102. Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.

Refs : [ElAm] El Amrani, Suites et séries numériques, suites et séries de fonctions. [Aud] Audin, Géométrie. [Goz] Gozard, Théorie de Galois. [Perr] Perrin, Cours d'algèbre. [FGN2] Algèbre 2. [Ulm] Ulmer, Théorie des groupes.

Devt : (44, 45) Polynômes cyclotomiques [Perr]
(47) Dirichlet faible [FGN1]

I. Nombres complexes de module 1.

1) Le groupe $\mathbb{U}$.

Def 1 : On note $\mathbb{U}$ le noyau du morphisme de groupes $\mathbb{C}^* \to \mathbb{R}_+^*$ envoyant z sur $|z|$. Il s'agit donc de l'ensemble des nombres complexes de module 1.

Ex 2 : $\pm 1, \pm i \in \mathbb{U}$.

Rq 3 : En identifiant $\mathbb{C}$ et $\mathbb{R}^2$, $\mathbb{U}$ est identifié à S^1.

Théo 4 : On a un isomorphisme $\mathbb{R}_+^* \times \mathbb{U} \to \mathbb{C}^*$ envoyant (r,u) sur ru (la suite exacte courte induite par le module est scindée).

Prop 5 : L'application $\mathbb{R} \to \mathbb{U}$ envoyant θ sur $e^{i\theta} \in \mathbb{C}$ est un morphisme de groupe surjectif de noyau $2\pi\mathbb{Z}$: $\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{U}$.

Prop 6 : Le groupe $\mathbb{U}$ est compact et connexe.

2) Applications trigonométriques.

Def 7 : On rappelle que l'exponentielle complexe $\exp : \mathbb{C} \to \mathbb{C}^*$ est une fonction entière définie par $\exp(z) = \sum_{n\in\mathbb{N}} \frac{z^n}{n!}$.

Prop 8 : On a $\overline{\exp(z)} = \exp(\bar{z})$, donc les fonctions $\mathrm{Re}(\exp)$ et $\mathrm{Im}(\exp)$ sont aussi holomorphes, on les note respectivement $\cos$ et $\sin$.

Rq 9 : On peut reformuler la proposition précédente par les formules de Moivre et d'Euler, respectivement

$$e^{iz} = \cos z + i \sin z \qquad \cos(z) = \frac{e^{iz}+e^{-iz}}{2} \qquad \sin(z) = \frac{e^{iz}-e^{-iz}}{2i}$$

Prop 10 : On peut définir π comme le double de la plus petite racine réelle positive de $\cos : \mathbb{R} \to \mathbb{R}$.

Ex 11 : $e^{i\pi} = -1$, $e^{i\frac{\pi}{2}} = i$, $i^i = e^{i\frac{i\pi}{2}} = e^{-\frac{\pi}{2}} \in \mathbb{R}$.

Appl 12 : On a $\sum_{k=0}^{n} \cos(kt) = \cos\frac{nt}{2}\,\frac{\sin\frac{n+1}{2}t}{\sin\frac{t}{2}}$ pour $t \notin 2\pi\mathbb{Z}$.

[ElAm] 411

Appl 13 : On peut faire un calcul similaire sur sinus, ce qui permet de calculer les noyaux de Dirichlet et de Féjer par la transformée de Fourier

$$D_N(t) = \frac{\sin((N+\frac{1}{2})t)}{\sin\frac{t}{2}} \qquad U_N(t) = \frac{1}{N+1}\left(\frac{\sin(N+\frac{1}{2})t}{\sin\frac{t}{2}}\right)^2$$

Appl 14 : Linéarisation de cos : $\cos^m(x) = \frac{1}{2^m}\sum_{k=0}^{m}\binom{m}{k}\exp(ix(2k-m))$

On peut inversement exprimer $\cos(mx)$ comme un polynôme en $\cos(x)$: ce sont les polynômes de Tchebychev.

3) Paramétrisation du cercle unité.

Prop 15 : Dans $\mathbb{C}$, $\mathbb{U}$ est le cercle de centre 0 et de rayon 1, il peut être paramétré par $\mathbb{R} \to \mathbb{R}^2$, $t \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ à l'exception de $(-1,0)$.

Cor 16 : Les points de $\mathbb{U}$ à coordonnées rationnelles sont denses dans $\mathbb{U}$.

