

Résumé de cours :  
Semaine 11, du 29 novembre au 03 décembre.

# Les complexes (fin)

## 1 Antilinéarisation

**Exercice.** Il faut savoir le démontrer.

Montrer que, pour tout  $n \in \mathbb{N}$ , il existe un unique polynôme  $T_n$  tel que, pour tout  $\theta \in \mathbb{R}$ ,  $T_n(\cos \theta) = \cos n\theta$ .  $T_n$  est appelé le  $n$ -ième polynôme de Tchebychev de première espèce.

## 2 Équations polynomiales

### 2.1 Racines $n$ -ièmes d'un complexe

Les racines  $n$ -ièmes de  $a \in \mathbb{C}^*$  sont les solutions de l'équation  $z^n = a$  en l'inconnue  $z \in \mathbb{C}^*$ .

Posons  $a = re^{i\varphi}$ . Alors, en notant  $z_0 = r^{\frac{1}{n}} e^{i\frac{\varphi}{n}}$  on a  $z_0^n = a$ . Ainsi,

$$z^n = a \iff z^n = z_0^n \iff \left(\frac{z}{z_0}\right)^n = 1 \iff \frac{z}{z_0} \in \mathbb{U}_n \iff (\exists k \in \{0, \dots, n-1\}, z = r^{\frac{1}{n}} e^{i\frac{2k\pi + \varphi}{n}}).$$

$a$  possède donc exactement  $n$  racines  $n$ -ièmes, disposées selon un polygone régulier à  $n$  côtés, inscrit dans le cercle de centre  $O$  et de rayon  $|a|^{\frac{1}{n}}$ .

### 2.2 Équations du second degré

#### 2.2.1 Racines carrées

$a = re^{i\varphi}$  (avec  $r > 0$ ) possède exactement deux racines carrées égales à  $\pm\sqrt{r}e^{i\frac{\varphi}{2}}$ .

Lorsque  $a = x + iy$  avec  $x, y \in \mathbb{R}$ , on peut déterminer les racines carrées de  $a$  selon le procédé suivant :

$$\text{Si } z = \alpha + i\beta, \text{ alors } z^2 = a \iff \begin{cases} \frac{x}{\sqrt{x^2 + y^2}} = \frac{\alpha^2 - \beta^2}{\alpha^2 + \beta^2} \\ \text{sgn}(y) = \text{sgn}(\alpha\beta) \end{cases}$$

#### 2.2.2 Racines d'un trinôme

**Formule :** Soit  $a, b, c \in \mathbb{C}$  avec  $a \neq 0$ . Les solutions de l'équation  $az^2 + bz + c = 0$  sont  $\frac{-b \pm \delta}{2a}$ , où  $\delta$  est une racine carrée du discriminant  $\Delta = b^2 - 4ac$ .

Ces deux racines sont égales si et seulement si  $\Delta = 0$ . Dans ce cas, l'unique racine vaut  $\frac{-b}{2a}$ . On dit que c'est une racine double.

Il faut savoir le démontrer.

**Propriété.** Soit  $a, b, c \in \mathbb{C}$  avec  $a \neq 0$ . Notons  $z_1$  et  $z_2$  les deux racines (éventuellement égales à une racine double) du trinôme  $aX^2 + bX + c$ . Alors 
$$\boxed{z_1 + z_2 = \frac{-b}{a} \text{ et } z_1 z_2 = \frac{c}{a}}.$$

**Propriété.** Soit  $s, p \in \mathbb{C}$ .

$\begin{cases} z_1 + z_2 = s \\ z_1 z_2 = p \end{cases}$  si et seulement si  $\{z_1, z_2\}$  est l'ensemble des racines du trinôme  $X^2 - sX + p$ .

**Propriété.** Soit  $P(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in \mathbb{C}[X]$  avec  $a_n \neq 0$ . Ainsi  $P$  est de degré  $n$ . Alors il existe  $\beta_1, \dots, \beta_n \in \mathbb{C}$  tel que  $P(X) = a_n \prod_{i=1}^n (X - \beta_i)$ . On dit que  $\beta_1, \dots, \beta_n$  sont les racines de  $P$ . Un même complexe peut apparaître plusieurs fois parmi les  $\alpha_i$ , auquel cas c'est une racine multiple de  $P$ . Ainsi, en comptant les racines avec multiplicité,  $P$  possède exactement  $n$  racines complexes. On en déduit que le seul polynôme possédant une infinité de racines est le polynôme nul.

