Leçon 102 - Groupe des nombres complexes de module 1. Racines de l'unité. Applications.

Extrait du rapport de jury

Les notions élémentaires concernant les nombres complexes de module 1 (définitions, exponentielle complexe, trigonométrie, etc.) doivent être présentés, avant d'aborder l'aspect "groupe" de $\mathbb{S}^1$ en considérant son lien avec $(\mathbb{R}, +)$ et en examinant ses sous-groupes (en particulier finis). Il est souhaitable de présenter des applications en géométrie plane. Plus généralement, la leçon invite à expliquer où et comment les nombres complexes de module 1 et les racines de l'unité apparaissent dans divers domaines des mathématiques : spectres de matrices remarquables, polynômes cyclotomiques, représentations de groupes, etc. On peut également s'intéresser aux sous-groupes compacts de $\mathbb{C}^*$.
Pour aller plus loin, on peut s'intéresser aux nombres de module 1 et aux racines de l'unité dans $\mathbb{Q}[i]$, ou à la dualité des groupes abéliens finis (notamment la preuve du théorème de structure par prolongement de caractère) ou encore aux transformées de Fourier discrètes et rapides. Des aspects analytiques du sujet peuvent être évoqués (théorème de relèvement, logarithme complexe, analyse de Fourier sur $\mathbb{R}^n$) mais ne doivent occuper ni le coeur de l'exposé, ni l'essentiel d'un développement.

Présentation de la leçon

Je vais vous présenter la leçon 102 intitulée : "Groupe des nombres complexes de module 1. Racines de l'unité. Applications.". Les nombres complexes sont un outil puissant, en géométrie comme en algèbre. Leur richesse est en grande partie déterminée par la sphère unité et les propriétés de ses éléments, notamment de ses sous-groupes. C'est tout ceci qui permet de justifier de leur intervention fréquente dans diverses questions.
Dans la première partie, on s'intéresse à l'étude générale du groupe des nombres complexes de module 1. On commence par définir $\mathbb{U}$ grâce au module et on montre que cet ensemble est en fait un groupe pour la multiplication. On cherche ensuite à aller plus loin en trouvant un (ou même des) isomorphisme(s) faisant intervenir $\mathbb{U}$. Pour cela, on introduit l'exponentielle complexe que l'on définit par sa série entière qui nous permet au passage de définir le nombre π. Tout cela nous conduit au théorème 6 et au corollaire 8 qui permettent d'énoncer les premiers isomorphismes faisant intervenir $\mathbb{U}$ ainsi qu'un résultat topologique sur $\mathbb{U}$. On termine cette sous-partie par quelques propriétés sur les fonctions cosinus et sinus complexes (notamment les formules d'Euler et de De Moivre) qui permettent de linéariser des polynômes en cosinus et en sinus.
On se recentre un peu plus dans une deuxième partie sur le groupe $\mathbb{U}$ en étudiant ses sous-groupes. On commence d'abord par parler de ses sous-groupes finis qui sont des groupes cycliques car générés par les racines primitives n-ièmes de l'unité qui joueront un rôle crucial dans la suite de cette partie. En particulier, on est capable de trouver une partition de $\mathbb{U}_n$ en fonction des racines primitives n-ièmes de l'unité. Cela nous conduit à nous intéresser à ces racines primitives de l'unité en construisant les polynômes cyclotomiques qui possèdent une relation particulière avec le polynôme $X^n - 1$. En effet, cette relation est intéressante pour deux raisons : tout d'abord elle permet de retrouver l'égalité de la proposition 24, mais en plus celle-ci permet de construire de manière récurrente ces polynômes cyclotomiques (inutile désormais de passer par les racines primitives de l'unité pour le déterminer). De plus, ces polynômes possèdent la propriété non immédiate d'être dans $\mathbb{Z}[X]$ et d'être irréductibles dans $\mathbb{Q}[X]$! On conclut cette partie par une utilisation des polynômes cyclotomiques au travers de trois applications très importantes en algèbre commutative et en arithmétique : le théorème de Wedderburn, le théorème de Dirichlet faible ainsi que le théorème de Kronecker.
On termine cette leçon avec une dernière partie consacrée à des applications des nombres complexes de module 1. Tout d'abord, on définit un argument d'un nombre complexe que l'on peut rendre unique au moyen d'une petite restriction. De manière plus générale, cette notion d'"angle" peut se retrouver dans un espace euclidien de dimension 2 quelconque au travers d'une matrice de rotation. On peut même aller un peu plus loin en parlant de mesure d'un angle orienté. Ensuite, on donne une autre application en rapport avec la géométrie avec les nombres constructibles à la règle non graduée et au compas. On commence par définir ce qu'est un nombre constructible avant de donner une caractérisation de la constructibilité d'un nombre complexe. On conclut avec le théorème de Gauss-Wantzel qui donne une condition nécessaire

