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:

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

Proving this

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

$$f(2) = (0,0)$$
$$f(0) = (0,0)$$

$2 \neq 0$ 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

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!

Class Notes; Week 8, 2/29/2016

Day 21

Going Over Quiz

Problem 1

$$\mathbb{Z}_6 \cong \mathbb{Z}_2 X \mathbb{Z}_3$$
$$f([a]_6) = ([a]_2, [a]_3)$$
$$f(0) = (0, 0)$$
$$f(1) = (1, 1)$$
$$\dots$$
$$f(5) = (1, 2).$$
$$f(a+b) = f(a) + f(b) \Rightarrow ([a+b]_2, [a+b]_3) = ([a]_2, [a]_3) + ([b]_2, [b]_3) = f(a) + f(b)$$
$$f(ab) = f(a)f(b)$$

Last Time

$\mathbb{Z}_{mn} \cong \mathbb{Z}_m X \mathbb{Z}_n$ if $(m, n) = 1$
Not hard if you pay attention to the map
Review- $f : R \to S$ * S commutative and f homomorphism: $f(ab) = f(ba) \Rightarrow f(a)f(b) = f(b)f(a)$

This Time

Chapter 4

Polynomial Rings

Let R be any ring, A be a polynomial with coefficients in R is an expression of the form:
$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ where n is a non-negative integer and $a_0, a_1, \dots a_n \in R$.

Assume x is a larger ring $R \subset R'$, $x \in R'$, $x \notin R$
$a_0 + a_1\pi + a_2\pi^2 \cdots + a_n\pi^n \in R$, $a_i \in \mathbb{Z}$

Theorem 4.1
If R is a ring, then there exists a ring P that contains an element x that is not in R and has the properties:

(1) $R \subset P$
(2) $xa = ax$ for every $a \in R$
(3) every element of P can be written in the form: $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ some $n \geq 0$ and $a_i \in R$
(4) representation of element P in (3) is unique in the sense:
if $n \leq m$ and $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$ then $a_i = b_i$ for $i \leq n$ and $b_i = 0_R$ for each $i > n$
(5) $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0_R \iff a_i = 0_R$

The ring P called polynomials with coeffiecients in R and denote it by $R[x]$.

Example. 1

$\pi x \notin \mathbb{Z}[x]$, $3x^2 + 5x + 6 \in \mathbb{Z}[x]$, not always true.

$\mathbb{Q}[x]$

$\mathbb{R}[x]$, $x^2 + 1 = 0$, disjoint and doesn't readily have 2 roots.

$\mathbb{C}[x]$, always has two roots.

Example. 2

Define addition on $R[x]$

$f(x) = 3x + 4$ in $\mathbb{Z}_7[x]$, $g(x) = 4x + 1$ in $\mathbb{Z}_7[x]$

$f(x) + g(x) = 7x + 5 - 5$ in $\mathbb{Z}_7[x]$

Example. 3

$h(x) = 2x + 1$ in $\mathbb{Z}_6[x]$, $k(x) = 3x$ in $\mathbb{Z}_6[x]$

$h(x) + k(x) = (2x + 1)(3x) = 6x^2 + 3x = 3x$ in $\mathbb{Z}_6[x]$

If we have: $(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)(b_0 + b_1x + b_2x^2 + \cdots + b_mx^m)$
For each $k \geq 0$ the coefficient of x^k given by: $a_0b_k + a_ib_{k-1} + a_2b_{k-2} + \ldots a_kb_o = \sum_{i=0}^{k} a_ib_{k-i}$

R without 1_R is $R[x]$ with/without $1_{R[x]}$?
$R[x]$ without $1_{R[x]}$

{ looking at $2\mathbb{Z}$: E is even integer set. $E[x] : 2x + 4$, ax... has no identity}
SO! R has multiplication identity 1_R it is the same identity for $R[x]$ ($1_{R[x]}$)

Set idea for next time: R integral domain is $R[x]$?

yes. R integral domain $\Rightarrow R[x]$ is also.

If R is a field, is $R[x]$?

Not always: $\mathbb{R}(x) = 3x + 1$ inverse $\frac{1}{3x+1} \notin P$.

Day 22

Definition

Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a polynomial in $R[x]$ with $a_n \neq 0_R$. Then a_n is called the leading coefficient of $f(x)$. The degree of $f(x)$ is the integer n (denoted by: $\deg f(x)$)

Example. 1

$f(x) = -3x^5 + 9x$

$\deg(x) = 5$ the constant polynomial is degree 0.

Theorem 4.2

If R is an integral domain and $f(x)$, $g(x)$ are nonzero polynomials in $R[x]$, then:
$\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.

Example. False/Counter
in $\mathbb{Z}_6[x] \to$ integral domain.
$f(x) = 3x$, $g(x) = 2x$
$f(x)g(x) = 6x^2 = 0$ in $\mathbb{Z}_6[x]$

Example. 2
$\mathbb{R}$ works because $\mathbb{R}$ is an integral domain.

Proving this

Suppose $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$
$f(x) \cdot g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{n+m}$
Since$R$ is an integral domain $\to a_n$, $a_m \neq 0_R$
$\deg f(x) = n$, $\deg g(x) = m$
So: $\deg(f \cdot g) = (n + m) = \deg f(x) + \deg g(x)$

Cor. 4.4

Let R be a ring. If $f(x)$, $g(x)$ and $f(x)g(x)$ are nonzero in $R[x]$, then:
$\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$

Cor. 4.3

If R is an integral domain, then so is $R[x]$.

