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

1 Généralités sur le groupe des nombres complexes de module 1

Notation 1. On note $\mathcal{U}$ l'ensemble des nombres complexes de module 1.

Proposition 1. *$(\mathcal{U}, \times)$ est un sous-groupe de $\mathbf{C}^*$.*

1.1 L'exponentielle complexe [Rud]

Définition 1. La fonction exponentielle est définie pour tout nombre complexe z par $\exp z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$.

Proposition 2. *L'exponentielle est un morphisme de $(\mathbf{C}, +)$ vers $(\mathbf{C}^*, \times)$.*

Définition 2. Pour $t \in \mathbf{R}$, on définit le cosinus et le sinus, notés cos et sin comme étant resp. la partie réelle et la partie imaginaire de l'exponentielle e^{it}.

Définition 3. On définit π comme étant le double du plus petit réel positif t tel que $\cos t = 0$. On a alors $e^{i\pi} + 1 = 0$.

Théorème 1. *L'exponentielle est une surjection de $(\mathbf{C}, +)$ vers $(\mathbf{C}^*, \times)$. Elle réalise un morphisme de groupes de $(\mathbf{R}, +)$ vers $(\mathcal{U}, \times)$, surjectif et de noyau $2\pi\mathbf{Z}$. En particulier $\mathcal{U}$ est isomorphe à $\mathbf{R}/2\pi\mathbf{Z}$.*

Ainsi, tout nombre complexe non nul z s'écrit de manière unique sous la forme $z = re^{i\theta}$, avec $r \in \mathbf{R}_+^*$ et $\theta \in \mathbf{R}/2\pi\mathbf{Z}$. r est le *module* de z et θ son *argument*.

1.2 Trigonométrie

Proposition 3. *Formule de De Moivre :* $\forall t \in \mathbf{R}, n \in \mathbf{N},\ (\cos t + i \sin t)^n = \cos(nt) + i \sin(nt)$.
Formules d'Euler : $\forall t \in \mathbf{R},\ \cos t = \frac{e^{it}+e^{-it}}{2},\ \sin t = \frac{e^{it}-e^{-it}}{2i}$.

Application. – Linéarisation de $\sin^n t$ et de $\cos^n t$ (en vue par exemple d'une intégration).
– Calcul des sommes $\sum_{n=0}^{N} \sin(nx)$ (en vue du théorème de Féjer par exemple).

1.3 Sous-groupes de $\mathcal{U}$

Proposition 4. *Les sous-groupes fermés de $\mathcal{U}$ sont $\mathcal{U}$ et les $\mathcal{U}_n = \{z \in \mathcal{U} \mid z^n = 1\}$ pour $n \in \mathbf{N}$.*

Proposition 5. *Les sous-groupes de $\mathcal{U}$ sont soit finis, soit denses.*

Exemple. – Pour p premier, on appelle p-ième groupe de Prüfer $O_p = \bigcup_{\alpha \in \mathbf{N}} \mathcal{U}_{p^\alpha}$. Les seuls sous-groupes de O_p sont les $\mathcal{U}_{p^\alpha}$ et lui-même ; O_p est indécomposable [FGN].
– Le sous-groupe de $\mathcal{U}$ constitué des éléments d'ordre fini est égal à $\bigcup_{n \in \mathbf{N}} \mathcal{U}_n$. Il est isomorphe à $\mathbf{Q}/\mathbf{Z}$.

2 Groupe des racines n-ièmes de l'unité

2.1 Étude du groupe $\mathcal{U}_n$

Proposition 6. *$\mathcal{U}_n$ est un groupe cyclique d'ordre n, ainsi il est isomorphe à $\mathbf{Z}/n\mathbf{Z}$. Réciproquement, tout sous-groupe fini de $\mathbf{C}$ est un des groupes $\mathcal{U}_n$.*

Définition 4. On appelle *racine n-ième primitive de l'unité* tout générateur de $\mathcal{U}_n$. On note μ_n^* l'ensemble des racines n-ièmes primitives.

Exemple. $\mu_3^* = \{j, j^2\}$, $\mu_4^* = \{i, -i\}$.

Exemple. Calcul du centre de $Sl(E)$, isomorphe à $\mathcal{U}_n$.

Proposition 7. *On a $\mu_n^* = \{e^{2ik\pi/n} \mid 1 \leq k \leq n, k \wedge n = 1\}$ et $\mathcal{U}_n = \sqcup_{d|n} \mu_d^*$. Ainsi il y a $\varphi(n)$ éléments dans μ_n^*. Soit $\xi \in \mu_n^*$. Alors les éléments de μ_n^* sont les ξ^k, avec $1 \leq k \leq n$ et $k \wedge n = 1$.*

Application. On a $n = \sum_{d|n} \varphi(d)$.

2.2 Cyclotomie

Définition 5. Le n-ième *polynôme cyclotomique* est $\Phi_n = \prod_{\xi \in \mu_n^*} (X - \xi)$.

Exemple. $\Phi_1 = X - 1$, $\Phi_2 = X + 1$, $\Phi_3 = X^2 + X + 1$...

Proposition 8. *Φ_n est unitaire et de degré $\varphi(n)$.*

Proposition 9. $X^n - 1 = \prod_{d|n} \Phi_d$.

Proposition 10. $\Phi_n \in \mathbf{Z}[X]$.

Application (Theoreme de Wedderburn). Tout corps fini est commutatif.

Dirichlet faible ?

