Def/Theorem: Let R be a ring, I an ideal

R/I = Quotient ring of R modulo I

Thm:/ The Factor group R/I is a ring with multiplication given by

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

$(\forall\ r+I,\ s+I \in R/I)$

Proof: [we know R/I is an Abelian under addition i.e. $r+I + s+I = (r+s)+I$]

show that mult. is well defined

Let $s+I, r+I \in R/I$, let $\hat{r} \in r+I \iff \hat{r}+I = r+I$
$\hat{s} \in s+I \iff \hat{s}+I = s+I$

show $\hat{r}\hat{s} + I = rs + I$

$\hat{r} \in r+I \Rightarrow \exists\, a \in I$ s.t $\hat{r} = r+a$

$\hat{s} \in s+I \Rightarrow \exists\, b \in I$ s.t $\hat{s} = s+b$

$$\hat{r}\hat{s} = (r+a)(s+b) = rs + \overbrace{as + rb + ab}^{\in I \text{ since } I \text{ is an ideal}}$$

$\therefore\ \hat{r}\hat{s} \in rs + I$

$\hat{r}\hat{s} + I = rs + I$

Distributivity say $r+I, s+I, w+I \in R/I$

show

$$(r+I)\left((s+I)+(w+I)\right) = r+I\left((s+w)+I\right)$$
$$= r(s+w)+I$$
$$= (rs+rw)+I$$
$$= (rs+I)+(rw+I)$$
$$= (r+I)(s+I)+(r+I)(w+I)$$

Associtivity is similar ... ∎

Thm. Let I be an ideal in a ring R.
The map $\psi: R \to R/I$ is a ring hom.
$: r \mapsto r+I$

and $\ker(\psi) = I$.

Proof: From Groups we know

$\psi: R \to R/I$ is a surjective group hom.

Show ψ is a ring hom.

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

From groups $\ker(\psi) = I$ ∎

$\psi: R \to R/I$ is sometimes called the natural or canonical Ring hom.

Thm. (First Isomorphism Thm. for rings)

Let $\phi : R \to S$ be a ring homomorphism.
Let $\psi : R \to R/\ker(\phi)$ be the canonical hom. Then there exists a unique isomorphism $\eta : R/\ker(\phi) \to \phi(R)$ s.t. $\phi = \eta \circ \psi$.

In particular
$$\underbrace{\phi(R)}_{\text{a subring of } S} \cong R/\ker(\phi)$$

or

$$\begin{tikzcd} R \arrow[rr, "\phi"] \arrow[dr, "\psi"'] & & S \\ & R/\ker(\phi) \arrow[ur, "\exists!\,\eta"'] & \end{tikzcd}$$

commutes.

Proof: Let $K = \ker(\phi)$. By the 1^{st} iso. thm. for groups $\exists$ a unique (well defined) group isomorphism

$$\eta : R/K \to \phi(R)$$
$$r + K \mapsto \phi(r)$$

$\therefore$ we need only show that η is a ring hom. [$\forall\, r+K,\ s+K \in R/K$]

$$\begin{aligned}\eta((r+K)(s+K)) &= \eta(rs+K)\\ &= \phi(rs)\\ &= \phi(r)\phi(s)\\ &= \eta(r+K)\,\eta(s+K).\end{aligned}$$

$\blacksquare$

Thm (Second Iso. Theorem)

Let I be a subring of a ring R, and let J be an ideal of R. Then $I \cap J$ is an ideal of I and

$$I/(I\cap J) \simeq \underbrace{(I+J)}_{=\{a+b \mid a\in I, b\in J\}}/J .$$

Proof:

- Show $I+J$ is a subring of R.

  we know $I+J$ is an abelian subgroup.

  Let $a, \hat{a} \in I$, $b, \hat{b} \in J$

  $$(a+b)(\tilde{a}+\hat{b}) = \underbrace{\underset{\in I}{a\hat{a}} + \overbrace{(b\hat{a} + a\hat{b} + b\hat{b})}^{\in J \text{ since } J \text{ is an ideal}}}_{\in I+J}$$

  $$\therefore (a+b)(\tilde{a}+\hat{b}) \in I+J$$

- Show J is an ideal of $I+J$;

  Let $a\in I$, $b \in J$, $c \in J$ [know J is a abelian subgroup of $I+J$ and also a subring since $(0+b)(0+\hat{b}) \in J$]

