# Nombres complexes, sous-groupe des unités et géométrie

*prérequis* :

**Table des matières**



## 1. Construction de $\mathbb{C}$ et premières propriétés

### 1.1. Nombres complexes. —

***Définition 1.1***. — $\mathbb{C}$ est le corps de rupture sur $\mathbb{R}$ du polynôme irréductible $X^2+1$.

*Remarque :* le fait que $X^2+1$ soit irréductible découle du fait qu'il ne prend que des valeurs $\geq 1$. En désignant par $i$ une racine quelconque de $X^2+1$ dans $\mathbb{C}$, la famille $(1,i)$ est alors une base de $\mathbb{C}$ en tant que $\mathbb{R}$ espace vectoriel ; autrement dit tout nombre complexe $z$ s'écrit de manière unique sous la forme $x+iy$. Le réel $x$ (resp. $y$) s'appelle *la partie réelle* (resp. *la partie imaginaire*) de $z$ et se note $\mathrm{Re}\,(z)$ (resp. $\mathrm{Im}(z)$).

Le corps $\mathbb{C}$ est aussi le corps de décomposition de $X^2+1$ sur $\mathbb{R}$ e sorte que l'extension $\mathbb{C}/\mathbb{R}$ est galoisienne (comme toute les extensions de degré 2 sur un corps de caractéristique nulle) : *son groupe de Galois* est $\{\mathrm{Id},\tau\}$ où $\tau(x+iy)=x-iy$ s'appelle la conjugaison complexe.

***Définition 1.2***. — Le module de $z\in\mathbb{C}$ est la racine carrée positive du réel positif $z\tau(z)=x^2+y^2$ ; on le note $|z|$.

*Remarque :* le module définit une norme sur $\mathbb{C}$ qui est multiplicative, i.e. $|zz'| = |z|.|z'|$. On en déduit en particulier que l'ensemble $\mathbb{U}$ des complexes de norme 1 est un sous-groupe multiplicatif de $\mathbb{C}^\times$.

***Théorème 1.3***. — *Toute extension du corps $\mathbb{R}$ est $\mathbb{C}$ ou le corps des quaternions.*

**1.2. L'exponentielle complexe.** — Comme $\mathbb{C}$ munie de la norme $|.|$ est complet, toute suite de Cauchy y admet une limite. Appliquons cela à la série $\sum_{n\geq 0} \frac{z^n}{n!}$ qui est une série entière de rayon de convergence $+\infty$ et appelons $e^z$ sa limite. On a alors les propriétés suivantes :
- $\tau(e^z) = e^{\tau(z)}$, $|e^z| = e^{\mathrm{Re}\ z}$ et $e^z \in \mathbb{U}$ si et seulement si $z \in i\mathbb{R}$ ;
- $e^{z+u} = e^z e^u$, pour $e^z \neq 0$, $(e^z)^{-1} = e^{-z}$ ;
- la dérivée de l'application $z \mapsto e^z$ est égale à $e^z$.

***Théorème 1.4***. — *L'application e est un morphisme continu, surjectif et non injectif de $(\mathbb{C}, +)$ dans $(\mathbb{C}^\times, \times)$ dont la restriction à $i\mathbb{R}$ est surjective à valeurs dans $\mathbb{U}$ et de noyau $2\pi\mathbb{Z}$ où $frm-e\pi$ est le plus petit réel $a > 0$ tel que $e^{ia} = 1$.*

***Définition 1.5***. — Pour $z \in \mathbb{C}^\times$, on note $\arg(z)$ l'antécédent de $\frac{z}{|z|}$ dans $\mathbb{R}/2\pi\mathbb{Z}$ induit par l'isomorphisme $f : \mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{U}$ ; on l'appelle l'argument de $z$.

***Corollaire 1.6***. — *tout morphisme continu de $(\mathbb{R}, +)$ dans $(\mathbb{C}^\times, \times)$ est de la forme $t \mapsto e^{i\alpha t}$.*

On définit ensuite les fonctions cosinus et sinus :

$$\cos z = \frac{e^{iz} + e^{-iz}}{2}, \quad \sin z = \frac{e^{iz} - e^{-iz}}{2i}$$

que l'on peut aussi exprimer sous forme de séries entières. On vérifie alors les faits suivants :
- $(\cos)' = -\sin$ et $(\sin)' = \cos$ ;
- $\cos^2 z + \sin^2 z = 1$ ;
- $\pi/2$ est le plus petit réel $a > 0$ tel que $\cos a = 0$ ;
- l'ensemble des périodes des restrictions de sin et cos à $\mathbb{R}$ est $2\pi\mathbb{Z}$.

**1.3. Polynômes et racines dans $\mathbb{C}$.** —

***Théorème 1.7***. — *(d'Alembert-Gauss) Pour tout $P \in \mathbb{C}[X]$ il existe $\alpha \in \mathbb{C}$ tel que $P(\alpha) = 0$.*

***Corollaire 1.8***. — *$\mathbb{C}$ est algébriquement clos.*

*Application :* elles sont nombreuses, citons :
- les polynômes irréductibles de $\mathbb{R}[X]$ sont de degré 1 ou 2 et dans ce dernier cas avec un discriminant strictement négatif ;
- tout endomorphisme de $\mathbb{C}^n$ est trigonalisable, ce qui permet en particulier de prouver le théorème de Cayley-Hamilton.

***Définition 1.9***. — Un nombre complexe $z$ tel que $\mathbb{Q}[z]$ est une extension finie de $\mathbb{Q}$ est dit algébrique, ce qui revient à dire qu'il est la racine d'un polynôme à coefficients dans $\mathbb{Q}$.

La réunion des nombres algébriques forme un corps $\bar{\mathbb{Q}}$ appelé la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$. L'ensemble des polynômes de degré $n$ à coefficients dans $\mathbb{Q}$ étant dénombrable, chacun possédant $n$ racines dans $\mathbb{C}$, on voit que $\bar{\mathbb{Q}}$ est dénombrable. Les nombres complexes $z$ non algébriques sont dits transcendants ce qui revient à dire que le sous-corps $\mathbb{Q}(z) \subset \mathbb{C}$ est isomorphe à $\mathbb{Q}(X)$. Bien que les nombres transcendants soient « très nombreux », il n'est pas si facile de les identifier,

***Théorème 1.10***. — *Le nombre réel $\pi$ est transcendant.*

*Remarque :* le résultat peut se déduire désormais du théorème de Lindemann-Weierstrass, car $e^{i\pi} = 1$ est algébrique de sorte que $i\pi$ est transcendant. De la même façon, le nombre complexe $i$ étant algébrique, d'après le théorème de Hermite-Lindemann, $e^i$ est transcendant. Citons alors le paradoxe amusant suivant du à Sierpinski et Mazurkiewicz.

***Proposition 1.11***. — *Soit $S = \{P(e^i),\ P \in \mathbb{N}[X]\} \subset \mathbb{C}$ et $A \subset S$ (resp. $B \subset S$) le sous-ensemble donné par les polynômes $P$ tels que $P(0) = 0$ (resp. $P(0) \neq 0$). On a alors*

$$S = A \coprod B, \quad S = B - 1, \quad S = e^{-i}A.$$

*Preuve :* En effet si $P(X) = a_n X^n + \cdots + a_0$ avec $a_i \geq 0$ et $a_0 > 0$ alors $Q(X) = P(X) - 1$ est tel que $Q(e^i) \in S$ et réciproquement tout $z = Q(e^i) \in S$ s'obtient ainsi. De la même façon si $P(X)$ est tel que $P(0) = 0$ alors $P(X) = XQ(X)$ avec $Q(e^i) = e^{-i}P(e^i) \in S$ et tout point de $S$ s'obtient ainsi. □

*Remarque :* contrairement au paradoxe de Banach-Tarski, on n'utilise pas ici l'axiome du choix, par contre l'ensemble $S$ n'est pas borné. On ne sait pas s'il existe un tel sous-ensemble $S$ de $\mathbb{C}$ « paradoxal » qui soit borné.

## 2. Racines $n$-èmes de l'unité

Dans la suite $n$ désigne un entier naturel non nul.

