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

I. Le groupe $\mathbb{U}$

1) Définition, exponentielle complexe

Déf. (1): On note $\mathbb{U}$ le noyau du morphisme de groupes $(\mathbb{C}^*, \times) \to (\mathbb{R}^{+*}, \times)$, $z \mapsto |z|$. Si $\mathbb{S}_1 = \{z \in \mathbb{C} / |z| = 1\}$, alors $\mathbb{U} = (\mathbb{S}_1, \times)$

Rq (2): Géométriquement, $\mathbb{S}_1$ est le cercle unité du plan complexe.

Th. (3): $f : \mathbb{R}^{+*} \times \mathbb{U} \to \mathbb{C}^*$, $(r, u) \mapsto ru$ est un morphisme de groupes multiplicatifs.

Déf. (4): On définit l'application exponentielle sur $\mathbb{C}$ par :

$\exp : \mathbb{C} \to \mathbb{C}$, $z \mapsto \sum_{n=0}^{+\infty} \frac{z^n}{n!}$. On notera $e^z = \exp(z)$ pour $z \in \mathbb{C}$

Th. (5): (admis) $\varepsilon : (\mathbb{R}, +) \to \mathbb{U}$, $x \mapsto e^{ix}$ est un morphisme de groupes surjectif et continu.

On a alors $\ker \varepsilon = 2\pi\mathbb{Z}$ et $\mathbb{U} \simeq \mathbb{R}/2\pi\mathbb{Z}$

Déf. (6): On définit $\cos : \mathbb{R} \to \mathbb{R}$, $x \mapsto \mathrm{Re}(e^{ix})$ et $\sin : \mathbb{R} \to \mathbb{R}$, $x \mapsto \mathrm{Im}(e^{ix})$

Prop. (7): 1) $\forall n \in \mathbb{Z}$, $(\cos x + i \sin x)^n = \cos(nx) + i \sin(nx)$ (Moivre)

2) $\cos x = \frac{e^{ix} + e^{-ix}}{2}$ et $\sin x = \frac{e^{ix} - e^{-ix}}{2i}$

3) $\cos^2 x + \sin^2 x = 1$

Appli. (8): $\forall \theta \in \mathbb{R} \setminus 2\pi\mathbb{Z}$, $\sum_{k=0}^{n} e^{ik\theta} = e^{in\frac{\theta}{2}} \times \frac{\sin\frac{(n+1)\theta}{2}}{\sin\frac{\theta}{2}}$

2) Argument d'un nombre complexe

Déf. (9): Soit $z \in \mathbb{C}^*$. On dit que $\theta \in \mathbb{R}$ est un argument de z si $e^{i\theta} = \frac{z}{|z|}$.
On note $\arg(z)$ l'ensemble des arguments de z.

Ex. (10): $0, -2\pi, \dots$ sont des arguments de $z = 3$

$\frac{\pi}{2}, \frac{5\pi}{2}, \dots$ sont des arguments de $z = i$.

Th. (11): Soit $z \in \mathbb{C}^*$. Alors $\arg(z) \neq \emptyset$ et pour tout $\theta_0 \in \arg(z)$, on a $\arg(z) = \{\theta_0 + 2k\pi, k \in \mathbb{Z}\} = \theta_0 + 2\pi\mathbb{Z}$.

Déf. (12): On appelle argument principal de $z \in \mathbb{C}^*$ l'unique élément de $\arg(z) \cap]-\pi, \pi]$. On le note $\mathrm{Arg}(z)$.

Appli. (13): Géométrie plane (VOIR ANNEXE)

L'angle d'un vecteur $z \in \mathbb{C}^*$ est l'unique $\theta \in [0, 2\pi[$ tel que $\frac{z}{|z|} = e^{i\theta}$

Appli. (14):

Soit $z \in \mathbb{C}^*$. Une forme trigonométrique de z est un couple $(r, \theta) \in \mathbb{R}_+^* \times \mathbb{R}$ tel que $z = re^{i\theta}$.

Exercice (15): (VOIR ANNEXE)

Soit $z = \sqrt{2} + i\sqrt{2}$. Placer z, puis z^3 dans le plan complexe.

