Class Notes; Week 7, 2/26/2016

Day 18

This Time

Section 3.3
Isomorphism and Homomorphism

Example. 1
[0], [2], [4] in $\mathbb{Z}_6$

+	0	4	2
0	0	4	2
4	4	2	0
2	2	0	4

*	0	4	2
0	0	0	0
4	0	4	2
2	0	2	4

So $\{[0], [2], [4]\}$ is a subring.
Now, in $\mathbb{Z}_3$

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

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Multiplication identity: 0, Addition identity: 1
3 elements form a ring: no other structure. They are identical.

Isomorphism

A ring R is isomorphic to a ring S (In symbols: $R \cong S$) if there is a function $f : R \to S$ such that:

(i) f is injective: $f(a) = f(b) \Rightarrow a = b$
(ii) f is surjective: $\forall a \in S \exists b \in R(f(a) = b)$
(iii) $f(a + b) = f(a) + f(b)$
(iv) $f(ab) = f(a)f(b)$

In this case F is called isomorphic.

In the example: $f : 0 \to 0$, $1 \to 4$, $2 \to 2$ for $0, 1, 2 \in \mathbb{Z}_3$ and $0, 4, 2 \in S$, $s = \{0, 2, 4\} \subset \mathbb{Z}_6$
$4 + 2 = 1 + 2$ and $4 * 2 = 1 * 2$
So (one-to-one, or injective):

Example. $f(x) = x$ is injective
$g(x) = x^2$ is not injective: because $g(2) = g(-2) = 4$ but $2 \neq -2$

When you have two distinct elements mapped to the same element they are not injective. $\Rightarrow a \neq b \Rightarrow f(a) \neq f(b)$

Also, onto = surjective.

Example. 1
From student: in $\mathbb{Z}_{12}$ $\{0, 4, 8\}$ to $\mathbb{Z}_3$

Example. 2
in $\mathbb{Z}_{10}$ $\{0, 2, 4, 6, 8\}$ to $\mathbb{Z}_5$

Example. 3

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_2(\mathbb{R})$$

k field has all $2X2$ matrices of this form.
Claim $k \cong \mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$ $(i = \sqrt{-1})$

$$\text{proof: } f : \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \to a + bi$$

$$\text{(formal notation: } f(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}) = a + bi)$$

$$\text{(i) injectivity: let } f(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}) = f(\begin{pmatrix} r & s \\ -s & r \end{pmatrix}) \in K$$

$$a + bi = r + si \Rightarrow a = r \text{ and } b = s \Rightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} r & s \\ -s & r \end{pmatrix}$$

Thus f is injective

$$\text{(ii) surjectivity: for any } a + bi \in \mathbb{C} \ \exists \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in K \text{ such that } f(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}) = a + bi$$

$$\text{(iii) } f(a + b) = f(a) + f(b). \text{ So: } f(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} r & s \\ -s & r \end{pmatrix}) = f(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}) + f(\begin{pmatrix} r & s \\ -s & r \end{pmatrix})$$

$$f(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} r & s \\ -s & r \end{pmatrix}) = f(\begin{pmatrix} a + r & b + s \\ -b - s & a + r \end{pmatrix}) = (a + r) + (b + s)i$$

$$f(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}) + f(\begin{pmatrix} r & s \\ -s & r \end{pmatrix}) = a + bi + r + si = (a + r) + (b + s)i$$

$$\text{(iv) } f(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} r & s \\ -s & r \end{pmatrix}) = f(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}) \cdot f(\begin{pmatrix} r & s \\ -s & r \end{pmatrix})$$

$$f(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} r & s \\ -s & r \end{pmatrix}) = f(\begin{pmatrix} ar - bs & as + br \\ -as - br & -bs + ar \end{pmatrix}) = (ac - bd) + (ad + bd)i$$

$$f(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}) \cdot f(\begin{pmatrix} r & s \\ -s & r \end{pmatrix}) = (a+bi)\cdot(r+si) = ac + cbi + adi - bd = (ac-bd) + (cb+ad)i$$

Therefore K is isomorphic to $\mathbb{C}$

Homomorphism

If only satisfying the (iii) and (iv) conditions of isomorphic definition.

Formal Definition

Let R and S be rings. A function : $R \to S$ is said to be homomorphic if $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$

Example. $f : \mathbb{C} \to \mathbb{C}$ called complex conjugate map

$f(a+bi) = a - bi$

we can verify f is an ismorphism.

Day 19

Section 3.3

Example. 1

For any ring $R \subset S$ the zero map from $Z : R \to S$ given by $Z(r) = 0_s$ for all $r \in R$

$Z(a+b) = 0_s = Z(a) + Z(b) = 0_s + 0_s$

$Z(ab) = Z(a)Z(b) = 0_s$

Example. 2

$f : \mathbb{Z} \to \mathbb{Z}_6$

$f(a) = [a]$ for any $a \in \mathbb{Z}$ you can check: $f(a+b) = [a+b] = f(a) + f(b) = [a] + [b] = [a+b]$

$f(ab) = [ab] = [a][b] = f(a)f(b)$

f is surjective: $f(1) = f(7)$, $1 \neq 7$ in $\mathbb{Z}$

Example. 3

The map $g : \mathbb{R} \to M_2(\mathbb{R})$ given by $g(r) = \begin{pmatrix} 0 & 0 \\ -r & r \end{pmatrix}$

If g is a homomorphism the map will become a ring and right hand side is a subring.