**2.1. Etude du groupe $\mathbb{U}$.** — On a vu que $\mathbb{U} \simeq \mathbb{R}/\mathbb{Z}$ dont le sous-groupe de torsion est $\mathbb{Q}/\mathbb{Z}$. Notons $G = \mathbb{Q}/\mathbb{Z}$ qui est clairement de torsion et pas de type fini puisque tout groupe de torsion de type fini est fini. On note $\mathbb{U}_n = \{z \in \mathbb{C} :\ z^n = 1\} \simeq \frac{1}{p^n}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ ; muni de la multiplication on obtient un groupe isomorphe à $\mathbb{Z}/n\mathbb{Z}$ dont les générateurs sont appelés les racines primitives $n$-èmes de l'unité. L'ensemble des racines primitives $n$-ème de l'unité est noté $\mathbb{U}'_n$ : il est de cardinal $\psi(n)$. Soit alors

$$G_p = \bigcup_{n \geq 1} \frac{1}{p^n}\mathbb{Z}/\mathbb{Z} = \frac{1}{p}\mathbb{Z}/\mathbb{Z} \subset \frac{1}{p^2}\mathbb{Z}/\mathbb{Z} \subset \cdots \subset \frac{1}{p^n}\mathbb{Z}/\mathbb{Z} \subset \cdots$$

***Lemme 2.1***. — *$G_p$ est l'unique pro-$p$-groupe de Sylow de $G$.*

*Preuve :* Remarquons tout d'abord que $G_p$ est un groupe : soient $x, y \in G$ alors il existe $n$ et $m$ tels que $x \in \frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$ et $y \in \frac{1}{p^m}\mathbb{Z}/\mathbb{Z}$ et donc pour $r = \max\{n, m\}$, $x, y \in \frac{1}{p^r}\mathbb{Z}/\mathbb{Z}$ qui est un groupe et donc $x - y \in G_p$. Par ailleurs si $x \in G$ est d'ordre une puissance de $p$, alors clairement $x \in G_p$. □

***Lemme 2.2***. — *Les sous-groupes stricts de $G_p$ sont les $\frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$.*

*Preuve :* Pour tout $n \geq 0$, $\frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$ est un sous-groupe de $G_p$. Réciproquement soit $H$ un sous-groupe de $G_p$ et supposons que $H$ ne soit pas de la forme $\frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$ de sorte que pour tout $n$, il existe $x \notin \frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$. Soit $m$ tel que $x \in \frac{1}{p^m}\mathbb{Z}/\mathbb{Z}$ avec donc $m > n$ de sorte que $p^{m-n}x$ est un générateur de $\frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$ et donc $\frac{1}{p^n}\mathbb{Z}/\mathbb{Z} \subset H$ et finalement $H = G_p$. □

***Lemme 2.3***. — *Tout sous-groupe $H$ de $G$ est la somme directe de ses sous-groupes de Sylow $H_p = H \cap G_p$.*

*Preuve :* Soit $x \in H$ et $n$ tel que $x \in \frac{1}{n}\mathbb{Z}/\mathbb{Z} \simeq \prod_p \frac{1}{p^{\alpha_p}}\mathbb{Z}/\mathbb{Z}$ où $n = \prod_p p^{\alpha_p}$ et donc $x = \sum_p x_p$ avec $x_p = \frac{n}{p^{\alpha_p}} x \in H \cap G_p$. Ainsi $H \subset \bigoplus_p H_p$, l'inclusion réciproque étant évidente. □

***Notation 2.4***. — *Le groupe $G_p$ ci-dessus est généralement noté $\mu_{p^\infty}$ et s'appelle le groupe de Prufer.*

**2.2. Polynômes cyclotomiques.** — Le $n$-ème polynôme cyclotomique est

$$\Phi_n(X) = \prod_{\zeta \in \mathbb{U}'_n} (X - \zeta),$$

de sorte que $X^n - 1 = \prod_{d|n} \Phi_d(X)$.
*Exemples* On a $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$, $\Phi_4(X) = X^2 + 1$, $\Phi_6(X) = X^2 - 2x + 1$ et $\Phi_8(X) = X^4 + 1$.
*Remarque :* en utilisant la formule d'inversion de Moebius, on obtient

$$\Phi_n(X) = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)}.$$

Par ailleurs si $n = p_1^{r_1}.\cdots.p_s^{r_s}$ alors $\Phi_n(X) = \Phi_{p_1.\cdots.p_s}(X^{p_1^{r_1-1}.\cdots.p_s^{r_s-1}})$ et si $p$ premier ne divise pas $n$ alors :

$$\Phi_{p^i n}(X) = \frac{\Phi_n(X^{p^i})}{\Phi_n(X^{p^{i-1}})}.$$

***Lemme 2.5***. — *Pour tout $n \geq 1$, on a $\Phi_n \in \mathbb{Z}[X]$.*

*Preuve :* On calcule $\Phi_n$ par récurrence en utilisant l'égalité $\Phi_n(X) = \frac{X^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d(X)}$ et donc $\Phi_n(X) \in \mathbb{Q}[X]$. En outre par récurrence les $\Phi_d(X)$ sont des polynômes de $\mathbb{Z}[X]$ unitaires, de sorte que l'égalité précédente nous donne que $\Phi_n(X)$ est aussi à coefficients dans $\mathbb{Z}$ et unitaire. □
*Application :* théorème de Wedderburn : tout corps fini est commutatif.

***Théorème 2.6***. — *Pour tout $n \geq 1$, le polynôme $\Phi_n$ est irréductible sur $\mathbb{Z}$.*

*Remarque :* la preuve consiste à montrer que $\Phi_n$ est le polynôme minimal d'une (et donc de toute) racine primitive $n$-ème de l'unité.
*Application :* version faible du théorème de Dirichlet : il existe une infinité de nombres premiers congrus à 1 modulo $n$.

***Théorème 2.7***. — *(Kronecker) Un polynôme unitaire de $\mathbb{Z}[X]$ dont les racines complexes sont toutes de module inférieur ou égal à 1 alors ce sont des racines de l'unité.*

**2.3. Corps cyclotomiques.** — Soit $\zeta_n \in \mathbb{U}'_n$ et notons $K_n = \mathbb{Q}[\zeta_n]$. De l'irréductibilité de $\Phi_n(X)$, on en déduit qu'il est le polynôme minimal de $\zeta_n$ et donc $[K_n : \mathbb{Q}] = \psi_n$. Par ailleurs tout élément $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$ est déterminé par $\sigma(\zeta_n) \in \mathbb{U}'_n$ qui est donc de la forme $\zeta_n^k$ pour $k \wedge n$. On définit ainsi une injection $\mathrm{Gal}(K_n/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ qui est donc surjectif par égalité des cardinaux. On a donc montré la proposition suivante.

***Proposition 2.8***. — *Le groupe de Galois de $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times$.*

*Remarque :* dans le cas particulier où $p$ est premier comme $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, il possède un unique sous-groupe de cardinal 2 (resp. d'indice 2) et donc $K_n$ possède un unique sous-corps $K$ tel que $[K:\mathbb{Q}] = (p-1)/2$ (resp. $[K:\mathbb{Q}] = 2$) qui est égal à $\mathbb{Q}[\cos(2\pi/n)]$ (resp. $\mathbb{Q}[\sqrt{\epsilon_p p}]$ où $\epsilon_p = 1$ si $p \equiv 1 \mod 4$ et $\epsilon_p = -1$ si $p \equiv 3 \mod 4$).
*Application :* les polygones réguliers constructibles à la règle et au compas sont ceux dont le nombre de côtés est $n$ de la forme $2^k p_1 \cdots p_r$ où les $p_i$ sont des nombres premiers de Fermat.
*Remarque :* si $G$ est un groupe abélien fini, il est alors de la forme $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ de sorte qu'en prenant des nombres premiers $p_i \equiv 1 \mod n_i$ et $N = p_1 \cdots p_r$, $G$ est isomorphe à un sous-groupe de $(\mathbb{Z}/N\mathbb{Z})^\times$. Ainsi il existe $K \subset \mathbb{Q}[\zeta_N]$ tel que $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$. Réciproquement on a le résultat suivant.

***Théorème 2.9***. — *(Kronecker-Weber) Toute extension $K$ de $\mathbb{Q}$ tel que $\mathrm{Gal}(K/\mathbb{Q})$ est abélien, est contenue dans une extension cyclotomique $\mathbb{Q}[\zeta_n]$ pour un certain entier $n$.*

En ce qui concerne les entiers algébriques de $\mathbb{Q}[\zeta_n]$ on peut montrer que ce sont exactement les éléments de $\mathbb{Z}[\zeta_n]$ ; nous nous proposons de montrer le cas $n = p$ premier.

***Proposition 2.10***. — *L'anneau des entiers $\mathcal{O}_p$ de $\mathbb{Q}[\zeta_p]$ est $\mathbb{Z}[\zeta_p]$.*

*Preuve :* L'inclusion $\mathbb{Z}[\zeta_p] \subset \mathcal{O}_p$ est évidente, il s'agit alors de montrer l'inclusion inverse. La trace de $\zeta_p^i$ est $T(\zeta_p^i) = T(\zeta_p) = \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = -1$ de sorte que

$$T(\sum_{i=0}^{p-2} a_i \zeta_p^i) = (p-1)a_0 - \sum_{i=1}^{p-2} a_i = pa_0 - \sum_{i=0}^{p-2} a_i$$

La norme de $1-\zeta_p$ est $N(1-\zeta_p) = \prod_{i=1}^{p-1}(1-\zeta_p^i) = \Phi_p(\zeta_p) = p$.

Soit alors $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \in \mathcal{O}_K$ et considérons $\alpha\zeta_p^{-k} - \alpha\zeta_p$. On a $T(\alpha\zeta_p^{-k} - \alpha\zeta_p) = T(a_0\zeta_p^{-k} + \cdots + a_k + \cdots + a_{p-2}\zeta_p^{p-k-2} - a_0\zeta_p - \cdots - a_{p-2}\zeta_p^{p-1})$ qui est donc égal à $pa_k - (a_0 + \cdots + a_{p-2}) - (-a_0 - \cdots - a_{p-2}) = pa_k$. Ainsi on obtient $b_k = pa_k \in \mathbb{Z}$.

