nécessairement une racine de Φ_p, donc $g(\zeta) \in \{\zeta, \zeta^2, \dots, \zeta^{p-1}\}$.
Il faudrait alors montrer qu'on définit bien ainsi des automorphismes du corps $\mathbb{Q}(\zeta)$; et alors

$$G = \left\{ g_k : \zeta \mapsto \zeta^k \middle| k \in [\![1, p-1]\!] \right\} \simeq \left(\mathbb{Z}/p\mathbb{Z} \right)^\times \underset{3}{\simeq} \mathbb{Z}/(p-1)\mathbb{Z}.$$

Désormais, g désignera un générateur de G.
Pour $i \in [\![0, n]\!]$, on note $K_i = \mathrm{Ker}\left(g^{2^i} - \mathrm{Id} \right)$; c'est un sous-corps de $\mathbb{Q}(\zeta)$.
De plus, $\forall i \in [\![0, n-1]\!], g^{2^{i+1}} = \left(g^{2^i} \right)^2$ implique $K_i \subseteq K_{i+1}$.
Comme g génère G, $\left(g^i(\zeta)\right)_{0 \leqslant i \leqslant p-2}$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\zeta)$.

Soit $z \in K_0$, $\exists \lambda_0, \dots, \lambda_{p-2} \in \mathbb{Q}$, $z = \sum_{i=0}^{p-2} \lambda_i g^i(\zeta)$; mais $z = g(z) = \lambda_{p-2}\zeta + \sum_{i=1}^{p-2} \lambda_{i-1} g^i(\zeta)$.

Tous les scalaires λ_i sont donc égaux et $z = \lambda_0 \sum_{i=0}^{p-2} g^i(\zeta) = \lambda_0 \sum_{j=1}^{p-1} \zeta^j = -\lambda_0 \in \mathbb{Q}$. Donc $K_0 = \mathbb{Q}$.

Pour montrer que $\forall i \in [\![0, n-1]\!], K_i \neq K_{i+1}$, il faudrait considérer l'élément $z = \sum_{h=0}^{2^{n-i-1}-1} g^{2^{i+1}h}(\zeta)$.[4]

On en déduit alors qu'on a la suite d'extensions :

$$\mathbb{Q} = K_0 \underset{\neq}{\subseteq} K_1 \underset{\neq}{\subseteq} \dots \underset{\neq}{\subseteq} K_n = \mathbb{Q}(\zeta).$$

Mais $2^n = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \prod_{i=0}^{n-1} \underbrace{[K_{i+1} : K_i]}_{\geqslant 2}$.
Ainsi, $\forall i \in [\![0, n-1]\!], [K_{i+1} : K_i] = 2$.
Par le théorème de Wantzel, tous les éléments de $\mathbb{Q}(\zeta)$ sont donc constructibles ; mais $\cos \frac{2\pi}{p} = \frac{\zeta + \zeta^{-1}}{2}$ en fait partie. ∎

Références

[MerCdG][5] D.-J. MERCIER – *Cours de géométrie, préparation au CAPES et à l'agrégation*, Publibook, 2008.

3. Pour la cyclicité de $\mathbb{F}_p^\times$, on renvoie à la page ??.

4. Okay, je le fais, mais c'est vraiment parce que c'est vous. On a : $g^{2^i}(z) = \sum_{h=0}^{2^{n-i-1}-1} g^{2^{i+1}h+2^i}(\zeta) \neq z$ car les vecteurs de base intervenant dans la décomposition ne sont pas les mêmes (on a décalé les coordonnées de 2^i, alors qu'entre deux coordonnées non-nulles, il y a $2^{i+1} - 1$ zéros). Et aussi : $g^{2^{i+1}}(z) = \sum_{h=0}^{2^{n-i-1}-1} g^{2^{i+1}(h+1)}(\zeta) = \sum_{h=1}^{2^{n-i-1}-1} g^{2^{i+1}h}(\zeta) + \underbrace{g^{2^{i+1}2^{n-i-1}}(\zeta)}_{=\zeta} = z$.

