In this note we give what is probably the shortest proof of Cauchy’s theorem. This proof is due to James McKay and uses the notion of group actions. The proof appeared in the American Mathematical Monthly in 1959.

**Theorem 1.** Let $G$ be a finite group and suppose a prime $p$ divides $|G|$. Then $G$ has an element of order $p$.

**Proof.** Set $n = |G|$. Let $$X = \{(g_1, \ldots, g_p) : g_1g_2\cdots g_p = e\}.$$ Then $|X| = n^{p-1}$ because $$X = \{(g_1, \ldots, g_{p-1}, (g_{p-1}|\cdots|g_1)^{-1}) : g_1, \ldots, g_{p-1} \in G\}$$ which shows that the first $p-1$ entries of an element of $X$ can be chosen arbitrarily, and the last component is then determined. In particular, $p$ divides $|X|$. Note that if $(g_1, \ldots, g_p) \in X$, then $g_1 \cdots g_p = e$. Conjugating by $g_1^{-1}$ gives $g_2 \cdots g_p g_1 = e$, so $(g_2, \ldots, g_p, g_1) \in X$. What this means is that the function $\sigma : X \to X$, defined by $\sigma(g_1, \ldots, g_p) = (g_2, \ldots, g_p, g_1)$ is a well-defined function. It is a permutation, since the function sending $(g_1, g_2, \ldots, g_p)$ to $(g_p, g_1, \ldots, g_{p-1})$ is the inverse of $\sigma$. Furthermore, $\sigma^p = id$, so we have a group homomorphism $\mathbb{Z}_p \to \text{Perm}(X)$ given by sending $\tau$ to $\sigma^r$. This amounts to having a group action of $\mathbb{Z}_p$ on $X$ which satisfies $\tau \cdot (g_1, \ldots, g_p) = (g_2, \ldots, g_p, g_1)$.

Because we have a group action, $X$ is the disjoint union of the various orbits of the action. If $x \in X$, then its stabilizer is a subgroup of $\mathbb{Z}_p$, which means it is either the entire group or the identity, by Lagrange’s theorem. If the stabilizer is $\mathbb{Z}_p$, then $x = (g, g, \ldots, g)$ for some $g \in G$, and so the orbit contains only one element. Note that $(e, e, \ldots, e)$ is such an element. If the stabilizer is the identity, then $|O(x)| = p$, the index of the stabilizer in $\mathbb{Z}_p$. Let $r$ be the number of orbits with $p$ elements and $s$ the number of orbits with 1 element. Then, since $X$ is the disjoint union of its orbits, we have $|X| = rp + s$. Consequently, as $p$ divides $|X|$, we see that $p$ divides $s$. Because $s \geq 1$ since there is at least one orbit with a single element, namely $\{(e, e, \ldots, e)\}$, we must have $s \geq p \geq 2$. This means there are at least 2 elements of $X$ with stabilizer $\mathbb{Z}_p$. Such an element has the form $(g, g, \ldots, g)$ for some $g \in G$. Therefore, there is $(g, g, \ldots, g) \in X$ with $g \neq e$. Since $(g, g, \ldots, g) \in X$, we have $g^p = e$. This proves that $G$ has an element of order $p$. 

\[\square\]