On pose $\lambda = 1 - \zeta_p$, de sorte qu'en substituant $1-\lambda$ à $\zeta_p$ dans $p\alpha = b_0 + \cdots + b_{p-2}\zeta_p^{p-2}$ on obtient

$$c_i = \sum_{j=i}^{p-2} (-1)^i \binom{i}{j} b_j \in \mathbb{Z} \qquad b_i = \sum_{j=i}^{p-2} (-1)^i \binom{i}{j} c_j.$$

En particulier on a $c_0 = b_0 + \cdots + b_{p-2} = p(-T(\alpha) + b_0)$ et donc $p | c_0$. Supposons alors que pour $k \geq 0$, et pour tous $i \leq k-1$, les $c_i$ sont divisibles par $p$. De l'égalité

$$p = N(1-\zeta_p) = (1-\zeta_p)^{p-1} \prod_{i=1}^{p-1} (1 + \zeta_p + \cdots + \zeta_p^{i-1}) = \lambda^{p-1}\kappa$$

on en déduit que $p$ appartient à l'idéal $(\lambda^{p-1})$ de $\mathcal{O}_K$ car $\kappa \in \mathbb{Z}[\zeta_p] \subset \mathcal{O}_K$. On reprend alors l'égalité $p\alpha = c_0 + \cdots + c_{p-2}\lambda^{p-2}$ que l'on regarde modulo $(\lambda^{k+1})$ ce qui donne $c_k\lambda^k \equiv 0 \mod (\lambda^{k+1})$ et donc $c_k = \mu\lambda$ pour $\mu \in \mathcal{O}_K$. En prenant les normes on obtient $c_k^{p-1} = pN(\mu)$ et donc $p$ divise $c_k$. On en déduit alors que $p$ divise $b_k$ et donc $a_k \in \mathbb{Z}$ ce qui prouve que $\mathcal{O}_p \subset \mathbb{Z}[\zeta_p]$ et donc l'égalité. □

*Remarque :* le discriminant de $\mathbb{Q}[\zeta_p]$ est égal à $(-1)^{(p-1)(p-2)/2} N(\Phi_p'(\zeta_p))$ avec $\Phi_p(X) = \frac{X^p-1}{X-1}$ et donc $\Phi_p'(\zeta_p) = \frac{-p\zeta_p^{p-1}}{\lambda}$ de sorte que $N(\Phi_p'(\zeta_p)) = p^{p-2}$.

**2.4. Dual d'un groupe abélien fini.** — Dans ce paragraphe bien que les groupes considérés soient tous commutatifs, nous les noterons multiplicativement.

***Définition 2.11***. — Pour $G$ un groupe abélien fini, on appelle caractère de $G$ tout morphisme de $G$ dans $\mathbb{C}^\times$ et on note $\hat{G}$ l'ensemble des caractères de $G$.

*Remarque :* si $G$ est fini de cardinal $n$, tout élément $\chi \in \hat{G}$ est à valeurs dans $\mathbb{U}_n$. Par ailleurs $\hat{G}$ est muni d'un loi de groupe commutatif par $\chi.\psi(g) = \chi(g).\psi(g)$. L'application qui à $G$ associe $\hat{G}$ est un foncteur contravariant, i.e. si $u : G \to H$ est un morphisme, $\hat{u}$ défini par $\hat{u}(\chi) = \chi \circ u$ est un morphisme $\hat{u} : \hat{H} \to \hat{G}$.
*Exemples* le groupe dual de $\mu_{p^\infty}$ est l'anneau des entiers $p$-adiques $\mathbb{Z}_p$.

***Proposition 2.12***. — *Si $G = H \times K$ alors $\hat{G} \simeq \hat{H} \times \hat{K}$.*

***Théorème 2.13***. — *Tout groupe abélien fini est non canoniquement isomorphe à son dual. Il est par contre canoniquement isomorphe à son bi-dual.*

*Remarque :* si $H$ est un sous-groupe de $G$ alors tout $\chi_H \in \hat{H}$ se prolonge en un élément $\chi \in \hat{G}$. On note aussi $H^\perp \subset \hat{G}$ l'ensemble des $\chi$ tel que $\chi_{|H} = 1$. On a alors $H^\perp \simeq \widehat{G/H}$ et $\hat{G}/H^\perp \simeq \hat{H}$.
*Exemples* un caractère de Dirichlet est un élément du groupe dual de $(\mathbb{Z}/n\mathbb{Z})^\times$.
*Remarque :* on veillera à ne pas confondre les caractères de ce paragraphe avec les caractères des représentations d'un groupe $G$ non abélien. En général un groupe non abélien $G$ possède peu de caractères de $\hat{G}$. Par exemple les seuls caractères du groupe symétrique sont l'identité et la signature ; pour le groupe alternée $\mathcal{A}_n$ avec $n \geq 5$, $\hat{\mathcal{A}}_n$ est réduit au caractère trivial.

**2.5. Analyse harmonique sur un groupe abélien fini.** — L'algèbre $\mathbb{C}[G]$ du groupe $G$ de cardinal $n$, qui s'identifie à l'ensemble des fonctions de $G$ dans $\mathbb{C}$, est munie d'une structure d'espace de Hilbert via la formule

$$a, b \in \mathbb{C}[G] \mapsto \langle a|b\rangle = \frac{1}{n}\sum_{g\in G} \overline{a(g)}b(g).$$

L'espace $\mathbb{C}[G]$ est munie d'une action linéaire $R$ de $G$ : pour $g \in G$, $R(g)f(h) = f(gh)$. On vérifie que les opérateurs $R(g)$ sont unitaires

$$\langle R(h)u, R(h)v\rangle = \frac{1}{n}\sum_{g\in G}[R(h)u](g)\overline{[R(h)v](g)} = \frac{1}{n}\sum_{g\in G} u(g+h)\overline{v(g+h)} = \langle u, v\rangle.$$

***Théorème 2.14***. — *L'ensemble $\hat{G} \subset \mathbb{C}[G]$ forme une base orthonormale qui diagonalise tous les $R(g)$.*

*Remarque :* autrement dit on a les relations suivantes

$$\frac{1}{n}\sum_{g\in G}\chi(g)\overline{\chi'(g)} = \begin{cases} 1 \text{ si } \chi = \chi' \\ 0 \text{ si } \chi \neq \chi' \end{cases}$$

Dualement en raisonnant sur $\hat{G}$, on a aussi

$$\frac{1}{n}\sum_{\chi\in\hat{G}}\chi(g)\overline{\chi(g')} = \begin{cases} 1 \text{ si } g = g' \\ 0 \text{ si } g \neq g' \end{cases}$$

***Définition 2.15***. — La transformée de Fourier de $a \in \mathbb{C}[g]$ est l'élément $\mathcal{F}a \in \mathbb{C}[\hat{G}]$ définie par

$$\chi \in \hat{G} \mapsto \frac{1}{\sqrt{n}} \sum_{g \in G} a(g)\overline{\chi(g)}.$$

*Remarque :* $\mathbb{C}[G]$ est munie d'une structure d'algèbre via le produit de convolution $a * b(g) = \sum_{h \in G} a(h)b(h^{-1}g)$. On vérifie alors que $\mathcal{F}a * b = \mathcal{F}a.\mathcal{F}b$.
*Application : Transformée de Fourier rapide* : on identifie $\mathbb{C}[\mathbb{Z}/n\mathbb{Z}]$ avec $\mathbb{C}[X]/(X^n - 1)$ en associant à la fonction qui à $\bar{k} \mapsto a_k$, le polynôme $P_a(X) = a_0 + \cdots + a_{n-1}X^{n-1}$ de sorte que $P_{a*b} = P_a P_b$. L'idée pour multiplier deux polynômes est alors d'utiliser la transformée de Fourier et l'égalité $\mathcal{F}a * b = \mathcal{F}a.\mathcal{F}b$ puis de réappliquer la transformation de Fourier. La tâche consistant à calculer la transformation de Fourier est facilité par le processus récursif suivant que l'on utilise via l'écriture en base 2 de $n$.

Pour $n = 2n'$, on pose $\zeta' = \zeta^2$ et $E' = A[X]/(X^{n'} - 1)$ et on définit $\mathcal{F}'$ et $\tilde{\mathcal{F}}'$ à l'aide de $\zeta'$. Pour $a \in E$, on note $a^0, a^1 \in E'$ en posant $a_i^0 = a_{2i}$ et $a_i^1 = a_{2i+1}$.

***Lemme 2.16***. — *Pour $0 \leq j \leq n' - 1$, on a*

$$(\mathcal{F}a)_j = (\mathcal{F}'a^0)_j + \zeta^j(\mathcal{F}'a^1)_j \text{ et } (\mathcal{F}a)_{n'+j} = (\mathcal{F}'a^0)_j - \zeta^j(\mathcal{F}'a^1)_j.$$

*Remarque :* en écrivant les entiers en base $b$, on obtient ainsi un algorithme de multiplication des grands entiers plus efficace que l'algorithme naïf, en $O(r(\ln r)^2)$ où $r$ est un majorant du nombre de chiffres des entiers à multiplier.

