Leçon 102 Groupe des nombres complexes de module 1, sous-groupes des racines de l'unité, applications

Dorian Cacitti-Holland

2020-2021

Références.

1. Cours de mathématiques 1 Algèbre de Arnaudiès et Fraysse
2. Algèbre et géométrie de François Combes
3. Géométrie de Michèle Audin
4. Extensions de corps Théorie de Galois de Josette Calais
5. Exercices d'algèbre de Pascal Ortiz
6. L'algèbre discrète de la transformation de Fourier de Gabriel Peyré
7. Eléments d'analyse et d'algèbre de Pierre Colmez

Développements.

1. Irréductibilité des polynômes cyclotomiques
2. Théorème de structure des groupes abéliens finis

Table des matières

1 Nombres complexes de module 1

1.1 Un groupe

(Chapitre VI.7 du Cours de mathématiques 1 Algèbre de Arnaudiès et Fraysse)

1. Proposition : L'application $|\cdot|$ est un morphisme de groupes de $\mathbb{C}^*$ dans $\mathbb{R}_+^*$
2. Définition : On note $\mathbb{U}$ le noyau de ce morphisme
3. $i, j = e^{\frac{2\pi}{3}} \in \mathbb{U}$
4. Remarque : Il s'agit donc d'un groupe
5. Remarque : $\mathbb{U} \simeq S^1$
6. Théorème : $(r, u) \in \mathbb{R}_+^* \times \mathbb{U} \longmapsto ru \in \mathbb{C}^*$ est isomorphisme de groupes
7. Théorème : $x \in \mathbb{R} \longmapsto e^{ix} \in \mathbb{U}$ est un morphisme de groupes surjectif de noyau $2\pi\mathbb{Z}$
8. Corollaire : $\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{U}$

1.2 Applications trigonométriques

(Chapitre VI.7 du Cours de mathématiques 1 Algèbre de Arnaudiès et Fraysse)

1. Définition : $cos(x) = Re(e^{ix}), sin(x) = Im(e^{ix})$
2. Remarque : On a donc $e^{ix} = cos(x) + isin(x)$
3. Proposition : Formule de Moivre : $e^{inx} = cos(nx) + isin(nx)$
4. Proposition : Formules d'Euler : $cos(x) = \frac{e^{ix}+e^{-ix}}{2}, sin(x) = \frac{e^{ix}-e^{-ix}}{2i}$
5. Exemple : $e^{\frac{2i\pi}{3}} = \frac{1+i\sqrt{3}}{2}, e^{\frac{i\pi}{2}} = i$
6. Application : $\sum_{k=0}^{n} e^{ikt} = e^{\frac{int}{2}} \frac{sin\left(\frac{(n+1)t}{2}\right)}{sin\left(\frac{n}{2}\right)}$, $\sum_{k=0}^{n} cos(kt) = cos\left(\frac{nt}{2}\right) \frac{sin\left(\frac{(n+1)t}{2}\right)}{sin\left(\frac{t}{2}\right)}$, $\sum_{k=0}^{n} sin(kt) = sin\left(\frac{nt}{2}\right) \frac{sin\left(\frac{(n+1)t}{2}\right)}{sin\left(\frac{t}{2}\right)}$
7. Proposition : $cos(x)^n = \frac{1}{2^n} \sum_{k=0}^{n} \binom{n}{k} e^{i(2k-n)x}$
8. Proposition : $cos(nx) = T_n(cos(x))$ avec T_n le n-ième polynôme de Tchebychev

1.3 Paramétrisation du cercle unité

(Chapitre 12.7 d'Algèbre et géométrie de François Combes)

1. Proposition : Il existe $(x, y, z) \in \mathbb{N}^3$ tel que $x^2 + y^2 = z^2 \Leftrightarrow \exists (X, Y) \in \mathbb{Q}^2, X^2 + Y^2 = 1$
2. Théorème : $t \in \mathbb{R} \longmapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \in \mathbb{U}\backslash\{(-1, 0)\}$ est une bijection
3. Remarque : Elle se prolonge en à $\mathbb{R} \cup \{\infty\}$ en associant $(-1, 0)$ à ∞
4. Application : Les points de $\mathbb{U}\backslash\{(-1, 0)\}$ à coordonnées rationnelles sont de la forme $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ avec $t \in \mathbb{Q}$
5. Application : Soit $(x, y, z) \in \mathbb{N}^3$, alors $x^2 + y^2 = z^2 \Longleftrightarrow \exists (d, u, v) \in \mathbb{N}^3, u \wedge v = 1, x = d(u^2 - v^2), y = 2duv, z = d(u^2 + v^2)$

