Ideals and factorization in number fields

Happy Indigenous Peoples' Day!

**Note:** the video from October 9 got corrupted while I was trying to post it, so there is a segment missing in the middle. I recorded a supplemental video to cover the gap.
The trace of an algebraic integer

Reminder: for any finite field extension
\[ \text{Trace}_{L/K}(x) = \text{Trace}(T_L \circ T_{x} : L \to L) \]

What if \( K = \mathbb{Q}, \ x \in \mathbb{Q}_L \)?

Then \( \text{Trace}_{L/K}(x) \in \mathbb{Q} \cap \mathbb{Z} = \mathbb{Z} \).
The trace pairing
$L/K$ finite field extension
For $x,y \in L$, define $\langle x,y \rangle = \text{trace}(xy)$
$K$-bilinear map $L \times L \to K$
Prop if $L/K$ is separable (and $x_1, \ldots, x_n$
is a basis of $L/K$) then $\langle x,y \rangle$ is
perfectly non-degenerate, i.e., $L \to \mathbb{C} = \text{Hom}_{K}(L,K)$

Pf. write $L=K(\theta)$, use $x \mapsto x_1 \mapsto \langle x,y \rangle$
compute det. of matrix (Vandermonde)
Integral bases

Corollary: If $L$ is a number field then $O_L$ is a free $\mathbb{Z}$-module. (i.e., a lattice in $\mathbb{R}$ as a $\mathbb{Q}$-vector space).

Proof: Pick a basis of $L$ consisting of elements of $O_L$, $x_1, \ldots, x_n$. Then for any $\beta \in O_L$, $\langle (x_1, \ldots, x_n) \cdot \beta \rangle \subseteq \mathbb{Q}$.

This gives an upper bound on $O_L$. If $\beta$ is a basis,
Ideals in rings of integers

\[
2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \text{ in } \mathbb{Z}[\sqrt{-5}]
\]

Kummer: fix this by adding "ideal numbers"

\[
\text{ie: } \gcd(2, 1 + \sqrt{-5})
\]

Dedekind: instead, consider set of maximal\text{ }\mathfrak{m}\text{-primary ideals} \mathfrak{m}

R is an ideal if \(x, y \in \mathfrak{I} \Rightarrow x + y \in \mathfrak{I}\)

\[
\mathfrak{I} \text{ is noetherian (ACC)}
\]
Dedekind domains

An integral domain \( R \) is a Dedekind domain if:

- \( R \) is noetherian
- \( R \) is integrally closed in \( \text{Frac}(R) \)
- Every nonzero prime ideal is maximal

Recall: \( I \) in \( R \) is prime if \( \forall x, y \in R, \) if \( xy \in I \) then \( x \in I \) or \( y \in I \).
Rings of integers are Dedekind domains

The aran $O_L$ is a Dedekind domain. 

- Noetherian 
- Integrally closed 

Let $I$ be a nonzero prime ideal. The $I \cap \mathbb{Z} \neq \{0\}$ is a nonzero prime ideal, say $(p)$. 

The ring $O_L/(p)$ is finite over $\mathbb{Z}/(p) = \mathbb{F}_p$ 

& is integral domain, so a field: 

$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \quad -a_n = x(x^{n-1} + a, x^{n-2} + \cdots)$ 

so $I$ maximal.
Statement of unique factorization in a Dedekind domain

Theorem For $R$ a Dedekind domain, every nonzero ideal $I$ admits a factorization as $I = P_1 P_2 \ldots P_r$, where $P_1, \ldots, P_r$ are prime ideals, which is unique up to order.

(Note: no units!)
A lemma on products of prime ideals

**Lemma:** For every nonzero ideal \( I \) in \( R \), there exists \( f_1, \ldots, f_r \) prime ideals of \( R \) such that \( I = f_1 \cdots f_r \).

Proof: Suppose there were a maximal counterexample, which cannot be prime. So \( \exists x, y \in R \) s.t. \( xy \in I \), but \( x + I, y + I \notin I \).

\[ x \in f_1 \cdots f_r, \quad y \in f_1 \cdots f_r \]

Therefore, \( f_1 \cdots f_r \notin I \), which contradicts the assumption that \( I \) is prime.