Proving this

$1_{R[x]}$ exists? 1_R exists since R is an integral domain.
$1_{R[x]} = 1_R$, $f(x)1_{R[x]} = f(x)1_R = f(x)$
is $R[x]$ commutative? [homework problem].

NOTE: homework 7 asks to prove $R[x]$ commutative by R commutative.
$f(x)g(x) = 0? \Rightarrow ? f(x) = 0$ or $g(x) = 0$

Directly

Saying: $f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{n+m} = 0$ means every coefficient is 0.
Without loss of generality: since R is an integral domain $a_0 = 0$ or $b_0 = 0$, $a_1 = 0$ or $b_1 = 0 \ldots$

Contradiction

If $f(x) \neq 0$, $g(x) \neq 0$; $a_n \neq 0$, $b_m \neq 0 \Rightarrow f(x)g(x) \neq 0$

Say R is commutative $\Rightarrow R[x]$ is
R is a ring with identity $\Rightarrow R[x]$ is
-what about if $R[x]$ is a ring with identity, so is R? Not always.

Example. 1
E is even numbers.
$E[x] = 2x+4$ or $2x+6$ or $2x+8$
-what about if R is a field, then $R[x]$ is too?
yes / no ? No, not necessarily.

Example. 2
$3x+1 \in \mathbb{R}[x] \Rightarrow \frac{1}{3x+1}? \in ?\mathbb{R}[x]$ no.

Cor. 4.5
Let R be integral domain $f(x) \in R[x]$. Then $f(x)$ is a unit in $R[x] \iff f(x)$ constant polynomial that is a unit in R. (not every element in R is a unit, same for $R[x]$).

Proving this

First: if $f(x)$ is a unit then by definition $f(x)g(x) = 1_{R[x]}$ some $g(x) \in R[x]$, $1_{R[x]} = 1_R$
by theorem 4.2: $\deg(f(x)g(x)) = 0 = \deg f(x) + \deg g(x)$.
know $\deg f(x) \geq 0$ and $\deg g(x) \geq 0$
forces: $\deg f(x) \geq 0$, $\deg g(x) \geq 0 \Rightarrow 0 = 0+0$
$f(x) = a_0$, $g(x) = b_0 \Rightarrow a_0 b_0 = 1 \Rightarrow a_0$ is a unit in R
Secondly: a is a unit $\Rightarrow$ there exists $b \in R$ such $a \cdot b = 1$

Example. 1
What is the unit in $\mathbb{Z}[x]$? 1 and -1.
1 and -1 are units in $\mathbb{Z}$ thus are units in $\mathbb{Z}[x]$.

Example. 2
If $5x+1 \in \mathbb{Z}_{25}[x]$ a unit?
$\mathbb{Z}_{25}[x]$ not an integral domain.
$5x+1 \in \mathbb{Z}_{25}[x]$: say it is a unit, what is the multiplicative inverse-
$(5x+1)(20x+1) = 1 \Rightarrow 100x^2 + 25x + 1 = 1$
So, when $R[x]$ not integral domain, it becomes difficult.

Day 23

Going over homework

Section 3.3 problem 42.

$$\mathbb{Z}_{12} \cong \mathbb{Z}_3 X \mathbb{Z}_4$$
$$f([a]_{12}) = ([a]_3, [a]_4)$$
Injective: $f([a]_{12}) = f([b]_{12}) \Rightarrow ([a]_3, [a]_4) = ([b]_3, [b]_4) \Rightarrow [a]_{12} = [b]_{12}$, $[a]_3 = [b]_3$ in $\mathbb{Z}_3$, $[a]_4 = [b]_4$
$$a \equiv b(\mod 12)$$

NOTE: $b = 3x + a$ for $k = 0, 1, 2, 3$

$b = a$ or $a + 3$ or $a + 6$ or $a + 9$ these all have different remainders thus: $b = a$ in $\mathbb{Z}_4$

Specifically.

More generally: $\mathbb{Z}_{mn} \cong \mathbb{Z}_m X \mathbb{Z}_n$ when $(n, m) = 1$

$$f(a + b) = ([a + b]_3, [a + b]_4) = ([a]_3 + [b]_3, [a]_4 + [b]_4) = ([a]_3, [a]_4) + ([b]_3, [b]_4) = f(a) + f(b)$$

problem 35.

(1)

$E \cong \mathbb{Z}$: no. E doesn't have identity, $\mathbb{Z}$ does.

* $f : E \to \mathbb{Z}$: $f(a) = \frac{a}{2}$

is a homomorphism under addition but not under multiplication

(2)

$$\mathbb{R}X\mathbb{R}X\mathbb{R}X\mathbb{R} \to M_2(\mathbb{R}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

commutative $\to$ not commutative

(3)

$\mathbb{Q} \to \mathbb{R}$

Student answer: infinity number of units

Professor: cardinality: countable infinity $\to$ uncountable infinity.

for bijection cardinality must equal.

(4)

$\mathbb{Z}X\mathbb{Z}_2 \to \mathbb{Z}$

cardinality doesn't match.

