Leçon 102 : compléments de cours et exercices

1 Le groupe des nombres complexes de module 1

Notation habituelle :

$$\mathbb{U} := \{z \in \mathbb{C} \,|\, |z| = 1\}.$$

C'est un sous-groupe de $\mathbb{C}^*$ et pour tout $z \in \mathbb{C}^*$, $1/z = \overline{z}$ (souvent utilisé !).

• L'exponentielle est surjective de $i\mathbb{R}$ dans $\mathbb{U}$, de noyau $2i\pi\mathbb{Z}$.

$\longrightarrow$ Cela se ramène à la surjectivité de $\cos, \sin : \mathbb{R} \to [-1, 1]$ et à la relation $\cos^2 + \sin^2 = 1$.

Exercice 1.1. Démontrer ceci à partir de la définition de l'exponentielle comme série complexe (c'est un développement).

Exercice 1.2. À partir de la formule $\exp(i\theta) = \cos(\theta) + i\sin(\theta)$ et du fait que exp est un morphisme de groupes, savoir retrouver les formules classiques de la trigonométrie (cosinus et sinus d'une somme, produit de cosinus, linéarisation, $\cos(n\theta)$ en fonction de $\cos(\theta)$ et $\sin(\theta)$, etc...).

$\longrightarrow$ Représentation du cercle unité et lien avec la trigonométrie. Points remarquables (angles $0, \pi/6, \pi/4, \pi/3, \pi/2, \pi$ et autres).

Exercice 1.3. Retrouver le calcul du périmètre du cercle unité par calcul intégral.

$\longrightarrow$ Isomorphisme avec $\mathrm{SO}_2(\mathbb{R})$ à savoir démontrer, lien avec la notion d'angle orienté de vecteurs.

Exercice 1.4. Interpréter cet isomorphisme comme provenant d'une action simplement transitive de $\mathrm{SO}_2(\mathbb{R})$ sur $\mathbb{U}$.

• Homéomorphisme (et morphisme de groupes) $\mathbb{R}/\mathbb{Z} \cong \mathbb{R}/2\pi\mathbb{Z} \cong \mathbb{U}$.

Exercice 1.5. En déduire les morphismes de groupes continus de $\mathbb{U}$ dans lui-même à partir de ceux de $\mathbb{R}$ dans lui-même.

$\longrightarrow$ Conséquences topologiques : connexité (par arcs), compacité, connexité.

Exercice 1.6. Est-ce qu'en tant qu'espace topologique, $\mathbb{U}$ est homoéomorphe à $\mathbb{R}$? À un intervalle compact ? Est-ce qu'on peut plonger $\mathbb{U}$ de manière continue dans $\mathbb{R}$ (ce qui reviendrait à *relever l'argument de manière continue*) ?

2 Racines de l'unité

• Les racines n-ièmes de l'unité dans $\mathbb{C}$ sont exactement les $\exp(2ik\pi/n)$ avec $k \in \{0, \cdots, n-1\}$. Elles forment un groupe isomorphe à $(\mathbb{Z}/n\mathbb{Z})$, souvent noté μ_n.

Exercice 2.1. Interlude sur les $\mathbb{Z}/n\mathbb{Z}$ (c'est-à-dire les groupes cycliques, tout est à savoir bien faire :

— Montrer que pour tout entier $k \in \mathbb{Z}$, la classe de k modulo n, notée $\overline{k}$, engendre $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si k est premier à n. En déduire qu'il y a $\varphi(n)$ générateurs avec φ l'indicatrice d'Euler.

— Montrer que pour tout diviseur d positif de n, il y a exactement un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d, qui est l'ensemble des $n/d\overline{k}$ avec $k \in \mathbb{Z}$, et qu'il est cyclique d'ordre d. En déduire que tout sous-groupe d'un groupe cyclique est cyclique.

— En déduire que pour tout $k \in \mathbb{Z}$, $\overline{k}$ engendre l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre $n/\operatorname{pgcd}(n,k)$.

— En comptant les générateurs par ordre, montrer que $\sum_{d|n} \varphi(d) = n$ où d parcourt les diviseurs positifs de n.

$\longrightarrow$ Expliciter les $\varphi(n)$ racines n-ièmes primitives de l'unité.

Exercice 2.2. Montrer que $\bigcup_{n\geq 1} \mu_n$ est un sous-groupe de $\mathbb{U}$ isomorphe à $\mathbb{Q}/\mathbb{Z}$. Ce groupe abélien est-il de type fini ?

Exercice 2.3. Montrer que les seuls sous-groupes fermés de $\mathbb{R}$ sont les $\mathbb{Z}\alpha$, $\alpha \in \mathbb{R}$. En déduire que les seuls groupes non denses de $\mathbb{U}$ sont les μ_n.

• Manipulation de sommes de racines de l'unité

Exercice 2.4. Montrer que pour ζ_n une racine n-ième primitive de l'unité et $a \in \mathbb{Z}$,

$$\sum_{b=0}^{n-1} \zeta_n^{ab} = \begin{cases} n & \text{si } a \equiv 0 \bmod n. \\ 0 & \text{sinon.} \end{cases}$$

En déduire la formule d'inversion de la transformée de Fourier discrète (implicite dans beaucoup de calculs sur les racines de l'unité).

