Exercises 4

③ $(\mathbb{R}^+, *)$, $a*b = \sqrt{ab}$

No. Associativity fails.

Let $a=1, b=1, c=4$

Then $(1*1)*c = \sqrt{\sqrt{1\cdot 1}\cdot 4} = \sqrt{4} = 2$

but $1*(1*c) = \sqrt{1\cdot\sqrt{1\cdot 4}} = \sqrt{\sqrt{4}} = \sqrt{2}$, and $2 \neq \sqrt{2}$.

⑤ $(\mathbb{R}^*, *)$, $a*b = a/b$

No, associativity fails. $(a*b)*c = (a/b)/c = \frac{a}{bc}$, but $a*(b*c) = a/(b/c) = \frac{ac}{b}$.

⑲ S = all real #'s except -1.

$a*b = a+b+ab$.

(a) We first show $*$ maps $S\times S$ into S. It is clear that $a+b+ab \in \mathbb{R}$.

Suppose that $a+b+ab = -1$. Then

$a(1+b) = -1-b$, so $a = \frac{-1-b}{1+b} = -\frac{1+b}{1+b} = -1 \notin S$.

We need to show $*: S\times S \to S$ is a function.

We first show it is well-defined. Let $a_1, a_2, b_1, b_2 \in S$

If $a_1 = a_2$ & $b_1 = b_2$, then $a_1*b_1 = a_1+b_1+a_1b_1 = a_2+b_2+a_2b_2 = a_2*b_2$.

As $*$ is defined on every pair $(a,b) \in S\times S$, $*$ is a function

(b) 1. $*$ is associative

$(a*b)*c = a*b+c+(a*b)\cdot c = a+b+ab+c+(a+b+ab)\cdot c =$

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

$a*(b*c) = a+b*c+a\cdot(b*c) = a+b+c+bc+a(b+c+bc)$

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

These are equal.

2. Identity elt is 0: for all $a \in S$, $a*0 = a+0+a\cdot 0 = a$. We showed in class we only need to check one side.

3. For each $a \in S$, the inverse of a is $\frac{-a}{1+a}$, which is a real # because $a \neq -1$.

Moreover, if $\frac{-a}{1+a} = -1$, then $\frac{a}{1+a} = 1$, so $a = 1+a$, which is not possible.

Thus $-a/(1+a) \in S$.

$a*(\frac{-a}{1+a}) = a + \frac{-a}{1+a} + \frac{-a^2}{1+a} = \frac{a+a^2}{1+a} + \frac{-a}{1+a} + \frac{-a^2}{1+a} = 0$, as desired.

Therefore, $(S,*)$ is a group.

(c) $2*x*3 = 7$ $\quad 2^{-1} = -\frac{2}{3}$, $3^{-1} = \frac{-3}{4}$

$x = 2^{-1}*7*3^{-1} = -\frac{2}{3}*7*\frac{-3}{4}$

$= (-\frac{2}{3}+7+\frac{-2}{3}\cdot 7)*\frac{-3}{4}$

$= -\frac{2}{3}+7+\frac{-2}{3}\cdot 7 + \frac{-3}{4} + (-\frac{2}{3}+7+\frac{-2}{3}7)\cdot(\frac{-3}{4})$

㉙ For every $a \in G$ with $a*a \neq e$, we have $a \neq a^{-1}$. Pairing up each such elt with its inverse gives an even number of elements. Adding the identity gives an odd number of elements. Since G has an even number of elements, this cannot be all of the elements. Therefore, there must be some $b \in G$ with $b*b = e$.

(31) Since $e*e=e$, every group has at least one idempotent element. If $x \in G$ and $x*x=x$, then $x*x=x*e$, so by left cancellation we have $x=e$. Therefore there is exactly one idempotent elt.

(32) Let $a,b \in G$. Then

$$(a*b)*(a*b)=e,$$

so, $a*((a*b)*(a*b))=a$

$$(a*a)*(b*(a*b))=a$$

$$e*(b*(a*b))=a$$

$$b*(a*b)=a.$$

Then, $b*(b*(a*b))=b*a$

$$(b*b)*(a*b)=b*a$$

$$e*(a*b)=b*a$$

$$a*b=b*a.$$

Therefore G is abelian.

(36) $(a*b)'=a'*b' \iff a*b=b*a$

($\Leftarrow$): $(a*b)'=b'*a'=a'*b'$.

