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

Développements :

Transformée de Fourier rapide, Structure des groupes abéliens finis.

Bibliographie :

Arnaudies, Peyré, Rombaldi, Analyse complexe des Queffelec, Audin, FGN, Gozard, Ortiz.

Rapport du jury :

Il ne faut pas uniquement aborder cette leçon de façon élémentaire sans réellement expliquer où et comment les nombres complexes de modules 1 et les racines de l'unité apparaissent dans divers domaines des mathématiques (exponentielle complexe et ses applications, polynômes cyclotomiques, spectre de matrices remarquables, théorie des représentations). Il ne faut pas non plus oublier la partie « groupe » de la leçon : on pourra s'intéresser au relèvement du groupe unité au groupe additif des réels et aux propriétés qui en résultent. De même les sous-groupes finis de S 1 sont intéressants à considérer dans cette leçon. On pourra aussi s'intéresser aux groupes des nombres complexes de Qris, et les racines de l'unité qui y appartiennent ; tout comme aux sous-groupes compacts de C*.

Cette leçon ne doit pas se cantonner aux aspects élémentaires. Elle doit donner l'occasion d'expliquer où et comment les nombres complexes de module 1 et les racines de l'unité apparaissent dans divers domaines des mathématiques (exponentielle complexe et ses applications, polynômes cyclotomiques, spectre de matrices remarquables, théorie des représentations). Il ne faut pas non plus oublier la partie « groupe » de la leçon : on pourra s'intéresser au relèvement du groupe unité au groupe additif des réels et aux propriétés qui en résultent. De même, il est pertinent d'étudier les sous-groupes finis de S1 dans cette leçon. On pourra aussi s'intéresser aux groupes des nombres complexes de $Q[i]$, et les racines de l'unité qui y appartiennent ; tout comme aux sous-groupes compacts de C^*. Les transformées de Fourier discrètes et rapides peuvent aussi être abordées dans cette leçon.

1 Nombres complexes de module 1

1.1 Le groupe U

Définition 1 (Arnaudies p226)**.** *U comme noyau du morphisme $z \mapsto |z|$.*

Remarque 2. *En identifiant le plan complexe à $\mathbb{R}^2$, U est le cercle unité S^1. C'est un groupe multiplicatif.*

Exemple 3. $\sqrt{2}/2 + i\sqrt{2}/2$.

Théorème 4 (Arnaudies p226)**.** *Isomorphisme entre $\mathbb{R}^{+*} \times U$ et $\mathbb{C}^*$.*

Proposition 5. *U est le plus grand sous-groupe borné de $\mathbb{C}^*$.*

Corollaire 6. *U est un compact connexe de $\mathbb{C}$.*

1.2 L'exponentielle complexe

Définition 7 (Arn p226)**.** *[H M Queffelec] Exponentielle sur $\mathbb{C}$ comme série entière.*

Proposition 8 (HM Queff p7)**.** *Surjection de $\mathbb{C}$ sur $\mathbb{C}^*$.*

Théorème 9 (Arnaudies p226)**.** *[Queffelec p7] $x \mapsto exp(ix)$ est un morphisme surjectif de groupes de noyau $2\pi\mathbb{Z}$. Donc $\mathbb{R}/2\pi\mathbb{Z} \simeq U$.*

Application 10 (Queffelec p9)**.** *Tout nombre complexe s'écrit sous la forme $z = rexp(i\theta)$ où $r \in \mathbb{R}^{+*}$ et $\theta \in \mathbb{R}$.*

Exemple 11. $\sqrt{2}/2 + i\sqrt{2}/2 = \exp^{\pi/4}$.

Proposition 12 (Mercier p169)**.** *Tout morphisme continu de $\mathbb{R}$ dans U est de la forme $t \mapsto exp(it\theta)$.*

Théorème 13 (Queffelec p9)**.** *[Rouvière p305] Relèvement.*

Application 14 (Bernis)**.** *Asymptotique de l'équation de Bessel.*

1.3 Trigonométrie

Définition 15 (Arnaudies p227)**.** *$cos(x) = \Re(exp(ix))$ et $sin(x) = \Im(exp(ix))$.*

Exemple 16. $\cos(\pi/4)$ ..

Proposition 17 (Admis)**.** $\cos^2 + \sin^2 = 1$.

