

Differential Equations Math 460 - Rosen, 2018

Trevor Klar

September 13, 2018

Contents

Introduction	1
1 Introduction	2
2 Rings	2
3 actual lecture starts here	3
4 Index	14

Note: If you find any typos in these notes, please let me know at trevor.klar.834@my.csun.edu. If you could include the page number, that would be helpful.

Note to the reader: I have highlighted topics which seem important to me, but the emphasis is mine, not Professor Fuller's. Bear that in mind when studying.

1 Introduction

This will be a course on ring theory and group theory, and we'll start with ring theory.

2 Rings

Definition. A ring R is a set with two binary operations, $+$ and \cdot which satisfy the following axioms $\forall a, b, c \in R$:

R1 $+$ commutative

R2 $+$ associative

R3 $+$ identity

R4 $+$ inverse

R5 \cdot associative

R6 \cdot left, right distributive

R5 \cdot identity (we are assuming all rings are rings with unity)

Definition. If, in addition, the ring has the \cdot commutative property, we say that it is a **commutative ring**.

Theorem. every element of a ring has a unique additive inverse:

Proposition. $a \cdot 0 = 0$

Proposition. $-a = -1 \cdot a$

Proposition. $(-a)b = a(-b) = -(ab)$

Definition. S is a **subring** of R if $s \subseteq R$ and $1_S = 1_R$ and S with the same $+$ and \cdot is ring.

To check S is a subring, just check

- closure under $+, \cdot$,
- $0_R \in S$
- $1_R \in S$
- $a \in S \implies -a \in S$.

Here are some examples of rings:

1. $\mathbb{Q}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$

2. R any ring, $R[x] =$ the set of all polynomials with coefficients in R .

$$R[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in R, n \text{ varies}\}.$$

3. $R[x, y] = R[x][y] = R[y][x]$

Definition. we say that $\deg 0- = \inf$ (or that 0 has no degree), and for some polynomial $P(x)$, $\deg(P(x))$ is what you think.

Definition. If R is a ring and there exists some $a, b \in R$ such that $a, b \neq 0$ and $ab = 0$, then we say a and b are **zero divisors**.

Definition. A commutative ring with no zero divisors is called an **integral domain**.

Proposition (Cancellation property for integral domains). for R an I.D. and $ab = ac$ with $a \neq 0$, then $b = c$.

[jpg]

Definition. a **field** is a commutative ring in which every nonzero element has a multiplicative inverse (which is unique, prove it) , ex $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

Proposition. every field is an I.D, because if $ab = 0$ and $a \neq 0$, then $a^{-1}(ab) = a^{-1}0$ which means $b = 0$.

Proposition. If R, S rings, then $R \times S$ is a ring (when equipped with componentwise addition and multiplication). By the way, unity is $(1_R, 1_S)$ and the identity is $(0_R, 0_S)$.

[jpg]
[jpg]
[jpg]

3 actual lecture starts here

Definition. A non-constant polynomial in $F[x]$ is called **irreducible** when if $f(x) = g(x)h(x)$, then either $g(x)$ or $h(x)$ is constant.

Proposition. Let $f(x) \in F[x]$. If $\deg f(x) = 2$ or 3 , then $f(x)$ is irreducible iff it has no roots in F .

Example. $f(x) = (x^2 + 1)^2 \in \mathbb{R}[x]$ is reducible, but has no real roots.

Theorem (Rational Root Test). Let $f(x) \in \mathbb{Z}[x]$ where $f(x) = a_n x^n + \cdots + a_1 x + a_0$.

$\frac{r}{s}$ (in lowest terms) is a rational root iff $r|a_0$ and $s|a_n$.

Theorem. Let $f(x) \in F[x]$ where $F[x]$ is a PID^a. $f(x)$ is irreducible iff $\langle f(x) \rangle$ is maximal (and hence $F(x)/\langle f(x) \rangle$ is a field).

^ais every field a PID? The notetaker didn't hear.

Theorem (Binomial Theorem).

$$(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i$$

Lemma 1. For p prime, $p| \binom{p}{i}$.

