Class Notes; Week 11, 3/28/2016

Day 30

Question from Exam

(1) Equation resulting in 4 roots under $\mathbb{Z}_6$
$x \cdot (x+1) = 0$ then $[0], [2], [3], [5]$ all are roots in $\mathbb{Z}_6$
(2) Equation resulting in 4 roots under $\mathbb{Z}_8$
$(x-2) \cdot (x-4) = 0$ then $[0], [2], [4], [6]$ are all roots in $\mathbb{Z}_8$

This Time

Lemma 4.22

Let $f(x), g(x), h(x) \in \mathbb{Z}[x]$ with $f(x) = g(x) \cdot h(x)$.
If p is a prime that divides every coefficient of $f(x)$ then either p divides every coefficient of $g(x)$ or p divides every coefficient of $h(x)$

(similar to $p|a \cdot b \Rightarrow p|a$ or $p|b$)

Proving This

$$f(x) = a_0 + a_1 x + \cdots + a_k x^k \text{ , } p|a_i \text{ for all } 0 \le i \le k$$
$$g(x) = b_0 + b_1 x + \cdots + b_m x^m \text{ and } h(x) = c_0 + c_1 x + \cdots + c_n x^n$$
$$f(x) = g(x)h(x)$$

Now: Assume the Lemma is false, then p does not divide some coefficient of $g(x)$ and for some coefficient of $h(x)$.

Let b_r be the first coefficient of $g(x)$ not divisible by p, and c_t be the first coefficient of $h(x)$ not divisible by p

$$\Rightarrow p|b_i \forall 0 \le i \le r \text{ and } p|c_j \forall 0 \le j \le t$$

Consider: a_{r+t} of $f(x)$ since $f(x) = g(x)h(x)$

$$\Sigma_{i=0}^{r+t} b_i c_{r+t-i} = a_{r+t} = b_0 c_{r+t} + b_1 c_{r+t-1} + \cdots + b_{r+t} c_0$$
$$b_r c_t = a_{r+t} - [b_0 c_{r+t} + \cdots + b_{r-1} c_{t+1}] - [b_{r+1} c_{t-1} + \cdots + b_{r+t} c_0]$$

Where we see that a_{r+t} is a multiple of p by definition, $p|b_i \forall 0 \le i \le r$, and $p|c_j \forall 0 \le j \le t$

Then, all are multiples of p. $b_r c_t$ is a multiple of p.

So $p|b_r$ or $p|c_t$ contradicting b_r and c_t not divisible by p.

Theorem 4.23

Let $f(x)$ be a polynomial with integer coefficients.
Then, $f(x)$ factor as a product of polynomials of degree m and n in $\mathbb{Q}[x] \iff f(x)$ factors as a product of polynomials of degree m and n in $\mathbb{Z}[x]$.

Example. $f(x) = (x-1)(x-2)$ reducible in $\mathbb{Z}[x]$
and is therefore reducible in $\mathbb{Q}[x]$ since $\mathbb{Z} \subset \mathbb{Q}$.
Conversely:
If $f(x) = g(x)h(x)$, $g, h \in \mathbb{Q}[x]$ why can we say that $g, h \in \mathbb{Z}[x]$??
This is a homework problem.

Theorem 4.24

Eisenstein's Criterion:

$f(x) = a_0 + a_1 x + \dots a_n x^n \in \mathbb{Z}[x]$.
$p | a_0, a_1 \dots a_{n-1}$ and $p \nmid a_n$, $p^2 \nmid a_0 \Rightarrow f$ is irreducible in $\mathbb{Q}[x]$ ($\mathbb{Z}[x]$).

Proving This

If $f(x)$ reducible: $f(x) = (b_0 + b_1 x + \dots b_r x^r)(c_0 + c_1 x + \dots c_s x^s)$.
$b_i, c_j \in \mathbb{Z}$: $a_0 = b_0 c_0$ and $p | a_0 \Rightarrow p | b_0$ or $p | c_0$.
Also, $p^2 \nmid a_0 \Rightarrow p \nmid c_0$ if $p | b_0$
$a_n = b_r c_s$: Let b_k be the first of b_i not divisible by p
$p | b_i$ for $i < k$ and $a_k = b_0 c_k + b_1 c_{k-1} + \cdots + b_k c_0 \Rightarrow b_k c_0 = a_k - [b_0 c_k + b_1 c_{k-1} + \cdots + b_{k-1} c_1]$.
This creates a contradiction. Neither b_k or c_0 could be divisible by p but this shows they are.