et suffisante pour construire un n-gone régulier. Enfin, on termine cette partie par des applications aux matrices avec tout d'abord les matrices unitaires sur un espace hermitien où l'on a deux propriétés remarquables : un nouvel isomorphisme faisant intervenir $\mathbb{U}$, ainsi que la diagonalisation de toute matrice unitaire avec ses valeurs propres dans $\mathbb{U}$ puis les matrices circulantes. et enfin quelques résultats généraux sur le groupe linéaire.

Plan général

Cours détaillé

I L'ensemble des nombres complexes de module 1

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

Définition 1 : Module d'un nombre complexe [Deschamps, p.154] :
On considère $z \in \mathbb{C}$.
On appelle **module de** z le réel positif $|z| = \sqrt{(\mathrm{Re}(z))^2 + (\mathrm{Im}(z))^2}$.

Définition 2 : L'ensemble $\mathbb{U}$ [Deschamps, p.156] :
On définit **l'ensemble** $\mathbb{U}$ comme étant l'ensemble des nombres complexes dont le module est égal à 1.

Exemple 3 :
On a $\{1; -1; i; -i\} \subseteq \mathbb{U}$.

Proposition 4 : [Deschamps, p.157]
L'ensemble $\mathbb{U}$ muni de la multiplication complexe est un groupe.

I.2 La fonction exponentielle complexe

Définition 5 : Fonction exponentielle complexe [Tauvel, p.43] :
On définit la fonction **exponentielle complexe** par :

$$\exp : \left| \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \sum_{n=0}^{+\infty} \frac{z^n}{n!} \end{array} \right.$$

Théorème 6 : [Rombaldi (1), p.267]
L'application $\varphi : t \longmapsto e^{it}$ réalise un morphisme de groupes continu de $(\mathbb{R}, +)$ dans $(\mathbb{U}, \times)$ qui est surjectif et de noyau $a\mathbb{Z}$ avec $a \in \mathbb{R}$.

Définition 7 : Nombre π [Rombaldi (1), p.268] :
On appelle **nombre** π le réel $\frac{a}{2}$.

Corollaire 8 :
On a l'isomorphisme : $\mathbb{U} \cong \mathbb{R}/2\pi\mathbb{Z}$.

Théorème 9 : [Rombaldi (1), p.271]
La fonction exponentielle complexe induit un morphisme de groupes de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$ continu qui est surjectif et de noyau $2i\pi\mathbb{Z}$.

Proposition 10 :
$\mathbb{U}$ est un ensemble compact et connexe de $\mathbb{C}$ mais qui n'est homéomorphe à aucune partie de $\mathbb{R}$.

I.3 Les fonctions cos et sin complexes

Définition 11 : Fonctions cosinus et sinus complexes [Tauvel, p.45] :
On appelle **fonction cosinus complexe** et **fonction sinus complexe** les fonctions respectivement définies par :

$$\cos : \left| \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \frac{1}{2}\left(e^{iz}+e^{-iz}\right) \end{array} \right. \quad \text{et} \quad \sin : \left| \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \frac{1}{2i}\left(e^{iz}-e^{-iz}\right) \end{array} \right.$$

Remarque 12 :
Les formules donnant la définition du cosinus et sinus complexes ci-dessus sont appelées les **formules d'Euler**.