PROOF Let $m = \binom{p}{i} = \frac{p!}{i!(p-i)!}$. Then,

$$p! = mi!(p-i)!$$

and since p divides $p!$ but not $i!$ or $(p-i)!$, then $p|m = \binom{p}{i}$. ■

Theorem (Binomial Theorem mod p). For $a, b \in \mathbb{Z}_p$, where p prime,

$$(a+b)^p = \sum_{i=0}^p \binom{p}{i} a^{p-i} b^i = a^p + b^p$$

Definition. Let R, R' be rings. A **ring homomorphism** between R and R' is a function $\theta : R \rightarrow R'$ such that

1. $\theta(r_1 + r_2) = \theta(r_1) + \theta(r_2)$
2. $\theta(r_1 r_2) = \theta(r_1)\theta(r_2)$
3. $\theta(1_R) = 1_{R'}$

Here are some propositions you should prove:

1. $f(0_R) = 0_{R'}$
2. $f(-a) = -f(a)$
3. If a is invertible in R , then $f(a)$ is invertible in R' . and $f(a)^{-1} = f(a^{-1})$.
4. f is 1-to-1 iff $\ker f = 0_R$.

Definition. We say an onto homomorphism is called an **epimorphism**, and a 1-1 homomorphism is called a **monomorphism**.

Definition. The kernel of a homomorphism is the set of all elements in R that map to $0_{R'}$ under θ .

Proposition. The kernel of a homomorphism $\theta : R \rightarrow R'$ is an ideal of R .

Proposition. A homomorphism $\theta : R \rightarrow R'$ is 1-1 iff $\ker \theta = \{0_R\}$.

Proposition. Let $\theta : R \rightarrow R'$ a homomorphism. If $\ker \theta = R$, then θ is the zero map.

Proposition. If f is onto, then $f(I) \trianglelefteq R'$.

Definition. If $\theta : R \rightarrow R'$ is a bijective homomorphism, then we say θ is a **ring isomorphism** and we write $R \cong R'$.

Definition. If $f : X \rightarrow Y$ is any function of set, then for any $B \subset Y$ let

$$f^{-1}(B) = \{x \in X | f(x) \in B\},$$

and we call this the **preimage** of B under f . Note that the preimage of a set is a set, and you should *not* think of a preimage as a function.

Proposition. Suppose $f : R \rightarrow R'$ is a ring homeomorphism, and let $I' \trianglelefteq R'$. Then $f^{-1}(I') \trianglelefteq R$.

(Try the proof. Prove that $f^{-1}(I')$ is closed, is an ideal, and contains $0_{R'}$.)

Some properties of preimages:

- $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$
- $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$
- If $A \subset B$, then $f^{-1}(A) \subset f^{-1}(B)$

Corollary. $\ker f = f^{-1}(\{0_{R'}\}) \subseteq f^{-1}(I')$

Example.

1. Suppose $R \subset S$ (Assume S is commutative). For any $s \in S$, define $\mu_s : R[x] \rightarrow S$ by

$$\mu_s(p(x)) = p(s).$$

Then we have that μ_s is a homomorphism (which we call the *substitution homomorphism*).

2. $\mu_i : \mathbb{R}[x] \rightarrow \mathbb{C}$ defined by

$$\mu_i(p(x)) = p(i)$$

Then, $(x^2 + 1) = \ker \mu_i$. (prove it using the division algorithm).

3. Consider $\mu_{2^{1/3}} : \mathbb{Q}[x] \rightarrow \mathbb{R}$. Then $\ker \mu_{2^{1/3}} = (x^3 - 2)$. (for the proof, use the division algorithm and the fact that $1, 2^{1/3}, 2^{2/3}$ are linearly independent in \mathbb{Q} .)

- 4.

The blackboard shows the following steps:

- Let $R = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$
- $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I$
- $\phi : \mathbb{C} \rightarrow R$
- $\phi(a+bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$
- * check if it's additive
- clearly $1 \mapsto I$ and onto
- $\therefore \phi \cong R$
- $\phi((a+bi)(c+di)) = \phi((ac-bd)+(ad+bc)i) = \begin{bmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{bmatrix}$
- $\phi(a+bi) \phi(c+di) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{bmatrix}$

Remark. When a subring generated by a set, use square brackets. When you know the subring is a field, use round brackets.

i.e. $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$, but for $\mathbb{Z}[\sqrt{2}]$ or $F[\sqrt{2}]$ dont use () if it's not a field.