Day 31

Got Exam 2 back

Going Over Exam

Problem 1 (1) $f(x)$ is irreducible: $\deg f < 4 \Rightarrow$ there exists y such that $f(y) = 0$
$\deg f = 1$ then it is not reducible
$\deg f < 4 \Rightarrow \deg f = 2$ or $\deg f = 3 \Rightarrow$ reducible implies having a degree 1 factor
If $\deg f = 2$ and reducible $\Rightarrow f = g(x)h(x)$ both degree 1. $f = g(x)h(x) = (ax+b)(cx+d) \Rightarrow f(\frac{-b}{a}) = 0$

Problem 3 (3) There exists a p prime
$p | a_i$, $0 \leq i < n$, $p \nmid a_n$ and $p^2 \nmid a_0$
then $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ irreducible in $\mathbb{Q}[x]$ / $\mathbb{Z}[x]$

(4) $x^5 + 7$
$p = 7$ then $7 \nmid a_5$, $7 | a_4, a_3, a_2, a_1, a_0$? , $7^2 \nmid a_0$

Problem 4 (1) $f(x) = x^{25} + 3x^4 - 8x^3 + 11x + 1$ divided by $x - 1$
Can do by long division, but quicker (correct way):
$f(1) = 1 + 3 - 8 + 11 + 1 = 8$

(2) Monic associate:
divide by i — $i \cdot (x^3 + 2 \cdot i \cdot x^2 - i \cdot x + i)$

(3) Is $x^3 - 3$ irreducible in $\mathbb{Z}_5$?

$$f(2) = 2^2 - 3 = 5 = 0$$
Thus $x - 2 | f(x)$.

Problem 5 (2) $\mathbb{Z}_6[x] : f(x) = x^2 + x$
Since $\mathbb{Z}_6$ no a field see: $0, 2, 3, 5$ are all roots

(3) $\mathbb{Z}_7$ is field
$f \in \mathbb{Z}_7[x]$ has four roots if $\deg f = 2$
No.

(4) $\mathbb{Z}_8[x] : f(x) = x^2 - 1$ with $1, 3, 5, 7$
or $g(x) = x^2 + 2x$ wih $0, 2, 4, 6$

This Time

From last time we know:
Theorem 4.23

$f(x)$ reducible in $\mathbb{Q}[x] \iff$ reducible in $\mathbb{Z}[x]$

Proving This

($\Leftarrow$) Trivial
$f(x) \in \mathbb{Z}[x]$. If $f(x) = g(x)h(x)$ and $g(x), h(x) \in \mathbb{Z}[x]$
then $g, h \in \mathbb{Q}[x]$ and f reducible in $\mathbb{Q}[x]$

($\Rightarrow$) If $f(x)$ reducible in $\mathbb{Q}[x]$
$f(x) = g(x)h(x)$ and $g(x), h(x) \in \mathbb{Q}[x]$

Side note: $q \in \mathbb{Q}$ then $q = \frac{b}{a}$ some $a, b \in \mathbb{Z}$ where $\gcd(a, b) = 1$

There exists: $c, d \in \mathbb{Z}$ such $c \cdot g(x) \in \mathbb{Z}[x]$ and $d \cdot h(x) \in \mathbb{Z}[x]$
Since $f = g \cdot h \Rightarrow c \cdot d \cdot f(x) = c \cdot g(x) d \cdot h(x)$. Where $c \cdot g(x) d \cdot h(x) \in \mathbb{Z}[x]$
and $c \cdot d \in \mathbb{Z}$ and $c \cdot d > 1$
There exists p prime such $p | c \cdot d \Rightarrow cd = pt$, $t \in \mathbb{Z}$
p divides every coefficient of $cdf(x)$.
By Lemma 4.22: p divides every coefficient of $c \cdot g(x)$ or p divides every coefficient of $d \cdot h(x)$
If p divides every coefficient of $c \cdot g(x)$ then $c \cdot g(x) = p \cdot k(x)$ some $k \in \mathbb{Z}[x]$
$\deg g(x) = \deg k(x)$
$p \cdot t \cdot f(x) = c \cdot d \cdot f(x) = c \cdot g(x) d \cdot h(x) = p \cdot k(x) d \cdot h(x) \Rightarrow t \cdot f(x) = k(x) d \cdot h(x)$
You repeat the process with any prime factor of t and cancel prime factors from both sides.