Appl 17 : Triplets pythagoriciens : Pour que $(x,y,z) \in \mathbb{N}^3$ soit solution de l'équation diophantienne $x^2+y^2=z^2$, il faut et il suffit d'avoir $d \in \mathbb{N}$, $u, v \in \mathbb{N}$ premiers entre eux, tels que (x,y,z) ou (y,x,z) soit égal à $(d(u^2-v^2), 2duv, d(u^2+v^2))$.

4) Mesure d'un angle orienté.

[Aud]

Def 18 : Pour $z \in \mathbb{C}^*$, on appelle argument de z tout réel θ tel que $e^{i\theta} = \frac{z}{|z|}$. L'argument est donc bien défini dans $\mathbb{T} = \mathbb{R}/2\pi\mathbb{Z}$. On le notera $\arg z$.

Ex 19 : $\arg i = \frac{\pi}{2}$, $\arg x = \pi$ ou 2π pour $x \in \mathbb{R}$.

Def 20 : On appelle forme trigonométrique d'un complexe z tout couple $(r,\theta) \in \mathbb{R}_+ \times \mathbb{R}$ tel que $z = re^{i\theta}$.
On appelle argument principal $\mathrm{Arg}\, z$ de $z \in \mathbb{C}$ le représentant de $\arg z$ dans $]-\pi, \pi]$.

Théo 21 : L'application $\mathbb{C}^* \to GL_2(\mathbb{R})$ envoyant $a+ib$ sur $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ induit un isomorphisme de groupes entre $\mathbb{U}$ et $SO_2(\mathbb{R})$, d'où un isomorphisme entre $SO_2(\mathbb{R})$ et $\mathbb{R}/2\pi\mathbb{Z} = \mathbb{T}$.

Def 22 : Soit $f \in SO_2(\mathbb{R})$, on appelle angle de f l'élément de $\mathbb{T}$ correspondant à f par l'isomorphisme précédent.

Prop 23 : Soient $u, v \in S^1$, il existe un unique $f \in SO_2(\mathbb{R})$ envoyant u sur v.

Def 24 : Pour deux couples $(u,v), (u',v') \in S^1$, on dit que (u,v) et (u',v') sont équivalents si la rotation $r \in SO_2(\mathbb{R})$ telle que $r(u) = v$ est également telle que $r(u') = v'$. On appelle angle orienté du couple (u,v) sa classe pour cette relation (qui est d'équivalence).

Prop25 : Il y a une bijection entre les angles orientés et $SO_2(\mathbb{R})$. On peut donc associer à un angle sa mesure, qui est un élément de $\mathbb{T}$.

Ex26 : l'angle entre 1 et $e^{i\theta}$ est $\theta\ [2\pi]$.

Rq27 : Si z et z' sont des nombres complexes non nuls, on peut appeler angle l'angle des normalisés $\frac{z}{|z|}$ et $\frac{z'}{|z'|}$.

II. Racines de l'unité et cyclotomie.

1) Sous groupe des racines de l'unité.

[Ro3] 67

Def28 : Soit $m \in \mathbb{N}^*$, on appelle racines m-ième de l'unité dans $\mathbb{C}$ tout nombre complexe z tel que $z^m = 1$. On note $\mathbb{U}_m$ leur ensemble, ~~on~~ dit que $\zeta \in \mathbb{U}_m$ est primitive si ζ est d'ordre m dans $\mathbb{C}^*$, on note μ_m l'ensemble de racines primitives m-ièmes de l'unité.

Prop29 : Pour $m \in \mathbb{N}^*$, $\mathbb{U}_m$ est un sous groupe cyclique d'ordre m de $\mathbb{U}$, engendré par $\zeta = e^{2i\pi/m}$. Les racines primitives sont les générateurs de $\mathbb{U}_m$.

Cor30 : Pour $m \geq 1$, on a $|\mu_m| = \varphi(m)$.

Prop31 : Un sous groupe de $\mathbb{U}$ est fini ou dense.

Ex32 : L'ensemble $\{\cos(n x) \mid n \in \mathbb{Z}\}$ est dense dans $[-1, 1]$.

Ex33 : Pour $p \in \mathbb{P}$ premier, on appelle groupe de Prüfer l'ensemble $\bigcup_{n \in \mathbb{N}} \mathbb{U}_{p^n}$, il s'agit d'un sous groupe de $\mathbb{U}$, infini et dont tous les éléments ont pour ordre fini une puissance de p.

Prop34 : On a $\mathbb{U}_d \subset \mathbb{U}_m \iff d \mid m$, et $\mathbb{U}_m = \bigcup_{d \mid m} \mu_d$

Appli35 : On a $m = \sum_{d \mid m} \varphi(d)$.