Proposition. Let R be any ring, with $I \trianglelefteq R$. Define $\pi : R \rightarrow R/I$ by $\pi(r) = r + I$. Then π is a ring homomorphism which is onto and $\ker \pi = I$.

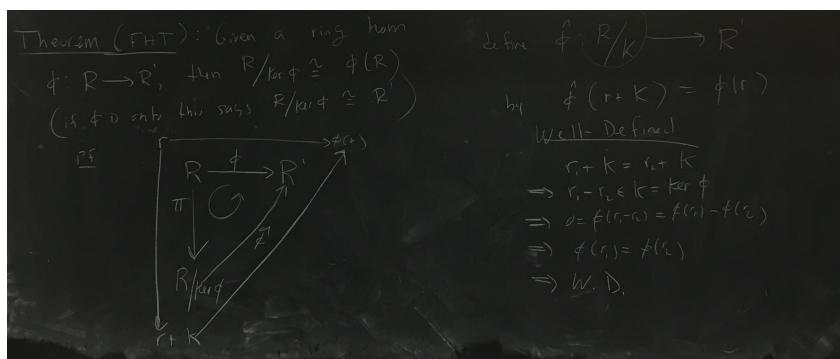
We call π the **canonical homomorphism**.

The next theorem is the converse of the above.

Theorem (Fundamental Homomorphism Theorem). Given a ring homomorphism $\phi : R \rightarrow R'$, then $R/\ker \phi \cong \phi(R)$.

This means that if $\phi : R \rightarrow R'$ is onto, then $R/\ker \phi \cong R'$.

PROOF



Show $\hat{\phi}$ additive:
 $\hat{\phi}((r_1 + K)(r_2 + K)) = \hat{\phi}(r_1 r_2 + K) = \hat{\phi}(r_1 r_2) = \hat{\phi}(r_1) \hat{\phi}(r_2) = \hat{\phi}(r_1 + K) \hat{\phi}(r_2 + K)$

$\hat{\phi}(1_K) = \hat{\phi}(1_R) = 1_{R'}$

$\hat{\phi}(r+K) = \phi(r) \Rightarrow r \in \ker\phi = K$
 $\phi(r+k) = \phi(r) \quad \text{def of } \hat{\phi}$
 $\phi(r) = \phi(r) \quad \text{def of } \phi$
 $\phi(r_1 r_2) = \phi(r_1) \phi(r_2)$
 $r_1 r_2 \in K \Rightarrow r_1 r_2 \in K$

$\Rightarrow r+K = r+K = \text{the zero elt. of } R/K$
 $\Rightarrow \hat{\phi} \text{ is 1-1}$

onto

$$\forall r' \in \text{im } \phi : r' = \phi(r) = \phi^n(r+k)$$

so ϕ^n is onto $\text{im } \phi$

$$\therefore \frac{\mathbb{R}}{\text{Ker } \phi} \cong \text{im } \phi$$

Example.

Ex's

Show $\mathbb{Q}(z^{1/3})$ is a field.

$$\mu_{z^{1/3}} : \mathbb{Q}(x) \xrightarrow{\text{onto}} \mathbb{Q}[z^{1/3}]$$

be the subs. map

$$\text{Ker } \mu_{z^{1/3}} = (x^3 - z)$$

$$\text{By FHT } \frac{\mathbb{Q}(x)}{(x^3 - z)} \cong \mathbb{Q}[z^{1/3}]$$

$x^3 - z \text{ mod } \Rightarrow$ the quotient is
a field; $\mathbb{Q}[z^{1/3}] / \mathbb{Q}(z^{1/3})$ field.

② Suppose R I.D. s.t. $R[x]$ is a P.I.D.

$$\mu_0 : R[x] \xrightarrow{x \mapsto 0} R$$

$$P = a_0 + a_1 x + \dots \in \ker \mu_0 \\ \text{iff } a_0 = 0 \\ \text{iff } p \in (x)$$

$$\text{onto } b/c \quad b, c \in R \quad \mu_0(r) = r \\ \ker \mu_0 = (x) \quad \text{By FHT}$$

$$R[x]/(x) \cong R \text{ I.D.}$$

(x) is a prime
in the P.I.D $R[x]$
 (x) is maximal

$R[x]/(x)$ is a field

$$\cong R \quad R \text{ is a field} \\ \frac{R[x]}{(x)} \cong R \quad \text{if } R \text{ is a field} \\ \frac{R[x]}{(x)} \cong \mathbb{F}(x;)$$

∴ field.