De plus,  $\sum_{i=1}^n \beta_i = -\frac{a_{n-1}}{a_n}$  et  $\prod_{i=1}^n \beta_i = (-1)^n \frac{a_0}{a_n}$ .

**Propriété.** Pour tout  $n \in \mathbb{N}$  avec  $n \geq 2$ ,

$$X^n - 1 = \prod_{k=0}^{n-1} (X - e^{\frac{2ik\pi}{n}}) \text{ et } X^{n-1} + \dots + X + 1 = \prod_{k=1}^{n-1} (X - e^{\frac{2ik\pi}{n}}).$$

## 3 Géométrie du plan complexe

### 3.1 Distances et angles

**Propriété.** Soit  $A, B, C$  trois points du plan usuel, d'affixes respectifs  $a, b, c \in \mathbb{C}$ .

- Le vecteur  $\overrightarrow{AB}$  est d'affixe  $b - a$ ;
- La distance  $AB$  entre  $A$  et  $B$  est égale à  $|b - a|$ ;
- L'angle orienté  $(\widehat{CA}, \widehat{CB})$  vérifie  $(\widehat{CA}, \widehat{CB}) \equiv \arg\left(\frac{b - c}{a - c}\right) [2\pi]$ .

**Il faut savoir démontrer la dernière propriété.**

### 3.2 Orthogonalité et colinéarité

**Propriété.** Soit  $\vec{u}$  et  $\vec{v}$  deux vecteurs non nuls d'affixes  $u = a + ib$  et  $v = c + id$ .

- $\vec{u} // \vec{v} \iff \frac{u}{v} \in \mathbb{R} \iff \text{Im}(\bar{u}v) = 0 \iff ad - bc \triangleq \begin{vmatrix} a & c \\ b & d \end{vmatrix} \triangleq \det(\vec{u}, \vec{v}) = 0$ .  
 $\det(\vec{u}, \vec{v})$  est le déterminant (auss appelé le produit mixte) des deux vecteurs  $\vec{u}$  et  $\vec{v}$ .
- $\vec{u} \perp \vec{v} \iff \frac{u}{v} \in i\mathbb{R} \iff \text{Re}(\bar{u}v) = 0 \iff ac + bd \triangleq \langle \vec{u}, \vec{v} \rangle = 0$ .  
 $\langle \vec{u}, \vec{v} \rangle$  est le produit scalaire des deux vecteurs  $\vec{u}$  et  $\vec{v}$ .

**Il faut savoir le démontrer.**

**Corollaire.** Soit  $A, B, C$  trois points du plan usuel, d'affixes respectifs  $a, b, c \in \mathbb{C}$ .

- ( $A, B$  et  $C$  sont alignés)  $\iff \frac{a - b}{c - b} \in \mathbb{R} \iff \text{Im}(\overline{(a - b)}(c - b)) = 0$ , c'est-à-dire  
 $C \in (AB) \iff \arg(c - a) \equiv \arg(b - a) [\pi] \iff (\exists t \in \mathbb{R}, c = (1 - t)a + tb)$ .
- (Le triangle  $ABC$  est rectangle en  $B$ )  $\iff \frac{a - b}{c - b} \in i\mathbb{R} \iff \text{Re}(\overline{(a - b)}(c - b)) = 0$ .

### 3.3 Équation d'un cercle

Notons  $C$  le cercle de centre  $\alpha = a + ib \in \mathbb{C}$  et de rayon  $r > 0$ . Alors

$$z = x + iy \in C \iff |z - \alpha| = r \iff (z - \alpha)(\bar{z} - \bar{\alpha}) = r^2 \iff x^2 + y^2 - 2ax - 2by = r^2 - a^2 - b^2.$$

Réciproquement, un ensemble admettant une équation cartésienne de la forme

$x^2 + y^2 - 2ax - 2by = c$  est un cercle éventuellement réduit à un point ou à l'ensemble vide.

### 3.4 Les similitudes

#### 3.4.1 Les similitudes directes

**Définition.** Une application  $f : \mathbb{C} \rightarrow \mathbb{C}$  est une isométrie si et seulement si elle conserve les distances, c'est-à-dire si et seulement si, pour tout  $z, z' \in \mathbb{C}$ ,  $|f(z) - f(z')| = |z - z'|$ .