This Time

R is an integral domain so is $R[x]$ (not always true for field)
Division Algorithm: $a, b \in \mathbb{Z}$ $b \neq 0$, $a = b \cdot q + r$
q and r unique and $0 \leq r < b$

Theorem 4.6

The division Algorithm in $F[x]$
Let F be a field and (x) , $g(x) \in F[x]$, $g(x) \neq 0$.
Then there exists unique $\mathbb{P}$ $g(x)$ and $r(x)$ such: $f(x) = g(x) \cdot q(x) + r(x)$
such either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

End of week 8!

Class Notes; Week 9, 3/18/2016

Day 24

Going Over Quiz

Problem 1

- $\mathbb{Z}_{16}$: 8 units and $\mathbb{Z}_4 X \mathbb{Z}_4$: 4 units. Units don't match, therefore not isomorphic.

- according to homomorphic properties:

$f(0) = (0, 0)$, $f(1) = (1, 1)$, $f(1 + 1) = (2, 2)$

But $f(4) = (4, 4) = (0, 0) = f(0)$ but since $0 \neq 4$ the function is not injective and therefore not isomorphic

Problem 2

1.) R : integral domain

unit $R[x] \iff$ constant polynomial a is a unit in R

Specifically: $\mathbb{R}[x]$ non-zero real number unit in $\mathbb{Z}[x]$ which only has the units: 1 and -1

2.) $5x + 1$ in $\mathbb{Z}25[x]$

No. $\mathbb{Z}25[x]$ not an integral in the first place.

- $(20x + 1)(5x + 1) = 1$ in $\mathbb{Z}25[x]$

- $(1 + 5x)(1 + 5x) = 1 + 25x = 1 + 0 = 1$. $(1 + 5x)(1 - 5x) = 1 - 25x = (1 + 5x)(1 + 20x)$

This Time

Section 4.2: Divisibility in F[x]

Definition: Let F be a field and $a(x), b(x) \in F[x]$ with $b(x) \neq 0$. We say $b(x)$ divides $a(x)$ [or $b(x)$ is a factor of $a(x)$] and write $b(x) \mid a(x)$ if $a(x) = b(x) \cdot h(x)$ for some $h(x) \in F[x]$.

Example. 1

$(2x + 1)|(6x^2 - x - 2)$ in $\mathbb{Q}[x]$

Show $(6x^2 - x - 2)$ can be represented by $(2x + 1)$ and something else

$(6x^2 - x - 2) = (2x + 1)(3x - 2)$

Example. 2

$(10x + 5)|(6x^2 - x - 2)$ is true, but why?

Because: the definition of field is that all nonzero elements are unit.

$6x^2 - x - 2 = (2x + 1)(3x + 2) \Rightarrow 6x^2 - x - 2 = \frac{1}{5}(10x + 5)(3x + 2)$

$\Rightarrow 6x^2 - x - 2 = (10x + 5)(\frac{3}{5}x - \frac{2}{5})$ in $\mathbb{Q}[x]$

Note

So be careful of the domain because it does play a role.

Example. 3

$x^2 + 1$ in $\mathbb{R}[x]$ it is impossible

$x^2 + 1$ in $\mathbb{Q}[x]$ is okay.

$x^2 + 1 = (x - i)(x + i)$

Note
Again: it is very important to be careful of the properties.

Theorem 4.7

Let F be a field and $a(x), b(x) \in F[x]$ with $b \neq 0$
(1) if $b(x)$ divides $a(x)$ then $c \cdot b(x)$ divides $a(x)$ for each non-zero $c \in F[x]$.
(2) Every divisor of $a[x]$ has degree less than or equal to deg$a(x)$

Example. $a|b \Rightarrow a \leq |b|$

Proving this

$$\text{(1) If } b(x) \text{ factor of } a(x) \Rightarrow a(x) = b(x) \cdot h(x)$$
By definition.
$$c \in F \ , \ c \cdot b(x)(c^{-1}h(x)) = a(x)$$
because $c \neq 0$, c is a unit and c^{-1} exists $\Rightarrow c \cdot b(x)|a(x)$

$$\text{(2) If } b(x)|a(x) \Rightarrow a(x) = b(x)h(x) \text{ [Division Algorithm]}$$
Then by theorem 4.2 - deg$a(x) =$ deg$b(x)+$ deg$h(x)$
Since the degrees are non-negative $\Rightarrow$ deg$b(x) \leq$ deg$a(x)$
$$\Rightarrow 0 \leq \deg b(x) \leq \deg a(x).$$

Definition: Let F be a field and $a(x), b(x) \in F[x]$ bot not zero. Greatest common divisor (GCD) if $a(x)$ and $b(x)$ is the monic polynomial of the highest degree that divides both $a(x)$ and $b(x)$.