Proposition. If R be an integral domain such that $R[x]$ is a PID, then R must be a field.

PROOF Define $\mu_0 : R[x] \rightarrow R$ by $x \mapsto 0$. So μ_0 is an onto homomorphism. Also, $p(x) \in \ker \mu_0$ iff $0 = \mu_0(p(x)) = p(0)$. Thus, $\ker \mu_0 = \langle 0 \rangle$.

$$\begin{aligned} & \text{By FHT, } R[x]/(x) \cong R \\ & \text{But } R \text{ is an integral domain} \\ & \Rightarrow (x) \text{ is a nonzero prime ideal} \\ & \text{in } R[x], \text{ a P.I.D} \Rightarrow (x) \text{ is} \\ & \text{maximal} \Rightarrow R[x]/(x) \cong \text{a} \\ & \text{field} \Rightarrow R \text{ is a field.} \end{aligned}$$

Proposition. Suppose R is a commutative ring and $I \trianglelefteq R$. Then $I[x] \trianglelefteq R[x]$ and $R[x]/I[x] \cong (R/I)[x]$.

PROOF

Prop R any comm ring & $I \trianglelefteq R$. Then
 $I[x] \trianglelefteq R[x]$ and $R[x]/I[x] \cong (R/I)[x]$.

Defn $\phi: R[x] \rightarrow (R/I)[x]$ by
 $\phi\left(\sum_{i=0}^n c_i x^i\right) = \sum_{i=0}^n (c_i + I)x^i = \sum_{i=0}^n \bar{c}_i x^i$

Check ϕ is add.

$$\begin{aligned} &\phi((c_0 + c_1 x + c_2 x^2 + \dots)(s_0 + s_1 x + s_2 x^2 + \dots)) \\ &= \phi\left(c_0 s_0 + (c_0 s_1 + c_1 s_0)x + (c_0 s_2 + c_1 s_1 + c_2 s_0)x^2 + \dots + c_n s_n x^n\right) \\ &= \phi\left(c_0 s_0 + (c_0 s_1 + c_1 s_0)x + (c_0 s_2 + c_1 s_1 + c_2 s_0)x^2 + \dots + (\sum_{i+j=n} c_i s_j)x^n\right) \\ &= \phi(s_0) + (\phi(s_1) + \phi(s_0))x + (\phi(s_2) + \phi(s_1) + \phi(s_0))x^2 + \dots + \phi(s_n)x^n \end{aligned}$$

$$\begin{aligned} &= (\bar{c}_0 + \bar{c}_1 x + \bar{c}_2 x^2 + \dots + \bar{c}_n x^n)(\bar{s}_0 + \bar{s}_1 x + \bar{s}_2 x^2 + \dots + \bar{s}_n x^n) \\ &= \phi(c_0 x^0 + c_n x^n) + (c_0 s_0 x^0 + \dots + c_n s_n x^n) \\ &\text{ONTO} \quad \text{an arb. elt in } (R/I)[x] \\ &\text{as } F_n: R[x] \rightarrow I_n[x] = \phi(c_0 x^0 + c_n x^n) \\ &\text{Kernel?} \quad r + I_n x^k + c_n x^n \in \ker \phi \iff r \in I_n \\ &\bar{\phi} = \phi \circ I = \phi(c_0 x^0 + c_n x^n) = \bar{c}_0 + \bar{c}_1 x + \dots + \bar{c}_n x^n \in I[0] \\ &\text{if } r_i \in I \text{ iff } r_i \in I \cdot \text{ker } \phi = I[0] \\ &\text{Hence } [R[x]/I[x]] \cong (R/I)[x] \quad \square \end{aligned}$$

Corollary. If P is a prime ideal of R , then $P[x]$ is a prime ideal of $R[x]$.