  Show for any $a+b \in I+J$ that $(a+b)c \in J$, $c(a+b) \in J$

  $(a+b)c = \underset{\in J}{ac} + \underset{\in J}{bc}$ since J is an ideal

  $c(a+b) = (ca + cb) \in J$ $\therefore$ J is an ideal of $I+J$

~~From Homework we know $I\cap J$ is an ideal of I.~~

Now define $\phi : I \longrightarrow (I+J)/J$
$a \longmapsto a+J$

$$\Big[\ \underset{\in I}{a} + \underset{\in J}{b} + J = \underbrace{a+J}_{\text{all elements of } I+J/J}\ \Big]$$

Show ϕ is a hom. of rings

$$\phi(a_1+a_2) = a_1+a_2+J = (a_1+J)+(a_2+J)$$
$$= \phi(a_1)+\phi(a_2)$$

$$\phi(a_1a_2) = a_1a_2+J = (a_1+J)(a_2+J) = \phi(a_1)\phi(a_2)$$

want $\phi(I) = I+J/J$, i.e. ϕ to be onto.

ϕ is onto since $\forall a\in I,\ b\in J$

$$\underbrace{a+b+J}_{\text{any element of } I+J/J} = a+J = \phi(a)$$

$$\ker(\phi) = \{a\in I \mid \phi(a) = 0+J,\ a+J = 0+J\}$$
$$= \{a\in I \mid a\in J\}$$
$$= I\cap J \qquad \therefore I\cap J \text{ is an ideal}$$

$\therefore\ \phi : I \longrightarrow (I+J)/J$ is an onto ring hom.

By the first Iso. Thm. for rings

$$\phi(I) \cong I/\ker(\phi)$$
$$I+J/J \cong I/I\cap J$$

■

Third Iso Thm

Let R be a ring, I, J ideals where $J \subseteq I$.
Then

$$R/I \simeq (R/J)/(I/J).$$

Corespondance Thm S a subring of R. I an ideal of R

Then $S \to S/I$ is a 1-1 corespodence ($I \subseteq S$)

$$\{\text{Subrings } S \text{ of } R \text{ s.t. } I \subseteq S\} \xleftrightarrow{1-1} \{\text{Subrings of } R/I\}$$

$$S \to S/I$$

$$\{\text{ideals } S \text{ of } R \text{ s.t. } I \subseteq S\} \longleftrightarrow \{\text{ideals of } R/I\}$$

Maximal and Prime Ideals

- When is R/I a field? an integral domain?

Idea: (This weeks home work)

The only ideals in a field R are $\{0\}$ and R

Since if I is an ideal in R, $I \neq \{0\}$

if $r \in I, r \neq 0 \Rightarrow r^{-1} \in R$ since I is an ideal

$$r^{-1}r \in I \Rightarrow 1 \in I$$

$$\Rightarrow s \cdot 1 \in I \quad \forall s \in R$$

$$\Rightarrow I = R.$$

Def: A proper ideal M of a ring R is called a <u>maximal ideal</u> if:

- M is <u>not</u> a proper subset of any ideal of R other than R

Equivalently $\Updownarrow$

- M is maximal if for any ideal I of R s.t. $M \subsetneq I \Rightarrow I = R$.

Theorem Let R be a commutative ring with $1 \in R$ and let M be an ideal of R. M is maximal if and only if R/M is a field.

proof:

Let M be a maximal ideal in R.

R commutative $\Rightarrow$ R/M commutative

$1 + M$ is the identity in R/M

Show inverses exist for non-zero elements of R/M

If $a + M \neq 0 + M$ in R/M $\Leftrightarrow$ $a \notin M$

Fix $a + M \neq 0 + M \in R/M$.

Let $I = \{ ra + m \mid r \in R, m \in M \} \subseteq R$

Show I is an ideal:

- I non-empty since $0 \cdot a + 0 = 0 \in I$.
- Let $r_1 a + m_1$, $r_2 a + m_2 \in I$

$$r_1 a + m_1 - (r_2 a + m_2) = \underbrace{\overbrace{(r_1 - r_2)}^{\in R} a + \overbrace{(m_1 - m_2)}^{\in M}}_{\in I}$$

- For any $\tilde{r} \in R$

$$\tilde{r}(ra + m) = \underbrace{\overbrace{\tilde{r} r}^{\in R} a} + \overbrace{\tilde{r} m}^{\in M} \in I$$

$\therefore$ I is an ideal.

