Proof. Observe that $e(1) = e(1^2) = (e(1))^2$, so $e(1)$ is either 0 or 1. In the former case, for all $x \in G$, $e(x) = e(1 \cdot x) = e(1)e(x) = 0$, so e is identically 0.

Otherwise, pick any $y \in G$ and consider the sequence $1, y, y^2, y^3, \ldots$. Since G is finite, the sequence has a cycle and we can find $0 \leq i < N$ and the smallest $0 < n$ such that $y^i = y^{i+n}$, implying that $y^n = 1$ and the cycle has length n. Therefore, Y generates the set $y = \{1, y, y^2, \ldots, y^{n-1}\}$, which is a subgroup of G of order n.

Define an equivalence relation for all $x, x' \in G$ by $x \sim x'$ if there exists $y \in Y$ such that $x = yx'$. Reflexivity and symmetry are easy to see. To show transitivity, pick $x, x', x'' \in G$ such that $x \sim x'$ and $x' \sim x''$. Then there exist $y, y' \in Y$ such that $x = yx'$ and $x' = y'x''$, implying that $x = (yy')x''$.

We now show that each equivalence class has exactly n members. For all $x \in X$ and $y, y' \in Y$ we have that $yx = y'x$ implies $y = y'$. Since $1, y, \ldots, y^{n-1}$ are unique, the equivalence class of x is $\{x, yx, y^2x, \ldots, y^{n-1}x\}$, which has cardinality n.

We have thus partitioned G into equivalence classes of cardinality n, which is only possible if $n|N$. Then $(e(y))^N = e(y^N) = e(y^{N \bmod n}) = e(1) = 1$. Thus, $e(y)$ is an N^{th} root of unity and has the form

$$e(y) = \exp\left(2\pi i \frac{r}{N}\right)$$

for some $r \in \{0, 1, \ldots, N-1\}$. $\square$