Proposition 1. *Soit $n \geq 2$. Soient $\gamma, \gamma' \in \mathfrak{S}_n$ deux cycles de supports disjoints. Notons ω, ω' les ordres de γ, γ', et Ω l'ordre de $\gamma\gamma'$. Alors,*

$$\Omega = \omega \vee \omega'$$

Avant de faire la démonstration, prenons un exemple. Soient $\gamma = (1\ 2)$ et $\gamma' = (3\ 4\ 5)$. Posons $\sigma = \gamma\gamma'$. Par la proposition, l'ordre de σ est 6. Voici les puissances de σ.

k	0	1	2	3	4	5	6
σ^k	id	$(1\ 2)(3\ 4\ 5)$	$(3\ 5\ 4)$	$(1\ 2)$	$(3\ 4\ 5)$	$(1\ 2)(3\ 5\ 4)$	id

Une fois sur deux, la transposition $(1\ 2)$ « disparaît », puisqu'elle est d'ordre 2. Une fois sur trois, le 3-cycle « disparaît », puisqu'il est d'ordre 3.

On rappelle la propriété essentielle suivante, que nous appellerons $(\mathcal{P})$: *si x est un élément d'un groupe $(G, \times)$ fini de neutre e alors, pour tout $k \in \mathbb{Z}$, $x^k = e$ si et seulement si l'ordre de x divise k.* La propriété $(\mathcal{P})$ sera utilisée 5 fois dans la preuve ci-dessous.

Démonstration. Remarquons tout d'abord que, comme les supports de γ et γ' sont disjoints, les deux cycles commutent et donc, pour tout $k \in \mathbb{Z}$, $(\gamma\gamma')^k = \gamma^k \gamma'^k$.

Étape 1 : $\Omega \mid \omega \vee \omega'$

Soit $k = \omega \vee \omega'$. k est un multiple de ω, donc, par $(\mathcal{P})$, $\gamma^k = id$. De même, $\gamma'^k = id$. Ainsi, $(\gamma\gamma')^k = id$. Il en résulte, par $(\mathcal{P})$, que Ω divise $\omega \vee \omega'$.

Étape 2 : $\omega \vee \omega' \mid \Omega$

Remarquons que $(\gamma\gamma')^\Omega = id$. Montrons que $\gamma^\Omega = \gamma'^\Omega = id$. Pour des raisons de symétrie, il suffit évidemment de faire la preuve pour γ. Donnons-nous $a \in [\![1, n]\!]$. Deux cas se présentent.

- Si $a \notin \operatorname{supp} \gamma$ alors $\gamma(a) = a$ et, a fortiori, $\gamma^\Omega(a) = a$.
- Si $a \in \operatorname{supp} \gamma$ alors, comme γ et γ' ont des supports disjoints, $a \notin \operatorname{supp} \gamma'$. Ainsi, $\gamma'(a) = a$. De là,

$$a = id(a) = \gamma^\Omega(\gamma'^\Omega(a)) = \gamma^\Omega(a)$$

Ainsi, pour tout $a \in [\![1, n]\!]$, $\gamma^\Omega(a) = a$. En conséquence, $\gamma^\Omega = id$. De même, $\gamma'^\Omega = id$.

Par $(\mathcal{P})$, on en déduit que Ω est un multiple de l'ordre de γ et de celui de γ', donc Ω est un multiple de $\omega \vee \omega'$. $\square$