***Proposition 2.17***. — *(égalité de Parseval) La transformée de Fourier est une isométrie entre les espaces de Hilbert $\mathbb{C}[G]$ et $\mathbb{C}[\hat{G}]$.*

***Proposition 2.18***. — *(formule de Plancherel) Pour tout $a \in \mathbb{C}[G]$, on a*

$$a = \frac{1}{\sqrt{n}} \sum_{\chi \in \hat{G}} \mathcal{F}a(\chi)\chi.$$

*Remarque :* autrement dit, en notant $\hat{\mathcal{F}}$ la transformée de Fourier sur $\mathbb{C}[\hat{G}]$, $\hat{\mathcal{F}} \circ \mathcal{F} = \mathrm{Id}$. De même on a aussi $\mathcal{F} \circ \hat{\mathcal{F}} = \mathrm{Id}$.

***Proposition 2.19***. — *(formule sommatoire de Poisson) Pour $H$ un sous-groupe de $G$ de cardinal $m$ et $a \in \mathbb{C}[G]$, on a*

$$\frac{1}{\sqrt{m}} \sum_{h \in H} a(h) = \frac{1}{\sqrt{n/m}} \sum_{\chi \in H^\perp} \mathcal{F}a(\chi).$$

*Application : Sommes de Gauss* : soit $\chi$ un caractère de $\mathbb{F}_p^\times$ que l'on prolonge en un élément de $\mathbb{C}[\mathbb{F}_p]$ en posant $\chi(0) = 0$. Soit alors la transformée de Fourier $G(\chi, .)$ de $\chi$ ; si $\psi$ est un caractère de $\mathbb{F}_p$, on obtient la somme de Gauss :

$$G(\chi, \psi) = \sum_{x \in \mathbb{F}_p^\times} \chi(x)\psi(x)$$

laquelle peut être utilisé, par exemple, pour prouver la loi de réciprocité quadratique.

**2.6. Séries thêta.** — Dans la preuve de l'équation fonctionnelle de la fonction zéta de Riemann, on utilise la fonction thêta usuelle

$$\theta(z) = \sum_{n\in\mathbb{Z}} e^{i\pi n^2 z}$$

pour $z = iy$, $y > 0$. Celle-ci définit une fonction holomorphe sur le demi-plan de Poincaré ; la formule sommatoire de Poisson donne par prolongement analytique l'équation fonctionnelle

$$\theta(-\frac{1}{z}) = (-iz)^{1/2}\theta(z)$$

où $(-iz)^{1/2}$ est donné par la branche de la fonction sur $\mathcal{H}$ qui envoie $iy$ sur $\sqrt{y}$. Cette relation jointe à la relation évidente $\theta(z+2) = \theta(z)$ donne une règle de transformation pour $f(\gamma z)$ pour tout $\gamma \in < T^2, S > \subset PSL_2(\mathbb{Z})$ agissant sur $\mathcal{H}$ par homographies. De même pour tout $k \geq 1$, $\theta(z)^k$ satisfait à des formules de transformation analogues. Par ailleurs les égalités

$$\theta(z)^k = \sum_{n\geq 0} r_k(n) e^{i\pi n z}$$

où $r_k(n)$ désigne le nombre de représentations de $n$ comme somme de $k$ carrés d'entiers, justifient à elles seules, l'acharnement qu'ont subies ces séries. En particulier, on peut montrer les identités suivantes :

$$\begin{aligned} r_2(n) &= 4\textstyle\sum_{d|n} \chi_4(d) \\ r_4(n) &= 8(3+(-1)^n)\textstyle\sum_{d|n} d \\ r_6(n) &= 16\textstyle\sum_{d|n} d^2\chi_4(\frac{n}{d}) - 4\sum_{d|n} d^2\chi_4(d) \end{aligned}$$

avec $\chi_4(n) = d_1(n) - d_3(n)$ où $d_1(m)$ (resp. $d_3(m)$) est le nombre de diviseur $d \equiv 1 \mod 4$ (resp. $d \equiv 3 \mod 4$) de $n$.

## 3. Nombres complexes et géométrie

On choisit un point $O$ du plan affine euclidien réel ainsi qu'une base orthonormale. Tout point du plan de coordonnées $(x, y)$ est repéré par le nombre complexe $z = x + iy$ appelé son affixe. La distance entre deux points du plan d'affixe respectives $z_1, z_2$ sont à distance $|z_2 - z_1|$.

**3.1. Géométrie affine euclidienne.** — Les vecteurs pointant vers deux points $M_1$ et $M_2$ sont orthogonaux (resp. colinéaires) si et seulement si $\bar{z}_1 z_2 + z_1 \bar{z}_2 = 0$ (resp. $\begin{vmatrix} z_1 & z_2 \\ \bar{z}_1 & \bar{z}_2 \end{vmatrix} = z_1\bar{z}_2 - \bar{z}_1 z_2 = 0$). Trois points d'affixes $z_0, z_1, z_2$ sont alignés si et seulement si

$$\begin{vmatrix} 1 & 1 & 1 \\ z_0 & z_1 & z_2 \\ \bar{z}_0 & \bar{z}_1 & \bar{z}_2 \end{vmatrix} = 0.$$

*Remarque :* une façon de le voir est d'écrire une équation cartésienne $ax + by + c = 0$ sous la forme $a\frac{z+\bar{z}}{2} + b\frac{z-\bar{z}}{2i} + c = 0$ et de remarquer que le vecteur $(c, (a-bi)/2, (a+bi)/2)$ est alors un vecteur propre de la matrice ci-dessus. Une autre façon de raisonner est de remarquer que l'angle $(\widehat{M_2 M_0 M_1})$ est l'argument du complexe $\frac{z_1 - z_0}{z_2 - z_0}$. Le déterminant précédent permet aussi de donner une équation de la droite passant par $z_1$ et $z_2$. En outre l'aire du triangle $z_0, z_1, z_2$ est égale à $\frac{i}{4}$ fois le déterminant précédent.

*3.1 — Géométrie du triangle* : le triangle formés par trois points d'affixes respectives $a, b, c$ est isocèle en $A$ si et seulement si $|a-b| = |a-c|$ ; il est rectangle en $A$ si et seulement si $\frac{b-a}{c-a} \in i\mathbb{R}$ ; il est équilatéral si et seulement si $a + bj + cj^2 = 0$ ou encore $(a-b)^2 + (b-c)^2 + (c-a)^2 = 0$.
*Application :* si on se donne trois arcs du cercle unité de longueur $\pi/3$ alors les milieux des cordes extérieures forment un triangle équilatéral
*Remarque :* plus généralement un polygone $A_0, \cdots, A_n$ est régulier direct si et seulement si

$$\forall k = 1, \cdots, n-2, \quad \sum_{i=0}^{n-1} a_i \zeta_n^{ki} = 0$$

où $\zeta_n = e^{2i\pi/n}$.
*3.2 — Cocyclicité* : quatre points distincts deux à deux : $A, B, C, D$ d'affixe respective $a, b, c, d$ sont cocycliques ou alignés si et seulement si le birapport

$$[a, b, c, d] = \frac{c-a}{c-b} : \frac{d-a}{d-b} \in \mathbb{R}.$$

Autrement dit si et seulement si

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ a & b & c & d \\ \bar{a} & \bar{b} & \bar{c} & \bar{d} \\ a\bar{a} & b\bar{b} & c\bar{c} & d\bar{d} \end{vmatrix} = 0.$$

*Remarque :* comme précédemment le déterminant précédent permet de donner l'équation du cercle droite passant par les points d'affixe $a, b, c$ dont le centre se calcule en faisant le quotient des coefficients de $\bar{z}$ et $z\bar{z}$ soit

$$\frac{(b-c)(|a|^2 - |c|^2) - (a-c)(|b|^2 - |c|^2)}{(b-c)(\bar{a} - \bar{c}) - (a-c)(\bar{b} - \bar{c})}.$$

De la même façon, l'équation de la conique passant par les 5 points d'affixe $a, b, c, d, e$ est donnée par

$$\begin{vmatrix} 1 & 1 & 1 & 1 & 1 & \\ z & a & b & c & d & e \\ \bar{z} & \bar{a} & \bar{b} & \bar{c} & \bar{d} & \bar{e} \\ z^2 & a^2 & b^2 & c^2 & d^2 & e^2 \\ \bar{z}^2 & \bar{a}^2 & \bar{b}^2 & \bar{c}^2 & \bar{d}^2 & \bar{e}^2 \\ z\bar{z} & a\bar{a} & b\bar{b} & c\bar{c} & d\bar{d} & \end{vmatrix} = 0.$$

*Application :* Soit $E$ l'ellipse d'équation $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ où $a$ et $b$ sont positifs distints et non nuls. On appelle **angle excentrique** d'un point $P \in E$ un réel $t$ tel que $P = (a\cos t, b\sin t)$.