II. Racines n-ièmes de l'unité $n \in \mathbb{N}^*$

1) Définition, premières propriétés

Prop. (16): $f : \mathbb{U} \to \mathbb{U}$, $z \mapsto z^n$ est un morphisme de groupes surjectif.

Déf. (17): $\mu_n = \ker f = \{z \in \mathbb{U} / z^n = 1\}$ est appelé groupe des racines n-ièmes de l'unité dans $\mathbb{C}$.

Prop. (18): μ_n est un sous-groupe cyclique de $\mathbb{U}$ de cardinal n.
On a donc $\mu_n \simeq (\mathbb{Z}/n\mathbb{Z}, +)$ et ses générateurs sont les éléments de l'ensemble $\mu_n^* = \{\zeta_k = \exp(\frac{2i\pi k}{n}), k \in \{0 \dots n-1\} \text{ et } k \wedge n = 1\}$.

Déf. / Prop. (19): Un élément de μ_n^* est appelé racine primitive n-ième de l'unité dans $\mathbb{C}$. On a de plus $|\mu_n^*| = \varphi(n)$, où φ est l'indicatrice d'Euler.

Ex. (20): $\mu_1 = \{1\}$ $\mu_1^* = \{1\}$; $\mu_2 = \{1, -1\}$ $\mu_2^* = \{-1\}$;
$\mu_3 = \{1, j, j^2\}$ $\mu_3^* = \{j, j^2\}$ où $j = \exp(\frac{2i\pi}{3})$
Si p est premier, $\mu_p^* = \mu_p \setminus \{1\}$.

Th. (21): L'unique sous-groupe fini de $(\mathbb{C}^*, \times)$ de cardinal n est μ_n

Rq (22): (VOIR ANNEXE)

Notons $\mu_n = \{\zeta_k = \exp(2i\pi\frac{k}{n}), k \in \{0 \dots n-1\}\}$. Dans le plan complexe, les ζ_k forment un polygone régulier à n côtés inscrit dans $\mathbb{S}_1$. La longueur d'un côté est $2\sin(\frac{\pi}{n})$ et l'angle formé entre deux côtés consécutifs est $(n-2)\frac{\pi}{n}$.

[AF]

2) Première application

Lemme (25) : Tout sous-groupe de $(\mathbb{R}, +)$ est :
- soit de la forme $a\mathbb{Z}$, où $a \in \mathbb{R}^+$
- soit dense dans $\mathbb{R}$.

238

Th. (24) : Soit G un sous-groupe compact de $(\mathbb{C}^*, \times)$. Alors :
- soit il existe $n \in \mathbb{N}^*$ tel que $G = \mu_n$
- soit $G = \mathbb{U}$.

III. Polynômes cyclotomiques $n \in \mathbb{N}^*$

1) Définition, propriétés fondamentales

[Per]

Notation (25) : Pour $n \in \mathbb{N}^*$, on pose $\Phi_n = X^n - 1 \in \mathbb{C}[X]$.

Rq (26) : Soit $p \in \mathbb{N}$ un nombre premier. Si $p \nmid n$, alors les racines de $X^n - 1 \in \mathbb{F}_p[X]$ dans son corps de décomposition $D_{\mathbb{F}_p}(X^n - 1)$ sont simples.

80

Déf. (27) : Le n-ième polynôme cyclotomique est :

$$\Phi_n = \prod_{\zeta \in \mu_n^*} (X - \zeta) \in \mathbb{C}[X].$$

Prop. (28) : 1) Φ_n est unitaire
2) $\deg(\Phi_n) = \varphi(n)$
3) $\Phi_n \mid P_n$, et on a $X^n - 1 = \prod_{d \mid n} \Phi_d$.

Conséquence (29) : On peut calculer les Φ_n à l'aide de la relation de récurrence $\Phi_n = \dfrac{X^n - 1}{\prod_{\substack{d \mid n \\ d < n}} \Phi_d}$

81

Ex. (30) : $\Phi_1 = X - 1$; $\Phi_2 = X + 1$; $\Phi_3 = X^2 + X + 1 = (X - j)(X - j^2)$
Si p est premier, $\Phi_p = X^{p-1} + \dots + X + 1$.