Proposition 13 : Formule de De Moivre [Deschamps, p.158] :
Pour tous $\theta \in \mathbb{R}$ et tous $z \in \mathbb{C}$, on a :

$$(\cos(\theta)+i\sin(\theta))^n = \cos(n\theta)+i\sin(n\theta)$$

Exemple 14 : [Deschamps, p.160]

$$\cos^5(\theta) = \frac{1}{32}\left(\cos(5\theta)+5\cos(3\theta)+10\cos(\theta)\right)$$

Proposition 15 : [Deschamps, p.159]
Soient $n \in \mathbb{N}$ et $\theta \in \mathbb{R}$.
On a :

$$\sin(n\theta) = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2k+1} \cos^{n-(2k+1)}(\theta)\sin^{2k+1}(\theta)$$

$$\cos(n\theta) = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} \cos^{n-2k}(\theta)\sin^{2k}(\theta)$$

II Racines de l'unité et polynômes cyclotomiques

II.1 Le groupe $\mathbb{U}_n$

Dans toute cette sous-partie, on considère $n \in \mathbb{N}^*$.

Définition 16 : L'ensemble $\mathbb{U}_n$ [Deschamps, p.168] :
On définit **l'ensemble** $\mathbb{U}_n$ comme étant l'ensemble des nombres complexes solutions de l'équation $Z^n = 1$.

Exemple 17 :
On a $\{1;-1;i;-i\} = \mathbb{U}_4$.

Proposition 18 : [Deschamps, p.168]
L'ensemble $\mathbb{U}_n$ muni de la multiplication complexe est un groupe de cardinal égal à n et dont les éléments sont les $e^{\frac{2ik\pi}{n}}$ avec $k \in [\![0; n-1]\!]$.

Définition 19 : Racine primitive n-ième de l'unité [Perrin, p.80] :
On appelle **racine primitive n-ième de l'unité** tout complexe ζ tel que $\zeta^n = 1$ et pour tout $d \in [\![1; n-1]\!]$, $\zeta^d \neq 1$

Remarque 20 : [Perrin, p.80]
Les racines primitives n-ièmes de l'unité sont en fait les $e^{\frac{2ik\pi}{n}}$ avec $k \in [\![0; n-1]\!]$ et k premier avec n.

Proposition 21 : [Perrin, p.80]
Soit ζ une racine primitive n-ième de l'unité.
Le groupe $\mathbb{U}_n$ est un groupe cyclique engendré par ζ et donc $\mathbb{U}_n \cong \mathbb{Z}/n\mathbb{Z}$.

Proposition 22 : [Perrin, p.80]
L'ensemble des racines primitives n-ièmes de l'unité (noté μ_n^*) est un groupe pour la multiplication au sens complexe et de cardinal $\varphi(n)$.

Exemple 23 :
$\mu_1^* = \{1\}$, $\mu_2^* = \{-1\}$, $\mu_3^* = \{-j; j\}$ et $\mu_4^* = \{-i; i\}$.

Proposition 24 : [Perrin, p.80]
Par unicité de l'ordre d'un élément, on a : $\mathbb{U}_n = \bigsqcup_{d|n} \mu_d^*$.
On a alors en particulier : $n = \sum_{d|n} \varphi(d)$.

II.2 Les polynômes cyclotomiques

Dans toute cette sous-partie, on considère $n \in \mathbb{N}^*$.

Définition 25 : n-ième polynôme cyclotomique [Perrin, p.80] :
On appelle **n-ième polynôme cyclotomique** le polynôme :

$$\Phi_n(X) = \prod_{\zeta \in \mu_n^*} (X - \zeta)$$

Remarque 26 : [Perrin, p.80]
$\Phi_n(X)$ est un polynôme unitaire et de degré $\varphi(n)$.