Prop36 : Dans $\mathbb{F}_q$ un corps fini, on a $x \in \mathbb{F}_q^*$ d'ordre m si et seulement si x est racine de $X^m - 1$ et pas de $X^d - 1$ pour $d \mid m$. On en a $\varphi(m)$ si $m \mid q-1$ et 0 sinon.

App37 : Le groupe des inversibles d'un corps fini est un groupe cyclique.

App38 (Wedderburn) Tout corps fini est commutatif (autrement dit tout corps gauche est infini).

Théo39 (Kronecker) Soit $P \in \mathbb{Z}[X]$ unitaire de degré m, et dont toute racine complexe est dans $\mathbb{D}$. Si $P(0) \neq 0$, alors toutes les racines de P sont des racines de l'unité.

2) Polynômes cyclotomiques.

[Per] 80 84

Def40 : Pour $m \in \mathbb{N}^*$, on appelle m-ième polynôme cyclotomique, noté ϕ_m, le polynôme $\phi_m(X) = \prod_{\zeta \in \mu_m} (X - \zeta) \in \mathbb{C}[X]$.

Prop41 : Pour $m \in \mathbb{N}^*$, on a $\prod_{d \mid m} \phi_d(X) = X^m - 1$, ça permet de calculer les polynômes cyclotomiques récursivement.

Ex42 : $\phi_1(X) = X - 1$, $\phi_2(X) = X + 1$, $\phi_3(X) = X^2 + X + 1$.

Rq43 : On peut considérer un polynôme cyclotomique sur tout corps $\mathbb{L}$ en regardant dans un corps de décomposition de X^{n-1} sur $\mathbb{k}$. Le polynôme est l'image de ϕ_d par l'homomorphisme canonique $\mathbb{Z} \to \mathbb{k}$ comme on le verra.

Théo44 : Pour tout $m \geq 1$, ϕ_m est à coefficients dans $\mathbb{Z}$, et irréductible sur $\mathbb{Z}$ et sur $\mathbb{Q}$. DVP

Cor45 : Soit $p \nmid m$, $q = p^a$, le degré d'un facteur irréductible de $\Phi_m \in \mathbb{F}_q[X]$ est toujours égal à l'ordre de q dans $(\mathbb{Z}/m\mathbb{Z})^\times$.

Rq46 : Ainsi, les polynômes cyclotomiques sur les corps finis ne sont pas toujours irréductibles.

[FGN1] 158, 159

Appl47 (Dirichlet). Soit $m \in \mathbb{N}^*$. il existe une infinité de nombres premiers congrus à 1 modulo m. DVP

III. Applications.

1) Algèbre linéaire.

[FGN2] 99-100

Def48 : On appelle matrice circulante toute matrice de la forme

$$\begin{pmatrix} a_0 & a_{m-1} & \cdots & a_1 \\ \vdots & a_0 & \ddots & a_2 \\ \vdots & \vdots & a_0 & \vdots \\ \vdots & \vdots & a_1 & \vdots \\ a_{m-1} & \cdots & \cdots & a_0 \end{pmatrix} \in \mathcal{M}_m(\mathbb{C}).$$

Théo49 : L'ensemble des matrices circulantes forme une sous-algèbre commutative de $\mathcal{M}_m(\mathbb{C})$. Ses éléments de A sont simultanément diagonalisables, les valeurs propres d'éléments de A sont les sommes de la forme $\sum_{k=0}^{m-1} a_k \omega^k$, $\omega \in \mathbb{U}_m$.

2) Constructibilité.

On se place dans un plan affine P muni de $(O, \vec{i}, \vec{j})$ un repère orthonormé direct. On identifie les points de P à leurs coordonnées dans $\mathbb{R}^2$ au sein de ce repère.

[Goz] 4749

Def 50 : Soit $X \subset P$ de cardinal ≥ 2. On considère :

a) Les droites passant par deux points distincts de X

b) Les cercles centrés en un point de X et passant par un autre point de X.

On dit que $M \in P$ est constructible en un pas à partir de X s'il se réalise comme intersection de $\gamma_1 \neq \gamma_2$ avec $\gamma_1, \gamma_2 \in a)$ ou $\gamma_1, \gamma_2 \in b$ ou $\gamma_1 \in a)$ $\gamma_2 \in b)$.

Rq 51 : $|X| \geq 2$ impose que X soit constructible en 1 pas à partir de X.