(1) Quatre points de $E$ d'angles excentriques respectifs $\alpha_i$, $i = 1, 2, 3, 4$ sont cocycliques si et seulement si la matrice $4 \times 4$ dont la $i$-ème ligne est

$$(1 \quad \cos\alpha_i \quad \sin\alpha_i \quad \cos 2\alpha_i)$$

est de déterminant nul.

(2) Le déterminant ci-dessus est égal à

$$32 \sin\left(\frac{\sum_{i=1}^4 \alpha_i}{2}\right) \prod_{1 \le i < j \le 4} \sin\left(\frac{\alpha_i - \alpha_j}{2}\right)$$

(3) Avec les notations de (1) et en supposant les points distincts, ils sont cocycliques si et seulement si la somme de leurs angles excentriques est un multiple entier de $2\pi$.

*Preuve :* (1) L'équation du cercle passant par les points $P_i = (x_i, y_i)$ pour $i = 1, 2, 3$, est

$$\begin{vmatrix} 1 & x & y & x^2+y^2 \\ 1 & x_1 & y_1 & x_1^2+y_1^2 \\ 1 & x_2 & y_2 & x_2^2+y_2^2 \\ 1 & x_3 & y_3 & x_3^2+y_3^2 \end{vmatrix} = 0$$

En remplaçant $(x_i, y_i)$ par $(a\cos\alpha_i, b\sin\alpha_i)$, on obtient une matrice dont la $i$-ème ligne est

$$ab(1 \quad \cos\alpha_i \quad \sin\alpha_i \quad a^2\cos^2\alpha_i + b^2\sin^2\alpha_i)$$

Or $a^2\cos^2\alpha_i + b^2\sin^2\alpha_i = \frac{1}{2}(a^2+b^2) + \frac{1}{2}(a^2-b^2)\cos(2\alpha_i)$. Le déterminant de cette matrice est donc égal à $[ab(a^2-b^2)/2]^4$ fois le déterminant de la matrice dont la $i$-ème ligne est $(1 \quad \cos\alpha_i \quad \sin\alpha_i \quad \cos 2\alpha_i)$.

(2) Le déterminant précédent est la partie réelle du déterminant de $(1 \quad \cos\alpha_i \quad \sin\alpha_i \quad e^{2\alpha_i})$. En utilisant les formules d'Euler pour le cos et le sin, on obtient

$$\frac{1}{2}\mathrm{Re}\ \det(1 \quad e^{i\alpha_i} \quad ie^{-i\alpha_i} \quad e^{2i\alpha_i})$$

En changeant l'ordre des colonnes et en mettant $e^{-i\alpha_i}$ en facteur dans chaque ligne, on fait apparaître un Vandermonde et on obtient

$$\frac{1}{2}\mathrm{Re}\left(e^{-i\sum_{j=1}^4\alpha_j}\prod_{1\le i<j\le 4}(e^{i\alpha_i}-e^{i\alpha_j})\right)$$

En mettant en facteur $e^{i\frac{\alpha_i-\alpha_j}{2}}$ pour chaque $i<j$, on obtient le résultat.

(3) C'est une conséquence directe de ce qui précède. □

*3.3 — Applications affines* : la translation de vecteur $a$ est $z \mapsto z+a$ ; l'homothétie de centre $\omega$ et de rapport $k \in \mathbb{R}$ est $z \mapsto kz + (1-k)\omega$ ; la rotation de centre $\omega$ et d'angle $\theta$ est $z \mapsto e^{i\theta}z + (1-e^{i\theta})\omega$ ; la symétrie par rapport à la droite d'équation $\bar{v}(z-c) + v(\bar{z}-\bar{c}) = 0$ est $z \mapsto -\frac{v}{\bar{v}}(\bar{z}-\bar{c}) + c$.

*3.4 — Géométrie du triangle* : soient $A, B, C$ trois points distincts du plan complexe. On note $A', B', C'$ les milieux des côtés $[BC]$, $[AC]$ et $[AB]$ ; $G$ désigne l'isobarycentre du triangle, $H$ l'orthocentre. L'homothétie de centre $G$ et de rapport $-1/2$ transforme les hauteurs de $ABC$ en celles de $A'B'C'$ qui sont les médiatrices de $ABC$ de sorte que $\overrightarrow{GO} = -1/2.\overrightarrow{GH}$ ; par ailleurs le centre $\Omega$ du cercle circonscrit de $A'B'C'$ est tel que $\overrightarrow{G\Omega} = -1/2.\overrightarrow{GO}$. La droite joignant $O, G, H, \Omega$ s'appelle *la droite d'Euler*. Notons $A_1, B_1, C_1$ les pieds des hauteurs et soient $U, V, W$ les milieux de $[A, H]$, $[B, H]$ et $[C, H]$. Comme $\Omega$ est le milieu de $[O, H]$, il appartient à la médiatrice de $[A', A_1]$ de sorte que $A_1, B_1, C_1$ appartiennent au cercle $\mathcal{C}$ circonscrit à $A', B', C'$ ; en outre l'homothétie de centre $H$ et de rapport $1/2$ envoie le cercle circonscrit à $ABC$ sur celui de $A'B'C'$ et donc $U, V, W$ appartiennent à $\mathcal{C}$ qui s'appelle *le cercle d'Euler*.

**Droite de Simson** : les pieds $A_1, B_1, C_1$ des trois perpendiculaires menées d'un point $P$ sur les trois côtés d'un triangle sont alignés si et seulement si $P$ appartient au cercle circonscrit.

*Preuve :* Supposons que $P$ appartienne au cercle circonscrit ; comme $A_1, B, C_1, P$ sont cocycliques on a

$$(\widehat{\overrightarrow{PC}, \overrightarrow{PA}}) = (\widehat{\overrightarrow{BC}, \overrightarrow{BA}}) = \pi - (\widehat{\overrightarrow{BC_1}, \overrightarrow{BA_1}}) = (\widehat{\overrightarrow{PA_1}, \overrightarrow{PC_1}}),$$

$$(\widehat{\overrightarrow{PA_1},\overrightarrow{PC}}) = (\widehat{\overrightarrow{PA_1},\overrightarrow{PA}}) - (\widehat{\overrightarrow{PC},\overrightarrow{PA}}) = (\widehat{\overrightarrow{PA_1},\overrightarrow{PA}}) - (\widehat{\overrightarrow{PA_1},\overrightarrow{PC_1}}) = (\widehat{\overrightarrow{PC_1},\overrightarrow{PA}}).$$

Comme $P, A_1, C, B_1$ sont cocycliques, on a $(\widehat{\overrightarrow{PA_1},\overrightarrow{PC}}) = (\widehat{\overrightarrow{B_1A_1},\overrightarrow{B_1C}})$ et comme $P, C_1, B_1, A$ sont cocycliques,

$$(\widehat{\overrightarrow{B_1A},\overrightarrow{B_1C_1}}) = \pi - (\widehat{\overrightarrow{PC_1},\overrightarrow{PA}}) = \pi - (\widehat{\overrightarrow{PA_1},\overrightarrow{PC}}) = \pi - (\widehat{\overrightarrow{B_1A_1},\overrightarrow{B_1C}}) = (\widehat{\overrightarrow{B_1A},\overrightarrow{B_1A_1}})$$

et donc $A_1, B_1, C_1$ sont alignés. Réciproquement on remonte les calculs ci-dessus de sorte que $(\widehat{\overrightarrow{PC},\overrightarrow{PA}}) = (\widehat{\overrightarrow{BC},\overrightarrow{BA}})$ et donc $P$ appartient au cercle circonscrit. □

**3.2. Géométrie conforme.** — Les références classiques sont [**?**] §2 et [**3**]. En dimension 2, il s'agit de la sphère de Riemann $S^2 = \mathbb{P}^1(\mathbb{C})$, en dimension quelconque on prend le plan affine euclidien $E$ auquel on rajoute un point à l'infini $\hat{E} = E \cup \{\infty\}$ (on passe de l'une à l'autre par la projection stéréographique) ; la topologie sur $\hat{E}$ est celle de $E$ à laquelle on rajoute les ouverts du type $(E\backslash K) \cup \{\infty\}$ où $K$ est un compact de $E$ ; la projection stéréographique est un homéomorphisme.

***Définition 3.5***. — L'inversion de pôle $\omega$ et de puissance $\mu \in \mathbb{R}^\times$ est $z \mapsto \omega + \frac{\mu}{z-\omega}$ ; l'homographie de $\mathbb{P}^1(\mathbb{C})$ associée à $A \in PGL_2(\mathbb{C})$ est $z \mapsto \frac{az+b}{cz+d}$. A conjugaison près une homographie possédant deux (resp. un) points fixes est une homothétie de centre $O$ (resp. une translation).