In other words: $d(x)$ is the gcd of $a(x)$ and $b(x)$ provided that $d(x)$ is the monic, and:
(1) $d(x)|a(x)$ and $d(x)|b(x)$
(2) If $c(x)|a(x)$ and $c(x)|b(x)$ then deg$c(x) \leq$ deg$d(x)$

Note
Monic: in a polynomial $F[x]$ is said to be monic if its leading coefficient is 1_F

Example. $a(x) = 2x^4 + 5x^3 - 5x - 2 = (2x+1)(x+2)(x+1)(x-1)$
$$b(x) = 2x^3 - 3x^2 - 2x = x(2x^2 - 3x - 2) = x(2x+1)(x-2)$$
then $\gcd(a(x), b(x)) = 2x + 1$?
No: $x + \frac{1}{2}$

Day 25

Hint towards Homework

Section 4.2 Problem 5
(c) $x^3 - ix^2 + 4x - 4i$, $x^2 + 1$ in $\mathbb{C}[x]$
$$x^3 - ix^2 + 4x - 4i = x^2(x-i) + 4(x-i) = (x^2+4)(x-i)$$
$$x^2 + 1 = (x-i)(x-i)$$

Last Time

$b(x)|a(x) \iff a(x) = b(x)h(x)$ for some $h(x) \in F[x]$

This Time

Theorem 4.8

Let F be a field and $a(x), b(x) \in F[x]$ both not zero, then there is a unique gcd $d(x)$ of $a(x), b(x)$ (where unique is similar to monic). Furthermore, there are (not necessarily unique) polynomials $u(x), v(x) \in F[x]$ such that: $d(x) = a(x)u(x) + b(x)v(x)$

RECALL

$d = \gcd(a, b)$ there exists $u, v \in \mathbb{Z}$ such that $d = a \cdot u + b \cdot v$ - Well-ordering Axiom
$p \mid b \cdot c \Rightarrow p \mid b$ or $p \mid c$ then p is prime.

Proving this

Step 1: Non-empty

Consider S: linear combination of $a(x)$ and $b(x)$, $S = \{a(x)m(x) + b(x)n(x)|m, n \in F[x]\}$
Find a monic polynomial of smallest degree in S.
Use the Well-ordering Principle to show that:
If $a(x) \in S$ then $a(x) \in F[x]$
Note: $a(x) \cdot a(x) + b(x) \cdot b(x) = a(x)^2 + b(x)^2 \geq 0$
$S^+ = \{a(x) \cdot m(x) + b(x) \cdot n(x)|m(x), n(x) \in F[x] \text{ and } a(x) \cdot m(x) + b(x) \cdot n(x) \geq 0\}$
So, S^+ is a non-empty set.
Then, by well-ordering principle, S^+ must contain the smallest polynomial, which we will call $t(x)$.

Step 2: Prove that $t(x) = \gcd(a(x), b(x))$

Must check two things:
(i) $t(x) \mid a(x)$ and $t(x) \mid b(x)$
(ii) If $c(x) \mid a(x)$ and $c(x) \mid b(x)$ then $c(x) \leq t(x)$

Proving (i): Show that $t(x) \mid a(x)$ **and** $t(x) \mid b(x)$

By Division Algorithim, there are $q(x), r(x) \in F[x]$ such that $a(x) = t(x)q(x) + r(x)$ where $0 \leq \deg r(x) < \deg t(x)$

$$r(x) = a(x) - t(x)q(x) = a(x) - (a(x) \cdot u(x) + b(x) \cdot v(x))q(x)$$
$$\Rightarrow r(x) = a(x) - a(x) \cdot u(x) \cdot q(x) - b(x) \cdot v(x) \cdot q(x)$$
$$\Rightarrow r(x) = a(x)(1 - u(x) \cdot q(x)) + b(x)(-v(x) \cdot q(x))$$

Thus, $r(x) = a(x)(1 - u(x) \cdot q(x)) + b(x)(-v(x) \cdot q(x)) \in S$ when $u(x), q(x), v(x) \in F[x]$
Since $\deg r(x) < \deg t(x)$ and $t(x)$ is the monic polynomial in S and $\deg r(x) \geq 0$
we know that $\deg r(x) = 0$
So, when $\deg r(x) = 0$ in $a(x) = t(x)q(x) + r(x) \Rightarrow t(x) \mid a(x)$
There is a similar arguement for $b(x)$.
We can show that $t(x) \mid b(x)$ in the same manner.

Proving (ii) : If $c(x) \mid a(x)$ **and** $c(x) \mid b(x)$ **then deg**$c(x) \leq$ **deg**$t(x)$

If $c(x) \mid a(x)$ and $c(x) \mid b(x)$ then $\exists k(x), s(x) \in F[x]$ such that $a(x) = c(x)k(x)$ and $b(x) = c(x)s(x)$
Again: t is the smallest polynomial of S.

$$t(x) = a(x) \cdot u(x) + b(x) \cdot v(x) = (c(x)k(x))u(x) + (c(x)s(x))v(x) = c(x)(k(x)u(x) + s(x)v(x))$$
Where $k(x)u(x) + s(x)v(x) \in f[x]$
This implies that $c(x) \mid t(x)$
Which implies that $\deg c(x) \leq \deg|t(x)| = \deg t(x)$

Corollary 4.9

Let F be a field and $a(x), b(x) \in F[x] \neq 0$. A monic polynomial $d(x) \in F[x]$ is gcd of $a(x), b(x) \iff$ (i) $d(x) \mid a(x)$ and $d(x) \mid b(x)$ and (ii) If $c(x) \mid a(x)$ and $c(x) \mid b(x)$ then $c(x) \mid d(x)$

