LECTURE 5 : RING HOMOMORPHISMS AND QUOTIENT RINGS

We continue to follow Dummit and Foote, §7.3, notice our definition of ring does not assume an identity 1 exists. We have to add the condition unital if need be.

Def^n/ Let R and S be rings.

(1.) A ring homomorphism is a map $\varphi : R \to S$ with

(a.)(i.) $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$,

(ii.) $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

(2.) $\ker\varphi = \varphi^{-1}\{0\} = \{ r \in R \mid \varphi(r) = 0 \}$ is the kernel

(3.) a bijective ring homomorphism is an isomorphism

This means a ring homomorphism is a group homomorphism from $(R,+)$ to $(S,+)$ with additional structure due to axiom (ii.) (preserve multiplication)

Def^n/ Rings R and S are isomorphic if $\varphi : R \to S$ an isomorphism exists. We write $R \cong S$ in this case

$\boxed{E1}$ Let $G = \{1, j\}$ be the cyclic group of order 2 $(j^2 = 1)$ and let R be a commutative ring with $1 \neq 0$. We defined $RG = \{ a + bj \mid a, b \in R \}$ (group ring)

then $R \times R = \{ (a,b) \mid a, b \in R \}$ defines product ring via,

$$(a,b) + (x,y) = (a+x, b+y) \quad \& \quad (a,b)(x,y) = (ax, by)$$

You can verify $R \times R$ is ring with identity $(1,1) \neq (0,0)$.

If $\exists\, \psi : RG \to R \times R$ a ring isomorphism then ψ ought to preserve structure. What should we preserve here?

We note $(1+j)(1-j) = 1-j^2 = 1-1 = 0$ thus $1 \pm j \in RG$ are zero divisors. What are the zero divisors in $R \times R$?

$$(a,b)(x,y) = (0,0) \Rightarrow (ax, by) = (0,0)$$
$$\Rightarrow ax = 0 \text{ and } by = 0$$

$\Rightarrow (1,0)$ and $(0,1)$ give zero divisors, there are many more generally, but these exist.

What about j, the idempotent element. Can we find such $(x,y) \in R \times R$ s.t. $(x,y)^2 = (1,1)$?

$$(x,y)^2 = (x^2, y^2) = (1,1) \Rightarrow x^2 = 1 \text{ and } y^2 = 1$$
$$\Rightarrow \underbrace{x = \pm 1 \text{ and } y = \pm 1}$$

at least these solutions exist, there could be more, $x = y = 1$ is just the identity so choose $(1,-1)$.

Wish List for $\psi : RG \to R \times R$

$\psi(1) = (1,1)$

$\psi(j) = (1,-1)$

$$\boxed{\psi(a+bj) = (a+b, a-b)}$$

We can check $\psi^{-1}(x,y) = \left(\frac{x+y}{2}\right) + j\left(\frac{x-y}{2}\right)$ and clearly $\psi(1) = (1,1)$ and $\psi(j) = (1,-1)$. It remains to check $\psi(z+w) = \psi(z) + \psi(w)$ and $\psi(zw) = \psi(z)\psi(w)$.

woo hoo.

$$\psi((a+bj)(c+dj)) = \psi(ac+bd+(ad+bc)j)$$
$$= (ac+bd+ad+bc, ac+bd-ad-bc)$$
$$= ((a+b)(c+d), (a-b)(c-d)) = (a+b, a-b)(c+d, c-d) = \psi(a+bj)\psi(c+dj)$$

Def^{n}/ Let $R_1, R_2, \dots, R_k$ be rings then $R_1 \times R_2 \times \cdots \times R_k$ forms the direct-product-ring whose addition and multiplication are defined component-wise

$$(x+y)_j = x_j + y_j \qquad (xy)_j = x_j y_j$$

for $j = 1, 2, \dots, k$. When $R_1 = R_2 = \cdots = R_k$ we write $R \times R \times \cdots \times R = R^k$.

