102 Groupes des nombres complexes de module 1. Sous groupe des racines de l'unité Applications

ARN p226

I. Le Groupe $\mathbb{U}$.

Def ①: l'application $\begin{array}{rcl}(\mathbb{C}^*, \times) & \xrightarrow{\varphi} & (\mathbb{R}_+^*, \times) \\ z & \longmapsto & |z|\end{array}$ est un morphisme de groupes. On note $\mathbb{U} = \ker(\varphi) = \{z \in \mathbb{C}, |z| = 1\}$ appelé groupe des nombres complexes de module 1.

Rq ②: $\mathbb{U}$ n'est rien d'autre que le cercle unité de $\mathbb{C}$.

Thm ③: L'application $\rho : \begin{array}{rcl}(\mathbb{R}_+^* \times \mathbb{U}) & \longrightarrow & \mathbb{C}^* \\ (r, u) & \longmapsto & ru\end{array}$ est un isomorphismes.

Def ④: l'application exponentielle notée exp est définie par $\exp : \begin{array}{rcl}\mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \sum_{n \in \mathbb{N}} \frac{z^n}{n!}\end{array}$.

Thm ⑤: l'application $\mathcal{E} : \begin{array}{rcl}\mathbb{R} & \longrightarrow & \mathbb{U} \\ x & \longmapsto & \exp(ix)\end{array}$ est un morphisme surjectif. Son noyau est $2\pi\mathbb{Z}$ où π est le plus petit réel > 0 tel que $Re(\mathcal{E}(\alpha)) = 0$, et $\mathbb{U} \simeq \mathbb{R}/2\pi\mathbb{Z}$

Def ⑥: On définit $\cos : \begin{array}{rcl}\mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & Re(\mathcal{E}(x))\end{array}$ et $\sin : \begin{array}{rcl}\mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & Im(\mathcal{E}(x))\end{array}$

ainsi, $\exp(ix) = \cos(x) + i\sin(x)$.

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

(ii) $\cos(x) = \frac{e^{ix} + e^{-ix}}{2}$ et $\sin(x) = \frac{e^{ix} - e^{-ix}}{2i}$ $\forall x \in \mathbb{R}$.

p228

application ⑧: $\sum_{k=0}^{n} e^{ik\theta} = e^{in\frac{\theta}{2}} \cdot \frac{\sin\left(\frac{n+1}{2}\theta\right)}{\sin\left(\frac{\theta}{2}\right)}$ $\forall \theta \in \mathbb{R} \setminus 2\pi\mathbb{Z}$

Def ⑨: soit $z \in \mathbb{C}^*$, un argument de z est un réel θ tel que $e^{i\theta} = \frac{z}{|z|}$. On note $\arg(z)$ l'ensemble de ces réels. p282

Prop ⑩: si $z \in \mathbb{C}^*$, $\arg(z) \neq \emptyset$ et pour θ_0 dans $\arg(z)$, $\arg(z) = \{\theta_0 + 2k\pi, k \in \mathbb{Z}\}$. p283

l'argument principal est alors l'unique $\theta \in \arg(z) \cap]-\pi, \pi[$

application ⑪: tout nombre complexe z s'écrit $re^{i\theta}$ où $r = |z| \in \mathbb{R}_+$ et $\theta \in \arg(z)$. C'est ce qu'on appelle la forme trigonométrique.

Ex ⑫: la forme trigonométrique de $z = 1 + \cos(\theta) + i\sin(\theta)$ est: $z = \begin{cases} 2\left|\cos\frac{\theta}{2}\right| e^{i\frac{\theta}{2}} & \text{si } \frac{\theta}{4\pi} - \left\lfloor \frac{\theta}{4\pi} \right\rfloor \notin]\frac{1}{4}, \frac{3}{4}[\\ 2\left|\cos\frac{\theta}{2}\right| e^{i\left(\frac{\theta}{2} + \pi\right)} & \text{sinon} \end{cases}$