Eventually: $f(x)$ is the product of two integer coefficient polynomials.

Example. $f(x) = x^5 + 8x^4 + 3x^2 + 4x + 7$ in $\mathbb{Z}[x]$
Prove f is irreducible.
$x = \pm 1$ or ± 7
$[f]_2 = x^5 + x^2 + 1$ irreducible in $\mathbb{Z}_2[x]$

$$\text{If } f(x) \text{ is irreducible in } \mathbb{Z}_p[x] \ (p \text{ prime}) \text{ then } f \text{ is irreducible in } \mathbb{Z}[x].$$
$$\iff f \text{ reducible in } \mathbb{Z}[x] \text{ then } f \text{ is reducible in } \mathbb{Z}_p[x].$$
$$f = gh \in \mathbb{Z}[x]$$
$$[f]_p = [g]_p[h]_p$$
$$f = (x^2+3)(x+1) \Rightarrow [f]_3 = [x^2(x+1)]$$

Day 32

Quiz Day

Going Over Homework

This Time

Example. $f(x) = x^5 + 8x^4 + 3x^2 + 4x + 7$ irreducible in $\mathbb{Q}[x]$
$[f(x)]_2 = x^5 + x^2 + 1$ in $\mathbb{Z}_2[x]$
Prove irreducible in $\mathbb{Z}_2[x] \Rightarrow$ irreducible in $\mathbb{Q}[x]$

Theorem 4.25

Let $f(x) = a_k x^k + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ and p is positive prime that does not divides a_k.
If $\bar{f}(x)$ irreducible in $\mathbb{Z}_p[x]$ then $f(x)$ irreducible in $\mathbb{Q}[x]$.
$\bar{f}(x) = [a_k]_p x^k + \cdots + [a_1]_p x + [a_0]_p$ in $\mathbb{Z}_p[x]$

Proving This

If f(x) reducible in $\mathbb{Z}[x]$ then $\bar{f}(x)$ reducible in $\mathbb{Z}_p[x] \iff$ If $\bar{f}(x)$ is irreducible in $\mathbb{Z}_p[x]$ then $f(x)$ is irreducible in $\mathbb{Z}[x]$.

$$(\Leftarrow) \text{ Then } f(x) = g(x)h(x) \ , \ g, h \in \mathbb{Z}[x]$$
$$[f(x)]_p = [g(x)]_p[h(x)]_p \Rightarrow \bar{f}(x) = \bar{g}(x)\bar{h}(x) \ , \ \bar{g}, \bar{h} \in \mathbb{Z}_p[x]$$
$$\text{So: } \bar{f}(x) \text{ reducible in } \mathbb{Z}_p[x].$$

Example. deg1 factor: x , $x+1$; $f(0) = 1$, $f(1) = 1 \neq 0$

deg2 factor: $x^2 + x + 1$, $x^2 + 1$, $x^2 + x$, x^2
Where: x^2 not possible–reducible as x
$x^2 + x$ not possible–reducible as $x(x+1)$
$x^2 + 1$ not possible–reducible as $(x+1)^2 = x^2 + 2x + 1 = x^2 + 1$
gh at least one of degree≤ 2

$$(\Rightarrow) \text{ If false: } f(x) \text{ irreducible in } \mathbb{Z}[x] \not\Rightarrow \bar{f}(x) \text{ irreducible in } \mathbb{Z}_p[x]$$

Example. $x^2 + 1$ ireducible in $\mathbb{Z}[x]$ but reducible in $\mathbb{Z}_2[x]$

Section 4.6: Irreduciblity in $\mathbb{R}[x]$ and $\mathbb{C}[x]$

Theorem 4.26

"Fundamental Theorem of Algebra"
Every non-constant polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C} \iff \deg f = n$, $f \in \mathbb{C}[x]$ then f has n roots in $\mathbb{C}$.

Cor. 4.27

A polynomial irreducible in $\mathbb{C}[x] \iff$ deg1 polynomials.

Cor. 4.28

Every non-constant polynomial $f(x)$ of degree n in $\mathbb{C}[x]$ can be written in the form : $c(x-a_1)(x-a_2)\ldots(x-a_n)$ for some $c, a_1, a_2, \ldots, a_n \in \mathbb{C}$
This factorization is unique except the order of factors.

End of week 11!