Proving this

Proving $\Rightarrow$

1. $\gcd(a(x), b(x)) = d(x) \Rightarrow$ (i) $d(x) \mid a(x)$ and $d(x) \mid b(x)$ and (ii) If $c(x) \mid a(x)$ and $c(x) \mid b(x)$ then $c(x) \mid d(x)$

(i) By definition: If $d(x) = \gcd(a(x), b(x))$ then $d(x) \mid a(x)$ and $d(x) \mid b(x)$
(ii) If $d(x) = \gcd(a(x), b(x))$ then $d(x) = a(x)u(x) + b(x)v(x)$ where $u(x), v(x) \in F[x]$ by Theorem 4.8
So, if $c(x) \mid a(x)$ and $c(x) \mid b(x)$ can we prove that $c(x) \mid d(x)$?
Let $a(x) = c(x)k(x)$ and $b(x) = c(x)s(x)$ for some $k(x), s(x) \in F[x]$
Plug in to $d(x) = a(x)u(x) + b(x)v(x)$
$d(x) = (c(x)k(x))u(x) + (c(x)s(x))v(x) \Rightarrow c(x)(k(x)u(x) + s(x)v(x))$ where $k(x)u(x) + v(x)s(x) \in F[x]$
Then by definition, $c(x) \mid d(x)$
Thus when $\gcd(a(x), b(x)) = d(x) \Rightarrow$ (i) $d(x) \mid a(x)$ and $d(x) \mid b(x)$ and (ii) If $c(x) \mid a(x)$ and $c(x) \mid b(x)$ then $c(x) \mid b(x)$

Proving $\Leftarrow$

2. (i) $d(x) \mid a(x)$ and $d(x) \mid b(x)$ and (ii) If $c(x) \mid a(x)$ and $c(x) \mid b(x)$ then $c(x) \mid b(x) \Rightarrow \gcd(a(x), b(x)) = d(x)$

If $d(x)$ is a polynomial that satisfies (i) and (ii) then $\gcd(a(x), b(x)) = d(x)$
Proving (i)
This is trivial: by definition this is true.
Proving (ii)
If $c(x) \mid a(x)$ and $c(x) \mid b(x)$ then $c(x) \mid d(x)$
This implies that $\deg c(x) \leq \deg|d(x)| = \deg d(x)$
Thus $\deg c(x) \leq \deg d(x)$
Thus when $c(x) \mid a(x)$ and $c(x) \mid b(x)$ then $c(x) \mid d(x) \Rightarrow \gcd(a(x), b(x)) = d(x)$

Since both conditions imply the $\gcd(a(x), b(x)) = d(x)$ we know the statement is true.

Therefore, $d(x) \in F[x]$ is gcd of $a(x), b(x) \iff$ (i) $d(x) \mid a(x)$ and $d(x) \mid b(x)$ and (ii) If $c(x) \mid a(x)$ and $c(x) \mid b(x)$ then $c(x) \mid d(x)$ is a true statement.

Theorem 4.10

Let F be a field and $a(x), b(x) \in F[x]$. If $a(x)|b(x)c(x)$ and $a(x), b(x)$ relatively prime ($d(x) = 1$) then $a(x)|c(x)$.

Proving this

Since $(a(x), b(x)) = d(x) = 1$ by Theorem 4.8 $\exists u(x), v(x) \in F[x]$ such that $a(x)u(x) + b(x)v(x) = 1$.

Multiply by $c(x)$

$a(x)u(x)c(x) + b(x)v(x)c(x) = c(x)$ and see $a(x) \mid b(x)c(x) \Rightarrow b(x)c(x) = a(x)r(x)$ for some $r(x) \in F[x]$

$$a(x)u(x)c(x) + v(x)(a(x)r(x)) = c(x)$$
$$a(x)(u(x)c(x) + v(x)r(x)) = c(x)$$

Thus, $a(x) \mid c(x)$

Section 4.3: Irreducibles and Unique Factorizations

$f(x)$ is an associate of $g(x)$ in $f[x] \iff f(x) = c \cdot g(x)$ for some $c \neq 0 \in F$

Example. $3x^2 + 2 \Rightarrow x^2 + \frac{2}{3}$

Definition: Let F be a field. A non-constant polynomial $p(x) \in F[x]$ is said to be irreducible if its only divisors are its associates and the non-zero constant.

Note

A constant polynomial that is not irreducible $\Rightarrow$ reducible.

Note

every degree 1 polynomial in $F[x]$ is irreducible in $F[x]$.

Theorem 4.11

Let F be a field. A non-zero polynomial $f(x)$ is reducible in $F[x] \iff f(x)$ can be written as a product of two polynomials of a lower degree.

Proving this

$\Rightarrow$ First. Assume $f(x)$ is reducible.

Then it must have a divisor $(g(x))$ that is neither an associate or a non-zero constant

such that $f(x) = g(x)h(x)$ some $h(x) \in F[x]$

(prove $g(x), h(x)$ degree strictly less then $f(x)$).

Second. Proof by Contradiction: $\deg f(x) = \deg g(x) \Rightarrow \deg h(x) = 0 \Rightarrow h(x)$ is a constant.

(same for $g(x) = c$) which contradicts the above statement that $g(x)$ is not an associate.

$\Leftarrow$ Almost trivial by definition.

If divisors both lower degree then they are not associate because associate $\Rightarrow$ same degree.

