LECTURE 25 (CHAPTER 12, §12.4 → ... from Stillwell's Elements of Number Theory)

Defn/ If A is an ideal then $\bar{A} = \{\bar{z} \mid z \in A\}$

It turns out every ideal divides principal ideal, this is seen through $\bar{A}$ as $A\bar{A}$ is principal

Thm/ If R is the ring of integers for $\mathbb{Q}(\sqrt{d})$ and $d<0$, squarefree then any ideal A has $A\bar{A} = (k)$ for some $k \in \mathbb{Z}$.

Proof: A an ideal of an imaginary quadratic field can be formed as a lattice by §11.6, $A = \{m\alpha + n\beta \mid m, n \in \mathbb{Z}\}$

Hence the conjugate ideal $\bar{A} = \{\tilde{m}\bar{\alpha} + \tilde{n}\bar{\beta} \mid \tilde{m}, \tilde{n} \in \mathbb{Z}\}$

Consider, by definition of product of ideals,

$$A\bar{A} = \{s\alpha\bar{\alpha} + t\beta\bar{\beta} + u\bar{\alpha}\beta + v\alpha\bar{\beta} \mid s, t, u, v \in \mathbb{Z}\}$$

Notice, the following elements are real ($\bar{z} = z$)

$$\overline{\alpha\bar{\alpha}} = \bar{\alpha}\bar{\bar{\alpha}} = \alpha\bar{\alpha} \quad \& \quad \overline{\beta\bar{\beta}} = \bar{\beta}\beta \quad \& \quad \overline{\bar{\alpha}\beta + \alpha\bar{\beta}} = \alpha\bar{\beta} + \bar{\alpha}\beta.$$

But, in §10.4 we proved real quadratic integers are ordinary integers (I'm not sure §10.4 is best, but I do recall talking about this somewhere). Thus

$$\alpha\bar{\alpha},\ \beta\bar{\beta},\ \bar{\alpha}\beta + \alpha\bar{\beta} \in \mathbb{Z}$$

$$\Rightarrow \gcd(\alpha\bar{\alpha}, \beta\bar{\beta}, \bar{\alpha}\beta + \alpha\bar{\beta}) \in \mathbb{Z}$$

$$\Rightarrow p\alpha\bar{\alpha} + q\beta\bar{\beta} + r(\bar{\alpha}\beta + \alpha\bar{\beta}) = k \quad \text{for some } p, q, r \in \mathbb{Z}.$$

Hence $k \in A\bar{A} \Rightarrow (k) \subseteq A\bar{A}$.

Conversely, to show $(k) \supseteq A\bar{A}$, we need to show k divides $\alpha\bar{\alpha}, \beta\bar{\beta}, \bar{\alpha}\beta, \alpha\bar{\beta}$.

continued.

Proof continued: showing $(h) \supseteq A\bar{A}$,

$h \mid \alpha\bar{\alpha}$ & $h \mid \beta\bar{\beta}$ by construction of h as gcd.

If $\alpha\bar{\beta}/h$, $\bar{\alpha}\beta/h \in R$ then $h \mid \alpha\bar{\beta}$ and $h \mid \bar{\alpha}\beta$.

But, observe, the following has $\mathbb{Z}$-coeff

$$\left(x - \frac{\alpha\bar{\beta}}{h}\right)\left(x - \frac{\bar{\alpha}\beta}{h}\right) = x^2 - \left(\frac{\alpha\bar{\beta} + \bar{\alpha}\beta}{h}\right)x + \frac{\alpha\bar{\alpha}\beta\bar{\beta}}{h^2} = 0$$

and takes $x = \frac{\alpha\bar{\beta}}{h}, \frac{\bar{\alpha}\beta}{h}$ as zeros thus $\alpha\bar{\beta}/h$, $\bar{\alpha}\beta/h$ are quadratic integers as desired. $\blacksquare$

§12.5 DIVISIBILITY AND CONTAINMENT

We've suggested that "divides" be replaced with "contains". We complete that investigation here for rings of integers of an imaginary quadratic field. Recall $ab | ac \Rightarrow b | c$ for $a \neq 0$.