Class Notes; Week 12, 4/4/2016

Day 33

Going Over Quiz

Question 2
(1) $\sqrt{p} \notin \mathbb{Q}$ for p positive prime.
$\sqrt{p} = \frac{m}{n} \Rightarrow p = \frac{m^2}{n^2}$ where $\gcd(m,n) = 1$
Eventually you get a contradiction.
(2) $x^2 - p$ has no rational roots $\rightarrow \pm\sqrt{p}$ is a root
By Rational root test: $ax + b$, $a|1$, $b|p \Rightarrow x = \pm 1$ or $\pm p$
Prove $f(\pm 1) \neq 0$, $f(\pm p) \neq 0$
$1 - p < 0$, $-1 - p < 0$, $p^2 - p = p(p-1) > 0$ which means none of the answers are rational
Thus: $\sqrt{p}$ irrational.

This Time

Lemma 4.29

If $f(x) \in \mathbb{R}[x]$ and $a + b_i$ is a root of $f(x)$ in $\mathbb{C}$ then $a - b_i$ is also a root of $f(x)$

Proving This

$$z = a + b_i \text{ , } \bar{z} = a - b_i$$
$$f \in \mathbb{R}[x] \text{ if } f(z) = 0 \Rightarrow f(\bar{z}) = 0$$
$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \text{ , } a_i \in \mathbb{R}$$
$$f(z) = 0 \Rightarrow a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$
$$\text{Here: we note the fact–}c \bar{+} d = \bar{c} + \bar{d} \text{ , also that–}\bar{cd} = \bar{c}\bar{d}$$
$$\text{If } \bar{c} = c \Longleftrightarrow c \in \mathbb{R}$$
$$0 = \bar{0} \Rightarrow f(\bar{z}) = a_n z^n + a_{n-1}z^{n-1}\bar{+} \cdots + a_1 z + a_0 = \bar{a_n}\bar{z^n} + \bar{a_{n-1}}\bar{z^{n-1}} + \cdots + \bar{a_1}\bar{z} + \bar{a_0} =$$
$$a_n \bar{z^n} + a_{n-1}\bar{z^{n-1}} + \cdots + a_1 \bar{z} + a_0 = f(\bar{z})$$
$$\text{Thus: } \bar{z} \text{ is also a root of } f(x)$$

Theorem 4.30

A ploynomial $f(x)$ is ireducible in $\mathbb{R}[x] \Rightarrow f(x)$ is a first degree polynomial of $f(x) = ax^2 + bx + c$ with $b^2 - 4ac < 0$

Proving This

Suppose $f(x)$ had deg≥ 2 and irreducible in $\mathbb{R}[x]$, then $f(x)$ has a root $w \in \mathbb{C}$ by theorem 4.26 (Fundamental Theorem).
By Lemma 4.29: $\bar{w}$ also a root of $f(x)$, $w \neq \bar{w}$
$f(x) = (x - w)(x - \bar{w})Q(x)$ in $\mathbb{C}[x]$ some $Q(x) \in \mathbb{C}[x]$.
Let $(x - w)(x - \bar{w}) = g(x)$ then $g(x) = (x - w)(x - \bar{w})$ where
$w = r + si \Rightarrow g(x) = (x - r - si)(x - r + si) = x^2 - 2rx + r^2 + s^2 \in \mathbb{R}[x]$

So: $g(x) \in \mathbb{R}[x]$. Then prove $Q[x] \in \mathbb{R}[x]$
By Division Algorithm: $f(x) = g(x)q(x) + r(x)$, $r(x) = 0$ or deg$r(x)$ <deg$g(x)$
Left for us to do on our own: Is $Q(x) \in \mathbb{R}[x]$.

Example. $x^4 + 1$
(1) $x^4 + 1 = (x - w)(x - \bar{w})Q(x) = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1) = x^4 + 1$
(2) $x^4 = -1 = cos(\pi) + isin(\pi) = e^{i\pi} = x^4 \Rightarrow x = e^{i\frac{\pi}{4}} = cos(\frac{\pi}{4}) + isin(\frac{\pi}{4}) = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i = w$

Cor. 4.31

Every polynomial of odd degree in $\mathbb{R}[x]$ has a root.

Proving This

By theorem 4.14:
$f(x) = p_1(x)p_2(x)\dots p_k(x)$ with p_i irreducible in $\mathbb{R}[x]$
Each $p_i(x)$ has degree of 1 or 2
deg$f$ =degp_1+deg$p_2 + \dots$ degp_k
Since $f(x)$ has odd degree at east 1 of $p_i(x)$ has deg$= 1$
then f has deg1 factor in $\mathbb{R}[x] \Rightarrow$ a root in $\mathbb{R}[x]$.