Th. (31) : $\Phi_n \in \mathbb{Z}[X]$, $\forall n \in \mathbb{N}^*$

Th. (32) : Φ_n est irréductible sur $\mathbb{Z}$ et sur $\mathbb{Q}$. DVP 1

83

2) Applications

[Per]
82

Th. (33) : (*Wedderburn*)
Tout corps fini est commutatif.

[FGN]
p31

Th. (34) : (*Dirichlet faible*)
Soit $n \in \mathbb{N}^*$. Alors il existe une infinité de nombres premiers congrus à 1 modulo n.

[Gou]
89

Th. (35) : (*Kronecker*)
Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré $n \geq 1$ et irréductible sur $\mathbb{Q}[X]$. On suppose que toutes les racines de P sont de module inférieur ou égal à 1.
Alors, $P = X$ ou P est un polynôme cyclotomique.

♡

Appli. (36) : Soit $\Pi \in \mathcal{O}_n(\mathbb{Z})$ une matrice orthogonale.
Alors son polynôme caractéristique $\chi_\Pi \in \mathbb{Z}[X]$ est produit de polynômes cyclotomiques.

IV. Caractères linéaires

1) Définition, premières propriétés

[Ba]
346

Déf. (37) : Soit $(G, \cdot)$ un groupe fini. Un caractère χ de G est un morphisme de groupes $\chi : G \longrightarrow (\mathbb{C}^*, \times)$.
L'ensemble des caractères linéaires de G, noté $\hat{G}$, est un groupe pour la multiplication des fonctions appelé groupe dual de G.

Prop. (38) : Soit $n = |G|$ et $\chi \in \hat{G}$. Alors χ est à valeurs dans μ_n.

347

Prop. (39) : Si G est un groupe cyclique d'ordre n, alors $\hat{G}$ est également cyclique d'ordre n. En particulier, $G \simeq \hat{G}$.
Soit g_0 un générateur de G et posons $\omega = e^{\frac{2i\pi}{n}} \in \mu_n^*$.
Les éléments de $\hat{G}$ sont les $\chi_j : G \longrightarrow \mathbb{C}^*$ pour $j \in \{0, \dots, n-1\}$
$g = g_0^k \longmapsto \exp\left(2i\pi \frac{kj}{n}\right) = \omega^{kj}$

[Pey]
4

Appli. (40) : La table de caractères de $\mathbb{Z}/n\mathbb{Z}$ est

	$\bar{0}$	$\bar{1}$	...	$\overline{n-1}$
χ_0	1	1		1
χ_1	1	ω		ω^{n-1}
$\vdots$	$\vdots$	$\vdots$		$\vdots$
χ_{n-1}	1	ω^{n-1}		$\omega^{(n-1)^2}$

2) Application : Le théorème de structure des groupes abéliens finis

[Bou]

Th. (41) : *(Lemme de prolongement des caractères)*

Soit $(G,.)$ un groupe abélien et $H \leq G$. Alors l'application de restriction $\rho_H : \hat{G} \longrightarrow \hat{H}$, $\chi \mapsto \chi_{|H}$ est un morphisme de groupes.

347

Si de plus $[G:H]$ est fini, alors ρ_H est surjectif.

DYP2

En particulier, si G est un groupe abélien fini, tout caractère linéaire de H se prolonge en un caractère linéaire de G.

Th. (42) : *(structure des groupes abéliens finis)*

358

Soit G un groupe abélien fini, $|G| \geq 2$.

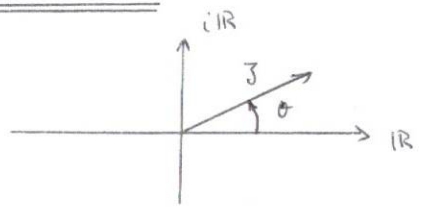
Alors, il existe des entiers $d_1, \dots, d_s \geq 2$ vérifiant $d_1 | d_2 | \dots | d_s$ tels que : $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$

De plus, $d_1 \dots d_s$ sont uniques.

