Winter 2017 MATH 15910 Section 55 HW2 Solution

Richard

Ex 1.5.6

Suppose $0<a$, $0<b$.

Then $a<b \iff a^2<b^2$

Proof.

$\because a<b$

$\therefore a+(-a)< b+(-a)$

$\therefore b-a > a+(-a) = 0$

$\because a>0, b>0$

$\therefore a+b > 0+b = b > 0$

by "Rules of order" — by field axiom — by assumption

We now have $b-a>0$, $b+a>0$.

By Facts 1.5.5 (2), $(b-a)(b+a)>0$.

$$(b-a)(b+a) = b(b-a)+a(b-a)$$
$$= b^2-ab+ab-a^2$$
$$= b^2-a^2 > 0$$

$\therefore b^2-a^2+a^2 > 0+a^2$

$\therefore b^2+(a^2-a^2) > a^2$

$\therefore b^2+0 > a^2$

$\therefore b^2 > a^2$

$\therefore a^2<b^2$.

Here are some interesting exercises helping you understand HW1 material.

1. List all subsets of $\emptyset$
2. List all subsets of $\{\emptyset\}$
3. List all subsets of $\{0\}$
4. List all subsets of $\{0,1\}$
5. List all elements of $\{0\}$
6. List all elements of $\{0,1\}$
7. List all elements of $\{\emptyset\}$.
8. List all subsets and all elements of $\{\{\emptyset\}\}$.

Ex 1.5.8

Show $2ab \le a^2+b^2$

By Facts 1.5.5 (5),

if $a-b\neq 0$, $(a-b)^2>0$

If $a-b=0$, $(a-b)^2=0$.

Therefore, $(a-b)^2 \geq 0$.

$$(a-b)^2 = (a-b)(a-b) = a(a-b) + (-b)(a-b)$$
$$= a^2-ab+b^2-ab$$
$$= a^2+b^2-2ab \geq 0$$

$\Rightarrow a^2+b^2-2ab+2ab \geq 0+2ab$

$\Rightarrow a^2+b^2+0 = a^2+b^2 \geq 2ab$.

p-5

Ex 1.6.2

Let R be a relation on X that

(a) $\forall a \in X, (a,a) \in R$

(b) $\forall a, b, c \in X$, if $(a,b), (b,c) \in R$, then $(c,a) \in R$.

Show R equivalence relation.

Proof We just check the axioms one by one.

(ER1) Reflexive $\forall a \in X, (a,a) \in R$ by def. ✓

(ER2) Symmetric Let $a, b \in X$, s.t. $(a,b) \in X$.

$\because$ R is reflexive

$\therefore$ $(b,b) \in X$

By def (b) of R, $(b,a) \in X$.

(ER3) Transitive

Let $a, b, c \in X$, s.t. $(a,b) \in R$, $(b,c) \in R$.

Then, by (b), $(c,a) \in R$.

By (ER 2), $(a,c) \in R$.

We're done.

Ex 1.6.14

As the problem describes, we are proving the following problem:

Let $X_\lambda \subset X$ where $\lambda \in \Lambda$ where Λ is the index set, ~~s.t.~~.
(X_λ's is not necessarily finite? Nor necessarily countable?)
s.t.
$X_{\lambda_i} \cap X_{\lambda_j} = \emptyset$ whenever $\lambda_i \neq \lambda_j$,
$\bigcup_{\forall \lambda \in \Lambda} X_i = X$

Define $\sim$ as follows:
Suppose $a, b \in X$,

$a \sim b$ if $\exists \lambda \in \Lambda$ s.t. $a, b \in X_\lambda \subset X$.

ER1
Let $a \in X$, then $a \sim a$ given $\exists \lambda \in \Lambda$ s.t. $a \in X_\lambda$.

ER2
Let $a, b \in X$, s.t. $a \sim b$.
Then $\exists \lambda \in \Lambda$ s.t. $a, b \in X_\lambda$
$\therefore b \sim a$ by def of $\sim$.

ER3 Let $a, b, c \in X$ s.t. $a \sim b$, $b \sim c$
Then $\exists \lambda_i \in \Lambda$ s.t. $a, b \in X_{\lambda_i}$
$\exists \lambda_j \in \Lambda$ s.t. $b, c \in X_{\lambda_j}$
Now,
$\lambda_i = \lambda_j$, because otherwise,
$b \in X_{\lambda_i}$, $b \in X_{\lambda_j}$, $X_{\lambda_i} \cap X_{\lambda_j} = \emptyset$.
(contradiction)

Then, $a, c \in X_{\lambda_i} = X_{\lambda_j}$
$\therefore a \sim c$

Ex 1.6.15

$\sim$. Here $\sim$ is defined as:
$(a,b) \sim (c,d)$, if $ad = bc$

ER1 Let $(a,b) \in F$.
$\because ab = ba$
$\therefore (a,b) \sim (a,b)$

ER2 Let $(a,b), (c,d) \in F$, s.t.
$(a,b) \sim (c,d)$,
$\therefore ad = bc$
$\therefore cb = da$
$\therefore (c,d) \sim (a,b)$ by def of $\sim$

ER3 Let $(a,b), (c,d), (e,f) \in F$ s.t.
$(a,b) \sim (c,d)$, $(c,d) \sim (e,f)$
$\therefore ad = bc$, $cf = de$
$\because b, f \neq 0$ as defined in F
$\therefore c = \frac{ad}{b}$, $c = \frac{de}{f}$
$\therefore \frac{ad}{b} = \frac{de}{f} \Rightarrow adf = bde$
$\because d \neq 0$ $\therefore af = be \Rightarrow (a,b) \sim (e,f)$

Ex 1.6.28

(i) Show addition and multiplication in $\mathbb{Z}_n$ are well-defined

Proof.