Exemple 27 : [Perrin, p.81]
$\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$ et $\Phi_4(X) = X^2 + 1$.

Proposition 28 : [Perrin, p.80]
On a la formule :

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Remarque 29 : [Perrin, p.81]
On retrouve la formule établie à la proposition 24 en considérant les degrés dans la proposition précédente.

Remarque 30 : [Perrin, p.81]
La formule de la proposition 28 permet de calculer les polynômes cyclotomiques par récurrence en écrivant :

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d(X)}$$

Proposition 31 : [Perrin, p.81]
On a $\Phi_n(X) \in \mathbb{Z}[X]$.

Développement 1 : [cf. PERRIN]

Théorème 32 : [Perrin, p.82]
Le polynôme $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$.

Corollaire 33 : [Perrin, p.83]
Si ζ est une racine primitive n-ième de l'unité dans un corps commutatif de caractéristique nulle, alors son polynôme minimal sur $\mathbb{Q}$ est $\Phi_{n,\mathbb{Q}}$ et $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

II.3 Applications en algèbre commutative et en arithmétique

Théorème 34 : Théorème de Wedderburn [Perrin, p.82] :
Tout corps fini est commutatif.

Théorème 35 : Théorème de Dirichlet faible [Gourdon, p.99] :
Soit $n \in \mathbb{N}$.
Il existe une infinité de nombres premiers $p \in \mathcal{P}$ tels que $p \equiv 1\ [n]$.

Théorème 36 : Théorème de Kronecker [Francinou (1), p.257] :
Soit $P \in \mathbb{Z}[X]$ unitaire dont les racines complexes sont de module inférieur ou égal à 1.
Si $P(0) \neq 0$, alors toutes les racines de P sont des racines de l'unité.

Corollaire 37 :
Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible.
Si toutes les racines complexes sont de module inférieur ou égal à 1, alors $P(X) = X$ ou $P(X) = \Phi_k(X)$ pour un certain $k \in \mathbb{N}^*$.

III Applications

III.1 Utilisation en géométrie

Définition 38 : Argument d'un nombre complexe [Deschamps, p.162] :
On considère un nombre complexe non nul z.
On appelle **argument de** z un réel θ tel que $\frac{z}{|z|} = e^{i\theta} = \cos(\theta) + i\sin(\theta)$ et on le note $\arg(z)$.

Remarque 39 : [Deschamps, p.162]
Le réel θ n'est unique que modulo 2π.

Définition 40 : Argument principal [Deschamps, p.162] :
On appelle **argument principal de** z l'unique entier $\theta \in [-\pi;\pi[$ tel que $\frac{z}{|z|} = e^{i\theta}$.

Proposition 41 :
Par l'écriture sous forme exponentielle d'un nombre complexe, on a l'isomorphisme suivant : $\mathbb{C}^* \cong \mathbb{R}_+^* \times \mathbb{U}$.

Dans toute la suite de cette sous-partie, on considère E un espace euclidien orienté de dimension 2.

Proposition 42 : [Deschamps, p.1326]
Les matrices orthogonales de $\mathcal{M}_2(\mathbb{R})$ sont les matrices de la forme :

$$R(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \text{ ou } S(\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$$

De plus, le groupe $\mathrm{SO}_2(\mathbb{R})$ est l'ensemble des matrices $R(\theta)$ pour $\theta \in \mathbb{R}$.

Proposition 43 : [Deschamps, p.1326]
$*$ Pour tout $(\theta, \theta') \in \mathbb{R}^2$, $R(\theta + \theta') = R(\theta)R(\theta')$.
$*$ Le groupe $(\mathrm{SO}_2(\mathbb{R}), \times)$ est commutatif.

Proposition 44 : [Deschamps, p.1326]
Soit r une isométrie positive du plan.
Il existe un unique réel θ modulo 2π tel que dans toute base orthonormale directe de E la matrice de r soit égale à :

$$R(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

Définition 45 : Rotation [Deschamps, p.1326] :
On considère r une isométrie positive du plan et $R(\theta)$ sa matrice dans une base orthonormée directe.
On dit que r est la **rotation d'angle** θ.