($\Rightarrow$): If $(a*b)'=a'*b'$, then since inverses are unique, $a'*b'=b'*a'$. Since then $(b*a)'=b'*a'$, we have

$$a'*b'=b'*a'$$

$$(a*b)'=(b*a)',$$

so $(a*b)*(a*b)'=(a*b)*(b*a)'$

$$e=(a*b)*(b*a)'.$$

Then $e*(b*a)=(a*b)*(b*a)'*(b*a)$

$$b*a=(a*b)*e$$

$$b*a=a*b.$$

(37) Suppose $a*b*c=e$.

Then $b*c=a^{-1}$, so $b*c*a=a^{-1}*a=e$.

Additional exercises:

1. Let G be a group, and suppose $e,e' \in G$ are both identity elements. Then for every $g \in G$, $ge=ge'$. By the left cancellation law, $e=e'$.

2. (a) φ_g is injective: Let $h_1,h_2 \in G$ be s.t.

$$\varphi_g(h_1)=\varphi_g(h_2).$$

Then,

$gh_1g^{-1}=gh_2g^{-1}$	by def. of φ_g
$h_1g^{-1}=h_2g$	by left cancellation
$h_1=h_2$	by right cancellation ✓

φ_g is surjective: Let $h \in G$. Then $g^{-1}hg \in G$, and

$$\varphi_g(g^{-1}hg)=g(g^{-1}hg)g^{-1}=(gg^{-1})h(gg^{-1})=h \quad ✓$$

(b) Let $a, b \in G$.

Then $\phi_g(ab) = gabg^{-1}$
$= gaebg^{-1}$
$= ga(g^{-1}g)bg^{-1}$
$= (gag^{-1})(gbg^{-1})$
$= \phi_g(a)\phi_g(b)$.

3. $\mathbb{Z}_n^\times = \{\bar{a} \in \mathbb{Z}_n \mid \exists\, \bar{c} \in \mathbb{Z}_n \text{ s.t. } \bar{a} \cdot_n \bar{c} = \bar{1}\}$

Recall that $\bar{a} \cdot_n \bar{b} = \overline{ab}$, by definition, where ab is multiplication in $\mathbb{Z}$.

- $\cdot_n$ is associative: Let $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n^\times$. Then $(\bar{a} \cdot_n \bar{b}) \cdot_n \bar{c} = \overline{ab} \cdot_n \bar{c} = \overline{(ab)c}$ $= \overline{a(bc)} = \bar{a} \cdot_n \overline{bc} = \bar{a} \cdot_n (\bar{b} \cdot_n \bar{c})$.
  [b/c multiplication of integers is associative.

- $\mathbb{Z}_n^\times$ is closed under $\cdot_n$: Let $\bar{a}, \bar{b} \in \mathbb{Z}_n^\times$. Then $\exists\, \bar{c}, \bar{d} \in \mathbb{Z}_n$ s.t. $\bar{a} \cdot \bar{c} = \bar{1}$ & $\bar{b} \cdot_n \bar{d} = \bar{1}$. Consider $\bar{d} \cdot_n \bar{c} \in \mathbb{Z}_n$. Then $(\bar{a} \cdot_n \bar{b}) \cdot_n (\bar{d} \cdot_n \bar{c}) = (\bar{a} \cdot_n (\bar{b} \cdot_n \bar{d})) \cdot_n \bar{c} = (\bar{a} \cdot_n \bar{1}) \cdot_n \bar{c} = \bar{a} \cdot_n \bar{c} = \bar{1}$, so $\bar{a} \cdot_n \bar{b} \in \mathbb{Z}_n^\times$.

- Identity: $\bar{1} \in \mathbb{Z}_n^\times$ (b/c $\bar{1} \cdot_n \bar{1} = \overline{1 \cdot 1} = \bar{1}$). We will show $\bar{1}$ is the identity elt. Let $\bar{a} \in \mathbb{Z}_n^\times$. Then $\bar{1} \cdot_n \bar{a} = \overline{1 \cdot a} = \bar{a} = \overline{a \cdot 1} = \bar{a} \cdot_n \bar{1}$, as desired.

- Inverses: First note that $\cdot_n$ is commutative: $\forall \bar{a}, \bar{b} \in \mathbb{Z}_n^\times$, $\bar{a} \cdot_n \bar{b} = \overline{ab} = \overline{ba} = \bar{b} \cdot_n \bar{a}$
  Let $\bar{a} \in \mathbb{Z}_n^\times$. Then by definition, $\exists\, \bar{c} \in \mathbb{Z}_n$ s.t. $\bar{a} \cdot \bar{c} = \bar{1}$, & since $\cdot_n$ is commutative $\bar{c} \cdot_n \bar{a} = \bar{1}$, as well. Thus $\bar{c} \in \mathbb{Z}_n^\times$, & is the inverse of $\bar{a}$.

Therefore, $(\mathbb{Z}_n^\times, \cdot_n)$ is a group.