

Problem 2.5 #52 from the Herstein text is very interesting—the statement of the problem is unexpected, and the proof is neat. Below I give hints for working through the problem in steps.

2.5 #52. Let G be a group and $\varphi: G \rightarrow G$ an automorphism of G such that $\varphi(x) = x^{-1}$ for *more than three-fourths* of the elements of G . Prove that $\varphi(y) = y^{-1}$ for *every* $y \in G$ (and use this to show that G is abelian).

Setup. Define

$$S = \{z \in G : \varphi(z) = z^{-1}\}.$$

Our given information is that $|S| > \frac{3}{4}|G|$. (The dihedral group can be used to give an example that shows that *greater than* $\frac{3}{4}$ is essential to this problem!)

Fix $x \in S$ and define the *centralizer of x* to be

$$C(x) = \{y \in G : xy = yx\}.$$

That is, the centralizer of x is the set of elements that commute *with* x . Our ultimate goal is to prove that $C(x) = G$.

Since the translation operators are bijections, we know that the set

$$x^{-1}S = \{x^{-1}z : z \in S\}$$

has exactly the same number of elements as S . If S was a subgroup then $x^{-1}S$ would be a left coset of S . Now, we don't know that S is a subgroup, it is still true that $x^{-1}S$ has exactly the same number of elements as S .

Step 1. Prove that

$$\forall x, y \in S, \quad xy \in S \iff xy = yx. \tag{1}$$

Then use this to prove that

$$S \cap C(x) = S \cap x^{-1}S.$$

Step 2. Show that $S \cap x^{-1}S$ has *more than half* of the elements of G . (Just think about it—both S and $x^{-1}S$ have more than $3/4$ of the elements, so how much overlap must there be between them?)

Step 3. Show that $C(x) = G$. (Remember, $C(x)$ is a subgroup and the order of a subgroup must divide the order of G .)

Step 4. Prove that $e \in S$ and S is closed under inverses.

Step 5. We need to prove that S is closed under products, for then we have shown that is a subgroup of G that contains more than $3/4$ of the elements of G . Since the order of a subgroup divides the order of the group, this implies that $S = G$ and finishes the proof.

To prove that S is closed under products, suppose that $x, y \in S$. Then $y \in G = C(x)$, so $xy = yx$. But then equation (1) above shows that $y \in S$!