Définition 46 : Mesure d'un angle [Deschamps, p.1326] :
On considère une rotation r.
On appelle **mesure de l'angle de la rotation** r l'unique réel θ modulo 2π tel que $r = R(\theta)$.

Corollaire 47 : [Deschamps, p.1326]
Les isométries positives du plan sont les rotations.

Lemme 48 : [Deschamps, p.1327]
Soient $\overrightarrow{u}$ et $\overrightarrow{v}$ deux vecteurs non nuls de E de même norme.
Il existe une unique rotation r telle que $r(\overrightarrow{u}) = \overrightarrow{v}$.

Définition 49 : Mesure d'un angle orienté [Deschamps, p.1327] :
On considère $\overrightarrow{u}$ et $\overrightarrow{v}$ deux vecteurs non nuls.
On appelle **mesure de l'angle orienté de vecteurs** $(\widehat{\overrightarrow{u};\overrightarrow{v}})$ une mesure θ de l'angle de l'unique rotation qui transforme $\frac{\overrightarrow{u}}{\|v\|}$ en $\frac{\overrightarrow{v}}{\|v\|}$ et l'on note :

$$(\widehat{\overrightarrow{u};\overrightarrow{v}}) \equiv \theta \ [2\pi]$$

Proposition 50 : Relation de Chasles [Deschamps, p.1327] :
Si $\overrightarrow{u}$, $\overrightarrow{v}$ et $\overrightarrow{w}$ sont trois vecteurs non nuls, on a alors :

$$(\widehat{\overrightarrow{u};\overrightarrow{w}}) \equiv (\widehat{\overrightarrow{u};\overrightarrow{v}}) + (\widehat{\overrightarrow{v};\overrightarrow{w}}) \ [2\pi]$$

Remarque 51 : [Deschamps, p.1327]
On a $(\widehat{\overrightarrow{u};\overrightarrow{u}}) \equiv 0 \ [2\pi]$ et $(\widehat{\overrightarrow{u};-\overrightarrow{u}}) \equiv \pi \ [2\pi]$.

Grâce à la relation de Chasles, on en déduit :

$(\widehat{\overrightarrow{u};\overrightarrow{v}}) \equiv -(\widehat{\overrightarrow{v};\overrightarrow{u}}) \ [2\pi]$, $(\widehat{-\overrightarrow{u};\overrightarrow{v}}) \equiv (\widehat{\overrightarrow{v};\overrightarrow{u}}) + \pi \ [2\pi]$ et $(\widehat{-\overrightarrow{u};-\overrightarrow{v}}) \equiv (\widehat{\overrightarrow{v};\overrightarrow{u}}) \ [2\pi]$

III.2 Nombres constructibles à la règle non graduée et au compas

Ici, chaque construction commencera de 0 et 1. Durant la construction, nous utiliserons seulement les règles suivantes :
$C1(\alpha,\beta)$: De $\alpha \neq \beta$, on peut tracer la ligne l qui passe par α et β.
$C2(\gamma,\alpha,\beta)$: De $\alpha \neq \beta$ et γ, on peut dessiner le cercle C de centre γ dont le rayon est la distance entre α et β.
$P1$: Le(s) point(s) d'intersection de deux lignes distinctes ℓ_1 et ℓ_2 construites comme ci-dessus.
$P2$: Le(s) point(s) d'intersection d'une ligne ℓ et d'un cercle C construits comme ci-dessus.
$P3$: Le(s) point(s) d'intersection de deux cercles distincts C_1 et C_2 construits comme ci-dessus.

Définition 52 : Nombre constructible [Berhuy, p.762] :
Un nombre complexe α est un **nombre constructible** lorsqu'il existe une suite finie de constructions à la règle non graduée et au compas utilisant $C1$, $C2$, $P1$, $P2$ et $P3$ qui commence avec 0 et 1 et fini avec α.