Day 34

Last Time

If $f \in \mathbb{R}[x]$ and f irreducible in $\mathbb{R}[x]$, deg$f \geq 2$ then f has a complex root $w \in \mathbb{C}$ ($w \notin \mathbb{R}$). f also has a root $\bar{w}$.
$f(x) = (x - w)(x - \bar{w})h(x)$ $h(x)? \in \mathbb{R}[x]$
If $w = r + si \Rightarrow (x^2 - 2rx + r2 + s^2)h(x) \Rightarrow f(x) = g(x)h(x)$
Division Algorithm.

This Time

$f(x)$ is real, $(x^2 - 2rx + r2 + s^2)$ is real $[\mathbb{R}[x]]$
Consider: $f(x) = g(x)q(x) + r(x)$ where $q(x), r(x)$ unique $\in \mathbb{R}[x]$
$q(x) = h(x)$, $r(x) = 0$
thus $h(x) \in \mathbb{R}[x]$.

Chapter 5

Congruence in $F[x]$ and Congruence Class Arithmetic

Definition

Let F be a field. $f(x), g(x), p(x) \in F[x]$ with $p(x) \neq 0$
Then $f(x)$ congruent to $g(x)$mod$p(x)$ (Noted: $f(x) \equiv g(x) \mod p(x)$)

Provided that $p(x)$ divides $f(x) - g(x)$.

Example. in $\mathbb{Q}[x]$.
$x^2 + x + 1 \equiv (x+2) \mod (x+1)$
$(x+1)h(x) = (x^2 + x + 1) - (x+2) = (x^2 - 1) = (x+1)(x-1)$
$\Rightarrow h(x) = x - 1$ and thus this is true.

Theorem 5.1

F is a field. $p(x) \neq 0$, $p(x) \in F[x]$. Then the relation of congruence class modulo $p(x)$ is:
(1) reflexive: $f(x) \equiv f(x) \mod p(x)$
(2) symmetric: if $f(x) \equiv g(x) \mod p(x)$ then $g(x) \equiv f(x) \mod p(x)$
(3) transitive: if $f(x) \equiv g(x) \mod p(x)$ and $g(x) \equiv h(x) \mod p(x)$ then $f(x) \equiv h(x) \mod p(x)$

Proving This

This is an adapted proof from Theorem 2.1

Theorem 5.2

F is a field. $p \neq 0$. $p(x) \in F[x]$.
If $f(x) \equiv g(x) \mod p(x)$ and $h(x) \equiv k(x) \mod p(x)$ then:
(1) $f(x) + h(x) \equiv g(x) + k(x) \mod p(x)$
(2) $f(x)h(x) \equiv g(x)k(x) \mod p(x)$

Proving This

This is an adapted proof from Theorem 2.2

Definition

F is a field. $f(x), p(x) \in F[x]$, $p \neq 0$.
Th congruence class (or residue class) of $f(x) \mod p(x)$ is denoted by: $[f(x)]$
And, consists of all polynomials in $F[x]$ that are congruent to $f(x) \mod p(x)$.
That is:
$[F(x)] = \{g(x) | g(x) \in F[x]$ and $g(x) \equiv f(x) \mod p(x)\}$
$[F(x)] = \{f(x) + k(x)p(x) | k(x) \in F[x]\}$

Example. 1
Congruence modulo $x^2 + 1$ in $\mathbb{R}[x]$
$[x^2 + 1] = \{2x + 1 + k(x)(x^2 + 1) | k(x) \in \mathbb{R}[x]\}$

Example. 2
Consider congruence modulo $x^2 + x + 1$ in $\mathbb{Z}_2[x]$
$[x^2] = [x+1] \iff x^2 \equiv (x+1) \mod (x^2 + x + 1)$
$x^2 + x + 1 | x^2 - (x+1) = x^2 + x + 1$

$$\{0,1\}\ ,\ ax+b \Rightarrow [0],[1],[x],[x+1]$$

Theorem 5.3

If $f(x) \equiv g(x) \mod p(x) \Longleftrightarrow [f(x)] = [g(x)]$

Cor. 5.4

2 congruence class modulo $p(x)$ are either disjoint or identical.