Def 52 : On pose $B_0 = X$ et B_{i+1} l'ensemble des points constructible en un pas à partir de B_i. On pose $B = \bigcup B_i$ l'ensemble des points constructible à partir de X. A partir d'ici, on dira constructible pour constructible à partir de (O, I).

Prop def 53 : Un nombre $x \in \mathbb{R}$ est dit constructible si $(x, 0)$ est constructible, ou si $(0, x)$ est constructible.

74 76

Prop def 54 : Soit $\theta \in \mathbb{R}$, le point $(\cos\theta, \sin\theta)$ est constructible si et seulement si l'un ou l'autre des réels $\cos\theta$, $\sin\theta$ est constructible, on dit alors que θ est un angle constructible.

Prop 55 : L'ensemble des angles constructible est un sous-groupe de $(\mathbb{R}, +)$.

Def 56 : On dit que le polygône régulier à n côtés est constructible si l'angle $\frac{2\pi}{n}$ est constructible.

Prop 57 : Soient $m, n \geq 1$ premiers entre eux. Le polygône régulier à mn côtés est constructible si et seulement si ceux à m et à n côtés le sont tous les deux.

Théo 58 : Pour $\alpha \in \mathbb{N}^*$, le polygône régulier à 2^α côtés est constructible. Si $p \geq 3$ est un nombre premier, le polygône régulier à p^α côtés est constructible si et seulement si $\alpha = 1$ et p est un nombre premier de Fermat.

Ex 59 : (Construction d'un 5-gone régulier) À partir de $\{O, I\}$

- Construire $J, -I$ - Construire $D = \text{milieu } [O, I]$ - Construire $E = [O, J] \cap \mathcal{C}(D, \|DJ\|)$
- Construire $F = \text{milieu } [O, E]$ - Construire Δ perpendiculaire à (OI) passant par F
- Construire $M_1 M_4 = \mathcal{C}(O, 1) \cap \Delta$ - Construire $\mathcal{C}(M_1, \|I M_1\|)$ et $\mathcal{C}(M_4, \|I M_4\|)$, on trouve M_2 (resp M_3) comme intersection de ces cercles et de $\mathcal{C}(O, 1)$ (l'autre point étant I dans les deux cas).

3] Représentation des groupes finis.

Def 60 : On rappelle qu'une représentation de G groupe fini d'ordre n est la donnée d'un morphisme $G \xrightarrow{\rho} GL(V)$ où V est un $\mathbb{C}$ espace vectoriel de dimension d. [Ulm]
On appelle caractère d'une représentation l'application $g \mapsto \text{tr}(\rho(g)) \in \mathbb{C}$.

Def 61 : On dit qu'une représentation (ρ, V) de G est irréductible si aucun sous espace vectoriel non trivial de V n'est stable sous l'action de G. Le caractère associé à une telle représentation est dit irréductible.

Prop 62 : Soit (ρ, V) une représentation de G. $\forall g \in G$, $\rho(g)$ est diagonalisable et ses valeurs propres sont dans $\mathbb{U}_n$ où $|G| = n$

Appli 63 : On pose $\overline{\mathbb{Z}}$ les éléments de $\mathbb{C}$ racines d'un polynôme unitaire à coefficients entiers, il s'agit d'un sous anneau de $\mathbb{C}$ avec $\mathbb{U}_n \subset \overline{\mathbb{Z}}$ quel que soit $n \geq 1$. [Rom]

Cor 64 : Le degré d'une représentation irréductible de G divise son ordre.

Prop 65 : Si G est abélien, alors tout caractère irréductible de G est de degré 1 et est un morphisme $G \to \mathbb{C}^*$. [Ulm]

Appl 66 : Si $G \cong \mathbb{Z}/n\mathbb{Z}$ est cyclique, et $\omega \in \mu_n$, la table de caractère de G est donnée par

	1	g_0	$\cdots$	g_0^{n-1}
$\mathbb{1}$	1	1		1
χ_1	1	ω		ω^{n-1}
$\vdots$		$\vdots$		$\vdots$
χ_{n-1}	1	ω^{n-1}		$\omega^{(n-1)^2}$

Appl 67 : Table de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$:

1	1	1	1
1	-1	1	-1
1	1	-1	-1
1	-1	-1	1

Table des groupes non abélien d'ordre 8 :

1	1	1	1	1
1	1	-1	1	-1
1	1	1	-1	1
1	1	-1	-1	1
2	-2	0	0	0