POW 2019-14

2016____ Chae Jiseok

September 30, 2019

Let S be a finite set such that $G = \langle S \rangle$. For convenience, for a group H given, we denote the identity element of H as e_H. Since G is residually finite, there exists a finite group K such that there exists a surjective homomorphism $\rho : G \to K$ such that if $g \neq e_G$ then $\rho(g) \neq e_K$. We begin by claiming the following.

Claim 1. *There can exist at most finitely many homomorphisms from* G *to* K.

Proof. Since G is generated by S, for any mapping $\Phi : S \to K$, there exists at most one homomorphism $\varphi : G \to K$ such that $\varphi|_S = \Phi$. Conversely, if a homomorphism $\varphi : G \to K$ is given, the restriction $\varphi|_S$ is uniquely determined. Therefore the number of homomorphisms from G to K is bounded by the number of functions from S to K. However both $|S|$ and $|K|$ are finite, which implies that $\left|K^S\right| < \infty$. It follows that the number of homomorphisms from G to K is also finite. □

Let $\psi : G \to G$ be a surjective homomorphism. For the sake of contradiction, suppose ψ is not injective. Then $\ker \psi \neq \{e_G\}$, so there exists $g \in G$ such that $g \neq e_G$ but $\psi(g) = e_G$. For any two positive integers m and n, without loss of generality assume that $m < n$, and consider two homomorphisms $\rho \circ \psi^m$ and $\rho \circ \psi^n$, both from G to K. Since ψ is surjective, and compositions of surjective functions are surjective, there exits $h \in G$ such that $\psi^m(h) = g$. Then from the property of ρ, we have $(\rho \circ \psi^m)(g) \neq e_K$. On the other hand, from $m < n$ we must have $\psi^n(h) = e_G$, hence $(\rho \circ \psi^n)(g) = e_K$. This shows that if $m < n$, then $\rho \circ \psi^m \neq \rho \circ \psi^n$. Henceforth for each $j = 1, 2, 3, \cdots$ we get distinct homomorphisms from G to K, namely $\rho \circ \psi^j$. However this contradicts our observation from the claim that there can exist at most finitely many homomorphisms from G to K. Hence our assumption that ϕ is not injective must be false. This shows that any surjective homomorhpism from G to itself must be also injective.

A surjective homomorphism which is also an injection is an isomorphism. Therefore any surjective homomorphism from G to itself is an isomorphism.