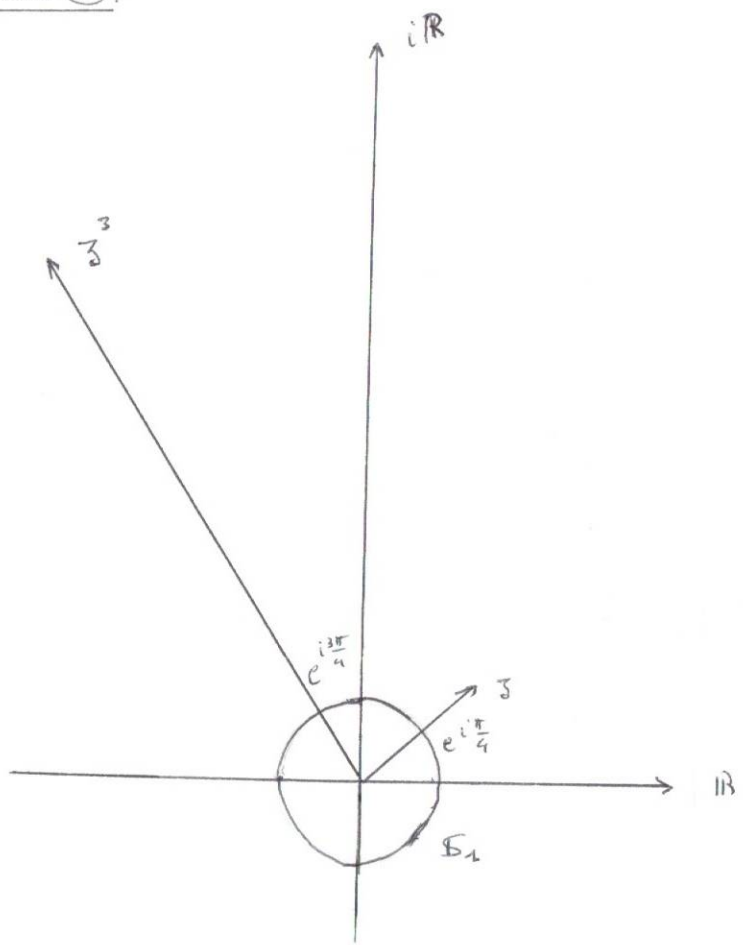
Coro. (43) : Si G est un groupe abélien fini, alors $G \simeq \hat{G}$

ANNEXE

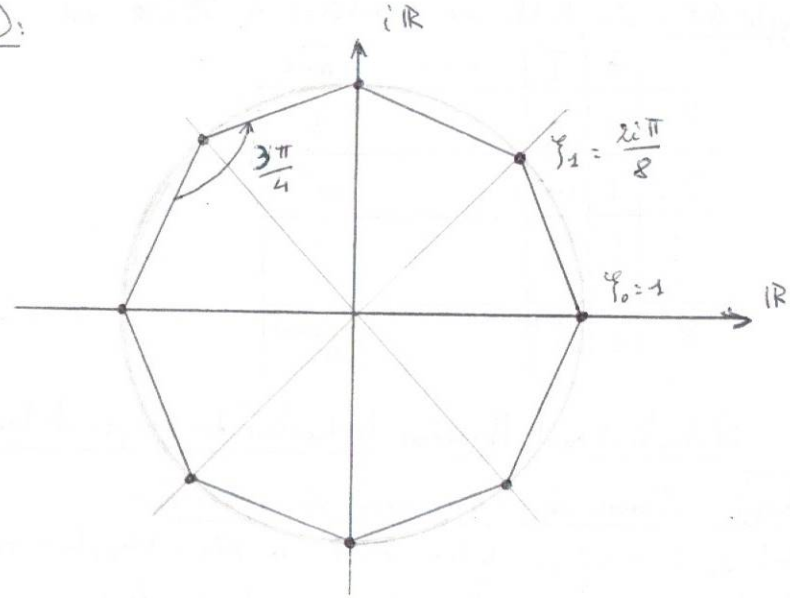
Appli. (13) :



Exercice (15) :



$\mathbb{R}_4$ (22) :



Références :

- [AF] Annoudiès, Fraysse, Cours de mathématiques Tome 1
- [Per] Perrin, Cours d'algèbre
- [Bur] Berhuy, Algèbre : le grand combat (2e éd.)
- [FGN1] Francinou, Gianella, Nicolas, Oraux X-ENS Algèbre 1
- [Pey] Peyré, Algèbre discrète de la transformée de Fourier
- [Gou] Gourdon, Algèbre (2e édition)