

A PROOF OF CAUCHY'S THEOREM

We give McKay's clever proof of Cauchy's theorem.

Lemma. *Let p be a prime number, and let G be a p -group (a finite group of order p^k for some $k \geq 1$) acting on a finite set S . Let Fix be the set of fixed points of the action (i.e., $\text{Fix} = \{x \in S : g \cdot x = x \ \forall g \in G\}$). Then*

$$|\text{Fix}| \equiv |S| \pmod{p}.$$

Proof. Let x_1, \dots, x_t represent the different orbits. Then

$$x_i \in \text{Fix} \iff G \cdot x_i = \{x_i\}.$$

Also, $|G \cdot x_i| = [G : G_{x_i}]$ divides $|G| = p^k$, so it is either 1 (if x_i is a fixed point) or a power of p (otherwise). Since the orbits partition G , we have

$$|S| = \sum_{i=1}^t [G : G_{x_i}] \equiv |\text{Fix}| \pmod{p}.$$

□

Theorem (Cauchy). *If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p (and therefore a subgroup of order p as well).*

Proof. Let

$$S = \{(x_1, x_2, \dots, x_p) : x_i \in G, x_1 x_2 \cdots x_p = 1\}.$$

Then $|S| = |G|^{p-1}$. The group $\mathbf{Z}/p\mathbf{Z}$ acts on S by cyclically right-shifting the indices of the x_i 's. If F denotes the number of fixed points of this action, then $F \equiv |G|^{p-1} \equiv 0 \pmod{p}$ by the Lemma. Since $(1, 1, \dots, 1)$ is fixed, there must be at least $p - 1$ other fixed points. All fixed points are of the form (x, x, \dots, x) with $x \in G$ and $x^p = 1$. Taking any $x \neq 1$ in Fix , we have $|x| = p$ and we're done. □