On reprends les notations du cours. En particulier,

$$G = \{e, -e, \alpha, -\alpha, \beta, -\beta, \gamma, -\gamma\} \subset \mathrm{SL}(2, \mathbb{C})$$

avec

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \beta = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \gamma = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Montrer que $G =< \alpha, \gamma >$.

Proof. — Notons $H =< \alpha, \gamma >$ le sous-groupe engendré par α et γ. Par définition, on a

$$H = \{\alpha^{e_1}\gamma^{f_1} \cdots \alpha^{e_n}\gamma^{f_n} \ : \ n \in \mathbb{Z}_{\geq 1}, \text{ et } e_k \ f_k \in \{0, +1, -1\} \text{ pour } 1 \leq k \leq n \ \}$$

Par suite, H contient le sous-ensemble suivant

$$H_1 := \{\alpha^k \gamma^\ell \ : \ k, \ell \in \mathbb{Z}\} \subset H.$$

Montrons que $H_1 \subset G$ est un sous-groupe. En effet, premièrement, on a $H_1 \neq \emptyset$ car il contient au moins α et γ. Ensuite, il suffit de démontrer

$$\forall \ x = \alpha^k \gamma^\ell \in H_1, \quad \forall \ y = \alpha^s \gamma^t \in H_1$$

on a $x \cdot y^{-1} \in H_1$. Or

$$x \cdot y^{-1} = \alpha^k \cdot \gamma^\ell \cdot \left(\alpha^s \cdot \gamma^t\right)^{-1} = \alpha^k \cdot \gamma^\ell \cdot \gamma^{-t} \cdot \alpha^{-s} = \alpha^k \cdot \gamma^{\ell - t} \cdot \alpha^{-s}.$$

Par suite, pour prouver $x \cdot y^{-1} \in H_1$, il suffit de prouver qu'il existe des entiers $j', r' \in \mathbb{Z}$ tels que

$$\gamma^j \cdot \alpha^r = \alpha^{r'} \cdot \gamma^{j'}. \qquad (*)$$

Comme $\alpha^2 = \gamma^2 = -e$. Il y a deux cas à distinguer:

- si $r = 2r_0$ est un entier pair, on a $\gamma^j \alpha^r = \gamma^j (\alpha^2)^{r_0} = \gamma^j \gamma^{2r_0} = \gamma^{j+r}$.
- Si $r = 2r_0 + 1$ est impair. On a $\gamma^j \alpha^r = \gamma^j \alpha^{2r_0} \alpha = \gamma^{j+2r_0} \alpha$. D'autre part, comme $\gamma\alpha = -\alpha\gamma = \alpha \cdot \gamma \cdot (-e) = \alpha \cdot \gamma \cdot \gamma^2 = \alpha \cdot \gamma^3$, on obtient

$$\begin{aligned} \gamma^j \alpha^r &= \gamma^{j+2r_0}\alpha = \gamma^{j+2r_0-1}\gamma\alpha = \gamma^{j+2r_0-1}\alpha\gamma^3 = \gamma^{j+2r_0-2}\gamma\alpha\gamma^3 \\ &= \gamma^{j+2r_0-2}\alpha\gamma^3\gamma^3 = \gamma^{j+2r_0-2}\alpha\gamma^6 = \cdots = \alpha\gamma^{3(j+2r_0)} \end{aligned}$$

L'assertion $(*)$ est donc démontrée. Ainsi, on montre que $H_1 \subset G$ est un sous-groupe. Comme H_1 contient également α, γ, par conséquent $< \alpha, \gamma > \subset H_1$. Donc $H = H_1$. Comme α est d'ordre 4, et comme $\gamma^2 = \alpha^2$, on obtient que

$$\begin{aligned} H = \{\alpha^k\gamma^\ell : k, \ell \in \mathbb{Z}\} &= \{\alpha^k\gamma^\ell : 0 \leq k \leq 3, 0 \leq \ell \leq 1\} \\ &= \{e, \alpha, \alpha^2, \alpha^3\} \cup \{\gamma, \alpha\gamma, \alpha^2\gamma, \alpha^3\gamma\} \end{aligned}$$

Comme $\gamma \notin \{e, \alpha, \alpha^2, \alpha^3\}$, l'union ci-dessus est disjointe. Il en résulte que le cardinal de H est égal à 8. Donc $H \subset G$ est un sous-groupe d'ordre 8, et on obtient finalement $H = G$. $\square$