Théorème 2. *Φ_n est irréductible sur $\mathbf{Q}$.*

Corollaire 1. *Si $\xi \in \mu_n^*$, alors son polynôme minimal sur $\mathbf{Q}$ est Φ_n. En particulier $[Q(\xi) : \mathbf{Q}] = \varphi(n)$.*

Théorème 3 (Kronecker)**.** *FGN.*

Proposition 11 ([Demazure])**.** *Réduction dans $\mathbf{F}_q$, application à la construction de corps.*

3 Applications

3.1 Groupe diédral

Cf Josette.

3.2 Angles

Soit E le plan euclidien.

Proposition 12. *Étant donnés deux vecteurs unitaires de E, il existe une unique rotation qui envoie l'un sur l'autre. Cela définit la relation d'équivalence $(u, v)R(u', v')$ ssi il existe une rotation r tq $r(u) = u'$ et $r(v) = v'$.*

Définition 6. La classe d'équivalence de (u, v) est appelée *angle orienté* de u et de v. On note $\mathcal{A}$ l'ensemble des angles orientés.

Proposition 13. *Soit $\varphi : \mathcal{A} \to SO(E)$, $(u, v) \mapsto r$ telle que r soit la rotation envoyant u sur v. φ est bien définie et est une bijection. On en déduit une structure de groupe sur $\mathcal{A}$ en posant $(u, v)+(u', v') = \varphi^{-1}(\varphi(u, v)\circ\varphi(u', v'))$, ce qui fait de φ un morphisme de groupes.*

Proposition 14 (Relation de Chasles)**.** $(u, v) + (v, w) = (u, w)$.

Remarque. On a défini les angles orientés sans orienter E.

On choisit désormais une orientation de E.

Proposition 15. *La matrice d'une rotation de E est la même dans toutes les bases orthonormées directes.*

Définition 7. On associe alors à tout angle (u, v) l'unique $\theta \in \mathbf{R}/2\pi\mathbf{Z}$ tel que $\varphi(u, v)$ soit représenté par la matrice $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. θ est appelé la *mesure* de l'angle (u, v).

Proposition 16. *$SO(E) \approx \mathbf{R}/2\pi\mathbf{Z}$, i.e. $SO_2(\mathbf{R}) \approx \mathcal{U}$.*

3.3 Constructibilité

Gauss et Gauss-Wantzel (Carrega).

3.4 Caractères

Soit G un groupe fini.

Définition 8. On appelle *caractère* de G tout morphisme de G dans $\mathbf{C}^*$. L'ensemble des caractères de G forme un groupe abélien pour la multiplication dans $\mathbf{C}$, noté $\widehat{G}$.

Exemple. Si $G = \mathfrak{S}_n$, alors la signature est un caractère sur G.
Si $G = \mathbf{Z}/n\mathbf{Z}$, alors $k \mapsto e^{2ik\pi/n}$ est un caractère sur G.

Remarque. Tout caractère $\chi : G \to \mathbf{C}$ se factorise en un morphisme $G/D(G) \to \mathbf{C}$. Ainsi supposera désormais le groupe G abélien.

Proposition 17. *Si $|G| = n$, alors les éléments de $\widehat{G}$ sont à valeurs dans $\mathcal{U}_n$.*

Proposition 18. *$\widehat{\mathbf{Z}/n\mathbf{Z}} \to \mathcal{U}_n$, $\chi \mapsto \chi 1$ est un isomorphisme. Ainsi tout groupe cyclique est isomorphe à son dual.*

Proposition 19. *Si H est un groupe abélien fini, alors $\widehat{G \times H} \equiv \hat{G} \times \hat{H}$.*

Lemme 1. *Soit H un sous-groupe de G. Alors tout caractère de H se prolonge en un caractère de G (suite exacte cf Serre).*

Théorème 4. *Soit G un groupe abélien fini. Alors il existe une unique suite d'entiers $a_1, \dots a_k$, soumis à $a_1 | \dots | a_k$, et $a_1 > 1$, tels que $G \approx \mathbf{Z}/a_1\mathbf{Z} \times \cdots \times \mathbf{Z}/a_k\mathbf{Z}$.*

Corollaire 2. *Tout groupe abélien fini est isomorphe à son dual.*

3.5 Loi de réciprocité quadratique

Définition 9. Soit p un nombre premier impair. Le *symble de Legendre* de n modulo p, noté $\left(\frac{n}{p}\right)$, est défini par :

$$\left(\frac{n}{p}\right) = \begin{cases} 0 \text{ si } a \equiv 0 \ [p] \\ 1 \text{ si } a \text{ est un carré non nul modulo } p \\ -1 \text{ si } a \text{ n'est pas un carré modulo } p \end{cases}$$

Proposition 20. *Le nombre de carrés dans $\mathbf{F}_p$ est $(p+1)/2$.*

Proposition 21. $\forall a \in \mathbf{Z}$, $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \ [p]$
$\left(\frac{-1}{N}\right) = (-1)^{(p-1)/2}$ *et* $\left(\frac{2}{N}\right) = (-1)^{(p^2-1)/8}$

Application (Dirichlet faible). Cf Perrin !

Théorème 5 (Loi de réciprocité quadratique)**.** *Soient p, q des nombres premiers impairs distincts. Alors on a :*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Cf Hindry p. 26

Exemple (Hindry p.10). Soit p un nombre premier s'écrivant $p = x^2 - 6y^2$, avec $x, y \in \mathbf{Z}$. Alors p ne divise pas y, car sinon p diviserait aussi x et donc p^2 diviserait p. Donc $6 \equiv (xy^{-1})^2\ [p]$, donc $\left(\frac{6}{p}\right) = 1$ i.e. $(-1)^{(p^2-1)/8}(-1)^{(p-1)/2}\left(\frac{p}{3}\right) = 1$, on en déduit des congruences de p modulo 24.