LECTURE 22: (CHAPTER 11, IDEALS, §11.7 – 11.9 from Stillwell's Elements of Number Theory)

At last, we define the product of ideals.

Def^n/ Let A, B be ideals in a ring R then

$$AB = \{ a_1b_1 + a_2b_2 + \cdots + a_nb_n \mid a_j \in A,\ b_j \in B \text{ for } j = 1,2,\dots,k \}$$

is the product AB.

I add a little theorem here,

Th^m/ Given ideals A, B of R the product AB is an ideal.

Proof: let $z, w \in AB$ and $r \in R$ then $\exists\, a_j, b_j, c_j, d_j \in R$ well, $a_j, c_l \in A$ and $b_j, d_l \in B$ for $j = 1, 2, \dots, k_1$ and $l = 1, 2, \dots, k_2$. Wlog let $k = \max(k_1, k_2)$ and assume

$$z = a_1b_1 + \cdots + a_kb_k$$
$$w = c_1d_1 + \cdots + c_kd_k$$

where we add zero to make the length of the Σ match if need be. With that obfuscation aside,

$$z + w = \underbrace{a_1b_1 + c_1d_1 + \cdots + a_kb_k + c_kd_k}_{\text{sum of products from } A,\,B} \in AB$$

Likewise

$$rz = ra_1b_1 + ra_2b_2 + \cdots + ra_kb_k \quad \text{using ideal } rA \subseteq A.$$
$$= a_1'b_1 + a_2'b_2 + \cdots + a_k'b_k \in AB$$

Hence AB is closed under $+$ and multiplication from R $\therefore$ AB is an ideal. //

Def^{n}/ An ideal P is <u>PRIME</u> if, whenever $P \supseteq AB$, P contains A OR P contains B

That is, if $P \supseteq AB \Rightarrow P \supseteq A$ OR $P \supseteq B$.
or if you wish to be a West Virginian,

$$AB \subseteq P \Rightarrow A \subseteq P \text{ or } B \subseteq P.$$

At the level of <u>elements</u>,

$$ab \in P \Rightarrow a \in P \text{ or } b \in P.$$

Th^{m}/ (Equivalent definitions for prime ideal) TFAE for an ideal P,

(1.) $AB \subseteq P \Rightarrow A \subseteq P$ or $B \subseteq P$ for ideals A, B.

(2.) $ab \in P \Rightarrow a \in P$ or $b \in P$

<u>Proof</u>: (1) $\Rightarrow$ (2). Suppose $AB \subseteq P \Rightarrow A \subseteq P$ or $B \subseteq P$.
Let $ab \in P \Rightarrow (ab) \subseteq P$ as P is an ideal and products of ab are once more in P.

Note $(a)(b) = \{ a_1 b_1 + \cdots + a_n b_n \mid a_j \in (a), b_j \in (b) \}$

$= \{ a_1 b_1 + \cdots + a_n b_n \mid a_j = \alpha_j a , b_j = \beta_j b \}$

$= \{ \alpha_1 a \beta_1 b + \cdots + \alpha_n a \beta_n b \mid \alpha_j, \beta_j \in R \}$

$= \{ (\alpha_1 \beta_1 + \cdots + \alpha_n \beta_n) ab \mid \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in R \}$

$= (ab)$.

Thus, $(ab) \subseteq P \Rightarrow (a)(b) \subseteq P \Rightarrow (a) \subseteq P$ or $(b) \subseteq P$ by assumption of (1) $\therefore a \in P$ or $b \in P$. //

(2) $\Rightarrow$ (1.) over

Proof continued:

(2.) $\Rightarrow$ (1.) Assume $ab \in P \Rightarrow a \in P$ or $b \in P$. Furthermore, suppose $AB \subseteq P$ and $A \not\subseteq P$ for some ideals $A, B \subseteq R$. We seek to show $B \subseteq P$. As $A \not\subseteq P \Rightarrow \exists a \in A$ for which $a \notin P$. Thus,

$$AB \subseteq P \Rightarrow ab \in P \text{ for all } b \in B$$ by def$^{\underline{n}}$ of the product ideal AB.