$g(r) = \begin{pmatrix} 0 & 0 \\ -r & r \end{pmatrix}$ is homomorphism.

$$g(r+s) = \begin{pmatrix} 0 & 0 \\ -r-s & r+s \end{pmatrix} = g(r) + g(s)$$

$$g(rs) = \begin{pmatrix} 0 & 0 \\ -rs & rs \end{pmatrix} = g(r)g(s)$$

Homework: g is injective but not surjective.
CAUTION: $f(x) = x + 2$ Is this homomorphic?

No; $f(a+b) = a+b+2 \neq a+2+b+2 = f(a)+f(b)$

Theorem

Let $f : \mathbb{R} \to S$ be a homomorphism of rings, then:

(i) $f(0_R) = 0_s$
(ii) $f(-a) = -f(a)$
(iii) $f(a-b) = f(a) - f(b)$
If R is a ring with 1_R and F is surjective:
(iv) S is a ring with identity $1_S = f(1_R)$
(v) If u is a unit of R, then $f(u)$ is a unit in S and $f(u)^{-1} = f(u^{-1})$

Proving this

(i) $f(0_R)+f(0_R) = f(0_R+0_R) \Rightarrow f(0_R)+f(0_R) = f(0_R) \Rightarrow f(0_R) = 0_S$ addition identity.
(ii) $f(a)+f(-a) = f(a+(-a)) = f(0_R) = 0_S$
So, $f(-a) = -f(a)$
(iii) $f(a-b) = f(a)+f(-b) = f(a)+f(-b) = f(a)-f(b)$
(iv) Consider: $f(r \cdot 1_R) = f(r)f(1_R) = f(r) \Rightarrow f(1_R) = S$
(v) If u is a unit of R, there exists u^{-1} where $f(u \cdot u^{-1}) = f(1_R) = 1_S$,
$f(u) \cdot f(u^{-1}) = 1_S \Rightarrow (f(u))^{-1} = f(u^{-1})$
If $f : R \to S$ is a function then the image of f is the subset of $S/$

(image) Imf $= \{s \in S | s = f(r)\}$ If f is surjective then Imf $= S$.

Cor. 3.4

If $R \to S$ is a homomorphism of ring then the image of f is a subring in S. By theorem 3.10:
(iii) [Closure under subtraction] and $f(ab) = f(a)f(b)$ [closure under multiplication]
Img f is a subring by theorem 3.6

Example. 1
$\mathbb{Z}_{12} \cong \mathbb{Z}_3 X \mathbb{Z}_4$ by multiplying principle we know right hand side has 12 elements.
for $RXS : (1_R, 1_S)$ will be the identity in (RXS)
Define: $f(1) = (1,1)$
$f(2) = f(1+1) = f(1)+f(1) = (2,2)$
$f(3) = (0,3)$
$f(4) = (1,0)$
$f(5) = (2,1)$
$f(6) = (0,2)$
$f(7) = (1,3)$
$f(8) = (2,0)$

$$f(9) = (0,1)$$
$$f(10) = (1,2)$$
$$f(11) = (2,3)$$
$$f(12) = (0,0)$$
$$f([a_{12}]) = ([a]_3, [a]_4) \Rightarrow f(11) = (2,3)$$

Prove homomorphism under addition and multiplication for homework.

Example. 2

The ring $\mathbb{Z}_4$ and $\mathbb{Z}_2 X \mathbb{Z}_2$

Assume f is homomorphism: $f(1) = (1,1)$

$$f(2) = (0,0)$$
$$f(0) = (0,0)$$
$$2 \neq 0 \text{ in } \mathbb{Z}_4$$

Therefore f is not injective.

Example. 3

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are not isomorphic to $\mathbb{Z}$

Is $\mathbb{Q} \cong \mathbb{Z}$??

$\mathbb{Q}$ has infinitely many units while $\mathbb{Z}$ has $2 : -1$ and 1

Day 20

Went over exam 1

Went over homework 0.1in
Section 3.3, problem 21

$a \oplus b = a + b - 1$, $a \otimes b = a + b - ab$ for $\mathbb{Z}^1$
Show isomorphic to $\mathbb{Z}$
Assume already prove injective and surjective.
$f(a+b) = f(a) \oplus f(b)$??
$\Rightarrow 1 - a - b? =?1 - a \oplus 1 - b = 1 - a + 1 - b - 1 = 1 - a - b$

This time

Example. 1

$$K. \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cong \mathbb{C}$$
$$\mathbb{Z}_{12} \cong \mathbb{Z}_3 X \mathbb{Z}_4$$
$$\mathbb{Z}_4 \ncong \mathbb{Z}_2 X \mathbb{Z}_3$$

Is it possible: $\mathbb{Z}_6 \cong \mathbb{Z}_{12}$?

Apparently no: cordinality is not the same.

So, if cardinality are different, immediately not isomorphic.

How about $\mathbb{Z}_8 \cong \mathbb{Z}_2 X \mathbb{Z}_4$?

No. number of units should be the same.

$\mathbb{Z}_8 : 1, 3, 5, 7$ and $\mathbb{Z}_2 X \mathbb{Z}_4 : (1,1), (1,3)$

$4 \neq 2$ impossible to be isomorphic.
How about $\mathbb{Z} \cong \mathbb{Q}$
$1, -1$ compared to infinitely many

Example. 2
If R commutative ring and $f : R \to S$ isomorphic then S is commutative.

proof
$\forall a, b \in R \; ab = ba$
$f(ab) = f(ba) \in S$
$f(a)f(b) = f(b)f(a)$
$\forall x, y \in S$, $xy = yx = f(r)$ some $r \in R$?
Show by proving surjectivity.
If not surjective, commutative proof fails.

Think about for next time

$\mathbb{Z}_{mn} \cong \mathbb{Z}_n X \mathbb{Z}_m$ if $(n, m) = 1$

End of week 7!