403/503 - L21

Quotient Rings.

Def Let R be a ring and $I \subseteq R$ an ideal. The *quotient ring* R/I is

$$R/I = \{r+I \mid r \in R\}$$

(the set of additive (left) cosets of I in R) with operations

$$(r+I)+(s+I) = (r+s)+I \quad , r,s \in R.$$

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

That $+$ is well-defined is known from group theory. Suppose $r+I = r'+I$ and $s+I = s'+I$. WTS $rs+I = r's'+I$. We have

$$r's' = r'\underbrace{(s'-s)}_{\in I} + \underbrace{(r'-r)}_{\in I}s + rs$$

Thus $r's'-rs \in I$ since I is an ideal, so multiplication in R/I is well-defined.

<u>Theorem</u> R/I is a ring with these operations.

<u>Proof</u> Already know $(R/I, +)$ is an abelian group, since $(R,+)$ is an abelian group and $I \trianglelefteq (R,+)$.

We check the associative law for $\cdot$;

$$\big((r+I)(s+I)\big)(t+I) = (rs+I)(t+I) =$$
$$= \big((rs)t\big) + I = r(st) + I \quad \text{since } R \text{ is a ring}$$
$$= \cdots = (r+I)\big((s+I)(t+I)\big).$$

Also $1_R + I$ is the multiplicative identity element of R/I.

Lastly we must check the two distributive laws. (Exercise.) ∎

Example $\mathbb{Z}_n = \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ is a ring

Example $\dfrac{\mathbb{F}[x]}{(p(x))}$ is a ring

Example $R/_{(0)} \cong R$

$$r+(0) \longleftarrow\!\shortmid\, r$$

Thm (1st Isomorphism Thm for Rings)
Let $\varphi: R \to S$ be a homomorphism.
Let $K = \ker\varphi$. Then φ induces
a ring isomorphism

$$\bar{\varphi} : R/_K \to \operatorname{im}\varphi$$

by $\quad \bar{\varphi}(r+K) = \varphi(r) \quad \forall r \in R.$

Proof Already know $\bar{\varphi}$ is a well-defined isomorphism of additive groups, by 1st isomorphism Theorem for groups. Furthermore,

$$\bar{\varphi}(1_{R/K}) = \bar{\varphi}(1_R + K) = \varphi(1_R) = 1_S$$

Since φ is a ring homomorphism.

Also

$$\bar{\varphi}((r+K)(s+K)) = \bar{\varphi}((rs)+K) = \varphi(rs) =$$

$$= \varphi(r)\varphi(s) = \bar{\varphi}(r+K)\,\bar{\varphi}(s+K),$$

So, $\bar{\varphi}$ is a ring homomorphism.

$\bar{\varphi}$ bijective $\Rightarrow$ $\bar{\varphi}$ ring isomorphism.

Prime Ideals.

Def Let R be a comm. ring.
An ideal $I \subseteq R$ is *prime* if
$\forall a, b \in R$:

$$ab \in I \Longrightarrow (a \in I \text{ or } b \in I),$$

Example. (0) is a prime ideal in $\mathbb{Z}$, since

$$ab \in (0) \Rightarrow ab = 0 \Rightarrow a = 0 \text{ or } b = 0$$
$$\Rightarrow a \in (0) \text{ or } b \in (0),$$

In fact, if R is a comm. ring, then R is an integral domain iff (0) is a prime ideal.

Example. When is (n) prime in $\mathbb{Z}$?

Note: $a \in (n) \Longleftrightarrow n \mid a$.

So (n) is prime iff

$$n \mid ab \Longrightarrow n \mid a \text{ or } n \mid b$$

From elementary number theory we recognize this as a characterizing property of prime numbers (when $n \neq 0$).

So (n) prime $\Longleftrightarrow$ $\boxed{\begin{array}{l} n = 0 \text{ OR} \\ n = \pm p,\ p \text{ a prime number} \end{array}}$

<u>Th</u>. Let I be an ideal of a commutative ring R. Then TFAE:

1) I is prime
2) R/I is an integral domain.

<u>proof</u> I is prime iff

$$ab \in I \implies a \in I \text{ or } b \in I$$

$$\Leftrightarrow \left[ab + I = 0 + I \implies a + I = 0 + I \text{ or } b + I = 0 + I\right]$$

$$\Leftrightarrow \left[(a+I)(b+I) = 0 + I \implies a + I = 0 + I \text{ or } b + I = 0 + I\right]$$

$$\Leftrightarrow \left[\bar{a}\,\bar{b} = \bar{0} \text{ in } R/I \implies \bar{a} = \bar{0} \text{ or } \bar{b} = \bar{0} \text{ in } R/I\right]$$

$\Leftrightarrow$ R/I is an integral domain

∎