Proof con't:

Since φ is bijective, $\varphi(g)$ can be any element in H. Hence, for all $h \in H$, there is a $g \in G$ with $\varphi(g) = h$.

Rewriting we have,

$h = h * \varphi(e_G) * h$

By uniqueness, $\varphi(e_G) = e_H$

1/21/11

$f, g, h : X \to X$

$\forall x \in X$

$(f \circ (g \circ h))(x) = ((f \circ g) \circ (h))(x)$

$= (f \circ g)(h(x)) = f(g(h(x)))$

$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$

NEW MENTORING HOURS

2:45 - 4:00 MW

2063 CB

- Recall we were proving:

Proposition: If $\varphi : \langle G, \cdot \rangle \to \langle H, * \rangle$ is an isomorphism, then

- $\varphi(e_G) = e_H$
- $\varphi(g^{-1}) = \varphi(g)^{-1}$ $\forall g \in G$

$\rightarrow$

Pf: - (rehash of 1^{st} part)

Take $g \in G$. Recall that for all $g_1, g_2 \in G$, $\varphi(g_1 \cdot g_2) = \varphi(g_1) * \varphi(g_2)$. Then

$$\varphi(g \cdot e_G) = \varphi(g)$$
$$\Downarrow$$
$$\varphi(g) * \varphi(e_G)$$

Similarly,

$$\varphi(g) = \varphi(e_G \cdot g) = \varphi(e_G) * \varphi(g)$$

So, $\varphi(e_G) * \varphi(g) = \varphi(g) * \varphi(e_G) = \varphi(g)$

For each $h \in H$, since φ is bijective there is a unique element $g \in G$ with $\varphi(g) = h$. replace $\varphi(g)$ with h to obtain:

$$\varphi(e_G) * h = h * \varphi(e_G) = h \quad \forall\, h \in H$$

Therefore $\varphi(e_G)$ is the identity element of $\langle H, * \rangle$. Since identities of groups are unique, $\varphi(e_G) = e_H$.

- for all $g \in G$, $\varphi(g^{-1}) = \varphi(g)^{-1}$

we know that $g \cdot g^{-1} = e_G = g^{-1} \cdot g$

apply φ to this equality to get:

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

Since $\varphi(e_G) = e_H$,

$$\varphi(g \cdot g^{-1}) = e_H = \varphi(g^{-1} \cdot g)$$

Recall $\varphi(g \cdot g^{-1}) = \varphi(g) * \varphi(g^{-1})$

and $\varphi(g^{-1} \cdot g) = \varphi(g^{-1}) * \varphi(g)$

Then $\varphi(g) * \varphi(g^{-1}) = e_H = \varphi(g^{-1}) * \varphi(g)$

which implies that $\varphi(g^{-1})$ is the inverse of $\varphi(g)$

since inverses in groups are unique, $\varphi(g^{-1}) = \varphi(g)^{-1}$ ■

Remark: $\mathbb{Z}_n$ is isomorphic to the set $\{0, 1, 2, \cdots, n-1\}$ with the operation of addition modulo n. (will see proof later).

CHAPTER 5 SUBGROUPS

Alternate definition: Let $\langle G, \cdot \rangle$ be a group. Let $H \subseteq G$ be nonempty. H is a subgroup of G if H is a group with the same identity and operation of $\langle G, \cdot \rangle$.

ex: let $S \subset M_3(\mathbb{C})$

$$S = \left\{ \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix} : a, b, c, d \in \mathbb{C} \right\}$$

Suppose we take the further subset of elements of S with $ad - bc \neq 0$, call the subset H.

Declare the identity of H to be:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} = e$$

for all $h = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix}$ $\quad eh = he = h$

The inverse of h is

$$\frac{1}{ad-bc} \begin{pmatrix} d & -b & 0 \\ -c & a & 0 \\ 0 & 0 & 0 \end{pmatrix} \in H$$

However, H is not a subgroup of invertible 3×3 matrices with complex entries, since

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \notin H$$

Remarks:

1) $\emptyset \neq H$

2) The following definition, used in the book, is equivalent:

$H \subseteq G$ is a subgroup iff $\forall g, h \in H$,
- $g^{-1} \in H$
- $g \cdot h \in H$

3) Notation. If H is a subgroup of $\langle G, \cdot \rangle$ write $H \leq G$

4) If $H \leq G$ and $H \neq G$, write $H < G$; we say that H is a proper subgroup of G

Examples:

1) $\{a + b\sqrt{17} : a, b \in \mathbb{Q}\} \setminus \{0\} =: H$ is a subgroup of $\langle \mathbb{R} \setminus \{0\}, \cdot \rangle$. (on 1st homework)

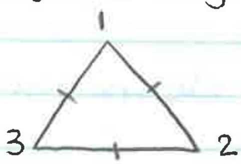
2) If $\langle G, \cdot \rangle$ and $\langle H, * \rangle$ are groups, recall the construction of the direct product $G \times H$.

If e_G and e_H are the identities of $\langle G, \cdot \rangle$ and $\langle H, * \rangle$ respectively, Then
$G \times \{e_H\}$ and $\{e_G\} \times H$ are subgroups of $G \times H$

Remark: $G \times \{e_H\}$ is isomorphic to $\langle G, \cdot \rangle$ and $\{e_G\} \times H$ is isomorphic to $\langle H, * \rangle$.

$\rightarrow$

3) Recall D_3 is the symmetry group of an equilateral triangle



D_3 has a subgroup H consisting of the identity (no movement) and rotation by $120°$ and $240°$. This is a 3 element subgroup.

If $g =$ rotation by $120°$ and $h =$ rotation by $240°$ then $g = h^{-1}$. In particular, $gh =$ identity, so H is a subgroup of D_3. H is isomorphic to $\mathbb{Z}_3$. $H \triangleleft D_3$ since H only contains rotations, not reflections.

4) Heisenburg Group

$G \subseteq M_3(\mathbb{R})$

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$$

with operation of matrix multiplication

Fun! Check that G is a group and that

$$H = \left\{ \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : a \in \mathbb{R} \right.$$

is a subgroup.