Proposition 18 (Arnaudies p227)**.** *Formule de Moivre.*

Proposition 19 (Arn p227)**.** *Formules d'Euler.*

Exemple 20 (Arn p227). *$exp(i\pi/2) = i$. $exp(2i\pi/3) = j$.*

Application 21 (Arn p228). *Somme des $cos(k\theta)$.*

Application 22 (Arn p228). *Linéarisation de $cos(x)^n$.*

Application 23 (Arn p229). *[Gourdon] Expression de cos comme polynôme en $cos(x)$, avec T_n polynôme de Tchebychev.*

Application 24. *Noyau de Fejer, de Dirichlet.*

Proposition 25. *Paramétrage d'un cercle et équation de Diophante.*

1.4 Angles et rotations

Définition 26 (Arn p234). *Argument principal.*

Définition 27 (Audin p61). *$SO_2(\mathbb{R})$. C'est un groupe.*

Proposition 28 (Audin p62). *$SO(2)$ est isomorphe et homéomorphe à U.*

Corollaire 29 (Audin p62). *$SO(2)$ est commutatif, connexe par arcs.*

Proposition 30 (Audin p63). *$\mathbb{R}/2\pi\mathbb{Z} \simeq SO(2)$.*

Définition 31 (Audin p63). *Rotation. Morphisme $\theta \mapsto R_\theta$. Angle d'une rotation.*

Proposition 32 (Audin p73). *Etant donnés deux vecteurs unitaires, il existe une unique rotation qui envoie l'un sur l'autre. (Transitivité de $SO(2)$ sur le plan.)*

Définition 33 (Audin p73). *$(u, v)R(u', v')$ si et seulement si il existe une rotation telle que $f(u) = u'$ et $f(v) = v'$.*
Classe d'équivalence=angle orienté.
A l'ensemble des angles orientés de vecteurs.

Proposition 34 (Audin p64). *Si E est un plan vectoriel orienté, la matrice d'une rotation ne dépend pas du choix de la base orthonormée directe dans laquelle elle est écrite.*

Proposition 35 (Audin p75). *L'application $A \to SO(2)$ qui à un angle de représentant (u, v) associe la rotation f telle que $f(u) = v$ est bien définie et bijective.*

Corollaire 36. *L'application $\theta \mapsto R_\theta$ est surjective et induit l'isomorphisme $\mathbb{R}/2\pi\mathbb{Z} \simeq SO(2) \simeq U$.*

2 Sous-groupes U et racines de l'unité

2.1 Sous-groupes de $\mathbb{R}$ et de U

Proposition 37 (FGN AN1 p29). *Un sous-groupe de $\mathbb{R}$ est soit dense dans $\mathbb{R}$,soit de la forme $n\mathbb{Z}$. (Ne pas mettre ça ici car on l'utilise pour la surjectivité de* exp.*)*

Corollaire 38 (FGN AN1 p30). *Un sous-groupe de U est soit fini, soit dense dans U.*

Application 39. *Les sous-groupes finis de $\mathbb{C}$ sont les $U_n = \{z \in U, z^n = 1\}$,*

Application 40. *Un sous-groupe de U fini est égal au groupe des racines n ièmes de l'unité où $n = |G|$.*

Proposition 41 (FGN p29). *Le sous-groupe engendré par $exp(i\theta)$ est dense si et seulement si $\theta \notin 2\pi Q$.*

Proposition 42 (TD3 5/2). *Si $\theta/2\pi$ estrationnel alors $\{exp(in\theta, n \in \mathbb{Z}\}$ est fini. Sinon, il est dense dans U.*

Proposition 43 (TD3 5/2). *Si $\theta/2\pi$ est irrationnel alors $\{exp(in\theta, n \in \mathbb{N}\}$ est dense dans U.*

Application 44 (FGN ALG1 1.13). *$\{exp(in), n \in \mathbb{N}\}$ est dense dans S^1.*
$(sin(n))_{n\in\mathbb{N}}$ est dense dans $[-1, 1]$.

2.2 Sous-groupe des racines de l'unité

Remarque 45. *Utiliser Arnaudies.*

Définition 46 (Perrin ?). *[Gozard p67] L'application $U \to U, z \mapsto z^n$ est un morphisme de groupes. Son noyau est le groupe des racines de l'unité, noté U_n.*

Exemple 47. *$1, j$ et j^2 sont les 3 racines troisièmes de l'unité.*

Proposition 48 (Gozard p67). *$\mathbb{Z}/n\mathbb{Z} \to U_n, k \mapsto exp(2ik\pi/n)$ est un isomorphisme de groupes. Donc U_n est un groupe cyclique d'ordre n.*

Proposition 49. *Les endomorphimes continus de U sont les $z \mapsto z^n$.*

Proposition 50. *Les racines nèmes de l'unité sont les sommets d'un polygone régulier à n côtés. Définition du groupe diédral, ordre et générateurs.*

Définition 51 (Gozard p67). *Racine primitive de l'unité. μ_n l'ensemble des racines n-ième de l'unité.*