Cor. 5.5

Let F be a field and $p(x) \in F[x]$.
deg$p(x) = n$ and consider congruence modulo $p(x)$:
(1) If $f(x) \in F[x]$ and $r(x)$ is the remainder when $f(x)$ is divided by $p(x)$, then $[f(x)] = [r(x)]$
(2) Let S be the set consisting of zero polynomials and all the polynomials of deg$< n$ in $F[x]$.
Then every congruence class modulo $p(x)$ is the class of some polynomial in S and the congruence classes of different polynomials in S are distinct.

SUPER IMPORTANT:
The set of all congruent class modulo $p(x)$ is denoted:
$F[x]/(p(x))$

Example. 1
Consider congruence modulo x^2+1 in $\mathbb{R}[x]$.
-consider the remainder on division by x^2+1
$= [ax+b]? \cong \mathbb{C}$

Example. 2
$\mathbb{Z}_2[x]/(x^3+x+1) = [ax^2+bx+c]$ where $a,b,c \in \{0,1\}$
8 element solutions

Example. 3
$\mathbb{Z}_n[x]/(p(x))$
if deg$p(x) = k$ then the remainder: $a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$
answer is n^k.

Day 35

Quiz Day

Going Over Homework

Problem 18: part c

$$x^5+4x^4+2x^3+3x^2-x+5 \text{ in } \mathbb{Q}[x]$$
$$x = \pm1, \pm5\text{: } f(1) \neq f(-1) \neq f(5) \neq f(-5) \neq 0$$
$\underline{X}$ deg2 or deg3 proving all parts in modulo 2:

$$x^5 + x^2 + x + 1$$
If $x^5 + x^2 + x + 1$ irreducible in $\mathbb{Z}_2[x] \Rightarrow f$ irreducible in $\mathbb{Z}[x]$.
$\underline{X}$ $[f]_2 = x^5 + x^2 + x + 1$, $\bar{f}(1) = 0$
$x^2 + x + 1$ only irreducible: $x + 1|\bar{f}$: $\bar{f}$ reducible in $\mathbb{Z}_2[x]$
$\underline{\ldots}$ if $(x^2 + bx \pm 1$ or $(\pm 5)|f(x)$
On pg. 115 there is a guide for solving this.
Eventually solve for b unsolvable in $\mathbb{Z}[x]$
$$(x^3 + bx^2 + cx + 5)(x^2 + bx + 1)$$
$$bx^4 + ax^4 = 4x^2 \Rightarrow b + a = 4 \Rightarrow a = 4 - b$$
$$1 + ab + c = 2 \Rightarrow (4 - b)b + c = 2 \Rightarrow 4b - b^2 + c = 2$$
$$5a + c = -1 \Rightarrow c = -1 - 5a \Rightarrow c = -1 - 5(4 - b) \Rightarrow c = -1 - 20 + 5b \Rightarrow c = -21 + 5b$$
So: $4b - b^2 - 21 + 5b = 2 \Rightarrow -b^2 + 9b - 21 = 2 \Rightarrow b^2 - 9b + 21 = -2$

This Time

Section 5.2

$F[x]/(p(x))$

Example. $\mathbb{Z}_2[x]/(x^2 + x + 1) = [ax + b]$
$[x], [x + 1], [0], [1] \cong$: $\mathbb{Z}_4$? $\mathbb{Z}_2 X \mathbb{Z}_2$? *none*?
$x^3 \in \mathbb{Z}_2[x]$, $x^3 = (x^2 + x + 1)q(x) + r(x)$

Assume brackets:

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

*	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

(1) Is $\mathbb{Z}_2[x]/(x^2 + x + 1)$ an integral domain?
If $ab = 0 \Rightarrow a = 0$ or $b = 0$
Yes.
Is it a field?
Yes. $1 \to 1$, $x \to x + 1$, $x + 1 \to x$.
(2) $\mathbb{Z}_4$ is not a field.
(3) $\mathbb{Z}_2 X \mathbb{Z}_2$ is not a field:
$(1, 0) \cdot (a, b) = (1, 1)$? no.
So: $\mathbb{Z}_2[x]/(x^2 + x + 1)$ is not congruent to any of them.

End of week 12!