Theorem 4.12

Let F be a field and $p(x)$ a non-constant polynomial in $F[x]$, then the following are equivalent:

(i) $p(x)$ is irreducible

(ii) $b(x), c(x) \in F[x]$ such if $p(x)|b(x)c(x)$ then $p(x)|b(x)$ or $p(x)|c(x)$

(iii) If $r(x), s(x) \in F[x]$ such that $p(x) = r(x)s(x)$ then $r(x)$ or $s(x)$ is a non-zero constant polynomial.

Day 26

Going over Homework

Section 4.3 Problem 6

$x^2 + 1 = (ax + b)(cx + d)$ in $\mathbb{Q}[x]$

$= acx^2 + (bc + ad)x + bd$ where $ac = 1$ and $bd = 0$ and $bc + ad = 0$

Show this impossible: $a = \frac{1}{c}$, $\frac{c}{d} + \frac{d}{c} = \frac{c^2+d^2}{cd} = 0$, $b = \frac{1}{d}$

$\Rightarrow c^2 + d^2 = 0$ But since c, d non-negative, only true is when $c^2, d^2 = 0$ which contradicts that they are not 0

This Time

Theorem 4.14

Let F be a field. Every non-constant polynomial $f(x) \in F[x]$ is a product of irreducible polynomials in $F[x]$. The factorization is unique in that:
if $f(x) = p_1(x)p_2(x)\dots p_r(x)$ and $f(x) = q_1(x)q_2(x)\dots q_s(x)$ with $p_i(x), q_i(x)$ irreducible then $r = s$

After re-ordering and re-naming: $p_i(x)$ is an associate of $q_i(x)$ for $i = 1, 2, \dots r$

Proving this
Prove by contradiction.

Let S be the set of all integers greater than 1 that are not a product of primes.

Prove that $S = \emptyset$

So say that $S = \emptyset$, then by Well - Ordering Axiom S contains the smallest positive element $m(x)$

$m(x)$ is not prime, then there exists $a(x), b(x) \in F[x]$ such that $m(x) = a(x) \cdot b(x)$

Know, this implies $a(x), b(x) \notin S$

which means that they are a product of primes.

$a(x)$ be represented by $a(x) = p_1(x) \cdot p_2(x) \cdot \dots p_r(x)$

$b(x)$ represented by $b(x) = q_1(x) \cdot q_2(x) \cdot \dots q_s(x)$

Where all $p_i(x), q_i(x)$ are primes $\Rightarrow a(x) \cdot b(x) = p_1(x) \cdot q_1(x) \cdot p_2(x)q_2(x) \cdot \dots p_r(x) \cdot q_s(x)$

Then, $m(x)$ is the product of primes.

This contradicts that $m(x)$ is an element of S which only holds the integers that are not products of primes.

Therefore, S must be the empty set.

Example. 1

$f(x) = (2x - 2)(\frac{1}{2}x - 1)(x - 3) = (x - 1)(x - 2)(x - 3) = (x^2 - 3x + 2)(x - 3)$

Example. 2

377121 is this a prime number: no.

quick way to so this: $x^{17} + x^5 + 1$ this is the same

no quick way to prove that it is irreducible

Section 4.4: Polynomial Functions, Roots, and Reducibility

If R is a commutative ring $a_nx^n + \dots a_2x^2 + a_1x + a_0 \in R[x]$ is a function $f : R \to R$ for each $r \in R$, $f(r) = a_nr^n + \dots a_2r^2 + a_1r + a_0$

Example. 1

$x^2 + 5x + 3 \in \mathbb{R}[x]$, $f(x) = 1 + 5 + 3 = 9$

Question: two polynomials in a ring, then for any r in function does $f(r) = g(r) \Rightarrow f(x) = g(x)$? What about for reals?

Example. 2

$f(x) = x^4 + x + 1 \in \mathbb{Z}_3[x]$. $f : \mathbb{Z}_3 \to \mathbb{Z}_3$

$f(0) = 1$, $f(1) = 0$, $f(2) = 16 + 2 + 1 = 19 = 1$

$g(x) = x^3 + x^2 + 1 \in \mathbb{Z}_3[x]$. $g : \mathbb{Z}_3 \to \mathbb{Z}_3$

$g(0) = 1$, $g(1) = 0$, $g(2) = 1$

So no.

$f(r) = g(r) \not\Rightarrow f(x) = g(x)$

Definition: Let R be commutative. $f(x) \in R[x]$. An element $a \in R$ is said to be a root (or zero) of polynomial $f(x)$ if $f(a) = 0_R$

Example. 1

The root of $f(x) = x^2 - 3x + 2 \in R[x]$ are: $(x - 2)(x - 1)$

So. 1 and 2

Example. 2

The root of $x^2 + 1 \in \mathbb{R}[x]$: none

But, in $\mathbb{C}$: $-i$ and i

Note

Some polynomials are reducible but do not have roots

Example. 3

$f(x) = (x^2 + 1)(x^2 + 1) \in \mathbb{R}[x]$

Has no roots in $\mathbb{R}[x]$ but is reducible

So, if F has roots $\Rightarrow f$ is reducible BUT f is reducible $\not\Rightarrow f$ has roots

Theorem 4.15: The remainder theorem

Let F be a field, $f(x) \in F[x]$ and $a \in F$. The remainder when $f(x)$ divided by the polynomial $x - a$ is $f(a)$

Proving this

Division Algorithm:

$f(x) = (x - a)Q(x) + r$ where $r \in F$

Consider $f(a) = r$

Example. $f(x) = x^8 + x^7 + 2$, $(x - 1)$
$f(1) = 4$

End of Week 9!