**Définition.** La translation de vecteur  $b \in \mathbb{C}$  est la transformation  $t_b : z \mapsto z + b$ . Elle est bijective, d'application réciproque  $t_{-b}$ , elle ne possède aucun point fixe lorsque  $b \neq 0$ , c'est une isométrie.

**Définition.** La rotation de centre  $z_0 \in \mathbb{C}$  et d'angle  $\theta \in \mathbb{R}$  est la transformation  $r_{z_0, \theta} : z \mapsto e^{i\theta}(z - z_0) + z_0$ . Elle est bijective, d'application réciproque  $r_{z_0, -\theta}$ , elle admet  $z_0$  comme unique point fixe lorsque  $\theta \notin 2\pi\mathbb{Z}$ , c'est une isométrie.

**Définition.** L'homothétie de centre  $z_0 \in \mathbb{C}$  et de rapport  $\lambda \in \mathbb{R}^*$  est la transformation  $h_{z_0, \lambda} : z \mapsto \lambda(z - z_0) + z_0$ . Elle est bijective, d'application réciproque  $h_{z_0, \frac{1}{\lambda}}$ , elle admet  $z_0$  comme unique point fixe lorsque  $\lambda \neq 1$ .

**Définition.** La similitude directe de centre  $z_0 \in \mathbb{C}$ , d'angle  $\theta \in \mathbb{R}$  et de rapport  $\lambda \in \mathbb{R}^*$  est  $s_{z_0, \theta, \lambda} = h_{z_0, \lambda} \circ r_{z_0, \theta} = r_{z_0, \theta} \circ h_{z_0, \lambda} : z \mapsto \lambda e^{i\theta}(z - z_0) + z_0$ . Elle est bijective, d'application réciproque  $s_{z_0, -\theta, \frac{1}{\lambda}}$ , elle admet  $z_0$  comme unique point fixe lorsque  $\lambda e^{i\theta} \neq 1$ , elle conserve les proportions (pour tout  $z, z' \in \mathbb{C}$ , en posant  $s = s_{z_0, \theta, \lambda}$ ,  $|s(z) - s(z')| = |\lambda||z - z'|$ ), elle conserve les angles (pour tout  $a, b, c$  deux à deux distincts,  $\widehat{(s(a)s(b), s(a)s(c))} = \widehat{(ab, ac)}$ ) : **Il faut savoir le démontrer.**

**Définition.** On dit que  $f$  est une similitude affine directe si et seulement si c'est une application de  $\mathbb{C}$  dans  $\mathbb{C}$  de la forme  $z \mapsto az + b$ , où  $a \in \mathbb{C}^*$  et  $b \in \mathbb{C}$ .

**Propriété.** Soit  $f : z \mapsto az + b$  une similitude directe.

Lorsque  $a = 1$ , c'est une translation.

Lorsque  $a \neq 1$ ,  $f$  possède un unique point fixe  $z_0 \in \mathbb{C}$  et  $f$  est la similitude directe de centre  $z_0$ , d'angle  $\arg(a)$  et de rapport  $|a|$ .

**Il faut savoir le démontrer.**

**Propriété.** L'ensemble  $S^+$  des similitudes affines directes est un sous-groupe de  $\mathcal{S}(\mathbb{C})$ .

**Il faut savoir le démontrer.**

**Propriété.** L'application qui à la similitude  $z \mapsto az + b$  associe  $a$  (resp :  $|a|$ ) est un morphisme de groupes, dont le noyau est le sous-groupe des translations (resp : des rotations et des translations).

**Corollaire.** Une composée, quel que soit l'ordre, de translations, de rotations dont la somme des angles est égale à  $\theta$  et d'homothéties dont le produit des rapports est égal à  $\lambda$  est une similitude directe de la forme  $z \mapsto \lambda e^{i\theta}z + b$ .

#### 3.4.2 Les similitudes indirectes

**Notation.** Notons  $c : \begin{matrix} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \bar{z} \end{matrix}$  l'opérateur de conjugaison, qui correspond à la réflexion par rapport à l'axe des  $x$ .

**Définition.** On note  $S^- = \{s \circ c / s \in S^+\} = \{c \circ s / s \in S^+\}$ .

Les éléments de  $S^-$  sont appelés les similitudes indirectes.

### 3.4.3 Triangles semblables

**Définition.** On dit que deux triangles du plan complexe sont directement semblables si et seulement si l'un est l'image de l'autre par une similitude directe.