Thus $a \in P$ or $b \in P$ by assumption of (2.). Therefore $b \in P$. But, as $b \in B$ was <u>arbitrary</u> we have $B \subseteq P$. //

Maximal and prime ideals are related, but, not the same...

Def$^{\underline{n}}$/ An ideal M in a ring R is <u>maximal</u> if $M \neq R$, but the only ideals containing M are R and M itself.

Th$^{\underline{m}}$/ Every maximal ideal is prime

<u>Proof</u>: suppose M is maximal ideal, $ab \in M$ and $a \notin M$. We seek to prove $b \in M$. Notice, as M is maximal and $a \notin M$ we have the ideal extending M by a

$$M[a] = \{ ar + ms \mid r, s \in R, m \in M \}$$

<u>must</u> be all of R. Thus $1 \in M[a]$ and so $\exists r, s \in R$ s.t. $1 = ar + ms \Rightarrow b = bar + bms$ and as $ba \in M \Rightarrow bar \in M$ by closure of M by R-mult. and $m \in M \Rightarrow m(bs) \in M$ again as $bs \in R$ and M an ideal $\therefore b = bar + bms \in M$ which demonstrates the primality of M according to Th$^{\underline{m}}$ on ②. //

Examples of prime ideals in $\mathbb{Z}[\sqrt{-5}]$

- in §11.5 we argued $(2)+(1+\sqrt{-5})$ is maximal we conclude it is <u>prime</u>.

- We could also show
$$J=(3)+(1+\sqrt{-5})=\{3m+(1+\sqrt{-5})n \mid m,n\in\mathbb{Z}\}$$
is maximal since outside J we'd have
$$\underline{3m'+1+(1+\sqrt{-5})n'}_{*} \quad \text{or} \quad \underline{3m''+2+(1+\sqrt{-5})n''}_{**}$$
type elements. If include $*$ then get 1 hence $K\supseteq J$ must have $1\in K \therefore K=R$.
If include $**$ in $K\supseteq J$ then $3,2\in K$
$\therefore 3-2=1\in K \Rightarrow K=R$.
Thus J is maximal and hence prime.

- $\bar{J}=(3)+(1-\sqrt{-5})$ is also maximal & $\therefore$ prime.
We say $\bar{J}$ is the conjugate of $J=(3)+(1+\sqrt{-5})$ as $\bar{J}=\{\bar{z}\mid z\in J\}$.

<u>Comment</u>: the shape of $(3)+(1+\sqrt{-5})$ is the same as $(2)+(1+\sqrt{-5})$. This observation is given a systematic discussion in §12.7 (p. 231)
$\mathbb{Z}[\sqrt{-5}]$ has class # 2 since $\exists$ two shapes of ideals.

§11.8 IDEAL PRIME FACTORIZATION

$\boxed{\text{Def}^{\underline{n}}/ \text{ an ideal } B \mid A \text{ if } \exists \text{ an ideal } C \text{ such that } A = BC}$

How does this fit with our suggestion $a \mid b$ be replaced with $(a) \supseteq (b)$ and so $B \mid A$ iff $B \supseteq A$?
We begin with examples.

$\boxed{\text{Def}^{\underline{n}}/ \ (\alpha, \beta) = (\alpha) + (\beta)}$

Example: $(2, 1+\sqrt{-5}) = (2) + (1+\sqrt{-5})$.
Seek an ideal C for which:

$$(2) = (2, 1+\sqrt{-5})C$$

Notice $(2, 1+\sqrt{-5}) \supseteq (2)$ so we expect $(2, 1+\sqrt{-5}) \mid (2)$.