*Remarque :* pour une similitude $f$ du plan affine euclidien, on la prolonge en posant $f(\infty) = \infty$ ; les inversion et les similitudes de $\hat{E}$ engendrent un groupe appelé le groupe conforme ou groupe des homographies ; la géométrie conforme est l'étude de l'action du groupe conforme sur $\hat{E}$. Si on rajoute la conjugaison, on obtient le groupe circulaire qui vu comme automorphismes de $S^2$, correspond aux automorphismes qui conservent les cercles tracés sur $S^2$. Une transformation circulaire droite ($z \mapsto \frac{az+b}{cz+d}$) (resp. gauche $z \mapsto \frac{a\bar{z}+b}{c\bar{z}+d}$) conserve (resp. change en son opposé) les angles orientés de droites.
*Remarque :* l'action de $PGL_2(\mathbb{R})$ sur le demi-point de Poincaré a pour domaine fondamental...
**Définitions** : - *la puissance d'un point $P$ par rapport à un cercle $\mathcal{C}(O,R)$* est la quantité $s = \overline{PA}.\overline{PB}$, où $A, B$ sont les points d'intersection d'une droite quelconque passant par $P$ et coupant $\mathcal{C}$ aux points $A, B$. En introduisant le point $A'$ diamétralement opposé à $A$ et en utilisant que le triangle $ABA'$ est rectangle en $B$, on a $s = \overrightarrow{PA}.\overrightarrow{PA'} = PO^2 - R^2$ et ne dépend donc pas de la droite choisie.

- *L'axe radical de $\mathcal{C}, \mathcal{C}'$* est l'ensemble des points d'égale puissance par rapport à $\mathcal{C}$ et $\mathcal{C}'$ donné par l'équation $OM^2 - O'M^2 = R^2 - R'^2$ soit $2.\overrightarrow{O'M}.\overrightarrow{O'O} = R'^2 - R^2 + O'O^2$ qui est donc la droite perpendiculaire à $OO'$ et passant par $I \in (OO')$ tel que $\overline{O'I} = \frac{R'^2 - R^2 + O'O^2}{2\overline{O'M}}$.

**Invariant conforme de deux cercles** : *soient $\mathcal{C}, \mathcal{C}'$ deux cercles de rayon respectifs $R, R'$ et de centre $O, O'$ avec $d = OO'$. La quantité $c = \frac{|R^2 + R'^2 - d^2|}{2RR'}$ est invariante par inversion.*
*Preuve :* Dans le cas où $\mathcal{C}$ et $\mathcal{C}'$ s'intersectent en un point $P$, dans le triangle $OO'P$, on a $OO'^2 = PO^2 + PO'^2 - 2.PO.PO'.\cos\widehat{OPO'}$ et donc l'invariant en question n'est autre que que le cosinus de l'angle $\widehat{OPO'}$ qui est aussi celui entre les tangentes en $P$ de $\mathcal{C}$ et $\mathcal{C}'$ lequel est conservé par inversion.

Dans le cas général, soit $P$ n'appartenant ni à $\mathcal{C}$ ni à $\mathcal{C}'$ le pôle de l'inversion et $\mu$ son rapport ; on note $\Gamma$ et $\Gamma'$ les cercles images de $\mathcal{C}$ et $\mathcal{C}'$, de centre $\omega, \omega'$ et de rayon $\rho, \rho'$. On rappelle que $\Gamma$ (resp. $\Gamma'$) est l'image de $\mathcal{C}$ (resp. $\mathcal{C}'$) par l'homothétie de centre $S$ et de rapport

$\frac{\mu}{s}$ (resp. $\frac{\mu}{s'}$) où $s$ (resp. $s'$) est la puissance de $S$ par rapport à $\mathcal{C}$ (resp. $\mathcal{C}'$) de sorte que la puissance de $S$ par rapport à $\Gamma$ (resp. $\Gamma'$) est $\sigma = \frac{\mu^2}{s}$ (resp. $\sigma' = \frac{\mu^2}{s'}$). Dans les triangles $POO'$ et $P\omega\omega'$, on écrit

$$d^2 = PO^2 + PO'^2 - 2.PO.PO'.\cos\widehat{OPO'}, \quad \omega\omega'^2 = \delta^2 = P\omega^2 + P\omega'^2 - 2P\omega.P\omega'.\cos\widehat{\omega P\omega'}$$

avec $\alpha = \widehat{OPO'} = \widehat{\omega P\omega'}$, de sorte que

$$\frac{R^2 + R'^2 - d^2}{\rho^2 + \rho'^2 - \delta^2} = \frac{s + s' - 2.PO.PO'\cos\alpha}{\sigma + \sigma' - 2.P\omega.P\omega'.\cos\alpha} = \frac{ss'}{\mu^2} = \frac{RR'}{\rho\rho'}$$

en utilisant $\frac{\sigma+\sigma'}{s+s'} = \frac{\mu^2}{ss'} = \frac{P\omega.P\omega'}{PO.PO'}$. □

*Remarque :* $\mathcal{C}$ et $\mathcal{C}'$ sont non sécants (resp. sécants, resp. tangents) si et seulement si $c >$ (resp. $c < 1$, resp. $c = 1$).

**Proposition** : *soient $\mathcal{C}(O, R)$ et $\mathcal{C}'(O', R')$ deux cercles non sécant ; les cercles orthogonaux à $\mathcal{C}$ et $\mathcal{C}'$ sont ceux centrés sur l'axe radical et passant par les points $L, L'$ tels que $LI^2 = L'I^2 = IO^2 - R^2 = IO'^2 - R'^2$.*

*Preuve :* Soit $\mathcal{C}"(\omega, \rho)$ un tel cercle de sorte que $R^2 + \rho^2 = O\omega^2$ et $R'^2 + \rho^2 = O'\omega^2$ et donc $O\omega^2 - R^2 = O'\omega^2 - R'^2 = \rho^2$ et donc $\omega$ appartient à l'axe radical. Notons $L, L'$ l'intersection de $\mathcal{C}" \cap (OO')$ : $LI^2 + I\omega^2 = L\omega^2 = \rho^2 = O\omega^2 - R^2$ et donc $LI^2 = OI^2 - R^2$ et de même $L'I^2 = O'I^2 - R'^2$ avec $LI = LI'$. □

**Corollaire** : *soient deux cercles $\mathcal{C}, \mathcal{C}'$ non sécants ; il existe alors une inversion $f$ telle que $f(\mathcal{C})$ et $f(\mathcal{C}')$ soient deux cercles concentriques.*

*Preuve :* Soit $f$ une inversion de pôle $L$ et de puissance $\mu$ quelconque. Les images $f(\mathcal{C})$ et $f(\mathcal{C}')$ sont des cercles qui sont orthogonales à tous les $f(\Sigma)$ où $\Sigma$ est un cercle quelconque centré sur l'axe radical de $\mathcal{C}, \mathcal{C}'$ et passant par $L$. Or les $f(\Sigma)$ sont des droites qui passent donc par les centres de $f(\mathcal{C})$ et $f(\mathcal{C}')$ lesquels sont donc dans l'intersection de tous les $f(\Sigma)$ et sont donc confondus. □

## 4. Quelques énoncés de géométrie

**4.1. Porisme de Steiner.** — Il s'agit d'un énoncé de géométrie conforme : *soient $\mathcal{C}$ et $\mathcal{C}'$ deux cercles non sécants tels que $\mathcal{C}'$ soit à l'intérieur de $\mathcal{C}$. On construit alors une chaîne de cercles $\mathcal{C}_1, \mathcal{C}_2, \cdots$ telle que $\mathcal{C}_1$ est tangent à $\mathcal{C}$ et $\mathcal{C}'$ quelconque, puis pour $i \geq 2$, $\mathcal{C}_i$ est tangent à $\mathcal{C}, \mathcal{C}'$ et $\mathcal{C}_{i-1}$. La chaîne est alors finie si et seulement si l'invariant conforme $c$ de $\mathcal{C}$ et $\mathcal{C}'$ est de la forme*

$$c = \frac{R^2 + R'^2 - d^2}{2RR'} = \frac{1 + \sin^2(\pi p/k)}{\cos^2(\pi p/k)},$$

*où $p$ est le nombre de tours. En particulier cela ne dépend pas du choix du cercle $\mathcal{C}_1$ de départ.*

*Preuve :* S'agissant clairement d'un énoncé de géométrie conforme, on applique une inversion de sorte que $\mathcal{C}$ et $\mathcal{C}'$ soient deux cercles concentriques : la figure étant alors clairement invariante par rotation, on remarque bien que l'alternative, la chaîne est finie ou infinie, est indépendante du choix de $\mathcal{C}_1$. La chaîne sera finie si et seulement si l'angle $\frac{\widehat{O_1OO_2}}{2\pi} \in \mathbb{Q}$. Notons $\alpha = \frac{1}{2}\widehat{O_1OO_2} = \widehat{O_1OT}$ où $T$ est le point de contact entre $\mathcal{C}_1$ et $\mathcal{C}_2$ : $\alpha = \pi\frac{p}{k}$. On note $\rho, \rho'$ les rayons des deux cercles concentriques de sorte que d'après ce qui précède $\frac{\rho}{\rho'} = c + \sqrt{c^2 - 1}$

avec $\sin\alpha = \frac{\rho-\rho'}{\rho+\rho'}$ et donc $\frac{\rho}{\rho'} = \frac{1+\sin\alpha}{1-\sin\alpha}$ soit

$$c + \sqrt{c^2-1} = \frac{1+\sin\frac{\pi p}{k}}{1-\sin\frac{\pi p}{k}}$$

ce qui donne le résultat. □

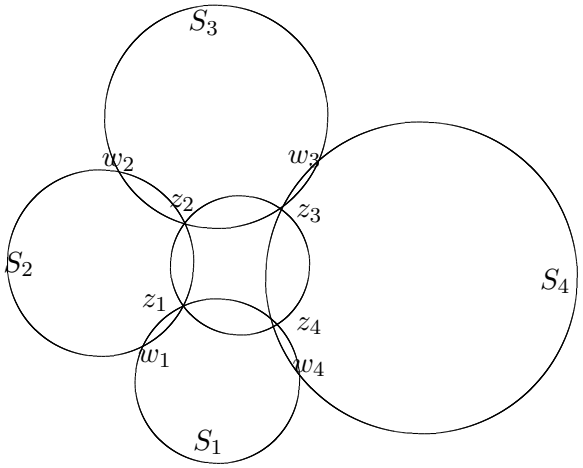
**4.2. Théorème de Miguel et applications.** — Commençons par une série de lemmes.

