HW4 MTH 450/550 Fall 2023 ①

p.36 #26 | Solved in Exam 1

p.36 #27 | If $\phi: S \to S'$ is an isomorphism between $\langle S, * \rangle$ and $\langle S', *' \rangle$
and $\psi: S' \to S''$ ——— $\langle S', *' \rangle$ and $\langle S'', *'' \rangle$,
then $\psi \circ \phi: S \to S''$ is an isomorphism between $\langle S, * \rangle$ and $\langle S'', *'' \rangle$.

Proof: Need to show that $\psi \circ \phi$ is 1-1, onto, and preserves structure.

1-1 | Let $(\psi \circ \phi)(x) = (\psi \circ \phi)(y)$

$$\downarrow \text{def of } \circ$$

$$\psi(\phi(x)) = \psi(\phi(y))$$

Since ψ is 1-1, we conclude that

$$\phi(x) = \phi(y).$$

Since ϕ is 1-1, we conclude $x = y$, completing the proof. □

onto | Let $z \in S''$. Since ψ is onto, $\exists\, a \in S'$ so that

$$\psi(a) = z$$

Since ϕ is onto, $\exists\, b \in S$ so that $\phi(b) = a$.

Thus $(\psi \circ \phi)(b) = \psi(\phi(b)) = \psi(a) = z$, completing the proof. □

structure-preserving |

$$(\psi \circ \phi)(x * y) = \psi(\phi(x * y)) \underset{\substack{\uparrow \\ \phi \text{ is} \\ \text{str. pres.}}}{=} \psi(\phi(x) *' \phi(y)) \underset{\substack{\uparrow \\ \psi \text{ is} \\ \text{str. pres.}}}{=} \psi(\phi(x)) *'' \psi(\phi(y))$$

$$= (\psi \circ \phi)(x) *'' (\psi \circ \phi)(y),$$

completing the proof that $\psi \circ \phi: S \to S''$ is an isomorphism. ■

p.45 | #1 | $\mathcal{G}_1$ holds (mult. is assoc)
$\mathcal{G}_2$ holds ($1 \in \mathbb{Z}$ is identity)
$\mathcal{G}_3$ fails → no inverse for, say 2
b/c $\nexists$ integer m s.t. $2 \cdot m = 1$
(b/c $m = 1/2$ is not $\in \mathbb{Z}$)

#2 | $\mathcal{G}_1$ holds (+ is assoc)
$\mathcal{G}_2$ holds (0 is identity)
$\mathcal{G}_3$ holds ($a^{-1} = -a$)

#4) $\mathcal{G}_1$ holds (mult. is assoc)

$\mathcal{G}_2$ holds (1 is identity)

$\mathcal{G}_3$ fails ($0 \in \mathbb{Q}$ has no inverse!)

#5)

$\mathcal{G}_1$ fails:

$$(a \star b) \star c = \frac{a}{b} \star c = \frac{a/b}{c} = \frac{a}{bc}$$

while

$$a \star (b \star c) = a \star \frac{b}{c} = \frac{a}{b/c} = \frac{ca}{b}$$

#12) multiplication

$\mathcal{G}_1$ holds (matrix mult is assoc)

$\mathcal{G}_2$ holds ($\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is identity)

$\mathcal{G}_3$ fails (e.g. $\begin{bmatrix} 2 & 4 \\ 1 & 2 \end{bmatrix}$ is not invertible since $\det \begin{bmatrix} 2 & 4 \\ 1 & 2 \end{bmatrix} = 0$)

X not a group

addition

$\mathcal{G}_1$ holds

$\mathcal{G}_2$ holds (zero matrix)

$\mathcal{G}_3$ holds ($A + (-A) = 0$ matrix)

✓ group

#19) $S = \mathbb{R} \setminus \{-1\}$ $\quad a \star b = a + b + ab$

(a) Need to show $\star : S \times S \to S$

Boils down to arguing that $\forall x, y \in S$, $x \star y \neq -1$

Suppose $\exists\, x, y \in S$ so that $x \star y = -1$

Then $x + y + xy = -1$

$$x(1+y) + y = -1$$

$$x(1+y) + (y+1) = 0$$

$(x+1)(y+1) = 0 \implies x = -1$ and $y = -1$, a contradiction since $x, y \in S$.