Thm/ If A, B, C are nonzero ideals of R and $AB \supseteq AC$ then $B \supseteq C$

Proof: if $A = (\alpha)$ is principal then, (special case ★)

$$
\begin{aligned}
AB \supseteq AC &\Rightarrow (\alpha)B \supseteq (\alpha)C && : \text{(typo in text here)} \\
&\Rightarrow \alpha B \supseteq \alpha C && : \text{by Lemma below.} \\
&\Rightarrow B \supseteq C && : \text{multiplying by } \alpha^{-1} \text{ which exists as } (\alpha) = A \neq 0.
\end{aligned}
$$

Hence, in general,

$$
\begin{aligned}
AB \supseteq AC &\Rightarrow \bar{A}AB \supseteq \bar{A}AC && : \bar{A} \text{ conj. ideal of } A \\
&\Rightarrow (h)B \supseteq (h)C && : \text{§12.4 we showed } \bar{A}A = (h) \text{ for some } h \in \mathbb{Z} \text{ in } \mathbb{Q}(\sqrt{d}) \ d<0 \text{ squarefree...} \\
&\Rightarrow B \supseteq C && : \text{by special case ★}
\end{aligned}
$$

Lemma: for $B, C \neq 0$ ideals of R and $\alpha \in R$, $\alpha \neq 0$ If $(\alpha)B \supseteq (\alpha)C$ then $\alpha B \supseteq \alpha C$.

Proof: $AB = \{ a_1 b_1 + \cdots + a_n b_n \mid a_j \in A,\ b_j \in B \text{ for } k \in \mathbb{N} \}$

Now, $A = (\alpha) \Rightarrow a_j = \alpha^{m_j}$ for some $m_j \in \mathbb{N}$. (remove zeros)

Hence $z \in (\alpha)B \Rightarrow z = \alpha^{m_1} b_1 + \cdots + \alpha^{m_n} b_n$

$$= \alpha \underbrace{(\alpha^{m_1 - 1} b_1 + \cdots + \alpha^{m_n - 1} b_n)}_{\text{since } B \text{ ideal this is just some element of } B} \in \alpha B$$

Thus $(\alpha)B \subseteq \alpha B$

Conversely it is clear $\alpha B \subseteq (\alpha)B$

Hence $(\alpha)B = \alpha B$ and likewise $(\alpha)C = \alpha C$ thus $(\alpha)B \supseteq (\alpha)C \Rightarrow \alpha B \supseteq \alpha C$ as desired. //

- Multiplying by conjugate $\bar{A}$ for A makes $\underbrace{\bar{A}A}$ principal. This is nice trick! Better yet, $\bar{A}A = (k)$ for $k \in \mathbb{Z}$

Th^m/ "Contains means divides"
If A & B are ideals of R and $B \supseteq A$ then $B \mid A$ in the sense that $\exists$ an ideal C for which
$$A = BC.$$

Proof: once again begin with special case; $B = (\beta)$

$$B \supseteq A \Rightarrow (\beta) \supseteq A$$
$$\Rightarrow A \subseteq (\beta) = \{\beta r \mid r \in R\}$$
$$\Rightarrow \beta \mid a \text{ for each } a \in A \quad (\text{as } a \in A \Rightarrow \exists r \in R \text{ st. } a = \beta r$$
$$\Rightarrow A = (\beta)\{\underbrace{r = a/\beta \mid a \in A}_{\text{can argue this is an ideal.}}\}$$
$$\Rightarrow A = BC.$$

Of course, not all B are principal, but $B\bar{B} = (k)$, so:

$$B \supseteq A \Rightarrow \bar{B}B \supseteq A\bar{B} \quad (\text{multiplying by } \bar{B})$$
$$\Rightarrow (k) \supseteq A\bar{B} \quad (\S 12.4)$$
$$\Rightarrow A\bar{B} = (k)C \quad (\text{by special case above}$$
$$\Rightarrow A\bar{B} = \bar{B}BC \quad (B\bar{B} = (k) \text{ once again})$$
$$\Rightarrow A = BC \quad (\text{by Th}^{\text{m}} \text{ on cancellation of ideals we proved earlier in } \S 12.5)$$