M is maximal, and $M \subsetneq I$ by construction since $a + M \neq 0 + M$ $\iff a \notin M$

$$I = \{ ra + m \mid r \in R,\ m \in M \} \subseteq R$$

$\Rightarrow$ $I = R$. $1 \in R$ and $I = R \Rightarrow 1 \in I$

$\therefore$ $b \in R$, $m \in M$ s.t. $1 = ba + m$

$$\begin{aligned} 1 + M &= (ba + m) + M = (ab + m) + M \\ &= ab + M \\ &= (a + M)(b + M) \\ &= (b + M)(a + M) \end{aligned}$$

$\therefore$ by def. $(a + M)^{-1} = b + M$ in R/M

$\therefore$ R/M is a field.

Now suppose M is an ideal and R/M is a field, show M is maximal.

$\Rightarrow$ $0 + M,\ 1 + M \in R/M$

$\therefore \quad M \neq R \quad$ (since if $M = R \quad R/M = \{0 + M\}$)

i.e $\quad M \subsetneq R$

Let I be any ideal of R s.t $M \subsetneq I$

Show $I = R$

Pick some $a \in I$, $a \notin M \quad a + M \neq 0 + M$

$\Rightarrow \exists \; \underset{\underset{(a+M)^{-1}}{\parallel}}{b+M}$ s.t. $\underset{\underset{(ab+M)}{\parallel}}{(a+M)(b+M)} = (1+M)$

$\Rightarrow \exists \; m \in M$ s.t. $ab + m = 1$

$\in I$ since I is an ideal

but $ab + m \in I$

$\in I$ since $M \subsetneq I$.

$\therefore \; 1 \in I \Rightarrow r \cdot 1 = r \in I \quad \forall r \in R$

$\Rightarrow I = R$

$\therefore M$ is a maximal ideal. ∎

Ex $p\mathbb{Z}$ is a maximal ideal in $\mathbb{Z}$ for p prime

since $\mathbb{Z}/p\mathbb{Z}$ is a field

Def A proper ideal P in a commutative ring R

is called a <u>prime ideal</u> if whenever $ab \in P$

then either $a \in P$ or $b \in P$.

Ex] $P = \{0, 2, \cdots, 10\} = 2\mathbb{Z}$ in $\mathbb{Z}_{12}$ is a prime ideal

Proposition | Let R be a commutative ring with $1 \in R$, $1 \neq 0$. Then P is a prime ideal in R if and only if R/P is an integral domain.

Proof:

First let P be an ideal of R, and let R/P is an int domain.

show P is prime

Suppose $ab \in P$ then

$$ab + P = 0 + P$$

$$\shortparallel$$

$$(a+P)(b+P) = 0 + P$$

$\therefore$ Since R/P is an integral domain

$\Rightarrow$ Either $a + P = 0 + P$ OR $b + P = 0 + P$

i.e.

Either $a \in P$ OR $b \in P$

$\therefore$ P is a prime ideal.

Now suppose P is prime, show R/P has no zero divisors

Suppose $(a+P)(b+P) = 0 + P$

$$\overset{\shortparallel}{ab} + P = 0 + P$$

$\Rightarrow \quad ab \in P$

$\Rightarrow$ since P is prime, either $a \in P$ or $b \in P$

$\Rightarrow$ either $a+P = 0+P$ or $b+P = 0+P$

$\therefore$ R/P is an integral domain ∎

Every field is in particular an integral domain

Cor.) Every maximal ideal in a commutative ring R with $1 \in R$ is also prime.

Proof: R/I a field $\Leftrightarrow$ I maximal

$\uparrow$ This is also and int. domain

$\therefore$ I is prime. ∎

$$x \equiv r \mod I \Leftrightarrow x + I = r + I$$

Polynomial Rings

Let R be a commutative ring with $1 \in R$

Any expression

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n$$

$a_i \in R$, $a_n \neq 0$ is a polynomial with coefficients in R and intermediate x.

a_n – leading coefficent

$a_n x^n$ – leading term

If $a_n = 1$, call $f(x)$ monic

If n is the largest non-negative $n \in \mathbb{Z}$ s.t.

$$a_n \neq 0 \Rightarrow \deg(f) = n$$

$\Updownarrow$

degree of $f(x)$ is n.