Thus $\star$ is a binary op.

(b) $\mathcal{G}_1$: $(a \star b) \star c = (a+b+ab) \star c = a+b+ab+c+[a+b+ab]c$

$$= a+b+ab+c+ca+cb+abc$$

$a \star (b \star c) = a \star [b+c+bc] = a+b+c+bc+a(b+c+bc)$

$$= a+b+c+bc+ab+ac+abc$$

equal!

$\mathcal{G}_2$: Need to find e so that for all $a \in S$,

$$a \star e = a$$

$$a \star e = \cancel{a} + e + ae = \cancel{a}$$

$$e + ae = 0$$

$$e(1+a) = 0$$

$$\Downarrow$$

$$e = 0$$

Check it:

$a \star 0 = a + 0 + a(0) = a + 0 + 0 = a$ ✓

$\mathcal{G}_3$ | Given any $a \in S$, need to find $a^{-1} \in S$ so that

$$a * a^{-1} = e = 0$$

$$a + a^{-1} + (a)(a^{-1}) = 0$$

$$a^{-1}[1+a] = -a$$

$$a^{-1} = \frac{-a}{1+a}$$ ← do we know that if $a \in S$, that $\frac{-a}{1+a} \in S$?

Sufficient to show that $\frac{-a}{1+a} \neq -1$

Suppose

$$\frac{-a}{1+a} = -1 \rightarrow -a = -1 - a$$
$$\rightarrow 0 = -1 \text{ false!}$$

Thus we have shown for any $a \in S$, $a^{-1} = \frac{-a}{1+a}$.

Thus $\mathcal{G}_1, \mathcal{G}_2$, and $\mathcal{G}_3$ hold, so $\langle S, * \rangle$ is a group.

#33 | Prove $(a*b)^n = (a^n)*(b^n)$ when $\langle G, * \rangle$ is abelian.

Proof: $(a*b)^1 = a*b = a^1 * b^1$ ~ base case $n=1$ works

Now suppose $(a*b)^N = a^N * b^N$.

Consider

$$(a*b)^{N+1} = (a*b)*(a*b)^N$$

$$\overset{\text{induction hypothesis}}{=} (a*b)*(a^N * b^N)$$

$$\overset{\text{commutative and associative props}}{=} a^{N+1} * b^{N+1},$$

completing the proof. ∎

#36 | Let $\langle G, * \rangle$ be a group. Prove $(a*b)^{-1} = a^{-1}*b^{-1}$ iff $a*b = b*a$.

Proof: $(a*b)^{-1} = a^{-1}*b^{-1} \rightarrow a*b = b*a$)

Suppose $(a*b)^{-1} = a^{-1}*b^{-1}$. Since we also know $(a*b)^{-1} = b^{-1}*a^{-1}$

because $(b^{-1}*a^{-1})*(a*b) = b^{-1}*(a^{-1}*a)*b = b^{-1}*e*b = b^{-1}*b = e$

and $(a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = \ldots = e$,

we conclude that $a^{-1}*b^{-1} = b^{-1}*a^{-1}$ since inverses are unique (Thm 4.17).

Multiply on left and right by b to get

$$b*a^{-1} = a^{-1}*b$$

Also mult on left and right by a to get

$$a*b = b*a,$$

completing this direction of the proof.