***Lemme 4.1***. — *Soient $S_1, S_2, S_3$ et $S_4$ quatre cercles du plan, tels que $S_1$ coupe $S_2$ en deux points $z_1, w_1$, qui lui-même coupe $S_3$ en $z_2, w_2$, qui coupe $S_4$ en $z_3, w_3$ qui coupe $S_1$ en $z_4, w_4$. On suppose que les points $z_1, z_2, z_3, z_4$ sont alignés ou cocycliques, alors il en est de même des points $w_1, w_2, w_3, w_4$.*

*Preuve :* Par construction les birapports suivant sont réels

$$W(z_1, w_2, z_2, w_1),\ W(z_2, w_3, z_3, w_2),\ W(z_3, w_4, z_4, w_3),\ W(z_4, w_1, z_1, w_4)$$

L'expression $\frac{W(z_1,w_2,z_2,w_1).W(z_3,w_4,z_4,w_3)}{W(z_2,w_3,z_3,w_2).W(z_4,w_1,z_1,w_4)}$ est donc réelle et se simplifie en $W(z_1, z_3, z_2, z_4)W(w_1, w_3, w_2, w_4)$. □




***Lemme 4.2***. — *Soient quatre droites en position générale : $D_1, D_2, D_3, D_4$. On pose $z_{i,j} = D_i \cap D_j$ et $S_{i,j,k}$ le cercle circonscrit aux triangles formés par les droites $D_i, D_j, D_k$.*

*(i) $S_{1,2,3}$ et $S_{1,2,4}$ qui se coupent en $z_{1,2}$ ne sont pas tangents ; on note $z_{1,2,3,4}$ le deuxième point d'intersection ;*

*(ii) $z_{1,2,3,4}$ appartient au cercle $S_{2,3,4}$ ;*

*(iii) les cercles $S_{1,2,3}, S_{1,2,4}, S_{2,3,4}, S_{1,3,4}$ sont concourants en $z_{1,2,3,4}$ ; on l'appellera le point central des droites $D_1, D_2, D_3, D_4$.*

*Preuve :* (i) En effet sinon $D_3$ et $D_4$ seraient parallèles : considérer une homothétie de centre $z_{1,2}$

(ii) - $S_{1,2,3}$ coupe $D_3$ en $z_{1,3}$ et $z_{2,3}$ ;
- $D_3$ coupe $D_4$ en $\infty$ et $z_{3,4}$ ;
- $D_4$ coupe $S_{1,2,4}$ en $z_{1,4}$ et $z_{2,4}$ ;

- $S_{1,2,4}$ coupe $S_{1,2,3}$ en $z_{1,2}$ et $z = z_{1,2,3,4}$

Comme les quatres points $z_{1,3}, \infty, z_{1,4}, z_{1,2}$ sont alignés (sur $D_1$), les quatre points $z_{2,3}, z_{3,4}, z_{2,4}, z$ sont alignés ou cocycliques ; les trois premiers sont sur le cercle $S_{2,3,4}$ et distincts, de sorte que $z$ est sur $S_{2,3,4}$.

(iii) De même $z_{2,3}, \infty, z_{2,4}, z_{1,2}$ sont alignés (sur $D_2$) donc $z_{1,3}, z_{3,4}, z_{1,4}, z$ sont cocyliques sur $Z_{1,3,4}$ d'où le résultat. (on peut aussi conclure par symétrie du problème : si 3 cercles sont concourants le quatrième aussi !) □

***Proposition 4.3***. — *Soient cinq droites $D_1, \cdots, D_5$ en position générale. Les 5 points centraux $z_{1,2,3,4}, z_{1,2,3,5}, z_{1,2,4,5}, z_{1,3,4,5}$ et $z_{2,3,4,5}$ des cinq quadruplets de droites sont cocycliques ou alignés.*

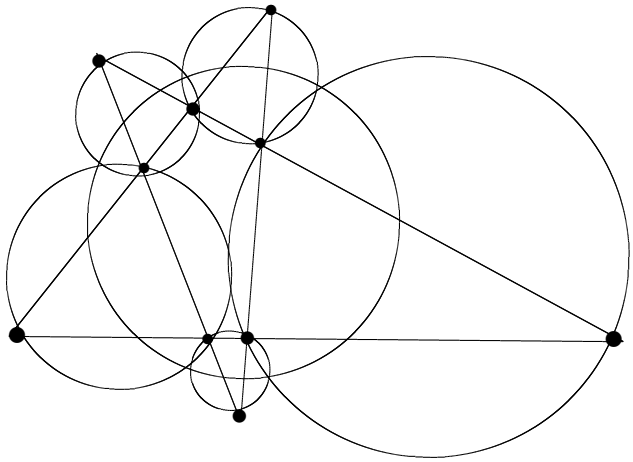
*Preuve :* - $z_{1,2,3,4}$ est l'intersection des cercles $S_{1,3,4}$ et $S_{1,2,3}$, l'autre intersection étant le point $z_{1,3}$ ;

- $z_{1,2,3,5}$ est l'intersection des cercles $S_{1,2,3}$ et $S_{1,2,5}$, l'autre intersection étant le point $z_{1,2}$ ;
- $z_{1,2,4,5}$ est l'intersection des cercles $S_{1,2,5}$ et $S_{1,4,5}$, l'autre intersection étant le point $z_{1,5}$ ;
- $z_{1,3,4,5}$ est l'intersection des cercles $S_{1,4,5}$ et $S_{1,3,4}$, l'autre intersection étant le point $z_{1,4}$ ;

Comme $(z_{1,3}, z_{1,2}, z_{1,5}, z_{1,4})$ sont alignés (sur $D_1$), les autres sont alignés ou cocylciques

Comme c'est vrai pour toute combinaison de quatre points parmi les cinq... □

***Corollaire 4.4***. — *(**Pékin 2000**) Les intersections des cercles circonscrits aux triangles externes successifs d'une étoile à cinq branches sont cocycliques.*



*Preuve :* Il s'agit du problème posé par Yang Zemin au congrès mondial (Pekin 2000) ; deux branches successives correspondent au choix de 4 droites sur les cinq qui portent les cotés du pentagone étoilé. L'intersection des cercles circonscrits (2 sur les 4) aux deux branches est donc le point central des 4 droites en question ... (ils ne peuvent pas être alignés) □

***Théorème 4.5***. — *« Pékin 2000 » : tout système de n droites en position générale avec n pair (resp. impair) détermine un point central (resp. un cercle central) qui est l'intersection*

*des cercles centraux des n systèmes possibles de $n-1$ de ces droites (resp. qui passe par les points centraux des n systèmes possibles de ces droites).*

### 4.3. Le théorème des 7 cercles. —

### 4.4. Ellipse de Steiner. —

***Théorème 4.6***. — *(**van der Berg** cf.* [**5**] *p.14) Soit $P \in \mathbb{C}[X]$ de degré 3 ; les racines de $P'$ sont les foyers de l'ellipse de Steiner du triangle formé par les racines de $P$.*

*Preuve :* Notons que pour $Q(z) = P(z - z_0)$ on a $Q'(z) = P'(z - z_0)$ de sorte que l'on peut placer l'origine en n'importe quel point. De même pour $Q(z) = P(re^{i\theta}z)$ on a $Q'(z) = re^{i\theta}P'(re^{i\theta})$ on peut appliquer une similitude à la figure sans changer l'énoncé. Enfin comme toute transformation affine est la composée d'une similitude avec une affinité de la forme $(x, y) \mapsto (x, y\cos\alpha)$, on peut supposer que les racines $A, B, C$ de $P$ sont les images des points d'affixes $1, j, j^2$ par

$$z \mapsto \frac{z+\bar{z}}{2} + \frac{z-\bar{z}}{2}\cos\alpha = z\cos^2\frac{\alpha}{2} + \bar{z}\sin^2\frac{\alpha}{2}.$$