5. On trouvera également dans cette référence une façon de construire le pentagone régulier à la règle et au compas.

Action de $PSL_2(\mathbb{R})$ sur le demi–plan de Poincaré

Arnaud GIRAND

5 juillet 2012

Référence :
- [Mé06], p. 568–570

Prérequis :
- espace $\mathbb{P}^1(\mathbb{C})$;
- homographies, birapport.

On considère le demi–plan de Poincaré, défini par $\mathcal{H} := \{z \in \mathbb{C} \,|\, \Im(z) > 0\} \cup \{\infty\} \subset \mathbb{P}^1(\mathbb{C})$. On appelle droite hyperbolique de $\mathcal{H}$ les demi–cercles (épointés) de $\mathcal{H}$ dont le centre est réel, ainsi que les demi–droites (toujours épointées) verticales (i.e parallèles à $i\mathbb{R}_+^*$) et on note D_h l'ensemble des telles droites.

Lemme 1
Soient z, w deux points distincts de $\mathcal{H}$.
Alors il existe une unique droite hyperbolique passant par z et w.

DÉMONSTRATION :
- *Existence.* Soit $\mathcal{C}$ le cercle ou droite de $\mathbb{P}^1(\mathbb{C})$ passant par w, z et $\bar{z}$. On remarque alors que $\overline{[z, w, \bar{z}, \bar{w}]} = [z, w, \bar{z}, \bar{w}]$ donc $[z, w, \bar{z}, \bar{w}] \in \mathbb{R}$. De fait, les points $z, w, \bar{z}$ et $\bar{w}$ sont cocycliques ou alignés (nécessairement verticalement,h vu la présence des conjugués), i.e $\bar{w} \in \mathcal{C}$. De fait, comme le conjugué $\bar{\mathcal{C}}$ de $\mathcal{C}$ contient les quatre points $z, w, \bar{z}, \bar{w} \in \mathcal{C}$ on a $\mathcal{C} = \bar{\mathcal{C}}$.
  De fait, $\mathcal{C}$ est une droite verticale ou un cercle de centre réelle, ce qui signifie que $\mathcal{C} \cap \mathcal{H} \in D_h$, d'où l'existence d'une droite hyperbolique passant par z et w.
- *Unicité.* C'est immédiat : soit z et w sont alignés verticalement, auquel cas on a unicité de la droite verticale passant par ces deux points et absence de demi–cercle de centre réel faisant de même, soit ils ne le sont pas et auquel cas il existe un unique demi cercle de centre réel passant par z et w (car ce cercle doit nécessairement passer par —par exemple— $\overline{z}$).

Proposition 1
On a les deux propriétés suivantes :
(i) $PSL_2(\mathbb{R})$ agit transitivement sur $\mathcal{H}$;
(ii) $PSL_2(\mathbb{R})$ agit transitivement sur D_h.

DÉMONSTRATION : Remarquons que deux matrices M et N donnent la même homographie si et seulement si il existe $\lambda \in \mathbb{R}$ tel que $M = \lambda N$; ainsi $PSL_2(\mathbb{R}) = \{h \in PGL_2(\mathbb{R}) \,|\, \det(h) > 0\}$: seul le signe du déterminant d'une homographie est bien défini.