II Racine n-ème de l'unité

Def ⑬: si $n \geq 2$, l'application $f_n : \begin{array}{rcl}\mathbb{U} & \longrightarrow & \mathbb{U} \\ z & \longmapsto & z^n\end{array}$ est un morphisme surjectif. on note $\mu_n = \ker(f) = \{z \in \mathbb{C}, z^n = 1\}$ l'ensemble des racine n-ème de l'unité dans $\mathbb{C}$. p235

Prop ⑭: Le groupe μ_n est cyclique et ses générateurs sont les éléments de $\mu_n^* = \{z_k = \exp\left(\frac{2ik\pi}{n}\right), k \in [0, n-1]$ et $k \wedge n = 1\}$

un tel élément est appelé racine primitive de l'unité.

Ex ⑮: • $\mu_2^* = \{-1\}$; $\mu_3^* = \{j, j^2\}$; $\mu_4 = \{i, -i\}$.

• $\mu_p^* = \mu_p \setminus \{1\}$ où p est premier.

p236

prop (16) : soit n un entier $\geqslant 2$. Le seul sous-groupe fini de $\mathbb{C}^*$ de cardinal n est μ_n.

Rq (17) : notons $\mu_n = \{ \xi_k = \exp(\frac{2ik\pi}{n}), k \in [\![0, n-1]\!] \}$, alors les ξ_k sont les sommets d'un polygone régulier à n côtés inscrit dans $\mathbb{U}$. La longueur d'un côté est $2\sin(\frac{\pi}{n})$ et l'angle formé entre deux côtés consécutifs est $(n-1)\frac{\pi}{n}$.

p238 Ex16

lemme (18) : tout sous groupe additif de $\mathbb{R}$ non réduit à $\{0\}$ est soit du type $a\mathbb{Z}$ où $a>0$, soit dense dans $\mathbb{R}$

Thm (19) : Soit G un sous-groupe compact de $(\mathbb{C}^*, \times)$ alors
- soit $\exists n \in \mathbb{N}^*$ tel que $G = \mu_n$
- soit $G = \mathbb{U}$.

III. Polynômes cyclotomiques

PERR p80

Def (20) : le n-ème polynôme cyclotomique $\phi_n \in \mathbb{C}[X]$ est donné par $\phi_n(X) = \prod_{\xi \in \mu_n^*} (X - \xi)$

Ex (21) : $\phi_1(X) = X - 1$; $\phi_2(X) = X+1$;
$\phi_3(X) = X^2 + X + 1$; $\phi_p(X) = X^{p-1} + \dots + 1$ pour p premier

Rq (22) : ϕ_n est unitaire de degré $\varphi(n)$

prop (23) : $X^n - 1 = \prod_{d|n} \phi_d(X)$
(en particulier, $n = \sum_{d|n} \varphi(d)$.

p81

cor (24) : $\phi_n \in \mathbb{Z}[X]$ $\forall n \in \mathbb{N}^*$.

Thm (25) (wedderburn) : soit A un anneau fini tel que $A^\times = A \setminus \{0\}$ alors A est commutatif. p82

Thm (26) : Le polynôme cyclotomique ϕ_n est irréductible sur $\mathbb{Z}$ (donc sur $\mathbb{Q}$)

cor (27) : soit ξ une racine primitive n-ème de l'unité, alors son polynôme minimal est ϕ_n et $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$.

FGN p 158 GOU p89

Thm (28) : (Kronecker) Soit P un polynôme unitaire de $\mathbb{Z}[X]$ dont les racines complexes sont de module inférieur ou égal à 1. On suppose que P est irréductible sur $\mathbb{Q}[X]$, alors $P = X$ ou P est un polynôme cyclotomique

application (29) : Soit $\Pi \in S_n(\mathbb{Z})$ $n \geqslant 1$ une matrice orthgonale à coefficient dans $\mathbb{Z}$, alors χ_Π est produit de polynômes cyclotomiques

IV Dual d'un groupe fini

PEY p?