Exemple 53 : [Berhuy, p.763]
Il est possible de construire une médiatrice d'un segment, le milieu d'un segment, une bissectrice d'un angle, la symétrie centrale et axiale d'un point, une perpendiculaire et une parallèle à une droite donnée.

Dans toute la suite de cette sous-partie, on note $\mathcal{C} := \{\alpha \in \mathbb{C} \text{ tq } \alpha \text{ est constructible}\}$.

Théorème 54 : [Berhuy, p.764 + 765]
L'ensemble $\mathcal{C}$ est un sous-corps de $\mathbb{C}$.
De plus, on a :
$*$ $\alpha := a + ib \in \mathcal{C}$ si, et seulement si, $a, b \in \mathcal{C} \cap \mathbb{R}$.
$*$ Si $\alpha \in \mathcal{C}$, alors chaque racine carrée de α appartient à $\mathcal{C}$.

Théorème 55 : [Berhuy, p.775]
Soit $\alpha \in \mathbb{C}$.
$\alpha \in \mathcal{C}$ si, et seulement si, il existe des sous-corps de $\mathbb{C}$ tels que :

$$\mathbb{Q} := F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}, \forall i \in [\![0; n-1]\!],\ [F_{i+1} : F_i] = 2 \text{ et } \alpha \in F_n$$

Corollaire 56 : [Berhuy, p.776]
Si $\alpha \in \mathcal{C}$, alors il existe $m \in \mathbb{N}$ tel que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$.

Remarque 57 :
$*$ Le corollaire précédent implique que tout $\alpha \in \mathcal{C}$ est algébrique sur $\mathbb{Q}$ et que le degré de son polynôme minimal est une puissance de 2. On a alors $\mathbb{Q} \subsetneq \mathcal{C} \subsetneq \mathcal{A}$ avec $\mathcal{A}$ l'ensemble des nombres algébriques sur $\mathbb{Q}$.
$*$ La contraposée du corollaire précédent est très utile car elle permet de voir que pour qu'un nombre n'est pas constructible, il suffit de déterminer le degré de son polynôme minimal sur $\mathbb{Q}$.

Théorème 58 : [Berhuy, p.929]
Soient $\alpha \in \mathbb{C}$ algébrique sur $\mathbb{Q}$ et $\mathbb{L}$ le corps de décomposition du polynôme minimal de α sur $\mathbb{Q}$.
α est constructible si, et seulement si, $[\mathbb{L} : \mathbb{Q}]$ est une puissance de 2.

Corollaire 59 : [Berhuy, p.787 - 788]
La trisection de l'angle, la duplication du cube et la quadrature du cercle sont impossibles à la règle non graduée et au compas.

Théorème 60 : Théorème de Gauss-Wantzel [Berhuy, p.795] :
Soit n un entier naturel supérieur ou égal à 2.
Le n-gone régulier est constructible à la règle non graduée et au compas si, et seulement si, $n := 2^s \prod_{i=1}^{r} p_i$ (avec $s, r \in \mathbb{N}$ et $p_1, ..., p_r$ qui sont r nombres de Fermat distincts).

Exemple 61 : [Berhuy, p.805]
Il est possible de construire le pentagone régulier avec la règle non graduée et le compas.

Remarque 62 :
Certaines constructions à la règle non graduée et au compas ne sont donc pas possibles (construction de l'heptagone régulier, trisection de l'angle, etc.) Mais que se passe-t-il si l'on modifie les règles du jeu (théorème de Mohr-Mascheroni, théorème de Poncelet-Steiner, règle avec deux graduations, allumettes, origamis, etc.) ?

III.3 Applications aux matrices

Dans toute la suite de cette sous-partie, on considère un espace hermitien E de dimension strictement positive notée n.