If $R_1, R_2, \dots, R_k$ are rings with unity then $(1, 1, \dots, 1)$ is the multiplicative identity for $R_1 \times R_2 \times \cdots \times R_k$. Notice

$$(1, 0, \dots, 0)(0, 1, 0, \dots, 0) = (0, 0, \dots, 0)$$

thus $e_1 = (1, \dots, 0)$ and $e_2 = (0, 1, 0, \dots, 0)$ are zero divisors.

If $a_1, a_2, \dots, a_k$ are units then $(a_1, a_2, \dots, a_k)$ is a unit since

$$\begin{aligned}(a_1, a_2, \dots, a_k)(a_1^{-1}, a_2^{-1}, \dots, a_k^{-1}) &= (a_1 a_1^{-1}, a_2 a_2^{-1}, \dots, a_k a_k^{-1}) \\ &= (1, 1, \dots, 1)\end{aligned}$$

and $(a_1^{-1}, a_2^{-1}, \dots, a_k^{-1})(a_1, a_2, \dots, a_k) = (1, 1, \dots, 1)$ as well.

QUESTION: do ring homomorphisms send units to units, zero-divisors to zero-divisors and 1 to 1 ?
I USED these as a guide to find $\psi : RG \to R \times R$ are these general principles ?

$\boxed{E2}$ $f : \mathbb{Z}_6 \to \mathbb{Z}_3$ given by $f([x]_6) = [x]_3$ is a function $[x]_6 = [y]_6 \hookrightarrow y = x + 6j$ then $[y]_3 = [x + 6j]_3 = [x]_3$ hence f well-defined.

$$f([x]_6 + [y]_6) = [x+y]_3 = [x]_3 + [y]_3 = f(x) + f(y)$$
$$f([x]_6[y]_6) = [xy]_3 = [x]_3[y]_3 = f(x)f(y)$$

So f is a ring homomorphism. Notice

$\underbrace{[2]_6}_{\text{zero divisor}} \notin \mathbb{Z}_6^{\times}$ yet $\underbrace{[2]_3}_{\text{unit.}} \in \mathbb{Z}_3^{\times}$ (ANSWER: NO.)

zero divisor maps to a unit.

PROPOSITION. Let R and S be rings and let $\varphi : R \longrightarrow S$ be a homomorphism.

(1.) image of φ is subring of S.

(2.) kernel of φ is subring of R and if $\alpha \in \ker\varphi$ and $r \in R$ then both $r\alpha \in \ker\varphi$ and $\alpha r \in \ker\varphi$

Proof: (1.) suppose $\varphi(a), \varphi(b) \in \text{image}(\varphi) = \varphi(R)$ then $a, b \in R$ and hence $a - b,\ ab \in R$ with

$$\varphi(a-b) = \varphi(a) - \varphi(b) \in im(\varphi)$$

$$\varphi(ab) = \varphi(a)\varphi(b) \in im(\varphi)$$

thus $im(\varphi)$ is subring of S.

(2.) Suppose $x, y \in \ker\varphi$ then $\varphi(x) = \varphi(y) = 0$. Thus $\varphi(x-y) = \varphi(x) - \varphi(y) = 0 - 0 = 0$ and $\varphi(xy) = \varphi(x)\varphi(y) = 0 \cdot 0 = 0 \therefore x-y, xy \in \ker\varphi$ and we find $\ker\varphi$ is subring of R.

If $\alpha \in \ker\varphi$ and $r \in R$ then observe $\varphi(\alpha) = 0$ and $\varphi(r\alpha) = \varphi(r)\varphi(\alpha) = 0$ and $\varphi(\alpha r) = \varphi(\alpha)\varphi(r) = 0$ thus $r\alpha, \alpha r \in \ker\varphi$.//

Remark: $\ker\varphi$ is an ideal of R if we know $\varphi : R \longrightarrow S$ is a homomorphism of rings.

Defn/ Let R be a ring and let $I \subseteq R$ and $r \in R$,

(1.) $rI = \{ra \mid a \in I\}$ and $Ir = \{ar \mid a \in I\}$

(2.) A subring $I \subseteq R$ is called

(i.) a <u>left-ideal</u> if $rI \subseteq I$ for all $r \in R$

(ii.) a <u>right-ideal</u> if $Ir \subseteq I$ for all $r \in R$

(3.) A subring $I \subseteq R$ which is both a left ideal and right ideal is called an <u>ideal</u> of R.