Exemple 52. *j et j^2.*

Proposition 53 (Gozard p67). *Description de μ_n, de cardinal $\phi(n)$.*

Exemple 54. *Racines primitives 2ème : -1, 3ème : j, j^2, 4ème : $i, -i$.*

Proposition 55. *$U_d \subset U_n$ si et seulement si $d|n$.*

Proposition 56 (Romb p384). *$U_n = \cup_{d|n}\mu_d$.*

Application 57 (Romb p387). *$n = \sum_{n|d} \phi(d)$.*

2.3 Cyclotomie

Définition 58 (Gozard p67). *Polynôme cyclotomique.*

Proposition 59 (Gozard p68). *[Perrin p81] $X^n - 1$ en fonction des polynômes cyclotomiques.*

Proposition 60 (Gozard). *Φ_n est unitaire, de degré $\phi(n)$ et irréductible sur $\mathbb{Z}$.*

Proposition 61 (Romb, Gozard). *Φ_p avec p premier.*

Exemple 62. *Quelques calculs.*

Proposition 63 (Romb p389). *Infinité de nombres premiers de la forme $\lambda m + 1$.*

Théorème 64 (FGN AL1). *Théorème de Kronecker. Soit $P \in \mathbb{Z}[X]$ dont les racines dans $\mathbb{C}$ sont non nulles et de module leq1. Alors les racines de P sont des racines de l'unité.*

Corollaire 65. *Si de plus P est irréductible, alors P est un polynôme cyclotomique.*

Proposition 66 (Ortiz p169). *Racines de l'unité dans les $Q[\sqrt{d}]$.*

3 Application dans la théorie des représentations

3.1 Caractère linéaire d'un groupe abélien fini

Définition 67 (Peyré p2). *Caractère d'un groupe abélien et dual.*

Exemple 68. *La signature est un caractère de S_n.*

Proposition 69 (Peyré p2). *Soit G un groupe fini de cardinal n. Les éléments de du dual de G sont les morphismes de G dans U_n.*

Remarque 70 (Peyré p3). *Le dual de G est donc un groupe fini commutatif.*

Proposition 71 (Peyré p4). *Si G est un groupe cyclique engendré par g_0 et w une racine primitive n-ième de l'unité alors les éléments du dual de G sont de la forme $\chi(g_0^k) = (w^j)^k$. En particulier, $G \simeq$ au dual de G.*

Exemple 72. *Table de caractère d'un groupe cyclique.*

Proposition 73. *Si G est abélien fini, il est isomorphe à son dual.*

Application 74. *Théorème de structure des groupes abéliens.*

Proposition 75 (Peyré p12). *Si G est un groupe fini, on a $\widehat{G} \simeq G/D(G)$.*

On est confronté à un manque de caractères. La solution est alors d'introduire la notion de représentations linéaires, qui généralise la notion de caractère ($\widehat{G}$ est constitué des caractères des représentations de dimension 1. En quelque sorte, un groupe non commutatif n'a pas assez de représentations en dimension 1 et il faut passer aux dimensions supérieures.

3.2 Transformée de Fourier discrète

Formule d'inversion.

3.3 Représentation linéaire des groupes finis

Rauch

Proposition 76. *Soit $n = |G|$. Si ρ est une représentation de G alors pour tout $g \in G$, $\rho(g)$ est diagonalisable à valeurs propres dans U_n.*

Proposition 77. *G est abélien si et seulement si tous ses caractères irréductibles sont de degré 1. Ce sont alors des morphismes de G dans U_n.*

Proposition 78. *Si χ est un caractère de G alors $\chi(g^{-1}) = \overline{\chi(g)}$.*

Application 79. *La table de caractères de S_n ne contient que des réels.*

Proposition 80. *Groupes distingués et noyaux de caractères.*

Remarque 81. *La connaissance des caractères des groupes abéliens permet de construire, par passage au quotient, des tables de caractères de groupes non abéliens.*

Exemple 82. *Si on note V_4 le sous-groupe de A_4 engendré par les bi-transpositions, A_4/V_4 est isomorphe à $\mathbb{Z}/3\mathbb{Z}$, et on déduit de la table de $Z/3Z$ celle de A_4.*

4 Applications en algèbre linéaire : matrices circulantes et stochastiques

Remarque 83. *Représentent des chaînes de Markov.*

Définition 84 (FGN). *Matrice circulante.*

Proposition 85 (FGN). *Leur spectre est inclus dans les racines n èmes de l'unité.*

Proposition 86 (FGN). *Eléments simultanément diagonalisables sur $\mathbb{C}$.*

Proposition 87. *Spectre des matrices stochastiques.*