Théorème 63 : [Ramis, p.265]
L'application det : $\mathbb{U}_n(\mathbb{C}) \longrightarrow \mathbb{U}$ est un morphisme de groupe surjectif de noyau le groupe spécial unitaire $\mathbb{SU}_n(\mathbb{C})$.
On a en particulier : $\mathbb{U}_n(\mathbb{C})/\mathbb{SU}_n(\mathbb{C}) \cong \mathbb{U}$.

Proposition 64 : [Berhuy, p.110]
Toute matrice $M \in \mathbb{U}_n(\mathbb{C})$ est diagonalisable en une base orthonormée formée de vecteurs propres et ses valeurs propres sont dans $\mathbb{U}$.

Définition 65 : Matrice circulante [Gourdon, p.190] :
On appelle **matrice circulante** toute matrice carrée telle que l'on passe d'une ligne à la suivante par décalage à droite des coefficients de façon circulaire. Une matrice circulante C de taille n s'écrit donc :

$$C = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}$$

où $a_1, a_2, ..., a_n$ sont des nombres complexes.

Développement 2 : [cf. GOURDON + CALDERO]

Proposition 66 : [Gourdon, p.153]
Si l'on note $P = \sum_{k=0}^{n-1} a_k X^k$ et $\omega = e^{\frac{2i\pi}{n}}$, alors $\det(C) = \prod_{i=0}^{n-1} P\left(\omega^i\right)$.

Proposition 67 : [Caldero, p.45]
Soient P un polygone du plan complexe dont les sommets sont notés $z_1, ..., z_n$ et $a, b \in]0;1[$ tels que $a + b = 1$.
Si l'on définit par récurrence la suite $(P_k)_{k\in\mathbb{N}}$ par $P_0 = P$ et $P_{k+1} = \mathcal{B}_{a,b}(P)$ le polygone $(z'_i)_{i\in[\![1;n]\!]}$ avec $z'_i = az_i + bz_{i+1}$, alors la suite $(P_k)_{k\in\mathbb{N}}$ converge vers l'isobarycentre de P.

Théorème 68 : Théorème de Burnside [Francinou (2), p.353] :
Soit G est sous-groupe de $\mathrm{GL}_n(\mathbb{C})$.
Si G est d'exposant fini, alors G est fini.

Théorème 69 : [Francinou (2), p.377]
Soit p un nombre premier impair.
Si G est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$, alors la restriction à G de la réduction modulo p de $\mathrm{GL}_n(\mathbb{Z})$ dans $\mathrm{GL}_n(\mathbb{F}_p)$ est injective.

Corollaire 70 : [Francinou (2), p.377]
Si G est un sous-groupe fini de $\mathrm{GL}_n(\mathbb{Z})$, alors on a la majoration suivante : $\mathrm{Card}(G) \leq \mathrm{Card}(\mathrm{GL}_n(\mathbb{F}_3)) = \prod_{k=0}^{n-1}\left(3^n - 3^k\right) \leq 3^{n^2}$.

Remarques sur la leçon

— On peut aussi parler du logarithme complexe, de la théorie des caractère et de la transformée de Fourier discrète (cependant cela doit rester minime) !

Liste des développements possibles

— Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}[X]$.

— Déterminant circulant et suite de polygones.

Bibliographie

— Claude Deschamps, *Tout-en-un MPSI*.

— Patrice Tauvel, *Analyse complexe pour la licence 3*.

— Jean-Étienne Rombaldi, *Mathématiques pour l'agrégation, Analyse et Probabilités*.

— Daniel Perrin, *Cours d'algèbre*.

— Xavier Gourdon, *Les maths en tête, Algèbre et Probabilités*.

— Serge Francinou, *Exercices de mathématiques, Oraux X-ENS, Algèbre 1*.

— Grégory Berhuy, *Algèbre : le grand combat*.

— Jean-Pierre Ramis, *Mathématiques, Tout-en-un pour la licence 2*.

— Philippe Caldero, *Carnet de voyage en Algébrie*.

— Serge Francinou, *Exercices de mathématiques, Oraux X-ENS, Algèbre 2*.