PROOF

Corollary: If P is a prime ideal of R , then $P[x]$ is a prime ideal of $R[x]$.

pf
By the Prop. $R[x]/P[x] \cong (R/P)[x]$
 P prime $\Rightarrow R/P$ is a domain $\Rightarrow (R/P)[x]$
is an ID. $\therefore R[x]/P[x]$ is an ID.
 $\Rightarrow P[x]$ is a prime ideal \square

Special Case. (reduction of coefficients mod P)

$$\phi : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x], p \text{ prime}$$

$$\sum a_i x^i \mapsto \sum \bar{a}_i x^i$$

Remark. let $R \xrightarrow{\phi} S \xrightarrow{\psi} T$ be homomorphisms. Then

$$\ker(\psi \circ \phi) = \phi^{-1}(\ker \psi)$$

Remark K

$$R \xrightarrow{\phi} S \xrightarrow{\psi} T$$

homomorphism

$$\begin{aligned} r \in \ker(\psi \circ \phi) &\iff 0 = \psi(\phi(r)) \\ &\iff \phi(r) \in \ker \psi, \text{ iff } r \in \phi^{-1}(\ker \psi) \end{aligned}$$

$\boxed{\ker(\psi \circ \phi) = \phi^{-1}(\ker \psi)}$

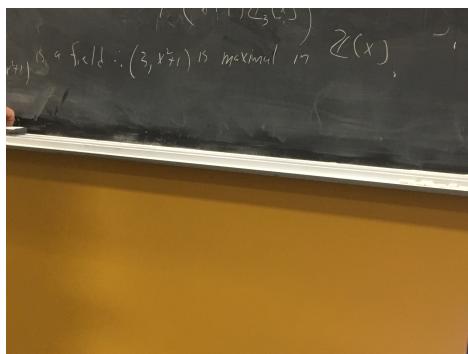
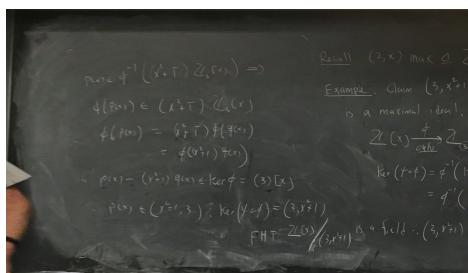
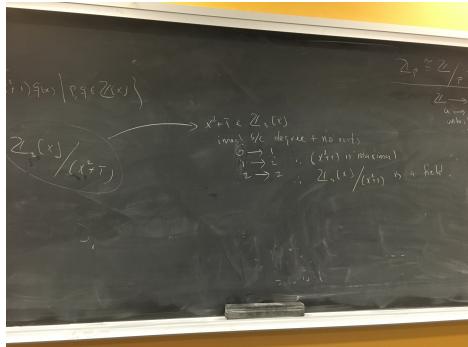
Example.

Recall $(\mathbb{Z}, +)$ max. $\triangle \mathbb{Z}(x)$

Example. Show $(\mathbb{Z}, x+1) = \left\{ \frac{1}{2}x+1, \frac{1}{2}x+1, \dots, \frac{1}{2}x+1 \right\} \subset \mathbb{Z}(x) \setminus \{0\} \subset \mathbb{Z}(x)$

is a maximal ideal.

$$\begin{aligned} \mathbb{Z}(x) &\xrightarrow{\phi} \mathbb{Z}_5[x] & \xrightarrow{\psi} \mathbb{Z}_5[x]/(x^2 - 1) \\ &\xrightarrow{\text{char}} & & x^2 - 1 \in \mathbb{Z}_5[x] \\ \ker(\phi \circ \psi) &= \psi^{-1}(\ker \psi) \\ &= \phi^{-1}((x^2 - 1)\mathbb{Z}_5[x]) \end{aligned}$$



Proposition. every ideal of $\mathbb{Z}[x]$ of the form $(p, f(x))$ where $f(x)$ is irreducible mod p is a maximal ideal in $\mathbb{Z}[x]$.

Theorem (Correspondence thm). let $\phi : R \rightarrow R'$ be an onto homomorphism. Then $I \leftrightarrow \phi(I)$ sets up a 1-to-1 correspondence between all the ideals of R containing $\ker \phi$ and all the ideals of R' .

Application. $\pi : R \rightarrow^{\text{onto}} R/I$, $\ker \pi = I$.

By the correspondence thm, an arb. ideal of R/I is of the form

$$\pi(J) = J/I$$

where $I \subseteq J$.

4 Index