Def (30) : soit G un groupe fini, un caractère de G χ est un morphisme $\chi : G \to \mathbb{C}^*$. On note $\hat{G}$ l'ensemble des caractères qui est un groupe pour la multiplication des applications, on l'appelle dual de G.

prop (31) : notons $n = |G|$, et $\chi \in \hat{G}$, alors χ est à valeurs dans μ_n. En particulier $\chi(g^{-1}) = \overline{\chi(g)}$.

prop 32 : soit $G = \langle g_0 \rangle$ un groupe cyclique de cardinal n et de générateur g_0. On note $\omega = e^{\frac{2i\pi}{n}}$ qui est une racine primitive n-ème de l'unité. Alors les éléments de $\widehat{G}$ sont de la forme pour $j \in [\![0, n-1]\!]$

$$\chi_j : \begin{array}{rcl} G & \longrightarrow & \mathbb{C}^* \\ g = g_0^k & \longmapsto & (\omega^j)^k = e^{\frac{2i\pi kj}{n}} \end{array}$$

en particulier, $G \simeq \widehat{G}$

Ex 33 : table de $\mathbb{Z}/n\mathbb{Z}$

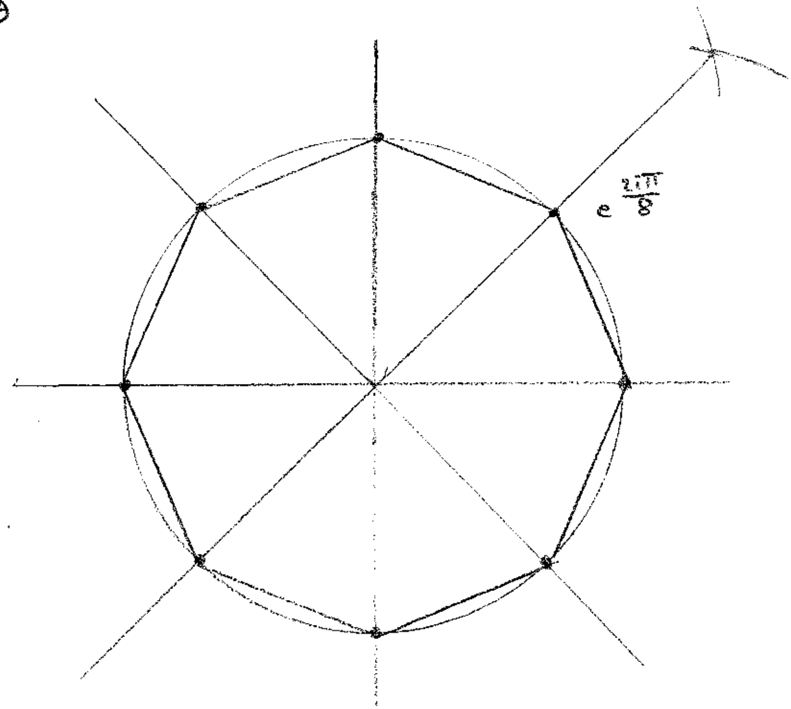
Thm 34 (Structure des groupes abéliens finis) : Soit G un groupe abélien fini, il existe des entiers $n_1 \dots n_r \in \mathbb{N}^*$ uniquement déterminés tels que $n_k \mid n_{k+1}$ et :

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}.$$

coro 35 : $\widehat{G} \simeq G$ pour G groupe abélien fini.

application 36 : soit K un corps et G un sous groupe fini de $(K^*, \cdot)$, alors G est cyclique.

Rq 17



Ex 33 :

	0	1	$\dots$	$n-1$
χ_1	1	1		1
χ_2	1	ω		ω^{n-1}
χ_n	1	ω^{n-1}		$\omega^{(n-1)^2}$

Références :

[ARN] Arnaudiès et Fraysse Tome 1 (partie I et II)
[PERR] Perrin (cours d'Algèbre) (partie III)
[GOU] Gourdon (Algèbre) (Kronecker)
[PEY] Peyré, Algèbre discrète de la TF (partie IV)