Class Notes; Week 13, 4/11/2016

Day 36

Going Over Quiz

Question 1
(1) $\mathbb{Z}_2[x]/(x^2+x+1)$ congruence classes:
$= [ax+b] = [0], [1], [x], [x+1]$
(2) Yes: because $\mathbb{Z}_2$ is a commutative ring $\Rightarrow \mathbb{Z}_2[x]/(x^2+x+1)$ is a commutative ring.
(3) Yes: every non-zero element has a multiplication inverse
$x(x+1) = x^2+x \equiv 1 \mod x^2+x+1$
(4) $\mathbb{Z}_2 X \mathbb{Z}_2$ is this a field?
No. $(1,0)\cdot(a,b) = (1,1)$, there does not exists (a,b) in $\mathbb{Z}_2 X \mathbb{Z}_2$.
(5)
(6) the choices for these are both not fields and it is thus impossible to have an isomorphic field to them.

Question 2
$\mathbb{Z}_3[x]/(x^3+2x+1) = [ax^2+bx+c]$ where $3^3 = 27$ congruence classes.
$[0], [1], [x], [x^2], [2], [2x], [2x^2], [x+1], [x+2], [x^2+x], [x^2+2x], [2x^2+x], [2x^2+2x], [2x+1], [2x+2], [x^2+1], [x^2+2], [2x^2+1], [2x^2+2], [2x^2+2x+2], [x^2+x+1], [x^2+x+2], [x^2+2x+1], [x^2+2x+2], [2x^2+x+1], [2x^2+x+2], [2x^2+2x+1]$
More generally $= [a_{n-1}x^{n-1} + \cdots + a_1x + a_0]$, $a_i \in \mathbb{Z}_k$ and k^n.

This Time

Theorem 5.7

Let F be a field and $p(x)$ a non-constant polynomial in $F[x]$.
Then the set $F[x]/(p(x))$ of congruence classes modulo $p(x)$ is a commutative ring with identity.
Furthermore– $F[x]/(p(x))$ contains a subring $F*$ isomorphic to F.

Example. $\mathbb{Z}_2[x]/(x^2+x+1)$ contains $\mathbb{Z}_2$ as a subring
(can be seen in the addition table)

Proving This

Let $F*$ as the subring of $F[x]/(p(x))$ consisting of the congruence classes of all the constant polynomials.
That is: $F* = \{[a] | a \in F\}$
$\varphi : F \to F*$
$\varphi(a) = [a]$
$\varphi(a+b) = [a+b] = [a]+[b] = \varphi(a)+\varphi(b)$
Similar for $\varphi(ab) = \varphi(a)\varphi(b)$
Definition shows φ is surjective.
If $\varphi(a) = \varphi(b) \Rightarrow a = b$. $[a] = [b]$. $a \equiv b \mod p(x) \Rightarrow a = b$ in F.
(proved bijection and homomorphism $\to$ isomorphism)

Example. $\mathbb{Z}/n \cdot \mathbb{Z} = \mathbb{Z}_n$
$[ab] = [a][b]$ and $[ba] = [b][a]$ we know integers are commutative.
So: $[ab] = [ba] \Rightarrow [a][b] = [b][a]$
(adapted from Theorem 2.7 for the rest of the proof)

$p(x)$ irreducible in $F[x]$ equivalent to saying $\mathbb{Z}_n$ is a field such that n prime.

Section 5.3: The Structure of F[x] / (p(x))

Theorem 5.10

Let F be a field and $p(x)$ a non-constant polynomial in $F[x]$.
Then the following statements are equivalent:
(1) $p(x)$ irreducible in $F[x]$
(2) $F[x]/(p(x))$ is a field.
(3) $F[x]/(p(x))$ is an integral domain.

Proving This

(1) $\rightarrow$ (2) by Theorem 5.9
(2) $\rightarrow$ (3) this is trivial
(3) $\rightarrow$ (1) refer to: $\mathbb{Z}_n$ is an integral domain $\Rightarrow n$ prime.
Also:
$\mathbb{Z}_p = \{[0], [1], \ldots, [p-1]\}$
Derive from: if $\gcd(a, b) = 1$ then there exists a $u, v \in \mathbb{Z}$ such $au + bv = 1$
$\gcd(a, p) = 1$ if $a \neq 0$, $au + bv = 1 \Rightarrow au \equiv 1 \mod p$ in polynomials readily prim means that only common factor is a constant.