In a commutative ring left & right ideals are interchangeable. Therefore, an example which distguishes left vs. right must involve a noncommutative ring.

$\boxed{E3}$ Let $R = \mathbb{Z}^{n\times n}$ and form $I_1 = \{A \in \mathbb{Z}^{n\times n} \mid col_1(A) = 0\}$ and $J_1 = \{A \in \mathbb{Z}^{n\times n} \mid row_1(A) = 0\}$ then notice

$$M[A_1|A_2|\cdots|A_n] = [MA_1|MA_2|\cdots|MA_n]$$

$$\begin{bmatrix} B_1 \\ \hline B_2 \\ \hline \vdots \\ B_n \end{bmatrix} M = \begin{bmatrix} B_1M \\ \hline B_2M \\ \hline \vdots \\ \hline B_nM \end{bmatrix}$$

these rules of matrix multiplication show I_1 & J_1 are closed under multiplication and thus I_1 & J_1 are subrings since it is clear I_1 & J_1 are closed under subtraction.

$$M[0|A_2|\cdots|A_n] = [0|MA_2|\cdots|MA_n] \in I_1 \qquad (RI_1 \subset I_1)$$

$$\begin{bmatrix} 0 \\ \hline B_2 \\ \hline \vdots \\ \hline B_n \end{bmatrix} M = \begin{bmatrix} 0 \\ \hline B_2M \\ \hline \vdots \\ B_nM \end{bmatrix} \in J_1 \qquad (J_1R \subset J_1)$$

Thus I_1 is a <u>left</u> ideal and J_1 is a <u>right</u> ideal but we can see I_1 is not a right ideal nor J_1 a left ideal.

PROPOSITION

If R is a ring and I is an ideal of R then $R/I = \{ a + I \mid a \in R \}$ is a ring w.r.t.

$$(r + I) + (s + I) = (r+s) + I$$

$$(r+I)(s+I) = (rs) + I$$

for all $r, s \in R$. Conversely, if I is any subgroup such that these operations are well-defined then I is ideal.

Defn/ Given R a ring with ideal I we say R/I given the operations in the above prop is the <u>quotient ring of R by I</u>.

Thm/ (FIRST ISOMORPHISM Thm for Rings)

If $\varphi : R \longrightarrow S$ is a homomorphism of rings, then $\ker \varphi$ is an ideal of R and the image of φ is a subring of S and $R/\ker\varphi \cong \varphi(R)$ as rings.

<u>Proof</u>: we already established $\mathrm{im}(\varphi)$ a subring of S and $\ker\varphi$ an ideal of R in our earlier Prop. on pg. 4. It remains to show $R/\ker\varphi \cong \varphi(R)$. But, we know $R/\ker\varphi \cong \varphi(R)$ as abelian groups via

$$\overline{\varphi}(a + \ker\varphi) = \varphi(a)$$

thus all that remains is to check $\overline{\varphi}$ preserves product,

$$\begin{aligned} \overline{\varphi}\big((a+\ker\varphi)(b+\ker\varphi)\big) &= \overline{\varphi}(ab + \ker\varphi) \\ &= \varphi(ab) \\ &= \varphi(a)\varphi(b) \\ &= \overline{\varphi}(a+\ker\varphi)\,\overline{\varphi}(b+\ker\varphi) \end{aligned}$$

thus $\overline{\varphi} : R/\ker\varphi \longrightarrow \mathrm{im}(\varphi)$ is bijective ring homomorphism. and thus $R/\ker\varphi \cong \mathrm{im}(\varphi)$. //

Th^m/ If I is any ideal of R then $\pi(r) = r + I$ defines $\pi : R \to R/I$ a surjective ring homorphism with $\ker(\pi) = I$. Furthermore, every ideal is the kernel of a ring homomorphism.