**Propriété.** Soit  $a, b, c$  trois complexes deux à deux distincts et  $a', b', c'$  trois autres complexes deux à deux distincts. Les deux triangles  $(a, b, c)$  et  $(a', b', c')$  sont directement semblables si et seulement si  $\frac{c-a}{b-a} = \frac{c'-a'}{b'-a'}$ , c'est-à-dire si et seulement si (en notant  $AB$  la distance entre deux points  $A$  et  $B$ ),  $\frac{ac}{ab} = \frac{a'c'}{a'b'}$  et  $\widehat{bac} = \widehat{b'a'c'}$ .

**Propriété.** Deux triangles non plats  $(a, b, c)$  et  $(a', b', c')$  du plan complexe sont directement semblables si et seulement si ils ont les mêmes angles.

## La structure de groupe

### 4 Définitions

**Définition.**  $(G, \cdot)$  est un groupe si et seulement si  $G$  est muni d'une loi interne " $\cdot$ " qui vérifie

- l'associativité : pour tout  $x, y, z \in G$ ,  $x(yz) = (xy)z$  ;
- l'existence d'un élément neutre  $1_G$  : pour tout  $x \in G$ ,  $1_G \cdot x = x \cdot 1_G = x$  ;
- l'existence, pour tout  $x \in G$ , d'un symétrique  $x^{-1}$  tel que :  $xx^{-1} = x^{-1}x = 1_G$ .

**Définition.** Pour un groupe, "commutatif" et "abélien" sont synonymes.

**Notation.** On utilise principalement deux notations pour désigner la loi interne d'un groupe :

◇ *Notation multiplicative* : dans un groupe  $(G, \cdot)$ , l'élément neutre est noté 1 ou  $1_G$ , le symétrique de  $x \in G$  est noté  $x^{-1}$  et si  $x_1, \dots, x_n \in G$ , on note  $x_1 \times \dots \times x_n = \prod_{i=1}^n x_i$ , en convenant que ce produit vaut  $1_G$  lorsque  $n = 0$  (produit vide).

◇ *Notation additive* : dans un groupe abélien  $(G, +)$ , l'élément neutre est noté 0 ou  $0_G$ , le symétrique de  $x \in G$  est noté  $-x$  et si  $x_1, \dots, x_n \in G$ , on note  $x_1 + \dots + x_n = \sum_{i=1}^n x_i$ , en convenant que cette somme vaut  $0_G$  lorsque  $n = 0$  (somme vide).

**Définition.** Si  $(G, \cdot)$  est un groupe fini, le cardinal de  $G$  est appelé l'**ordre** de  $G$ .

### 5 Calculs dans un groupe

**Propriété.** Soit  $(G, \cdot)$  un groupe et  $a \in G$ . Alors  $a$  est régulier (ou simplifiable) à gauche et à droite, c'est-à-dire que  $\forall x, y \in G$ ,  $[ax = ay \implies x = y]$  et  $[xa = ya \implies x = y]$ .

**Propriété.** Dans un groupe  $(G, \cdot)$ ,  $(x_1 \times \dots \times x_n)^{-1} = x_n^{-1} \times \dots \times x_1^{-1}$ .

**Propriété.** Dans un groupe abélien  $(G, +)$ , on pose  $x - y \triangleq x + (-y)$ .

On dispose des formules :  $x - (y + z) = x - y - z$  et  $x - (y - z) = x - y + z$ .

## 6 Construction de groupes

### 6.1 Groupe produit

**Définition.** Le groupe produit des  $n$  groupes  $((G_i, \cdot_i))_{i \in \{1, \dots, n\}}$  est  $(G, \cdot)$ , où  $G = G_1 \times \dots \times G_n$  et où la loi “ $\cdot$ ” est définie par :  $(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) = (x_1 \cdot_1 y_1, \dots, x_n \cdot_n y_n)$ .

### 6.2 Produit fonctionnel

**Définition.** Soit  $(G, \cdot)$  un groupe et  $A$  un ensemble quelconque. Pour tout  $f, g \in G^A$ , on convient que  $f.g$  est l’application de  $A$  dans  $G$  définie par :  $\forall a \in A, (f.g)(a) = f(a).g(a)$ .

Alors  $G^A$  est un groupe, dont l’élément neutre est l’application constante  $a \mapsto 1_G$  et pour lequel le

symétrique de  $f \in G^A$  est  $f^{-1} : A \longrightarrow G$   
 $a \longmapsto [f(a)]^{-1}$ .

### 6.3 Le groupe symétrique

**Propriété.** Si  $E$  est un ensemble, alors l’ensemble des bijections de  $E$  dans  $E$  est un groupe pour la loi de composition. On l’appelle le groupe symétrique de  $E$  et on le note  $\mathcal{S}(E)$ . Son élément neutre est l’application identité  $Id_E$  et, pour tout  $f \in \mathcal{S}(E)$ , le symétrique de  $f$  est la bijection réciproque de  $f$ , dont la notation  $f^{-1}$  est en cohérence avec cette propriété.

## 7 Sous-groupes

### 7.1 Définition

**Propriété et définition :** Soit  $(G, \cdot)$  un groupe et  $H$  une partie de  $G$ .

$H$  est un groupe pour la restriction de la loi “ $\cdot$ ” à  $H \times H$ , avec le même élément neutre  $1_G$  si et seulement si

- $H \neq \emptyset$ ;
- $\forall (x, y) \in H^2, xy \in H$  (stabilité du produit);
- $\forall x \in H, x^{-1} \in H$  (stabilité du symétrique).

Cet ensemble de conditions est équivalent à

- $H \neq \emptyset$ ;
- $\forall (x, y) \in H^2, xy^{-1} \in H$ .

Dans ce cas, on dit que  $H$  est un **sous-groupe** de  $G$ .

**Propriété de transitivité :** Un sous-groupe d’un sous-groupe d’un groupe  $G$  est un sous-groupe de  $G$ .

### 7.2 Groupe engendré par une partie

**Propriété.** Soit  $I$  un ensemble non vide, éventuellement infini. Soient  $G$  un groupe et  $(H_i)_{i \in I}$  une famille de sous-groupes de  $G$ . Alors l’intersection  $\bigcap_{i \in I} H_i$  est un sous-groupe de  $G$ .

**Il faut savoir le démontrer.**

**Définition.** Soit  $G$  un groupe et  $A$  une partie de  $G$ .

Notons  $\mathcal{S}$  l’ensemble des sous-groupes de  $G$  contenant  $A$ .  $\mathcal{S}$  est non vide car  $G \in \mathcal{S}$ .

Alors  $\bigcap_{H \in \mathcal{S}} H$  est un sous-groupe de  $G$  contenant  $A$  et, par construction, c’est le plus petit sous-groupe contenant  $A$ . On le note  $Gr(A)$ .

**Propriété.** Si  $A \subset B$ , alors  $Gr(A) \subset Gr(B)$ .

**Propriété.** Soit  $(G, \cdot)$  un groupe et  $A$  une partie de  $G$ . Notons  $A^{-1} = \{a^{-1} / a \in A\}$ .

Alors  $Gr(A) = \left\{ \prod_{i=1}^n a_i / n \in \mathbb{N}, \forall i \in \{1, \dots, n\}, a_i \in A \cup A^{-1} \right\}$ .

Il faut savoir le démontrer.

**Définition.** Si  $H$  et  $K$  sont deux sous-groupes d'un groupe abélien  $(G, +)$ , on note  $H + K = \{h + k / (h, k) \in H \times K\}$ . C'est le groupe engendré par  $H \cup K$ .

**Définition.** Soit  $G$  un groupe et  $A$  une partie de  $G$ .  
 $A$  est une **partie génératrice** de  $G$  si et seulement si  $Gr(A) = G$ .

### 7.3 Puissances d'un élément d'un groupe

**Définition.** Soit  $(G, \cdot)$  un groupe et  $a \in G$ . On définit la famille  $(a^n)_{n \in \mathbb{Z}}$  par les relations suivantes :

- Initialisation :  $a^0 = 1_G$  (encore le produit vide) ;
- Itération : pour tout  $n \in \mathbb{N}$ ,  $a^{n+1} = a \cdot a^n$  (donc pour  $n \in \mathbb{N}^*$ ,  $a^n = \underbrace{a \times \dots \times a}_{n \text{ fois}}$ ) ;
- Symétrique : pour tout  $n \in \mathbb{Z}$  avec  $n < 0$ ,  $a^n = (a^{-n})^{-1}$ .

**Formules :** pour tout  $n, m \in \mathbb{Z}$ ,  $a^n a^m = a^{n+m}$  et  $(a^n)^m = a^{nm}$ .

Si  $ab = ba$  (on dit que  $a$  et  $b$  commutent), pour tout  $n \in \mathbb{Z}$ ,  $(ab)^n = a^n b^n$ .

**Remarque.** Si  $a$  et  $b$  commutent, alors pour tout  $n, k \in \mathbb{Z}$ ,  $a^n$  et  $b^k$  commutent également entre eux.

Il faut savoir le démontrer.

En notation additive, dans le cadre des groupes commutatifs, ce qui précède devient :

**Définition.** soit  $(G, +)$  un groupe commutatif et  $a$  un élément de  $G$ . On **définit** la famille  $(na)_{n \in \mathbb{Z}}$  par les relations suivantes :

- Initialisation :  $0.a = 0_G$  ;
- Itération : pour tout  $n \in \mathbb{N}$ ,  $(n+1).a = a + (n.a)$   
 (donc pour  $n \in \mathbb{N}^*$ ,  $n.a = \underbrace{a + \dots + a}_{n \text{ fois}}$ ) ;
- Symétrique : pour tout  $n \in \mathbb{Z}$  avec  $n < 0$ ,  $n.a = -((-n).a)$ .

**Propriété.** Soit  $(G, +)$  un groupe abélien et  $a, b \in G$ . Pour tout  $n, m \in \mathbb{Z}$ ,  
 $(n.a) + (m.a) = (n+m).a$ ,  $m.(n.a) = (nm).a$  et  $n.(a+b) = (na) + (nb)$ .

**Propriété.** Soit  $(G, +)$  un groupe abélien et  $A$  une partie de  $G$ .

Alors  $Gr(A) = \left\{ \sum_{a \in A} n_a.a / (n_a)_{a \in A} \in \mathbb{Z}^{(A)} \right\}$ .

**Remarque.** En particulier,  $Gr(\{x_1, \dots, x_p\}) = \left\{ \sum_{i=1}^p n_i x_i / (n_i)_{1 \leq i \leq p} \in \mathbb{Z}^p \right\}$ .

### 7.4 Groupe monogène

**Propriété.** Soit  $(G, \cdot)$  un groupe et  $a \in G$ . Alors le groupe engendré par la partie  $\{a\}$  est  $Gr(\{a\}) = \{a^n / n \in \mathbb{Z}\}$ . On le note plus simplement  $Gr(a)$ .

**Propriété.** Soit  $(G, +)$  un groupe abélien et  $a \in G$ . Alors le groupe engendré par la partie  $\{a\}$  est  $Gr(\{a\}) = \{na / n \in \mathbb{Z}\}$ . On le note  $Gr(a)$ . On peut donc écrire  $Gr(a) = \mathbb{Z}.a$ .

**Propriété.** Les sous-groupes de  $(\mathbb{Z}, +)$  sont les  $n\mathbb{Z}$ , où  $n \in \mathbb{N}$ .

Il faut savoir le démontrer.

**Définition.** Soit  $a$  un élément d'un groupe  $G$ . Lorsque  $Gr(a)$  est de cardinal fini, ce cardinal est appelé l'ordre de  $a$ .

**Définition.** On dit qu'un groupe  $(G, .)$  est *monogène* si et seulement si il existe  $a \in G$  tel que  $G = Gr(a)$ . On dit alors que  $a$  est un *générateur* de  $G$ .

**Remarque.** Tout groupe monogène est abélien.

**Définition.** Un groupe  $G$  est dit *cyclique* si et seulement si  $G$  est monogène et fini.

**Exemple.**  $\mathbb{U}_n = \{e^{2i\pi \frac{k}{n}} / k \in \{0, \dots, n-1\}\}$  est un groupe cyclique.

**Propriété.** Soit  $(G, .)$  un groupe,  $a \in G$  et  $n \in \mathbb{N}^*$ .

Les propriétés suivantes sont équivalentes :

- i)  $Gr(a)$  est cyclique de cardinal  $n$ .
- ii)  $\{k \in \mathbb{N}^* / a^k = 1\}$  est non vide et son minimum est égal à  $n$ .
- iii) Pour tout  $k \in \mathbb{Z}$ ,  $[a^k = 1 \iff k \in n\mathbb{Z}]$ .
- iv) Les éléments de  $Gr(a)$  sont exactement  $1, a, \dots, a^{n-1}$  et ils sont deux à deux distincts.

Dans ce cas,  $n$  est l'ordre de  $a$  et de  $Gr(a)$ .

Il faut savoir le démontrer.