1.4 Mesure d'un angle orienté

(Chapitre III.1 de Géométrie de Michèle Audin et VI.8 de Algèbre et géométrie de François Combes)

1. Proposition : Soit $(u,v) \in (S^1)^2 \simeq \mathbb{U}^2$, alors il existe une unique rotation $r \in SO(\mathbb{R}^2)$ tel que $r(u) = v$
2. Exemple : La rotation entre i et -1 est donnée par $z \longmapsto e^{i\frac{\theta}{2}}z = iz$ car la rotation entre $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ et $\begin{pmatrix} -1 \\ 0 \end{pmatrix}$ est donnée par $\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = R\left(\frac{\pi}{2}\right)\begin{pmatrix} x \\ y \end{pmatrix}$
3. Remarque : La proposition est fausse en dimension 3
4. Définition : $(u,v)R(u',v')$ s'il existe une rotation r tel que $r(u) = u', r(v) = v'$
5. Proposition : c'est une relation d'équivalence
6. Définition : L'angle orienté de u et v est la classe d'équivalence de (u,v), A leur ensemble
7. Proposition : $(u,v) \in A \longmapsto r \in SO(\mathbb{R}^2)$ est une bijection
8. Corollaire : A est muni d'une structure de groupe
9. Proposition : Relation de Chasles : $(u,v) + (v,w) = (u,w)$

2 Racines de l'unité et utilisations

2.1 Sous-groupe des racines de l'unité

(Chapitre 6.1 de Extensions de corps de Josette Calais)

1. Définition : On appelle racine n-ième de l'unité toute racine de $X^n - 1$, et on note $\mathbb{U}_n$ leur ensemble
2. Proposition : $\mathbb{U}_n$ un sous-groupe cyclique de $\mathbb{C}^*$, d'ordre n
3. Proposition : $k \in \mathbb{Z}/n\mathbb{Z} \longmapsto e^{i\frac{2k\pi}{n}} \in \mathbb{U}_n$ est un isomorphisme de groupes
4. Définition : On appelle racine n-ième primitivede l'unité tout générateur de $\mathbb{U}_n$, et on note Ω_n leur ensemble
5. Remarque : Soit $\omega \in U_n$, alors $\omega \in \Omega_n$ si et seulement si ω est d'ordre n dans U_n, ie $\omega^n = 1$ et $\forall k \in [\![1, n-1]\!], \omega^k \neq 1$
6. Proposition : $\Omega_n = \{e^{i\frac{2k\pi}{n}}, k \in [\![0, n-1]\!], k \wedge n = 1\}$
7. Corollaire : $|\Omega_n| = \varphi(n)$
8. Exemple : $\Omega_1 = \{1\}, \Omega_2 = \{-1\}, \Omega_3 = \{j, j^2\}, \Omega_4 = \{i, -i\}$
9. Propositon : $\mathbb{U}_n = \bigcup_{d|n} \Omega_d$
10. Corollaire : $n = \sum_{d|n} \varphi(d)$

2.2 Polynômes cyclotomiques

(Chapitres 6.2 de Extensions de corps de Josette Calais, III.4 du Cours d'algèbre de Daniel Perrin et Exercice III.29 de Exercices d'algèbre de Pascal Ortiz)

