1/15

Judson

Herstein - also found a pdf online.

Quiz 1:

Last time we talked about binary operations.

We define an operation to be 1) associative,

2) commutative.

function $*: A \times A \to A$

~~These~~ ~~were~~ Gave examples of binary operations.

The definitions are universally quantified sentences.

1) $\forall x, y, z \in A \quad (x*y)*z = x*(y*z)$.

2) $\forall x, y \in A \quad x*y = y*x$.

Def 3. Let A be a set and $*$ a binary operation

An element $e \in A$ is called a $*$-identity

Ex $a \Delta b = a$ $\quad (1,3) \to 1$

1) $(a \Delta b) \Delta c = a \Delta c = a$
$a \Delta (b \Delta c) = a \Delta b = a$ } assoc. ✓

2) $a \Delta b = a$ $\quad (1,2) \to 1$
$b \Delta a = b$ $\quad (2,1) \to 2$ $\neq$ not commutative.

2 $\quad A = \mathbb{Z}$

$a * b = a + b - ab$

Let $a, b, c \in A$

$(a*b)*c = (a+b-ab)*c = a+b-ab+c-(a+b-ab)c$

$= \boxed{a+b-ab+c-ac-bc+abc}$

$a*(b*c) = a*(b+c-bc) = a+b+c-bc-a(b+c-bc)$

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

equal

so associative ✓

$a*b = a+b-ab$

$b*a = b+a-ba$

equal

Ex $\quad a*b = a-b-ab \quad$ not comm

$1*2 = 1-2-2 = -3$

$2*1 = 2-1-2 = -1$

Def 3 $\quad$ A is a set w/ an binar operation $*$.

a $*$-identity is an element $e \in A$ that satisfies

$\forall a \in A, \quad e*a = a*e = a.$

Ex $(\mathbb{Z}, +), (\mathbb{R}, +) \qquad \square + a = a$

0 is the additive identity.

Ex $(\mathbb{Z}, \cdot), (\mathbb{R}, \cdot) \qquad \square \cdot a = a \qquad$ 1 is the mult. identity.

(3) identities might not exist.

<u>Strategy</u> on how to find the identity (if it exists).

$e * a = a$ set equal to each other

$e * a$ use definition   + solve for e.

<u>Ex</u> $a \triangle b = a + b - 5$ $(1,2) \xrightarrow{\triangle} -2$

$e \triangle a = e + a - 5 = a$

$\boxed{e = 5}$ 5 is the $\triangle$-identity.

<u>Ex</u> $a \square b = a + 2b$ $(1,2) \to 5$

$(3,-1) \to 1$

$e \square a = e + 2a = a$

$e = \underline{-a}$ no <u>identity</u>

$\left\{ \frac{a}{b} \,\middle|\, \begin{array}{l} a,b \in \mathbb{Z}, \\ b \neq 0 \end{array} \right\}$

rational

<u>Ex</u> $a * b = 2ab$

$e * a = 2ea = a$

careful can't just divide a (cuz $a = 0$?)

$2e = 1$

$e = \frac{1}{2}$

$A_1 = \mathbb{N}$

no $*$-identity

$A_2 = \mathbb{Q}$

claim $\frac{1}{2}$ is the

$\frac{1}{2} * a = 2(\frac{1}{2})a$

$= a$ ✓

$\frac{1}{2}$ is the $*$-id

(4)

Def 4 a group is a pair $(A, *)$ s.t. A is a set and $*$ is a binary operation on A that satisfies the following 3 properties:

1) $*$ is associative
2) $*$ has an identity ($\exists e \in A \ \forall a \in A \quad e*a = a*e = a$)
3) $\forall a \in A \ \exists b \in A$ s.t. $a*b = b*a = e$.

The element b given in 3) will be called a $*$-inverse for a

Ex $(\mathbb{Z}, +)$ the identity is 0.

the additive inverse of a is $-a$

$(\mathbb{Z}, \cdot)$ the mult. identity is 1

the mult. inv. of 2 we would like it be $1/2$

$2 \cdot \frac{1}{2} = 1$

but $1/2 \notin \mathbb{Z}$

$1 \cdot 1 = 1$

$(-1)(-1) = 1$

$(\mathbb{Z}, \cdot)$ is not a group.

5 $(\mathbb{Q}, \cdot)$ 1 is the mult. identity.

$$\frac{a}{b} \cdot \frac{b}{a} = 1$$

$0 \cdot \_ = 1$ 0 has no mult. inverse.

So $(\mathbb{Q}, \cdot)$ is not a group.

$\underline{\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}}$ $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

$(\mathbb{Q}^*, \cdot)$ ~~is a~~ are group.
$(\mathbb{R}^*, \cdot)$

$(\mathbb{Z}, +)$ $(\mathbb{Q}, +)$
$(\mathbb{R}, +)$ are groups

$\mathbb{N}, +$
$(\mathbb{N} \cup \{0\}, +)$ not groups

Denote $\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$ $|\mathbb{Z}_n| = n$

$n \in \mathbb{N}$ $n > 1$

(6) Cayley

$\mathbb{Z}_3 = \{0,1,2\}$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\mathbb{Z}_5$

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$V = \{e, a, b, c\}$

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Prop if $(A, *, e)$ is a group. then there is a unique identity.

Pf. Let e, f be $*$-identities

WTS $e = f$.

$e * f = f$ e is a $*$-ident

$e * f = e$ f is a $*$-ident.

so $e = f$. ∎

Prop Let $(A, *, e)$ be a group and $a \in A$. The $*$inverse of a is unique.

Pf: Let b_1, b_2 be $*$ inverses of a.

$$b_1 \underset{e\text{ ident}}{=} b_1 * e \underset{a*b_2=e}{=} b_1 * (a * b_2) \underset{\text{assoc.}}{=} (b_1 * a) * b_2 = e * b_2 = b_2$$

$\therefore b_1 = b_2$ ∎

(7) Since inverses are unique. we use the suggestive notation a^{-1}

Except when $* = +$ we instead write $-a$

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

thm Cancellation   Let $(A, *, e)$ be a group

if $a * b = a * c$, then $b = c$.

Pf. $a * b = a * c$ mult. on left by a^{-1}

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

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

$= e * b = e * c$

$\boxed{\Rightarrow b = c}$

$b * a = c * a$

$\Rightarrow b = c$