**Prof. Alexandru Suciu**

**MATH 3175** **Group Theory** **Summer 2, 2022**

# A problem on prime order normal subgroups

---

**Problem.** Let $G$ be a finite group and let $N$ be a normal subgroup of prime order $p$ with $\gcd(|G|, p-1) = 1$. Show that $N \subseteq Z(G)$.

*Proof.* Since $|N| = p > 1$, there is an element $x \in N$ with $x \neq e$. Since $N$ is a subgroup, the whole cyclic subgroup generated by $x$ must be contained in $N$, that is, $\langle x \rangle \leq N$. Hence, by Lagrange's theorem, $|\langle x \rangle|$ must divide $|N| = p$. Since $p$ is prime and $|\langle x \rangle| \neq 1$ (because $x \neq e$), we must have $|\langle x \rangle| = p$. Therefore,

$$N = \langle x \rangle = \{e, x, x^2, \dots, x^{p-1}\}. \tag{1}$$

Now, since $N$ is a *normal* subgroup, $N$ is a union of conjugacy classes (in $G$). One such conjugacy class is $\{e\}$. Let

$$C \coloneqq \mathrm{Cl}(x) = \{gxg^{-1} : g \in G\} \tag{2}$$

be the conjugacy class of $x$ in $G$. Then $x \in C \subset N$, but $e \notin C$. Thus,

$$1 \leq |C| \leq p - 1. \tag{3}$$

**Claim.** $|C| = 1$.

*Proof of Claim.* Suppose $|C| > 1$. Then there is a $y \in C$ with $y \neq x$. But $C \subset N = \langle x \rangle$, and so $y = x^k$, for some $k \geq 0$ with $k \neq 0$ (since $y \neq e$), $k \neq 1$ (since $y \neq x$), and $k < p$ (since $\mathrm{ord}(x) = |\langle x \rangle| = p$). To sum up, there is an element $g \in G$ and an integer $k$ with $1 < k < p$ such that

$$gxg^{-1} = x^k. \tag{4}$$

Conjugating again by $g$, we get $g^2xg^{-2} = gx^kg^{-1} = (gxg^{-1})^k = (x^k)^k = x^{k^2}$. Proceeding in like manner, we get $g^\ell x g^{-\ell} = x^{k^\ell}$, for all $\ell \geq 0$. Hence, all these elements are conjugate to $x$, i.e.,

$$\{x, x^k, x^{k^2}, \dots, x^{k^{p-2}}\} \subseteq C. \tag{5}$$

Now note that all the elements in the list on the left side of (5) are distinct, since $\mathrm{ord}(x^k) = p$. But there are $p-1$ elements in this list, and so $p - 1 \leq |C|$. Since we also know from (3) that $|C| \leq p-1$, we infer that

$$|C| = p - 1. \tag{6}$$

On the other hand, we also know from the theory leading to the Class Equation that $C$ is in bijection with $G/C(x)$, and thus, by Lagrange's Theorem,

$$|C| \mid |G|. \tag{7}$$

Putting together (6) and (7), we conclude that $|C|$ divides both $|G|$ and $p-1$, and thus $|C|$ divides the gcd of $|G|$ and $p-1$. But, by the hypothesis of the problem, $\gcd(|G|, p-1) = 1$. This contradicts our supposition that $|C| > 1$, and so the claim is proved. □

From the claim just proved, we get that $\mathrm{Cl}(x) = \{x\}$, which is equivalent to $x \in Z(G)$. Since $Z(G)$ is a subgroup of $G$, we must also have $\langle x \rangle \subset Z(G)$. But we also know that $N = \langle x \rangle$, and so we have proved that $N \subset Z(G)$. □