Pf: Assume G is finite. Then G has K elements $\{g_1, g_2, \ldots, g_K\}$. If $g \in G$, then

$g \cdot g_i = g_j \quad \forall\, i,\ 1 \le i \le K$ and some $j,\ 1 \le j \le K$

If $i_1 \neq i_2$ then if $g \cdot g_{i_1} = g \cdot g_{i_2}$,

multiply on the left by g^{-1} to get

$g_{i_1} = g_{i_2}$, contradiction.

Show: If $g g_{i_1} = g_{j_1}$ and $g g_{i_2} = g_{j_2}$

then $j_1 = j_2$ iff $i_1 = i_2$.

permutation $j \mapsto i$

2/17/11

If $g \in G$, define $\sigma : G \to S_K$

$\sigma(g)(i) = j$ iff $g \cdot g_i = g_j$ $(\forall\, i,j \in \{1, 2 \ldots k\})$

For brevity, write $\sigma(g) = \sigma_g$

Check:

σ is well defined; ie. σ_g is a bijection on $\{1, 2 \ldots k\}$

Injectivity suppose $i, j \in \{1, 2 \ldots k\}$ and $\sigma_g(i) = \sigma_g(j)$ This means $g \cdot g_i = g \cdot g_j$

multiply on the left by g^{-1}

Then $g_i = g_j$ so $i = j$

Surjectivity suppose $j \in \{1, 2 \ldots k\}$. want to find $i \in \{1, 2 \ldots k\} \ni \sigma_g(i) = j$

$\sigma_g(i) = j$ iff $g \cdot g_i = g_j$

Set $g_i = g^{-1} \cdot g_j$. Since $G = \{g_1, g_2 \ldots g_K\}$

$g^{-1} \cdot g_j \in \{g_1, g_2 \ldots g_K\}$

$g \cdot g_i = g \cdot (g^{-1} \cdot g_j) = (g \cdot g^{-1}) \cdot g_j = e_G \cdot g_j = g_j$

Hence $\sigma_g(i) = j$

We now want to show:

1) $\sigma(G)$ is a subgroup of S_K

2) $\sigma : G \to \sigma(G)$ is an isomorphism.

$\rightarrow$

continuation of proof:

1) We need to show, for $g,h \in G$

a) $(\sigma_g)^{-1} \in \sigma(G)$

b) $\sigma_g \sigma_h \in \sigma(G)$

we'll show $(\sigma_g)^{-1} = \sigma_{g^{-1}}$ and $\sigma_g \sigma_h = \sigma_{gh}$

let $i,j \in \{1,2,\dots k\}$

a) Suppose $(\sigma_g)^{-1}(i) = j$. Applying σ_g to both sides, $i = \sigma_g(j)$. This happens iff $g \cdot g_j = g_i$. Apply g^{-1} (on the left) to both sides, $g_j = (g^{-1}) \cdot g_i$. This implies $\sigma_{g^{-1}}(i) = j$ hence $\forall i \in \{1,2 \dots k\}$ $\sigma_{g^{-1}}(i) = (\sigma_g)^{-1}(i)$. so, $\sigma_{g^{-1}} = (\sigma_g)^{-1}$

b) let $g,h \in G$. consider $\sigma_g(\sigma_h(i)) = (\sigma_g \cdot \sigma_h)(i)$

$\sigma_h(i) = j$ iff $h \cdot g_i = g_j$. We have $\sigma_g(j) = m \in \{1,2 \dots k\}$ iff $g \cdot g_j = g_m$.

We then have $(g \cdot h)(g_i) = g \cdot (h g_i) = g \cdot g_j = g_m$. Then $\sigma_{gh}(i) = m$ and $(\sigma_g \sigma_h)(i) = \sigma_g(j) = m$ Hence $\sigma_{gh} = \sigma_g \sigma_h$ $\forall g,h \in G$. We've shown:

$(\sigma_g)^{-1} = \sigma_{g^{-1}} \in \sigma(G)$ and $\sigma_g \sigma_h = \sigma_{gh} \in \sigma(G)$

so, $\sigma(G)$ is a subgroup of S_K.

2) Show $\sigma: G \to \sigma(G)$ is an isomorphism

a) σ is bijective

b) $\sigma(g \cdot h) = \sigma_g \sigma_h$

We've just shown b)

For a) surjectivity is immediate since we map into the image of σ. For injectivity suppose $\sigma_g = \sigma_h$ then $\sigma_g(i) = \sigma_h(i)$ $\forall i \in \{1,2 \dots k\}$

This implies $g \cdot g_i = h \cdot g_i$ $\forall i \in \{1,2 \dots k\}$

Choose i with $g_i = e_G$ Then $g = h$ ∎

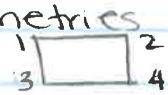
Ex: $\mathbb{Z}_3$ is isomorphic to a subgroup of S_3. But $\mathbb{Z}_3 \neq S_3$. $\mathbb{Z}_3$ is isomorphic to $\{e, (1\,2\,3)\,(1\,3\,2)\}$

Chapter 10

Order

<u>Def:</u> let G be a group. The <u>order</u> of G, denoted by $|G|$, is the number of elements in G.

<u>Remark:</u> If G has finitely many elements, the order of G is equal to its cardinality as a set. If G has infinitely many elements, we typically only write "$|G| = \infty$" for order (no cardinality distinction)

<u>Ex:</u> 1) $|\mathbb{Z}_n| = n$
2) $|S_n| = n!$
3) $|D_n| = 2n$ (n rotations, n reflections)
D_n = symmetries of a regular n-gon
D_4 = 

4) $U_n = \{ k \in \mathbb{Z}_n : \exists\, m \in \mathbb{Z}_n,\ m \cdot k = 1 \pmod{n} \}$
This is a group since the product of invertible elements is invertible
$|U_n| = \varphi(n)$ [Euler's totient function]
= the number of natural numbers that are both less than and relatively prime to n
check that $|U_5| = 4$ but, $|U_6| = 2$
one can show that U_n is isomorphic to $\mathrm{Aut}(\mathbb{Z}_n)$

<u>Def:</u> let $g \in G$. we define <u>order</u> of g, written $\mathrm{ord}(g)$, as $|\langle g \rangle|$. This is equal to the smallest natural number $n \in \mathbb{N}$ with $g^n = e_G$ and ∞ if no such n exists.

<u>Remark:</u> If $\Phi : G \to H$ is an isomorphism, then $\mathrm{ord}(g) = \mathrm{ord}(\Phi(g))\ \forall\, g \in G$