Theorem 5.9

Let F be a field and $p(x)$ a non constant in $F[x]$.
If $f(x) \in F[x]$ and relatively prime to $p(x)$ then $[f(x)]$ is a unit in $F[x]/(p(x))$

Proving This

By Theorem 4.5 we see there exists $u(x), v(x)$ such that $f(x)u(x) + p(x)v(x) = 1 \Rightarrow f(x)u(x) \equiv 1 \mod p(x)$ and $[u(x)]$ is multiplicative inverse of $[f(x)]$ in $F[x]/(p(x))$.

Day 37

F is a field.
$F[x]/(p(x))$ -definition
-commutative with identity.

Theorem 5.10

Let F be a field and $p(x)$ a non-constant polynomial in $F[x]$.

Then the following statements are equivalent:
(1) $p(x)$ irreducible in $F[x]$
(2) $F[x]/(p(x))$ is a field.
(3) $F[x]/(p(x))$ is an integral domain.

SIDENOTE: R is a field $\Rightarrow R[x]$ ia an integral domain.
$\mathbb{Z}_2[x]/(x^2+x+1)$, $\mathbb{Z}_2[x]/(x^2)$, $\mathbb{Z}_2[x]/(x^2+1)$

Proving This

$$(3) \Rightarrow (1)\ F[x]/(p(x)) \text{ is an integral domain} \Rightarrow p \text{ ireducible in } F[x]$$
$$\text{Contra-positive } p \text{ reducible} \Rightarrow F[x]/(p(x)) \text{ not an integral domain.}$$
$$p(x) = r(x)s(x)\ ,\ [r(x)], [s(x)] \in \mathbb{R}$$
$$\deg r\ ,\ \deg s < \deg p$$
$$[r(x)][s(x)] = [p(x)] = 0$$

Theorem 5.11

Let F be a field and $p(x)$ irreducible in $F[x]$.
Then $F[x]/(p(x))$ is an extension field of F that contains a root of $p(x)$

$$(F \subseteq G \text{ both fields, the } G \text{ extension of } F)$$

Proving This

$$F[x]/(p(x)) \text{ is a field by Theorem 5.10 and contains } F$$
$$\text{Let } \alpha = [x]\ ,\ p(x) = a_n x^n + \cdots + a_1 x + a_0\ ,\ a_i \in F$$
$$a_n\alpha^n + \cdots + a_1\alpha + a_0 \in F[x]/(p(x)) \Rightarrow a_n[x]^n + \cdots + a_1[x] + a_0 = p(x) = 0$$

Cor. 5.12

F be a field.
$f \in F[x]$. f not constant then there exists an extension field K of F containing a root of $f(x)$.

Example. $F[x]/(p(x))$. $\mathbb{R}[x]/(x^2+1) \neq \mathbb{R}[i] \cong \mathbb{C} = \{ai + b | a, b \in \mathbb{R}\}$
So: anything $\mathbb{R}[x]/(x^2+1) = [ax+b]$, $a, b \in \mathbb{R}$

Can we define a map φ
$[ax+b][cx+d] = [acx^2 + (ad+bc)x + bd] | (x^2+1)$
$= (ad+bc)x + bd - ac$
$= (ad+bc)i + bd - ac$
$(ai+b)(ci+d) = (ad+bc)i + bd - ac$

Example. $\mathbb{Q}(\sqrt{2}) = \{a\sqrt{2} + b | a, b \in \mathbb{Q}\} \cong \mathbb{Q}[x]/(x^2-2)$

Day 38

Going over Homework

Chapter 6

Ideals

Definition

A subring I of a ring R is an ideal if $\forall r \in R$ and $a \in I$ then $ra \in I$ and $ar \in I$

Example. 1

In $\mathbb{Z}$, $3\mathbb{Z} = \{0, \pm 3, \pm 6 \dots\}$ is an ideal in $\mathbb{Z}$

Example. 2

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \text{ is an ideal in } M_2(\mathbb{R}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} |a, b, c, d \in \mathbb{R}\}$$

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} ar + sb & 0 \\ at + ub & 0 \end{pmatrix}$$

$$\text{BUT: } \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \cdot \begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} ar & as \\ br & bs \end{pmatrix}$$

Example. 3

$$g \in I = \{f : \mathbb{R} \to \mathbb{R} \text{ and } f(2) = 0 \text{ , } f \text{ is continuous } \}$$

$$f \in \mathbb{R} \text{ continuous function } \mathbb{R} \to \mathbb{R}$$

$$fg \in I \text{ and } gf \in I$$

$$f(2)g(2) = g(2)f(2) = 0$$

End of Week 13!