Class Notes; Week 10, 3/23/2016

Day 27

Going Over Quiz

Problem 1
$3x + 2$ in $\mathbb{Z}_9$
$1, 2, 3, 4, 5, 6$
$6x + 4$, $2x + 6$, ...

Problem 2
Find gcd $x + a + b | x^3 + a^3 + b^3 - 3abx$
$x^3 + a^3 + b^3 - 3abx = (x + a + b)(x^2 + a^2 + b^2 - ax + bx - ab)$
replace x, a, b symmetric $xa^2 + xb^2$

This Time

Theorem 4.15

Let $F[x]$ be a field, $f(x) \in F[x]$ and $a \in F$, then a is a root of $f(x) \iff x - a$ is a factor of $f(x)$

Proving this
$f(a) = 0 \iff x - a | f(x)$

$(\Rightarrow)$
If $f(a) = 0$, $f(a)$ is a remainder of $f(x)$
dividing $x - a$ see: $f(x) = (x - a)Q(x) + f(a)$ where $f(x) = (x - a)Q(x) \Rightarrow (x - a)|f(x)$
$(\Leftarrow)$
If $f(x) = (x - a)Q(x)$
Replace $x = a$ then: $f(a) = (a - a)Q(x) = 0Q(x) = 0$

Example. $f(x) = x^3 - x^2 + x - 1$
$f(1) = 0 \Rightarrow x - 1 | f(x) \Rightarrow$ reducible
If $f(x)$ has a root r, then $f(x)$ is reducible
(*) $(\Leftarrow)$ $f(x) = (x^2 + 1)(x^2 + 2) \in \mathbb{R}$

Corollary 4.17

Let F be a field $f(x) \in F$ with $\deg f \geq 2$. If f is irreducible in $F[x]$ then $f(x)$ has no roots.

Corollary 4.18

If $\deg f \leq 3$ and f reducible (except $\deg f = 1$) then f has a root in F

(*) deg$f \leq 3 \Rightarrow$ when f is reducible $\Rightarrow f$ has a degree 1 factor $\Rightarrow f$ has a root.

Corollary 4.19

If deg$f = 2$ or 3, f is irreducible $\iff f$ has not roots in F.

Example. Prove $x^3 + x + 1$ irreducible in $\mathbb{Z}_5[x]$:
$f(0) = 1$, $f(1) = 3$, $f(2) = 8 + 2 + 1 = 1$
$f(3) = 27 + 3 + 1 = 1$, $f(4) = 64 + 4 + 1 = 4$
None are 0 and has no roots.

Note
Proving it has no roots is not enough, also state if ddeg2 or deg3.

Section 4.5: Irreducibility in $\mathbb{Q}[x]$

Rational root test

polynomial in $Q[x] \Rightarrow f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots a_2x^2 + a_1x + a_0$. If $r \neq 0$ and $\frac{r}{s}$ is a root of $f(x)$ then $r|a_0$ and $s|a_n$.
(*) $\frac{r}{s} \Rightarrow sx - r|f(x)$

Example. $f(x) = 2x^4 + x^3 - 21x^2 - 14x + 12$
x could $= \pm 1, 2, 3, 4, 6, 12$ and $2x$ could $= \pm 1, 3$
$f(-3) = 0$, $x + 3|f(x)$, $f(\frac{1}{2}) = 0 \Rightarrow 2x - 1|f(x)$
So. $(x + 3)(2x - 1)(x^2 - 2x - 4)$

Question: prove $f(x) = x^{18} + 2x^6 + 4x^5 + 10x - 2$ is irreducible?

Theorem 4.23 (Eisenstein's Criterion)

$f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$. If there is a prime p such that $p|a_0 \ldots a_{n-1}$ but $p \not| a_n$ and $p^2 \not| a_0$ then $f(x)$ irreducible.

Example. 1
Pick 2 for $f(x) = x^{18} + 2x^6 + 4x^5 + 10x - 2$.
$2|a_i$ for all a_i , $1 \leq i \leq 18$
$2|a_18$, $2^2 \not| a_0$ by Eisenstein criterion

Example. 2
$x^{17} + 6x^{13} - 15x^4 + 3x^2 + 12$
$p = 3$

Proving this

if $f(x)$ irreducible: $f(x) = (b_0 + b_1x + \ldots b_rx^r) \cdot (c_0 + c_1x + \ldots c_sx^s)$
then $a_0 = b_0 \cdot c_0$
$p^2 \not| a$ and $p|a_0 \Rightarrow p|b_0$ or $p|c_0$

Day 28

Review for Exam 2

Question 1
Definition: What is a ring isomorphism? example.

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.

Example
field of $2X2$ matrices of $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_2(\mathbb{R})$

Question 2
Definition: What is a ring homomorphism? example (only homomorphic not isomorphic).

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 $a, b \in R$

Question 3
$f : \mathbb{R} \to \mathbb{R}$ where $f(x) = ax + b$. If f is a homomorphism, can we solve for a, b?