Proof: Let $\pi(r) = r + I$ for I an ideal of the ring R. Then $\pi(a+b) = a+b+I = (a+I)+(b+I) = \pi(a) + \pi(b)$ and $\pi(ab) = ab + I = (a+I)(b+I) = \pi(a)\pi(b)$. Notice $I = 0 + I$ is zero of R/I since $(x+I)+(0+I) = x+I$ for all $x+I$ thus

$$\ker \pi = \{r \in R \mid \pi(r) = I = r+I\}$$
$$= \{r \in R \mid r \in I\}$$
$$= I.$$

Examples of Ideals

(1.) R a ring has R and $\{0\}$ as ideals. We call $\{0\}$ the trivial ideal whereas any ideal $I \neq R$ is called a proper ideal.

(2.) every ideal of $\mathbb{Z}$ has the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. We define $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$

(3.) $R = \mathbb{Z}[x]$ then consider $I = \{ \sum_{n=1}^{\infty} a_n x^n \in \mathbb{Z}[x] \}$

then $f(x) \in I \Rightarrow f(x) = a_1 x + a_2 x^2 + \cdots + a_n x^n$.

$f(x) + I = g(x) + I \Rightarrow f(x) - g(x) \in I$

thus $f(x) + I = g(x) + I \Leftrightarrow f(x)$ & $g(x)$ have same constant term.

$\mathbb{Z}[x]/I \cong \mathbb{Z}$

(3.) continued, let $\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}$ be defined by $\varphi(f(x)) = f(0)$ or if you prefer $\varphi(a_0 + a_1 x + \cdots + a_n x^n) = a_0$ then φ is a ring homomorphism where $\ker \varphi$ is simply the set of nonconstant polynomials. Since φ is surjective, $\mathbb{Z}[x]/I \cong \mathbb{Z}$

(4.) $J = \{ a_2 x^2 + \cdots + a_n x^n \mid a_2, \dots, a_n \in \mathbb{Z}, n \in \mathbb{N} \text{ for } n \geq 2 \}$ is an ideal of $\mathbb{Z}[x]$ and

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + J = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m + J$$

$$\Rightarrow a_0 + a_1 x = b_0 + b_1 x$$

Here if $a(x) + J = [a(x)]$ then we have that $[a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n] = [a_0 + a_1 x]$. Notice $x^2 + J = J$ and $(x + J)(x + J) = x^2 + J = J$ thus $x + J$ is zero divisor in $\mathbb{Z}[x]/J$

<u>Remark</u>: $\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}$ given by $\varphi(f(x)) = f''(x)$ naturally has $\ker \varphi = J$ since $f''(x) = 0$ implies $2a_2 + 6a_3 x + \cdots + n(n-1)a_n x^{n-2} = 0 \Rightarrow$ only $a_0, a_1 \neq 0$ possible for $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \ker \varphi$.

THE EVALUATION HOMOMORPHISM

Defⁿ/ Let X be a set and A a ring then if $R = \mathcal{F}(X, A)$ then for any $c \in X$ we define <u>evaluation</u> at c by $\text{eval}_c(f(x)) = f(c)$ or if you prefer $E_c(f) = f(c)$

Proposition: the evaluation map is a homomorphism.

<u>Proof</u>: Let X be set containing c and let A be a ring Suppose $f, g \in \mathcal{F}(X, A)$ then

$$\begin{aligned} \text{eval}_c(f+g) &= (f+g)(c) \\ &= f(c) + g(c) \\ &= \text{eval}_c(f) + \text{eval}_c(g) \end{aligned}$$

and $\text{eval}_c(fg) = (fg)(c) = f(c)g(c) = \text{eval}_c(f)\text{eval}_c(g)$. //

Thᵐ/ For X a set, A a ring and $R = \mathcal{F}(X, A)$ the map $\text{eval}_c : R \to A$ is surjective ring homo. and $R/\ker(\text{eval}_c) \cong A$ for any $c \in X$.

