Lecture 24 (Chapter 12, Prime Ideals from Stillwell's Elements of Number Theory)

Here we study the needed theory to treat ideals as #'s in their own right. Congruence mod I is defined and R/I like $\mathbb{Z}/n\mathbb{Z}$ is shown to be logical. Maximal, prime ideals are compared and contrasted & divisibility is generalized to ideals as forecasted in our earlier studies. The conjugate ideal & class # are used to help understand the structure and finally in conclusion primes of form x^2+5y^2 are studied in light of ideals of $\mathbb{Z}[\sqrt{-5}]$.

#

§12.1 Ideals & Congruence

We began our study of $\mathbb{Z}$ by using congruence modulo n. We now abstract that a bit by letting an ideal I play the role $n\mathbb{Z} = (n)$ did before. Btw, notice we use the algebraically convenient version to abstract.

Def^{n}/ Given a commutative ring with identity R and an ideal I we define

$$a \equiv b \ (\text{mod } I) \text{ iff } a - b \in I$$

Claim: $\equiv$ mod I forms an equivalence relation on R

Proof: ① $a \equiv a \mod I$ as $a - a = 0 \in I \ \forall a \in R$.

② $a \equiv b \mod I \Rightarrow a - b \in I \Rightarrow b - a \in I \Rightarrow b \equiv a \mod I$.

③ $a \equiv b$ and $b \equiv c \mod I \Rightarrow a-b,\ b-c \in I$ hence $(a-b)+(b-c) = a-c \in I \therefore a \equiv c \mod I$.

(I used a Lemma see →)

Lemma: If $I \subseteq R$ is an ideal and $x, y \in I$ then $x - y \in I$ and $-x \in I$. Also, $0 \in I$.

Proof: we have $1 \in R$ and $1 \cdot x = x \ \forall x \in R$. Also, $-1 \in R$ and $1 + (-1) = 0$ by closure of R under additive inverses. Note that, if $x \in R$ then

$$(1-1) \cdot x = 1 \cdot x + (-1) \cdot x = x + (-1) \cdot x$$

But, $1 - 1 = 0 \therefore (1-1) \cdot x = 0 \cdot x = 0$ hence

$0 = \underline{x + (-1)x = x + (-x)}$ as $-x$ exists for each $x \in R$. But, subtracting x from both sides of $*$ yields $(-1) \cdot x = -x$. We find $x \in I$ has $-x = (-1) \cdot x \in I$ as $-1 \in R$ and I an ideal closed under mult. from R. Finally as $x, y \in I$ $\Rightarrow -y \in I$ hence $x + (-y) = x - y \in I$ as I is closed under $+$. //

Remark: now you know what I pushed under the rug by glibly claiming I was closed under subtraction. It is, but, it requires a little algebra.

We should know from Math 200 etc... any equivalence relation provides a <u>partition</u> of the set into disjoint equivalence classes. We define,

$$\boxed{\text{Def}^{\text{n}}/ \quad I+a = \{ i+a \mid i \in I \}}$$

We say $I+a$ is <u>represented</u> by a. To define operations on $I+a$, $I+b$ etc. we must show independence from representative as $I+a = I+a'$ only implies $a-a' \in I$, not that $a=a'$ necessarily.

Th^m/ If $I+a = I+a'$ and $I+b = I+b'$ then

$$I+(a+b) = I+(a'+b')$$

$$I+ab = I+a'b'$$

<u>Proof</u>: notice $I+a = I+a'$, $I+b = I+b' \Rightarrow a-a', b-b' \in I$ thus $(a+b)-(a'+b') = (a-a')+(b-b') \in I$ as I closed under $+$. Also, $ab-a'b'$ has

$$
\begin{aligned}
ab - a'b' &= ab + ab' - ab' - a'b' \\
&= a(b+b') - (a+a')b' \quad \leftarrow \text{who cares} \\
&= a\underbrace{(b-b')}_{\in I} + \underbrace{(a-a')}_{\in I}b' \quad \leftarrow \text{better}
\end{aligned}
$$

Hence $ab - a'b' \in I$ and the th^m follows.

Thus define,

$$\boxed{\begin{aligned} \text{Def}^{\text{n}}/ \quad (I+a)+(I+b) &= I+(a+b) \\ (I+a)(I+b) &= I+ab \end{aligned}}$$

This provides $R/I = \{ I+a \mid a \in R \}$ a sum and product

Thm/ If $R/I = \{I+a \mid a \in R\}$ then R/I paired with $+$ and $\times$ defined as on pg. 3,

$$(I+a)+(I+b) = I+(a+b)$$
$$(I+a)(I+b) = I+ab$$

forms a commutative ring with identity

well, sometimes

Proof: steal from R as we did for $\mathbb{Z}/n\mathbb{Z}$ from $\mathbb{Z}$.

$$\begin{aligned}(I+a)+(I+b) &= I+(a+b) \\ &= I+(b+a) \\ &= (I+b)+(I+a)\end{aligned}$$

And,

$$(I+0)+(I+a) = I+(0+a) = I+a = (I+a)+(I+0)$$

Thus, $I+0=I$ plays role of zero. Other multiplicative properties for R/I are proved similarly (see p. 223 for $(I+a)(I+b)=(I+b)(I+a)$.

Another,

$$(I+1)(I+a) = I+(1\cdot a) = I+a = (I+a)(I+1)$$

Hence $I+1$ serves as "1" in R/I. If $1 \in I$ then R/I has no multiplicative identity. //

Remark: another way to look at our current endeavor; this proves $\mathbb{Z}/n\mathbb{Z}$ is well-defined. Indeed, as we continue, it's fun to apply our work back to $I=(n)$ in $R=\mathbb{Z}$.

§12.2 PRIME AND MAXIMAL IDEALS

In §11.7 (p. 213) we saw maximal ideals are prime. However, prime ideals are only sometimes maximal. The pair of th^m's we consider here tell us when...

<u>Characterization of Prime Ideals</u>:

I is a prime ideal of a ring $R \iff R/I$ has no zero divisors.

<u>Proof</u>: $\Rightarrow$) Suppose I is prime. We seek to show $(a+I)(b+I) = I \Rightarrow a \in I$ or $b \in I$. Observe,

$$\begin{aligned} I+ab = I &\Rightarrow ab \in I \\ &\Rightarrow a \in I \text{ or } b \in I \text{ as } I \text{ is prime.} \\ &\Rightarrow R/I \text{ has no zero divisors.} \end{aligned}$$

$\Leftarrow$) Suppose R/I has no zero divisors, we need to show I is prime.

$$\begin{aligned} ab \in I &\Rightarrow I+ab = I \\ &\Rightarrow (I+a)(I+b) = I \\ &\Rightarrow I+a = I \text{ or } I+b = I \quad \text{since } R/I \text{ has no no zero divisors} \\ &\Rightarrow a \in I \text{ or } b \in I \\ &\Rightarrow I \text{ is a prime ideal.} // \end{aligned}$$

Th$^{\underline{m}}$ (Characterization of Maximal Ideals)
I is a maximal ideal of a ring $R \iff R/I$ is a field.

Proof: ($\Rightarrow$) Suppose I is maximal, we seek to show R/I a field.

$I + a \neq I \Rightarrow a \notin I$

$\Rightarrow J = \{ ir + as \mid s \in R, i \in I \}$ an ideal must be $J = R$. (by maximality)

$\Rightarrow 1 = ir + as$ for some $r, s \in R$ and $i \in I$

$\Rightarrow I + as = I + 1$

$\Rightarrow (I+a)(I+s) = (I+1)$

$\Rightarrow I + a$ has inverse $I + s$

$\Rightarrow R/I$ is a field (every nonzero element has multiplicative inverse)