Definition:

An isomorphism from a group to itself is called an **automorphism**.

Example:

$$\begin{aligned}
\phi_A\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) &= A \begin{bmatrix} a & b \\ c & d \end{bmatrix} A^{-1} \\
&= \left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) \cdot \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \\
&= \left(\begin{bmatrix} a+c & b+d \\ c & d \end{bmatrix}\right) \cdot \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} a+c & (b+d)-(a+c) \\ c & d-c \end{bmatrix}
\end{aligned}$$

In Class Work

1. Let $\mathbb{R}^+$ be the group of positive real numbers under multiplication. Show that the mapping $\phi(x) = \sqrt{x}$ is an automorphism of $\mathbb{R}^+$.

2. Find Aut($\mathbb{Z}$).

   Hint: It may be helpful to remember that $\mathbb{Z} =< 1 >$.

3. Let $r \in U(n)$. Prove that the mapping $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ defined by $\alpha(s) = sr$ mod n for all s in Z_n is an automorphism of $\mathbb{Z}_n$

Solutions

1. Let $\mathbb{R}^+$ be the group of positive real numbers under multiplication. Show that the mapping $\phi(x) = \sqrt{x}$ is an automorphism of $\mathbb{R}^+$.

- **well-defined?** $x = y \implies \sqrt{x} = \sqrt{y}$.
- **1-1?** $\phi(x) = \phi(y) \implies \sqrt{x} = \sqrt{y} \implies (\sqrt{x})^2 = (\sqrt{y})^2 \implies x = y$.
- **onto?** Let $y \in \mathbb{R}^+$. NTS $\exists x \in \mathbb{R}^+$ such that $\phi(x) = y$. That is, NTS $\exists x \in \mathbb{R}^+$ such that $\sqrt{x} = y$. Choose $x = y^2$. Then $\phi(x) = \sqrt{y^2} = y$ (since y positive)
- **operation preserving?** $\phi(xy) = \sqrt{xy} = \sqrt{x}\sqrt{y} = \phi(x)\phi(y)$.

Thus ϕ is indeed an automorphism of $\mathbb{R}^+$.

Solutions

2. Find Aut($\mathbb{Z}$).

Let $\phi : \mathbb{Z} \to \mathbb{Z}$ be any automorphism on $\mathbb{Z}$.

$\mathbb{Z}$ is of course cyclic, generated by 1.

Property 4, Thm 6.2 $\Longrightarrow \phi(1)$ must also generate $\mathbb{Z}$.

From hw, you know $\mathbb{Z} =< 1 >=< -1 >$; no other generators

Thus $\phi(1)$ must be either 1 or -1.

- **Case 1:** $\phi(1) = 1$. Then for all $n \in \mathbb{Z}$,

  $$\phi(n) = \phi(n \cdot 1) = \phi(\text{“}1^n\text{”}) = \text{“}[\phi(1)]^n\text{”} = n \cdot \phi(1) = n.$$

  Since $\phi(n) = n$ for all $n \in \mathbb{Z}$, ϕ is the identity function.

- **Case 2:** $\phi(1) = -1$. Then for all $n \in \mathbb{Z}$,

  $$\phi(n) = \phi(n \cdot 1) = n \cdot \phi(1) = -n.$$

Thus Aut($\mathbb{Z}$) $= \{id, f\}$, where f is the function that sends every element to its inverse.

Solutions

3. Let $r \in U(n)$. Prove that the mapping $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ defined by $\alpha(s) = sr \mod n$ for all s in Z_n is an automorphism of $\mathbb{Z}_n$

- **well-defined?**

$$s = t \mod n \Longrightarrow sr \mod n = tr \mod n.$$

- **1-1?**

$$\begin{aligned} \alpha(s) = \alpha(t) &\Longrightarrow sr \mod n = tr \mod n \\ &\Longrightarrow n|(sr - tr) \\ &\Longrightarrow n|(s-t)r. \end{aligned}$$

Since $r \in U(n)$, we know that $gcd(n, r) = 1$, and so if $n|(s-t)r$, we must have that $n|s - t$, and so $s = t \mod n$.

Solutions

3. (continued)

- **onto?** Let $y \in \mathbb{Z}_n$. NTS $\exists x \in \mathbb{Z}_n$ such that $\alpha(x) = y$. That is, NTS $\exists x \in \mathbb{Z}_n$ such that $xr = y \mod n$.

$$\begin{aligned} gcd(n,r) = 1 &\implies \exists a,b \in \mathbb{Z} \text{ such that } an + br = 1 \\ &\implies \exists a,b \in \mathbb{Z} \text{ such that } (ya)n + (yb)r = y \\ &\implies \exists a,b \in \mathbb{Z} \text{ such that } (yb)r = y \mod n \end{aligned}$$

  Let $x = yb \mod n$. Then $\alpha(x) = (yb \mod n)r = y \mod n$, so α is onto.

- **operation-preserving?**

  Let $a, b \in \mathbb{Z}_n$.

  $\alpha(a+b \mod n) = (a+b \mod n)r = ar+br \mod n = \alpha(a)+\alpha(b)$.

Thus α is indeed an automorphism of $\mathbb{Z}_n$.