403/503 L20

Ideals

If $\varphi: R \to S$ is a ring homomorphism then we know

$$\ker \varphi = \{r \in R \mid \varphi(r) = 0\}$$

is a subroup of $(R, +)$. With respect to $\cdot$ we notice that if $r \in R$ and $x \in \ker \varphi$ then

$$\varphi(rx) = \varphi(r)\varphi(x) = \varphi(r) \cdot 0_S = 0_S$$

Therefore $rx \in \ker\varphi \ \forall r \in R \ \forall x \in \ker \varphi$.
Similarly $x \cdot r \in \ker\varphi \ \forall r \in R \ \forall x \in \ker \varphi$.

Def An *ideal* I of a ring R is a subset such that

i) I is a subgroup of $(R, +)$

ii) For any $r \in R$ and $a \in I$ we have $r \cdot a \in I$ and $a \cdot r \in I$.

Property ii) means that I is closed under left and right multiplication by elements from R.

Example 1) For any ring homomorphism $\varphi: R \to S$, $\ker \varphi$ is an ideal of R.

2) $\{0_R\}$ is an ideal of any ring R, called the zero ideal.

3) R is an ideal of R (for any ring R). If I is an ideal and $I \neq R$ we say I is a proper ideal. (R is then the "improper" ideal of R)

4) Let R be any commutative ring and let $x \in R$. Define

$$(x) = \{ r \cdot x \mid r \in R \}$$

Then (x) is an ideal of R:

i) $(x) \neq \emptyset$ since $0 \cdot x \in (x)$. If $a, b \in (x)$ then $a = r \cdot x$, $b = s \cdot x$ for some $r, s \in R$, so $a - b = rx - sx = (r - s)x \in (x)$.

So (x) is a subgroup of $(R,+)$

ii) Let $r \in R$ and $a \in (x)$. Then $a = sx$, for some $s \in R$. So

$$ra = rsx = (rs)x \in (x) \quad \text{and}$$

$$ar = sxr = (sr)x \in (x).$$

($sxr = (sr)x$ since R commutative)

This proves (x) is an ideal of R.

Definition An ideal I of a commutative ring R is called principal if $I = (x)$ for some $x \in R$.

Example 1) $\{0_R\} = (0_R)$ and $R = (1_R)$ are principal ideals.

2) If $n \in \mathbb{Z}$ then $n\mathbb{Z} = (n)$ is a principal ideal of $\mathbb{Z}$.

3) If $p(x) \in \mathbb{F}[x]$ then

$$(p(x)) = \{ r(x)p(x) \mid r(x) \in \mathbb{F}[x] \}$$

$$= \{ f(x) \in \mathbb{F}[x] \mid p(x) \mid f(x) \}$$

That is, the set of all poly's $f(x)$ divisible by $p(x)$ is a principal ideal.

4) Consider the ring $R = \mathbb{Z}[x]$ and let

$$I = \{ f(x) \in \mathbb{Z}[x] \mid f(x) \text{ has even constant term} \}$$

$$= \{ f(x) \in \mathbb{Z}[x] \mid f(0) \in 2\mathbb{Z} \}$$

Then I is an ideal (check!)

But I is not principal:

Suppose $I = (p(x))$, for some $p(x) \in \mathbb{Z}[x]$. Then, since the constant polynomial $2 \in I$ we must have $2 = r(x) \cdot p(x)$, for some $r(x) \in \mathbb{Z}[x]$. Taking degrees on both sides we get $0 = \underbrace{\deg r(x)}_{\geq 0} + \underbrace{\deg p(x)}_{\geq 0}$

$\Rightarrow p(x) = C$, some constant, which is even since $p(x) = 1 \cdot p(x) \in I$. In fact $C = \pm 2$, WLOG $C = 2$. But then:

$I = (p(x)) = (2) = \{ g(x) \cdot 2 \mid g(x) \in \mathbb{Z}[x] \}$

which is the set of poly's where all coefficients are even integers.

This contradicts that the polynomial x belongs to I (having even constant term).

Theorem

a) Every ideal in $\mathbb{Z}$ is principal.

b) Every ideal in $\mathbb{F}[x]$ is principal ($\mathbb{F}$ is a field).

Proof a) Let $I \subseteq \mathbb{Z}$ be an ideal.

If $I = \{0\}$ then $I = (0)$ principal.

Suppose $I \neq \{0\}$. Note that if $a \in I$ then $-a = (-1)a \in I$. So the set $S = \{a \in I \mid a > 0\} = I \cap \mathbb{Z}_{>0}$ is non-empty.

Let d be the smallest element of S (Well-ordering Principle ensures d exists.)

We claim $I = (d)$.

Let $a \in I$. By the Division Algorithm,

$$a = qd + r$$

for some $q \in \mathbb{Z}$ and $r \in \mathbb{Z}$, $0 \leq r < d$.

Since $a, d \in I$ we have $qd \in I$ and thus $a - qd \in I$. So $r \in I$.

Since $r < d$ we must have $\underline{\underline{r = 0}}$ otherwise r would contradict minimality of d. Thus $d \mid a$.

So $I = (d)$.

b) Similar, using degree of pdly's & Division Algorithm.

Theorem Any finite integral domain is a field.

Proof Let $r \in R$, $r \neq 0$. Define

$L_r : R \to R$, $L_r(x) = rx$.

Since R is an integral domain,

L_r is injective: $L_r(x) = L_r(y) \Rightarrow$

$rx = ry \Rightarrow r(x-y) = 0 \Rightarrow x = y$

↑ R integral domain

Since R is finite, L_r is also surjective. So $\exists\, x \in R : L_r(x) = 1$.

That means $rx = 1$

$= xr$ (R comm)

$\Rightarrow r$ is a unit.

Thus R is a field.

∎