§12.6 FACTORIZATION OF IDEALS

Here we show existence and uniqueness for the prime factorization of ideals of the ring R of integers in the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$. The logic here is guided by prime $\Leftrightarrow$ maximal ideal. For #'s we found smaller & smaller factors, for ideals, we find larger & larger ideal factors with R as a ceiling. The proofs which follow are like those for $\mathbb{Z}$.

Existence: Every nonzero ideal $A \neq R$ is product of prime ideals. (§11.7)

Proof: If A is not prime then A not maximal, hence $\exists$ ideal $B \supsetneq A$ with $B \neq R$. Thus $\exists\, C$ an ideal such that $A = BC$ (since $B \supseteq A \Rightarrow B/A$ by §12.5) Then either C is prime or we can factor it as with A above. This process goes on until we run out of ~~non~~ ideals inside R. At each step we absorb at least one element of the form $I + r$ and there are only finitely many such $I + r$. //

Uniqueness: the factorization of a nonzero ideal is unique, up to the order of the factors.

Proof: as with $\mathbb{Z}$, the proof is by prime divisor property. Note, if $P \mid AB$ then $P \mid A$ or $P \mid B$. This is true since a prime ideal has

$$P \supseteq AB \Rightarrow P \supseteq A \text{ or } P \supseteq B$$

But, then by "contains means divides" theorem of §12.5 we find $P \mid AB \Rightarrow P \mid A$ or $P \mid B$. Then see the argument we gave back in Chapter 2 for $\mathbb{Z}$. //
(p. 29)

§12.7 Ideal Classes

$\boxed{\text{Thm/ The class number of } \mathbb{Z}[\sqrt{-5}] \text{ is } 2}$

The class number is the # of ideal shapes in a given ring. For $\mathbb{Z}[\sqrt{-5}]$ we either have $\underbrace{\mathbb{Z}[\sqrt{-5}]}$ or (α) a principal ideal. The non-principal proof is found on p. 232, it's geometric and somewhat like arguments we've seen before.

In § 12.9 we learn more about history of class number:

- 1773 idea of Lagrange for reducing binary quadratic forms to count inequivalent forms,
- 1801 Gauss extended to forms with negative determinant
- 1839 Dirichlet used L-series of Euler (this also is what Dirichlet used to prove other difficult things like arithmetic progression we mentioned in §9.9)
- modular functions: periodic in $\mathbb{C}$-plane, if $ad-bc=\pm 1$

  $$j\left(\frac{az+b}{cz+d}\right) = j(z)$$

  So j is fnct. of "lattice shapes" (See p. 237) (well 238 1st paragraph)
- Kronecker ~~1857~~ (1857) found class # of $\mathbb{Q}(\sqrt{d})$ is degree of $j(\sqrt{d})$. For example,

  $$j(i) = 1728 \leftarrow \text{degree } 1$$

  Hence $\mathbb{Z}[i]$ has one shape of idea.

- Cox's book should be in our Library sometime soon if you're interested in more...

§ 12.8 PRIMES OF THE FORM x^2+5y^2

Observations about $\mathbb{Z}[\sqrt{-5}]$ (see p. 233–234 for details)

- primes of form x^2+5y^2 have form $\underline{20n+1}$ or $\underline{20n+9}$
- -5 is square mod p when $p = 20n+1$ or $20n+9$ (p a prime)

$\boxed{\text{Thm: Primes of the form } x^2+5y^2 \text{ are precisely those of the form } 20n+1 \text{ or } 20n+9}$

Proof: we need to show primes of form $20n+1$ or $20n+9$ are of the form x^2+5y^2. The proof is by the arithmetic of ideals of $\mathbb{Z}[\sqrt{-5}]$. We'll follow the calculation of 234–235. It's nice & clear: