

Corrigé du DM 1

Soit p un nombre premier, on note :

$$\mathcal{G}_p = \left\{ z \in \mathbb{C} \mid \exists k \in \mathbb{N}, z^{(p^k)} = 1 \right\}$$

et pour tout $k \in \mathbb{N}$, on note :

$$V_k = \mathbb{U}_{p^k} = \left\{ z \in \mathbb{C} \mid z^{(p^k)} = 1 \right\}.$$

1. a) Soit $k \in \mathbb{N}$, V_k est l'ensemble des racines (p^k) -ième de l'unité, donc : $V_k = \left\{ e^{\frac{2ij\pi}{p^k}} ; \text{ avec } j \in \mathbb{Z} \right\} = \left\{ (e^{\frac{2i\pi}{p^k}})^j ; \text{ avec } j \in \mathbb{Z} \right\}$ et $e^{\frac{2i\pi}{p^k}} \in \mathbb{C}^*$, donc : $V_k = \text{gr}(e^{\frac{2i\pi}{p^k}})$ est le sous-groupe engendré par $e^{\frac{2i\pi}{p^k}}$ dans $(\mathbb{C}, \times)$; en particulier c'est un sous-groupe et son cardinal est p^k .

Pour tout $k \in \mathbb{N}$, V_k est un sous-groupe de $(\mathbb{C}^*, \times)$ de cardinal p^k .

b) Soit $k \in \mathbb{N}$ et $z \in V_k$,

donc : $z^{(p^k)} = 1$,

donc : $z^{(p^{k+1})} = z^{p^k \times p} = \left(z^{(p^k)} \right)^p = 1^p = 1$

donc : $z \in V_{k+1}$.

On a montré que $V_k \subset V_{k+1}$.

De plus, $\text{Card}(V_k) = p^k < p^{k+1} = \text{Card } V_{k+1}$, donc $V_k \neq V_{k+1}$.

Conclusion

la suite $(V_k)_{k \in \mathbb{N}}$ est strictement croissante pour l'inclusion.

2. a) Soit $z \in \mathbb{C}$,

$$z \in \mathcal{G}_p \Leftrightarrow \exists k \in \mathbb{N}, z^{(p^k)} = 1$$

$$\Leftrightarrow \exists k \in \mathbb{N}, z \in V_k$$

$$\Leftrightarrow z \in \bigcup_{k \in \mathbb{N}} V_k.$$

Donc :

$$\mathcal{G}_p = \bigcup_{k \in \mathbb{N}} V_k.$$

b) • $\forall k \in \mathbb{N}, V_k \subset \mathbb{C}^*$, donc $\mathcal{G}_p = \bigcup_{k \in \mathbb{N}} V_k \subset \mathbb{C}^*$.

• Pour $k = 0$, on a $1^{p^k} = 1$ donc $1 \in \mathcal{G}_p$.

- Soit $x, y \in \mathcal{G}_p$,
donc : il existe $k, l \in \mathbb{N}$ tels que $x \in V_k$ et $y \in V_l$,
or $(V_k)_{k \in \mathbb{N}}$ est croissante, donc pour $m = \max(k, l)$, $x, y \in V_m$. De plus, V_m est un sous-groupe de $(\mathbb{C}^*, \times)$, donc donc : $xy^{-1} \in V_m \subset \mathcal{G}_p$.

Donc :

$\mathcal{G}_p$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

3. Soit $z \in V_{k+1} \setminus V_k$, on note α l'ordre de z dans V_{k+1} .

On sait que $z \notin V_k$, donc : $z^{(p^k)} \neq 1$,

donc : α ne divise pas p^k .

De plus : V_{k+1} est de cardinal p^{k+1} donc, d'après le théorème de Lagrange, α divise p^{k+1} ,

donc $\alpha \in \{1, p, p^2, \dots, p^k, p^{k+1}\}$

et comme α ne divise pas p^k , $\alpha = p^{k+1}$.