<u>Proof</u>: we've already shown $\text{eval}_c : \mathcal{F}(X, A) \to A$ is a ring homomorphism. Let $a \in A$ then define $f(x) = a$ for all $x \in X$ then $\text{eval}_c(f) = a$ thus eval_c is onto and 1st iso Thᵐ for rings yields

$$R/\ker(\text{eval}_c) \cong A. //$$

<u>Remark</u>: Examples (5), (6), (7) on p. 244-245 of D&F are helpful. I already touched on (8) earlier. I'm skipping ahead to finish the section with Thᵐ(8) and the definition for $I+J$ and IJ...

Th^{m}/ Let R be a ring.

2nd isomorphism Th^{m} for rings → (1.) Let A be a subring and B an ideal of R. Then $A+B = \{a+b \mid a \in A, b \in B\}$ is subring of R and $A \cap B$ is an ideal of A and $\frac{A+B}{B} \cong \frac{A}{A \cap B}$

3rd isomorphism Th^{m} for ring → (2.) Let I and J be ideals of R with $I \subseteq J$. Then J/I is an ideal of R/I and $\frac{R/I}{J/I} \cong \frac{R}{J}$

Lattice Isomorphism Th^{m} for rings → (3.) Let I be an ideal of R. The correspondence $A \longleftrightarrow A/I$ is an inclusion preserving bijection between the set of subrings of A of R that contain I and the set of subrings of R/I. Furthermore, A (a subring containing I) is an ideal of R iff $\frac{A}{I}$ is ideal of $\frac{R}{I}$

E4) $R = \mathbb{Z}$, $I = 12\mathbb{Z}$ then $\bar{R} = R/I = \mathbb{Z}/12\mathbb{Z}$ has ideals $2\mathbb{Z}/12\mathbb{Z}$, $3\mathbb{Z}/12\mathbb{Z}$, $4\mathbb{Z}/12\mathbb{Z}$, $6\mathbb{Z}/12\mathbb{Z}$ and $12\mathbb{Z}/12\mathbb{Z} = 0$ corresponding to $2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}, 12\mathbb{Z}$ respectively.

Def^{n}/ Let I, J be ideals of R then

(1.) $I+J = \{x+y \mid x \in I, y \in J\}$ the sum of I & J.

(2.) $IJ = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J \text{ for } n \in \mathbb{N}\}$ is the product of I and J, its formed from all finite sums of products from I & J.

(3.) I^n is set of all finite sums of products formed from n-elements taken from I.

Th^{m}/ $I+J$, IJ, I^n as above are ideals. of R.

$\boxed{E5}$ $\left.\begin{array}{l} I = 6\mathbb{Z} \\ J = 10\mathbb{Z} \end{array}\right\}$ ideals in $\mathbb{Z}$

$$I + J = \{ 6j + 10k \mid j,k \in \mathbb{Z} \}$$
$$= \{ 2(3j+5k) \mid j,k \in \mathbb{Z} \}$$
$$= 2\mathbb{Z}$$

since $\gcd(3,5) = 1$ we know $\exists\, a,b \in \mathbb{Z}$ s.t. $3a + 5b = 1$ and thus $3j + 5k$ takes value x since $3ax + 5bx = x$ for any $x \in \mathbb{Z}$.
($a = 2$, $b = -1$ for instance)

$IJ = 60\mathbb{Z}$ since sum of $(6j)(10k) = 60jk$

$\boxed{E6}$ $\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}/2\mathbb{Z}$ by $\varphi(f(x)) = [f(0)]_2$ gives homomorphism with $\ker\varphi = I$, the ideal of all polynomials in $\mathbb{Z}[x]$ with even constant term.
Then $2, x \in I$ and thus $4 = 2 \cdot 2$ and $x^2 = x \cdot x$ are in I^2 as $x^2 + 4 \in II$. Observe

$$x^2 + 4 \neq p(x)q(x) \text{ for some } p(x), q(x) \in I$$

(this shows why the product ideal formed by linear combinations of products cannot be same as the set $\underbrace{\{ab \mid a \in I, b \in J\}}_{\text{not } IJ \text{ generally.}}$)