$f(x + y) = a(x + y) + b$
$f(x) + f(y) = ax + ay + b + b = a(x + y) + 2b$
Then, for $f(x + y) = f(x) + f(y) \Rightarrow b = 0$
$f(xy) = axy + b = axy$
$f(x)f(y) = (ax + b)(ay + b) = (ax)(ay) = a^2xy$
Then for $f(xy) = f(x)f(y) \Rightarrow a = 1$ or 0

Question 4
If R is commutative then $R[x]$ commutative. Prove this.

Suppose $f(x) = a_0 + a_1x + a_2x^2 \ldots a_nx^n$ and $g(x) = b_0 + b_1x + b_2x^2 \ldots b_mx^m$
R commutative: $g(x)f(x)b_0a_0 + (b_1a_0 + b_0a_1)x \ldots$ and $f(x)g(x) = g(x)f(x)$
Largest x is $n + m$ but $a_nb_m \neq 0_R$ because $a_n \neq 0_R$ and $b_m \neq 0_R$
So. $\deg[f(x)g(x)] = n + m = \deg f(x) + \deg g(x)$ and $f(x)g(x)$ non-zero.

Question 5
a.) If R is an integral domain, so is $R[x]$? T or F.
b.) If R is a field, so is $R[x]$? T or F.

a.) True: Similar to last proof :
$f \neq 0$, $g \neq 0 \Rightarrow fg \neq 0$
If $fg = 0 \Rightarrow f = 0$ or $g = 0$
b.) Not always true, so the question is false.
$\mathbb{R}(x) = 3x + 1$, $\mathbb{R}(x) \in \mathbb{R}[x]$
the inverse is $\frac{1}{3x+1} \notin \mathbb{R}[x]$

Question 6
GCD of $x^5 + x^4 + 2x^3 - x^2 - x - 2$ in $\mathbb{Q}[x]$ and $x^4 + 2x^3 + 5x^2 + 4x + 4$ in $\mathbb{Q}[x]$

$$x^5 + x^4 + 2x^3 - x^2 - x - 2 = x^3(x^2 + x + 2) - 1(x^2 + x + 2) = (x^3 - 1)(x^2 + x + 2)$$
$$x^4 + 2x^3 + 5x^2 + 4x + 4 = x^2(x^2 + x + 2) + x(x^2 + x + 2) + 2(x^2 + x + 2) = (x^2 + x + 2)^2$$
and the gcd= $x^2 + x + 2$

Question 7
Find monic associate of $3x^5 - 4x^2 + 1$ in $\mathbb{Z}_5[x]$

$1, 2, 3, 4$ units in $\mathbb{Z}_5[x]$:
$3x^5 - 4x^2 + 1$, $x^5 - 3x^2 + 2$, $4x^5 - 2x^2 + 3$, $2x^5 - x^2 + 4$
all monic associates.

Question 8
a.) Prove if $f(x)$ has a root in F then $f(x)$ reducible
b.) Is converse statement correct? If not, give an example.

a.) $\exists r \in F$ such that $f(x) = r \iff x - r | f(x)$, $\Rightarrow f(x) = (x - r)Q(x)$
then f is reducible
b.) No.
ex. $f(x) = (x^2 + 1)(x^2 + 2)$

Question 9
a.) If $f(x)$ is reducible in $\mathbb{Q}[x]$ is it reducible in $\mathbb{Z}[x]$?
b.) If $f(x)$ reducible in $\mathbb{Z}[x]$ is it reducible in $\mathbb{Q}[x]$?

a.) No. Consider $f(x) = 2x^2 + x$
b.) Yes.
Proof by contradiction: Assume it does not.
Let p be a prime factor of the content $f(x)g(x)$, and apply the ring homomorphism $S : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ with $s : \mathbb{Z} \to \mathbb{Z}_p$ by $s(x) = S[x]$.
Then: $0 = S(f(x)g(x)) = S(f(x)S(g(x))$ so the product of the two non-zero polynomials in the integral domain of $\mathbb{Z}_p[x]$ is equal to zero.
This is a contradiction.

Suppose $f(x) \in \mathbb{Z}[x]$. divide $f(x)$ by its content and assume that it is primitive.
Suppose $f(x) = g(x)h(x)$ so that $g(x), h(x) \in \mathbb{Q}[x]$ have lower degrees.
Then $abf(x) = ag(x)bh(x)$ so that $a, b \in \mathbb{N}$ are the smallest integers so that $ag(x), bh(x) \in \mathbb{Z}[x]$.
Suppose c and d are the contents of $ag(x)$ and $bh(x)$ respectively, then $abf(x)$ has content ab and $abf(x) = ag(x)bh(x) = (c(g'(x))(d(h'(x))$ given that $g'(x), h'(x)$ are primitive.
Suppose if $f(x), g(x) \in \mathbb{Z}[x]$ primitive, then $f(x)g(x)$ is also. Then, $g'(x)h'(x)$ is primitive so that cd is the content of $abf(x)$.
$\Rightarrow ab = cd$
Thus. if $f(x)$ is reducible in $\mathbb{Z}[x]$ then it is reducible in $\mathbb{Q}[x]$.

You should be able to do all of these one your own.
Students went up in class and answered the first 7 questions, but you can find them in these notes.

Good Luck on Exam 2!

Day 29

Exam day

End of Week 10!