Les demi-axes $a, b$ de l'ellipse considérée sont alors égaux à $\frac{1}{2}$ et $\frac{\cos\alpha}{2}$ ; la distance entre les foyers $F_1, F_2$ est $\sqrt{a^2-b^2} = \frac{\sin\alpha}{2}$. L'homothétie de rapport

$$(\frac{\sin\alpha}{2})^{-1} = \Big(\sin\frac{\alpha}{2}\cos\frac{\alpha}{2}\Big)^{-1}$$

transforme alors $F_1$ et $F_2$ en $\pm 1$. La composition de cette homothétie avec l'affinité précédente est la transformation $z \mapsto z\cot\frac{\alpha}{2} + \bar{z}\tan\frac{\alpha}{2}$ de sorte qu'en posant $a = \cot\frac{\alpha}{2}$ le polynôme de racines $A, B, C$ est

$$P(z) = \Big(z - a - \frac{1}{a}\Big)\Big(z - aj - \frac{1}{aj}\Big)\Big(z - aj^2 - \frac{1}{aj^2}\Big)$$

et on vérifie que les racines de $P'(z) = 3z^2 + 3j + 3j^2 = 3x^2 - 3$ sont bien $\pm 1$. □

## 5. Développements

- condition d'alignement ou de cocyclicité en terme de birapport (thm des 6 rapports)
- constructibilité à la règle et au compas
- description des groupes $O_3$ et $O_4$ par les quaternions [**4**]
- thm de Morley (en précisant l'affixe des sommets du triangle équilatéral et en utilisant les nombres complexes) [**?**] [**?**]
- action de $GL_2(\mathbb{R})$ sur le demi-plan de Poincaré [**?**] [**1**]
- applications conformes [**2**]
- paradoxe de Sierpinski-Mazurkiewicz

## 6. Questions

***Exercice 6.1***. — ***Transcendance de $\pi$***

*(i) Soit $f$ un polynôme à coefficients réels de degré $m$. Montrez que pour tout nombre complexe $z$, l'intégrale complexe*

$$I(f;z) = \int_0^1 z e^{z(1-u)} f(zu) dz$$

*vérifie*

$$I(f;z) = e^z \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(z)$$

*ainsi que la majoration*

$$|I(f;z)| \leq |z| e^{|z|} \sup_{u\in[0,1]} |f(zu)|$$

*(ii) Soit $f$ un polynôme à coefficients entiers. Montrez que pour tout $n \geq 0$, il existe un polynôme $f_n$ à coefficients entiers tel que $f^{(n)} = n! f_n$.*

*(iii) Pour un polynôme $f$ et $g : \mathbb{C} \to \mathbb{C}$ une fonction, on note $\sum_{f(\alpha)=0} g(\alpha)$ la somme $g(\alpha_1) + \cdots + g(\alpha_n)$ où les $\alpha_i$ sont les racines de $f$ répétées autant de fois que leur multiplicité. Montrez que si $f$ est à coefficients entiers de coefficient $a$, alors pour tout $n \geq 0$, $a^n \sum_{f(\alpha)=0} \alpha^n$ appartient à $\mathbb{Z}$.*
*Indication : on pourra introduire une matrice dont la trace est $a^n \sum_{f(\alpha)=0} \alpha^n$.*

*(iv) Soit $f$ un polynôme à coefficients entiers tel que $f(0) \neq 0$ et de coefficient dominant $a$. Pour $p$ un nombre premier, soit $g(x) = x^{p-1} f^p(x)$ et $J_p = \sum_{f(\alpha)=0} I(g;\alpha)$. Montrez qu'il existe un entier $M$ tel que*

$$\frac{a^{m-p}}{(p-1)!} J_p = a^{m-p} N f(0)^p + pM$$

*où $N = \sum_{f(\alpha)=0} e^\alpha$. En déduire que $N$ n'est pas un entier non nul.*

*(v) On veut montrer que $\pi$ est transcendant. On raisonne par l'absurde : soit $f$ un polynôme irréductible à coefficients entiers tel que $f(i\pi) = 0$ dont on note $\alpha_1, \cdots, \alpha_n$ les racines.*

*(a) En développant l'égalité $\prod_{f(\alpha)=0}(1 + e^\alpha)$ montrez que*

$$\sum_{\epsilon\in\{0,1\}^n} exp(\sum \epsilon_j \alpha_j) = 0.$$

*(b) Soit $Q(X) = \prod_{\epsilon\in\{0,1\}^n}(X - \sum \epsilon_j \alpha_j)$. Montrer que $Q(X) \in \mathbb{Q}[X]$.*

*(c) En utilisant la question (4), aboutissez à une contradiction.*

## 7. Solutions

**6.1** (1) On intègre par partie soit

$$\begin{aligned} I(f;z) &= [-e^{z(1-u)} f(zu)]_0^1 + \textstyle\int_0^1 e^{z(1-u)} z f'(zu) du \\ &= -f(z) + e^z f(0) + I(f';z); \end{aligned}$$

d'où le résultat par récurrence sur le degré de $f$. Pour obtenir la majoration de $|I(f;z)|$, il suffit d'intégrer sur $[0,1]$, l'inégalité

$$|z e^{z(1-u)} f(zu)| \leq |z| e^{|z|} \sum_{u\in[0,1]} |f(zu)|,$$

valable pour tout $u \in [0,1]$.

(2) Par linéarité, il suffit de considérer le cas de $f = X^m$ ; $f^{(m)} = m(m-1)\cdots(m-n+1)X^{m-n}$. Le polynôme $f_n := C_n^m X^{m-n}$ est à coefficients entiers et vérifie $f^{(n)} = n! f_n$.

(3) Soit $m$ le degré de $f$ et notons $A$ la matrice compagnon du polynôme $f/a$. Par construction $aA \in \mathbb{M}_m(\mathbb{Z})$ de sorte que $a^n A^n$ est aussi à coefficients entiers ainsi que sa trace. Or les valeurs propres de $a^n A^n$ sont les $(a\alpha)^n$, $\alpha$ parcourant les racines de $f$ avec multiplicités.

(4) On a

$$J_p = N\Big(\sum_n g^{(n)}(0)\Big) - \sum_n \Big(\sum_{f(\alpha)=0} g^{(n)}(\alpha)\Big).$$

Si $f(\alpha) = 0$, $\alpha$ est un zéro d'ordre $p$ de $g$ et donc $g^{(n)}(\alpha) = 0$ pour tout $n < p$. D'autre part si $n \geq p$, d'après ce qui précède, $g_n = g^{(n)}/p!$ est un polynôme à coefficients entiers de degré $m-n$ et

$$a^{m-n} \sum_{f(\alpha)=0} g^{(n)}(\alpha)$$

est entier, multiple de $p!$. En 0, on a $g^{(n)}(0) = 0$ pour $n < p-1$ et pour $n \geq p$ alors que

$$g^{(p-1)}(0) = (p-1)! f(0)^p$$

Ainsi, il existe un entier $M$ tel que

$$\frac{a^{m-p}}{(p-1)!} J_p = a^{m-p} N f(0)^p + pM$$

Le second membre de cette égalité est entier et si $p$ ne divise pas $aNf(0)$, il n'est pas multiple de $p$ ; il est en particulier non nul et donc au moins égal à 1 en valeur absolue. Ainsi

$$|J_p| \geq (p-1)! a^{p-m} = (p-1)! p^{1-p\deg f}$$

Or la majoration de l'intégrale $I$ dans (1) implique qu'il existe un réel $c > 0$ tel que $|J_p| \leq c^p$ pour tout $p$. Quand $p$ tend vers l'infini, la formule de Stirling rend ces deux inégalités incompatibles, d'où le résultat.

(5) (a) c'est clair

(b) Les $\sum \epsilon_j \alpha_j = 0$ sont les racines du polynôme

$$P_0 = \prod_{\epsilon \in [0,1]^n} (X - \sum_j \epsilon_j \alpha_j)$$

dont les coefficients s'expriment comme des polynômes symétriques en les $\alpha_j$ : ce sont donc des polynômes en les fonctions symétriques élémentaires des $\alpha_j$, donc en les coefficients de $f$. Ce sont donc des nombres rationnels.

(c) Soit un entier $N$ tel que $NP_0 \in \mathbb{Z}[X]$ et soit $q \geq 1$ la multiplicité del a racine 0 dans $P_0$. On pose $P := NF_0/X^q$ : c'est un polynôme à coefficients entiers avec $P(0) \neq 0$. De plus on a

$$0 \sum_{\epsilon \in [0,1]^n} \exp(\sum_j \epsilon_j \alpha_j) = q + \sum_{P(\beta)=0} e^{\beta}$$

ce qui contredit (4).

## Références

[1] M. Alessandri. *Thèmes de géométrie. Groupes en situation géométrique*. Dunod, 1999.

[2] M. Audin. *Géométrie*. EDP Sciences, 2006.

[3] M. Berger. *Géométrie 2*. Nathan, 1990.

[4] D. Perrin. *Cours d'algèbre*. Ellipses, 1998.

[5] V. Prasolov. *Polynomials*. Springer, 2004.