Functions Composition & Permutation Groups

October 3, 2022

Theorem 1 *The group identity element is unique.*

Proof (by contradiction)

Assume there are two identities e_1, e_2 with $e_1 \neq e_2$. Then,

$$e_2 = e_1 * e_2 = e_1$$

Theorem 2 *Every element in a group has a unique inverse.*

Proof (by contradiction)

Suppose x has two distinct inverses y and z. Then,

$$x * y = y * x = x * z = z * x = e$$

Thus,

$$x * y = z * x$$

Premultiplying both sides by z, and using associativity, we get

$$(z * x) * y = z * (z * x)$$

This simplifies to

$$e * y = z * e$$

or

$$y = z$$

Theorem 3 *Group equations have unique solutions. That is $g_1 * x = g_2$ has exactly one solution (not more, nor less) where x is unknown and g_1 and g_2 are two known elements of the group (possibly equal).*

left multiplying both sides by g_1^{-1} and using associativity, we get,

$$x = g_1^{-1} * g_2$$