Donc : $\text{gr}(z)$ est un sous-groupe de V_{k+1} de cardinal p^{k+1} qui est le cardinal de V_{k+1} .

Donc : $\text{gr}(z) = V_{k+1}$.

Conclusion :

$z \in V_{k+1} \setminus V_k$, alors z est générateur de V_{k+1} .

4. Soit H un sous-groupe propre de $\mathcal{G}_p$ tel que $\forall k \in \mathbb{N}, H \neq V_k$, montrons que $H = \mathcal{G}_p$.

a) Supposons par l'absurde qu'il existe $k \in \mathbb{N}$ tel que $H \subset V_k$.

Soit $A = \{j \in \mathbb{N} \mid H \subset V_j\}$, A est une partie de $\mathbb{N}$ non vide car $k \in A$ et $0 \notin A$ car $H \not\subset V_0 = \{1\}$.

Soit l le plus petit élément de A , donc $l \geq 1$, $H \subset V_l$ et $H \not\subset V_{l-1}$.

Donc : il existe $z \in H \setminus V_{l-1} \subset V_l \setminus V_{l-1}$ et d'après la question précédente z est un générateur de V_l .

De plus H est un sous-groupe de $\mathcal{G}_p$, donc : $V_l = \text{gr}(z) \subset H$.

Donc : $H = V_l$ ce qui est une contradiction.

On a montré que : $\forall k \in \mathbb{N}, H \not\subset V_k$.

b) Soit $k \in \mathbb{N}$ montrons que $V_k \subset H$.

On sait que $H \not\subset V_k$ donc il existe $z \in H \setminus V_k$.

On considère l'ensemble $A = \{j \in \mathbb{N} \mid z \in V_j\}$, A est une partie de $\mathbb{N}$, non vide car $z \in \mathcal{G}_p = \bigcup_{j \in \mathbb{N}} V_j$.

Donc : A a un plus petit élément l et $z \in V_l$.

Or : $z \notin V_k$ et la suite $(V_j)_{j \in \mathbb{N}}$ est strictement croissante, donc $l > k \geq 0$ et $V_k \subset V_l$.

Par définition de l , $z \in V_l \setminus V_{l-1}$,

donc, $V_l = \text{gr}(z) \subset H$.

Donc : $V_k \subset V_l \subset H$.

On a montré que :

$\forall k \in \mathbb{N}, V_k \subset H$.

c) On sait que $\mathcal{G}_p = \bigcup_{k \in \mathbb{N}} V_k$, donc d'après la question précédente : $H = \mathcal{G}_p$.

Donc les sous-groupes de $\mathcal{G}_p$ sont : les V_k , avec $k \in \mathbb{N}$ et $\mathcal{G}_p$; de plus les V_k sont cycliques et aucun d'entre eux n'est maximal pour l'inclusion car la suite $(V_k)_{k \in \mathbb{N}}$ est strictement croissante.

Conclusion :

les sous-groupes propres de $\mathcal{G}_p$ sont les V_k avec $k \in \mathbb{N}^*$, ils sont cycliques et aucun d'entre eux n'est maximal.

5. Soit $F = \{z_1, \dots, z_n\}$ une partie finie de $\mathcal{G}_p$.

Pour tout $j \in \llbracket 1; n \rrbracket$, $z_j \in \mathcal{G}_p = \bigcup_{k \in \mathbb{N}} V_k$, donc il existe $k_j \in \mathbb{N}$ tel que $z_j \in V_{k_j}$.

On pose $K = \max_{j \in \llbracket 0; n \rrbracket} k_j$.

La suite $(V_k)_{k \in \mathbb{N}}$ est strictement croissante,

donc : $\forall j \in \llbracket 1; n \rrbracket, z_j \in V_K$.

Or : V_K est un sous-groupe propre de $\mathcal{G}_p$,

donc : $\text{gr}(F) \subset V_K$ et $\text{gr}(F) \neq \mathcal{G}_p$.

Conclusion :

$\mathcal{G}_p$ n'est pas engendré par une partie finie.