Assume $\overline{a'} = \overline{a}$, $\overline{b'} = \overline{b}$ $\in \mathbb{Z}_n$, where $n \in \mathbb{Z}$.

Then $a', b' \in \mathbb{Z}$, and

$\exists k_1, k_2 \in \mathbb{Z}$ s.t.

$a' = a + k_1 n$,

$b' = b + k_2 n$

$\Rightarrow a' + b' = (a + k_1 n) + (b + k_2 n)$

$= (a+b) + (k_1 + k_2) n$.

$\Rightarrow \overline{a' + b'} = \overline{a+b}$

Now, WTS: $\overline{a' \cdot b'} = \overline{a \cdot b}$

$a' \cdot b' = (a + k_1 n) \cdot (b + k_2 n)$

$= ab + a k_2 n + b k_1 n + k_1 k_2 n^2$

$= ab + n(a k_2 + b k_1 + k_1 k_2 n)$

$\Rightarrow \overline{a' \cdot b'} = \overline{a \cdot b}$

(ii) W/ these ops, $\mathbb{Z}_n$, is a commutative ring with 1.

Check $(A_1) - (A_5)$

$(M1) - (M4)$

(D) on textbook P10

(iii) $\mathbb{Z}_n$ cannot satisfy order axioms no matter how $>$ is defined.

Suppose for contradiction that $\exists$ order $>$ on $\mathbb{Z}_n = \{\overline{0}, \dots, \overline{n-1}\}$

① Suppose $\overline{1} > \overline{0}$

By order axioms,

$\overline{1} + \overline{n-2} > \overline{0} + \overline{n-2} > \overline{0}$

$\Rightarrow \overline{n-1} > \overline{0}$

$\Rightarrow \overline{n-1} + \overline{1} > \overline{0} + \overline{1}$

$\Rightarrow \overline{0} > \overline{1}$ (contradiction)

② Suppose $\overline{0} > \overline{1}$

Similar

(iv) $\mathbb{Z}_2$ is a field, $\mathbb{Z}_4$ is not

By def 1.6.19, we only need to check (M5).

$\underline{\mathbb{Z}_2}$ $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$

We have proved in (A4) that $\overline{0}$ is the identity.

$\because \overline{1} \cdot \overline{1} = \overline{1}$

$\therefore$ (M5) is satisfied

$\underline{\mathbb{Z}_4}$ $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$

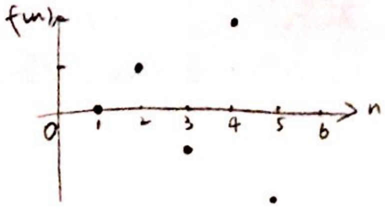
We can check $\forall x \in \mathbb{Z}_4$, $x \cdot \overline{2} \neq \overline{1}$.

$\Rightarrow$ (M5) not satisfied.

Ex 1.7.22 $f: \mathbb{N} \to \mathbb{Z}$

$$f(n) = \begin{cases} \frac{n}{2}, & \text{if } n \text{ even} \\ \frac{1-n}{2}, & \text{if } n \text{ odd} \end{cases}$$

f is a bijection



<u>Proof.</u>

<u>Pf of f surjective (onto)</u>

Let $y \in \mathbb{Z}$.

① if $y > 0$ (note that $y \neq 0$).

We find that $2y \in \mathbb{N}$ and $f(2y) = y$ given $2y$ is even.

② if $y \leq 0$

Consider the value $1-2y$.

$\because y \leq 0$

$\therefore -2y \geq 0$

$\therefore 1-2y \geq 1$

$\because y \in \mathbb{Z}$, $1-2y \geq 1$

$\therefore 1-2y \in \mathbb{N}$, and in particular, $1-2y$ is odd

$\Rightarrow f(1-2y) = \frac{1-(1-2y)}{2} = y$

We have proved that $\forall y \in \mathbb{Z}$, $\exists x \in \mathbb{N}$ s.t. $f(x) = y$.

$\therefore f$ is surjective.

<u>Pf of f injective (one-to-one)</u>

Let $a, a' \in \mathbb{N}$ s.t. $f(a) = f(a')$

<u>Claim</u>:

Let $x \in \mathbb{N}$. If $f(x) > 0$, then x is even. If $f(x) \leq 0$, then x is odd.

<u>Pf of claim</u>

We have proved that if $f(x) > 0$, $\exists$ even $x \in \mathbb{N}$. However, suppose $x \in \mathbb{N}$ and x is odd,

$\therefore x \geq 1$

$\therefore 1 - x \leq 0$

$\therefore f(2k+1) = \frac{1-x}{2} \leq 0$

contradicting the fact that $f(x) > 0$. Therefore, if $f(x) > 0$, then x even.

The other half of the claim can be proven similarly.

Now, ① if $f(a) > 0$, a is necessarily even, and $a = 2f(a)$.

$\because f(a) = f(a')$ $\therefore a = a'$

② if $f(a) \leq 0$, a is necessarily odd

$\therefore a = 1 - 2f(a)$

$\because f(a) = f(a')$

$\therefore a = a'$

We have now proved that

if $a, a' \in \mathbb{N}$ s.t. $f(a) = f(a')$,

then $a = a'$.

Therefore f is injective.

$\because$ f is both surjective and injective

$\therefore$ f is bijective.