(i) Soit $z \in \mathcal{H}$ et $h : z \mapsto \frac{az+b}{cz+d} \in PSL_2(\mathbb{R})$. Alors, si on pose $z = x + iy$ on a :

$$\begin{aligned}
h(z) &= \frac{ax + b + iay}{cx + d + icy} \\
&= \frac{(ax + b + iay)(cx + d - icy)}{(cx + d)^2 + (cy)^2} \\
&= \frac{acx^2 + ad - iacyx + bcx + bd - ibcy + iacyx + iady + 1acy^2}{(cx + d)^2 + (cy)^2}
\end{aligned}$$

De fait, $\Im(h(z))$ est du signe de $-bcy + ady = (ad - bc)\Im(y) > 0$ car $ad - bc > 0$. Ainsi, par stabilité, $PSL_2(\mathbb{R})$ agit sur $\mathcal{H}$. Enfin, $PSL_2(\mathbb{R})$ contient les translations et homothéties de rapport positif, d'où la transitivité (faire un dessin, sans oublier que l'on ne part jamais vraiment de l'axe réel donc que les homothéties positives font remonter "en diagonale").

(*ii*) Comme les homographies conservent les cercles ou droites, $PGL_2(\mathbb{R})$ agit naturellement sur l'ensemble des cercles ou droites de $\mathbb{P}^1(\mathbb{C})$. De plus, les homographies positives conservent $\mathcal{H}$ (cf. supra), donc on a bien une action de $PSL_2(\mathbb{R})$ sur D_h. Soit $z \in \mathcal{H}$ et soit $D \in D_h$ passant par z. D'après le point (i), il existe $g \in PSL_2(\mathbb{R})$ tel que $g(z) = i$: $g(D)$ est alors une droite hyperbolique passant par i.

Soit D_i une droite hyperbolique passant par i telle que $D_i \neq i\mathbb{R}_+^*$: c'est alors un demi-cercle coupant l'axe réel en deux points ; considérons l'un de ces points, soit t. Il existe alors un unique réel $\theta \in (-\pi, \pi)$ tel que $\tan(\theta) = t$. On note alors $h_\theta \in PSL_2(\mathbb{R})$ l'homographie associée à la rotation $\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \in SL_2(\mathbb{R})$ et on remarque que :

$$\begin{aligned} h_\theta(i) &= \frac{i\cos(\theta) - \sin(\theta)}{i\sin(\theta) + \cos(\theta)} \\ &= e^{-i\theta}(i\cos(\theta) - \sin(\theta)) \\ &= e^{-i\theta}i(\cos(\theta) + \sin(\theta)) \\ &= i \end{aligned}$$

Ainsi $h_\theta \in \mathrm{Stab}_{PSL_2(\mathbb{R})}(i)$. De plus :

$$\begin{aligned} h_\theta(t) &= \frac{t\cos(\theta) - \sin(\theta)}{t\sin(\theta) + \cos(\theta)} \\ &= \frac{\tan(\theta)\cos(\theta) - \sin(\theta)}{t\sin(\theta) + \cos(\theta)} \\ &= 0 \end{aligned}$$

In fine, si on note D_i' le cercle ou droite correspondant à D_i dans $\mathbb{P}^1(\mathbb{C})$, $h_\theta(D_i')$ passe par i et 0. Comme $h_\theta(D_i)$ est une droite hyperbolique, on a nécessairement $h_\theta(D_i') = i\mathbb{R}$ et donc $h_\theta(D_i) = i\mathbb{R}_+^*$.

Ainsi, quitte à remplacer g par une composée de la forme $h_\theta \circ g$, avec θ bien choisi, on a $g(D) = i\mathbb{R}_+^*$: l'action considérée est bien transitive.

Détails supplémentaires :

- Soient quatre points $a, b, c, d \in \mathbb{P}^1(\mathbb{C})$; on suppose $[a, b, c, d] \in \mathbb{R}$. Notons h l'homographie définissant ce birapport, i.e telle que $h(a) = 0, h(b) = 1, h(c) = \infty$. Alors $h(a), h(b), h(c)$ et $h(d) = [a, b, c, d]$ sont alignés et comme l'homographie h^{-1} conserve les cercles ou droites on a bien que a, b, c et d sont alignés ou cocycliques.

Références

[Mé06] Jean-Yves Mérindol. *Nombres et algèbre.* EDP Sciences, 2006.