$\boxed{\text{Claim: } (2) = (2, 1+\sqrt{-5})^2}$

Proof: from definition of the product of ideals

$$4 = 2 \times 2 \in (2, 1+\sqrt{-5})^2$$

$$2 + 2\sqrt{-5} = 2 \times (1+\sqrt{-5}) \in (2, 1+\sqrt{-5})^2$$

$$-4 + 2\sqrt{-5} = (1+\sqrt{-5})(1+\sqrt{-5}) \in (2, 1+\sqrt{-5})^2$$

Thus $4 + (2+2\sqrt{-5}) + (-4+2\sqrt{-5}) = 2 \in (2, 1+\sqrt{-5})^2$.
It follows $(2) = 2\mathbb{Z}[\sqrt{-5}] \subseteq (2, 1+\sqrt{-5})^2$. Likewise,

$$z \in (2, 1+\sqrt{-5})^2 \Rightarrow z = \sum (2m + n(1+\sqrt{-5}))(2j + k(1+\sqrt{-5}))$$

$$= \sum \underbrace{4mj + (2mk+2nj)(1+\sqrt{-5})}_{\text{multiple of } 2} + nk\underbrace{(1+\sqrt{-5})^2}_{-4+2\sqrt{-5}}$$

Thus $z \in (2)$ therefore $(2, 1+\sqrt{-5})^2 \subseteq (2)$ and $(2) \subseteq (2, 1+\sqrt{-5})^2$

Consequently $(2, 1+\sqrt{-5})(2, 1+\sqrt{-5}) = (2)$. //

$\boxed{\text{Claim: } (3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})}$

Proof: begin by noting a few identities which follow from arithmetic and the def$^{\underline{n}}$ of the product ideal,

$$9 = 3 \times 3 \in (3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = J\bar{J}$$

$$6 = (1+\sqrt{-5})(1-\sqrt{-5}) \in (3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = J\bar{J}$$

just giving it a name for my convenience.

Thus $9 - 6 = 3 \in J\bar{J}$ as ideals are closed under subtraction. Hence $(3) \subseteq J\bar{J}$ as multiples of 3 are once again in $J\bar{J}$. Conversely, suppose $z \in J\bar{J}$ this means z is formed by sum of $J, \bar{J}$ products,

$$\begin{aligned} z &= \sum \big(3m + n(1+\sqrt{-5})\big)\big(3a + b(1-\sqrt{-5})\big) \\ &= \sum \big(3^2 ma + \cancel{3(mb+na)(1+\sqrt{-5}) + nb \ldots} \\ &\qquad + 3mb(1-\sqrt{-5}) + 3na(1+\sqrt{-5}) + nb(1+\sqrt{-5})(1-\sqrt{-5})\big) \\ &= \sum \underbrace{3^2 ma + 3mb(1-\sqrt{-5}) + 3na(1+\sqrt{-5}) + 6nb}_{\text{multiple of } 3 \text{ in } \mathbb{Z}[\sqrt{-5}]} \\ &\qquad\qquad \in (3). \end{aligned}$$

Hence $J\bar{J} \subseteq (3)$ and $(3) \subseteq J\bar{J}$ $\therefore$ $(3) = J\bar{J}$. //

$$\boxed{\begin{aligned}\text{Claim: } (1+\sqrt{-5}) &= (2, 1+\sqrt{-5})(3, 1+\sqrt{-5}) \\ (1-\sqrt{-5}) &= (2, 1+\sqrt{-5})(3, 1-\sqrt{-5})\end{aligned}}$$

Proof: exercice for reader.

FITTING THE PIECES TOGETHER

$$\begin{aligned}(6) &= (2)(3) \\ &= \underbrace{(2, 1+\sqrt{-5})(2, 1+\sqrt{-5})}_{\text{from } 5}\underbrace{(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})}_{\text{from } 6} \\ &= (2, 1+\sqrt{-5})(3, 1+\sqrt{-5})(2, 1+\sqrt{-5})(3, 1-\sqrt{-5}) \\ &= (1+\sqrt{-5})(1-\sqrt{-5})\end{aligned}$$

We see the distinct prime factorizations $6 = 2 \times 3$ and $6 = (1+\sqrt{-5})(1-\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$ both follow from rearranging the prime ideal factorization of (6)