If no such n exists $\Rightarrow f = 0$

$$\deg(0) = -\infty$$

$$a_0 + a_1 x + \cdots + a_n x^n = b_0 + b_1 x + \cdots + b_m x^m$$

if and only if $a_i = b_i \quad \forall\, i \geq 0$

$R[x] = \{$ set of polynomials $f(x)$ in intermediat x with coeffrcents in $R \}$

Addtion is given by

$$= \overset{p(x)}{(a_0 + a_1 x + \cdots + a_n x^n)} + \overset{q(x)}{(b_0 + b_1 x + \cdots + b_m x^m)}$$

say $n \geq m$

$$= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$$

mult.

$$p(x)q(x) = \sum_{i=0}^{m+n} \left(\sum_{k=0}^{i} a_k b_{i-k} \right) x^i$$

Ex] work in $\mathbb{Z}_{12}[x]$

$$p(x) = 3 + 3x^3 \quad , \quad q(x) = 4 + 4x^2 + 4x^4$$

$$p(x) + q(x) = 7 + 4x^2 + 3x^3 + 4x^4$$

$$p(x)q(x) = 0$$

Theorem/ Let R be a commutive ring with $1 \in R$. Then $R[x]$ is a commutive ring with identity.

Proof:

Show $R[x]$ is an additive abelian group.

- $f(x) = 0 \in R[x]$ = add. identity
- Add. inverse of $p(x) = \sum a_i x^i$ is $-p(x) = \sum -a_i x^i$
- poly. add is commutive since done in coefficents.

Show mult. properties, i.e. mult is Associative, Distributive,

Note $f(x) = 1 \in R[x]$

Show mult is associtive

$$p(x) = \sum_{i=0}^{m} a_i x^i \quad , \quad q(x) = \sum_{i=0}^{n} b_i x^i \quad r(x) = \sum_{i=0}^{s} c_i x^i$$

$$\left(p(x) \cdot q(x) \right) \cdot r(x) = \left[\left(\sum_{i=0}^{m} a_i x^i \right) \left(\sum_{i=0}^{n} b_i x^i \right) \right] \left(\sum_{i=0}^{s} c_i x^i \right)$$

$$= \left[\sum_{i=0}^{m+n} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i \right] \left(\sum c_i x^i \right)$$

$$= \sum_{i=0}^{m+n+s} \left(\sum_{j=0}^{i} \left[\sum_{k=0}^{j} a_k b_{j-k} \right] c_{i-j} \right) x^i$$

$$= \sum_{i=0}^{m+n+s} \left(\sum_{j+k+l=i} a_j b_k c_l \right) x^i$$

$$= \sum_{i=0}^{m+n+s} \left[\sum_{j=0}^{i} a_j \sum_{k=0}^{i-j} b_k c_{i-j-k} \right] x^i$$

$$= \left(\sum_{i=0}^{m} a_i x_i \right) \left[\sum_{i=0}^{n+s} \left(\sum_{j=0}^{i} b_j c_{i-j} \right) x^i \right]$$

$$= p(x) \left[q(x) \cdot r(x) \right]$$

∎

<u>Prop</u> / Let $p(x), q(x) \in R[x]$ where R is an integral domain. Then $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$ and $R[x]$ is an integral domain.

<u>Proof:</u>

Let $p, q \in R[x]$, $p \neq 0$, $q \neq 0$

$$p = a_m x^m + \cdots + a_1 x + a_0$$

$$q = b_n x^n + \cdots + b_0$$

$\deg(p) = m$, $\deg(q) = n$, Leading term of $p(x)q(x)$ is $a_m x^m \cdot b_n x^n$ since $a_m \neq 0$, $b_n \neq 0$ and R is an integral Domain

$\therefore a_m \cdot b_n \neq 0$

$\therefore \deg(p \cdot q) = m + n$

and further $p(x)q(x) \neq 0$ since it's leading term is non-zero

$\therefore$ $R[x]$ is an integral domain. $\boxtimes$

Multivariant polynomial Rings

i.e. $f = x^2 - 3xy + 2y^3$

- $R[x]$ is a commutative ring with 1 (since R is com. with $1 \in R$)

$(R[x])[y]$ – commutative ring with 1

$(R[y])[x]$ – commutative ring with 1

Show $(R[x])[y] \simeq (R[y])[x]$.