1. Définition : $\phi_n = \prod_{\omega \in \Omega_n} (X - \omega)$ est appelé le n-ième polynôme cyclotomique
2. Exemple : $\phi_1 = X - 1, \phi_2 = X + 1, \phi_3 = X^2 + X + 1, \phi_4 = X^2 + 1$
3. Proposition : $\phi_n \in \mathbb{Z}[X]$ unitaire irréductible dans $\mathbb{Z}[X]$ de degré $\varphi(n)$
4. Proposition : $X^n - 1 = \prod_{d|n} \phi_d$
5. Corollaire : Si $p \in \mathcal{P}$ alors $\phi_p = X^{p-1} + ... + 1$
6. Corollaire : Si $p \in \mathcal{P}$ et $q = p^n$ alors $\phi_q = \sum_{i=0}^{p-1} \left(X^{p^{n-1}}\right)^i$
7. Théorème de Wedderburn : Un anneau intègre unitaire où tout élément non nul admet un inverse est commutatif, autrement dit un corps gauche fini est un corps

2.3 Utilisation avec les matrices circulantes

1. Définition : Soit $a_1, ..., a_n \in \mathbb{C}$, alors $det \begin{pmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ a_n & a_1 & \dots & a_{n-2} & a_{n-1} \\ \vdots & \vdots & & \vdots & \vdots \\ a_2 & a_3 & \dots & a_n & a_1 \end{pmatrix}$ est appelé déterminant circulant des a_i
2. Proposition : $det \begin{pmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ a_n & a_1 & \dots & a_{n-2} & a_{n-1} \\ \vdots & \vdots & & \vdots & \vdots \\ a_2 & a_3 & \dots & a_n & a_1 \end{pmatrix} = \prod_{k=0}^{n-1} P(e^{\frac{2ki\pi}{n}})$ avec $P = \sum_{j=0}^{n-1} a_{j+1} X^j$
3. Application : Soit $(z_1, ..., z_n) \in \mathbb{C}^n$, $P^0 = (z_1, ..., z_n)$ et $\forall k \in \mathbb{N}, P^{k+1} = \left(\frac{P_1^k + P_2^k}{2}, ..., \frac{P_n^k + P_1^k}{2}\right)$, alors $P^k \underset{k \to +\infty}{\longrightarrow} (g, ..., g)$ avec $g = Isobar(z_1, ..., z_n)$ (à connaître)

2.4 Utilisations en théorie des caractères

(Chapitres I.2 de VIII.1 de L'algèbre discrète de la transformation de Fourier de Gabriel Peyré et 0.3.2 et I.2.5 de Eléments d'analyse et d'algèbre de Pierre Colmez)

Soit G un groupe abélien fini.

1. Définition : Un caractère de G est un morphisme de groupes de G dans $\mathbb{C}^*$, on note $\hat{G}$ leur groupe, appelé dual de G
2. Exemple : Le morphisme trivial est un caractère de G
3. Lemme : Les groupes G et $\hat{\hat{G}}$ sont isomorphes
4. Lemme : Il existe $g \in G$ d'ordre $N(G) = PPCM(o(h), h \in G)$
5. Proposition : Soit $\chi \in \hat{G}$ d'ordre N, alors $\chi(G)$ est un sous-groupe de Ω_N

6. Théorème de strucuture des groupes abéliens finis : Il existe $r \in \mathbb{N}$ et $(d_1, ..., d_r) \in \mathbb{N}^r$ tel que $\forall i \in [\![1, r-1]\!], d_{i+1} \mid d_i$ et $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times ...\mathbb{Z}/d_r\mathbb{Z}$
7. Définition : Soit V un $\mathbb{C}$-espace vectoriel et $\rho : G \longrightarrow GL(V)$, alors on dit que (ρ, V) est une représentation linéaire de G si ρ est un morphisme de groupes, de plus $\chi = tr \circ \rho$ est appelé caractère linéaire de G
8. Définition : On dit que (ρ, V) est une représentation irréductible de G s'il n'existe pas de sous-espace non trivial de V stable par G, dans ce cas on dit que χ est irréductible
9. Théorème : G abélien si et seulement si toutes ses représentations irréductibles sont de degré 1
10. Proposition : Si G groupe cyclique engendré par g_0 d'ordre n alors les caractères irréductibles χ_j de G sont de la forme $\forall g = g_0^k \in G, \chi_j(g) = e^{i\frac{2jk\pi}{n}} \in \omega_n$
11. Corollaire : La table de caractères de $\mathbb{Z}/n\mathbb{Z}$ est une matrice de Vandermonde associée à $e^{\frac{2i\pi}{n}}$