$(a*b=b*a \to (a*b)^{-1}=a^{-1}*b^{-1})$

Suppose $a*b=b*a$. Compute

$$(a*b)*(a^{-1}*b^{-1}) = (b*a)*(a^{-1}*b^{-1})$$
$$= b*(a*a^{-1})*b^{-1}$$
$$= b*e*b^{-1} = e$$

and similarly

$$(a^{-1}*b^{-1})*(a*b) = (a^{-1}*b^{-1})*(b*a)$$
$$= a^{-1}*(b^{-1}*b)*a$$
$$= a^{-1}*e*a$$
$$= e.$$

Thus $a^{-1}*b^{-1}$ is the inverse of $a*b$, completing the proof. ∎

Grad students:

p.36 #28 Define $\mathcal{R}$ by $\langle X,*\rangle \mathcal{R} \langle Y,\tilde{*}\rangle$ iff $\langle X,*\rangle$ is isomorphic to $\langle Y,\tilde{*}\rangle$.

reflexive $\langle X,*\rangle \mathcal{R} \langle X,*\rangle$ because the isomorphism $\phi: X\to X$, $\phi(x)=x$ shows all BAS are isomorphic to themself

symmetric $\langle X,*\rangle \mathcal{R} \langle Y,\tilde{*}\rangle \longleftrightarrow \langle Y,\tilde{*}\rangle \mathcal{R} \langle X,*\rangle$ because given any isomorphism $\phi: X\to Y$, we know $\phi^{-1}: Y\to X$ is also an isomorphism (see Exercise 26)

transitive Follows because of exercise 27: compositions of isomorphisms are isomorphisms.

p.45 #10 a) Show $\langle n\mathbb{Z},+\rangle$ is a group

$\mathcal{G}_1$: $(a+b)+c = a+(b+c)$ (since integer $\oplus$ is assoc)

$\mathcal{G}_2$: $0\in n\mathbb{Z}$ is identity

$\mathcal{G}_3$: for $a\in n\mathbb{Z}$, $-a\in n\mathbb{Z}$ is inverse

b) Let $\phi: n\mathbb{Z}\to\mathbb{Z}$ defined by $\phi(a)=\frac{a}{n}$.

ϕ is 1-1 $\phi(a)=\phi(b)$

$\frac{a}{n}=\frac{b}{n} \to a=b$ ✓

ϕ is onto

for any $x \in \mathbb{Z}$, $nx \in n\mathbb{Z}$ obeys $\phi(nx) = \frac{nx}{n} = x$ ✓

ϕ preserves structure: let $x, y \in \mathbb{Z}$:

$$\underset{\substack{\uparrow \\ \text{addition} \\ \text{in } n\mathbb{Z}}}{\phi(nx+ny)} = \frac{nx+ny}{n} = \underset{\substack{\uparrow \\ \text{addition} \\ \text{in } \mathbb{Z}}}{x+y}$$

Thus ϕ is an isomorphism.

#24

$\star$	e	a	b
e	e	a	b
a	a	e	a
b	b	b	e

break assoc

$(a \star b) \star a = a$

$a \star (b \star a) = b$

satisfies $\mathcal{G}_2$ ~ e is identity

$\mathcal{G}_3$ ~ $a^{-1} = a$ and $b^{-1} = b$

but fails $\mathcal{G}_1$:

$a \star (b \star a) = a \star b = a$

but

$(a \star b) \star a = a \star a = e$

not equal!

#31 Consider $\langle G, \star \rangle$ to be a group with identity e.

We argue that the soln to $x \star x = x$ is $x = e$.

$\downarrow$ mult by x^{-1} on left

$x^{-1} \star (x \star x) = x^{-1} \star x$

$(x^{-1} \star x) \star x = e$

$\uparrow$ assoc prop

$e \star x = e$

$x = e$.

#35 If $(a \star b)^2 = a^2 \star b^2$, then $a \star b = b \star a$.

Pf: $(a \star b)^2 = \underbrace{(a \star b) \star (a \star b) = a^2 \star b^2}$

$a \star (b \star a) \star b = a \star (a \star b) \star b$

$\downarrow$ mult by a^{-1} on left

$(b \star a) \star b = (a \star b) \star b$

$\downarrow$ mult by b^{-1} on right

$b \star a = a \star b$,

completing the proof. ■