• Le n-ième polynôme cyclotomique sur $\mathbb{C}$ est défini par

$$\Phi_n(X) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} (X - e^{2ik\pi/n}),$$

c'est-à-dire le polynôme dont les racines simples sont les racines n-ièmes primitives de l'unité.

$\longrightarrow$ Formule-clé : pour tout n, $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Exercice 2.5. En déduire par récurrence que pour tout entier $n \geq 1$, $\Phi_n(X)$ est à coefficients entiers.

Donner le développement de $\Phi_n(x)$ pour $n = p$ avec p premier puis pour $n = p^\alpha$.

Calculer les 8 premiers polynômes cyclotomiques.

Théorème 2.6. *Les polynômes cyclotomiques sont tous irréductibles dans* $\mathbb{Z}[X]$.

Exercice 2.7. Grâce à une astuce et au critère d'Eisenstein, démontrer rapidement ce résultat pour Φ_p avec p premier.

Donner un exemple de polynôme cyclotomique qui réduit modulo p n'est pas irréductible dans $\mathbb{F}_p[X]$.

Exercice 2.8. (s'approche de la théorie de Galois) Montrer que le groupe des automorphismes de corps de $\mathbb{Q}(\zeta_n)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$.

Développements possibles : sommes de Gauss et loi de réciprocité quadratique, théorème de Kronecker.

3 Groupe diédral

Par définition, le groupe diédral (noté D_{2n}) est le groupe des isométries du polygone régulier à n côtés inscrit dans le cercle unité (faire un dessin).

Proposition 3.1. *Notons* $\omega = e^{2i\pi/n}$. *Le groupe diédral est constitué des isométries définies par*

$$z \mapsto \omega^k \text{ ou } z \mapsto \omega^k \overline{z}$$

avec $k \in \{0, \cdots, n-1\}$, *ce qui définit bien* $2n$ *isométries exactement, dont* n *directes.*

Exercice 3.2. Montrer que le groupe diédral est engendré par la rotation $r : z \mapsto \omega z$ et la symétrie $s : z \mapsto \overline{z}$, et que pour toute rotaton r^k avec $k \in \mathbb{Z}$, $sr^k s^{-1} = r^{-k}$.

En déduire que les rotations en forment un sous-groupe cyclique distingué d'ordre n, le reste étant formé par les symétries orthogonales.

En déduire (pour ceux qui connaissent) que le groupe diédral est isomorphe au produit semi-direct de $\mathbb{Z}/n\mathbb{Z}$ par $\mathbb{Z}/n\mathbb{Z}$.

Exercice 3.3. Calculer le centre et le groupe dérivé du groupe diédral. Calculer ses classes de conjugaison (il y a une distinction entre n pair et n impair). Étudier dans quels cas il peut être isomorphe à un groupe de permutation $\mathfrak{S}_k$.

Autres considérations géométriques : polygones constructibles à la règle et au compas, théorème de Wantzel.

4 Applications en algèbre linéaire, dualité et théorie des représentations

• Pour tout endomorphisme $u \in \mathrm{GL}(E)$ avec E un espace vectoriel réel ou complexe de dimension finie, si $u^n = \mathrm{Id}_E$, ses valeurs propres sont des racines n-ièmes de l'unité.

Exercice 4.1. Pour $M \in \mathrm{SL}_2(\mathbb{Z})$ telle que $M^k = I_2$, montrer que $k = 1, 2, 3, 4$ ou 6.

(pour les habitués des réseaux) En déduire que les seuls réseaux de $\mathbb{R}^2$ avec un groupe d'isométries directes non réduit à $\pm I_2$ sont les réseaux carrés ou hexagonaux.

$\longrightarrow$ Pour toute représentation $\rho : G \to \mathrm{GL}(V)$ d'un groupe G fini d'ordre n, le caractère associé χ_V est une somme de racines n-ièmes de l'unité pour tout n, en particulier un entier algébrique.

Exercice 4.2. Avec les mêmes notations, démontrer que pour tout $g \in G$, $\chi_V(g) = \dim V$ si et seulement si $\rho(g) = \mathrm{Id}_V$.

En montrant que tout groupe fini admet une représentation fidèle (pas forcément irréductible) puis que tout sous-groupe distingué de G est le noyau d'une représentation de V, en déduire qu'on peut voir tout sous-groupe distingué de G grâce à la table des caractères.

Appliquer ceci à $\mathfrak{A}_4$ et retrouver le groupe de Klein.

• Pour G un groupe fini, on note $\widehat{G}$ le groupe multiplicatif des caractères (linéaires) $G \to \mathbb{C}^*$.

Exercice 4.3. Tout caractère linéaire $G \to \mathbb{C}^*$ se factorise par $G/D(G)$ donc on peut se ramener à G abélien.

Démontrer que $(\mathbb{Z}/n\mathbb{Z})^* \cong \mu_n \cong \mathbb{Z}/n\mathbb{Z}$, le premier isomorphisme étant même canonique.

Démontrer que pour deux groupes finis G et G', $\widehat{G \times G'} \cong \widehat{G} \times \widehat{G'}$. Si on admet le théorème de structure des groupes abéliens finis, en déduire que pour tout G abélien fini, $\widehat{G} \cong G$ (non canoniquement) et $\widehat{\widehat{G}} \cong G$ (canoniquement).

$\longrightarrow$ Table des caractères de $\mathbb{Z}/n\mathbb{Z}$.

Développements possibles : table des caractères de D_{2n}, déterminant des matrices circulantes.