

Here is a quick run-through on problem #23 in §1.6. Following the hint, I want to establish the surjectivity of the map $x \mapsto x^{-1}\sigma(x)$ from G to G . Since G is finite, the map is surjective if and only if it is injective. For injectivity, we have to examine the condition $x^{-1}\sigma(x) = y^{-1}\sigma(y)$. This unravels to read $yx^{-1} = \sigma(y)\sigma(x)^{-1}$, but the right-hand side is $\sigma(yx^{-1})$. By hypothesis, σ fixes only the identity. Accordingly, if $x^{-1}\sigma(x) = y^{-1}\sigma(y)$, then yx^{-1} is the identity, meaning that $y = x$. Thus $x \mapsto x^{-1}\sigma(x)$ is indeed injective, and it follows that it is surjective as well because of the finiteness of G . Now σ sends $x^{-1}\sigma(x)$ to $\sigma(x)^{-1}x$ because σ is an automorphism and $\sigma \circ \sigma$ is the identity. In other words, σ sends elements of the form $x^{-1}\sigma(x)$ to their inverses. Since all elements of G are in fact of this form (by the discussion that began this proof), the automorphism σ is simply the inversion map $g \mapsto g^{-1}$ on G .

The final point is that the inversion map is an automorphism precisely when it is compatible with multiplication in the sense that $(tu)^{-1} = t^{-1}u^{-1}$ for all $t, u \in G$. This equation may be written as the statement that t and u commute with each other. Hence if inversion is an automorphism, G is abelian. (Elements of G commute with each other.) Since σ is an automorphism that turns out to be inversion, G is necessarily abelian.