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 $L/K$ finite field extension

$\text{Trace}_{L/K} : L \rightarrow K \quad \text{Trace}_{L/K}(x) = \text{trace}(T_x : L \rightarrow L)$

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 \( L/K \) for \( K \)-field extension.

For \( x, y \in L \), define \( \langle x, y \rangle = \text{trace}_{L/K}(xy) \).

The bilinear map \( \langle \cdot, \cdot \rangle : L \times L \to K \).

Prop: if \( L/K \) is separable (and \( x_1, \ldots, x_n \) is a basis of \( L/K \)), then \( \langle x, y \rangle \) is perfect and generates \( L \) (i.e., \( L \subseteq L = \text{Hom}_K(L, K) \)).

Pf. \( \dim_K L = [L:K] \), use \( x \rightarrow x^l \rightarrow \langle x, y \rangle \).

Compute det of matrix \( (\langle x_i, x_j \rangle) \).
Integral bases

**Corollary** if $L$ is a number field then $\mathcal{O}_L$ is a free $\mathbb{Z}$-module. (i.e., a lattice in $\mathbb{R}$ as a vector space)

Pick a basis of $L$ consisting of elements of $\mathcal{O}_L$.

This gives an upper bound on $\mathcal{O}_L/\mathbb{Z}$, namely it is perfect.
Ideals in rings of integers

\[ L = \# \text{ field} \]

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

Kummer: fix this by adding \textit{ideal numbers} (i.e., \text{gcd}(2, 1 + \sqrt{-5})

Dedekind: instead, consider \textit{sets of multiples}

\text{Ring: } \mathcal{R} = \mathbb{Z}[\sqrt{-5}]

\text{Ideal: } \mathcal{I} = \text{ideal if } \bullet x, y \in \mathcal{I} \Rightarrow x + y \in \mathcal{I}

\text{Principal ideal: } \mathcal{P}

\text{If } \theta \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: $I \subseteq R$ is a **prime ideal** if for all $x, y \in R$, if $x + y \in I$, then $x \in I$ or $y \in I$. 

(e.g. $2$)
Rings of integers are Dedekind domains

The ring $\mathcal{O}_K$ is a Dedekind domain. Let $\mathfrak{p}$ be a non-zero prime ideal. Then $\mathfrak{p}^n \neq \{0\}$ is a non-zero prime ideal, say $(p)$. The ring $\mathcal{O}_K$ is finite over $\mathbb{Z}$, $(p) = \mathfrak{p}$ is an integral domain, so a field.

$\alpha x^n + a_1 x^{n-1} + \ldots + a_n = 0 \implies \alpha = x(x^{n-1} + a_1 x^{n-2} + \ldots) \implies \alpha$ maximal.
Statement of unique factorization in a Dedekind domain

Theorem: For $R$ a Dedekind domain, every nonzero ideal $I$ admits a factorization as $I = f_1 \cdots f_r$, where $f_i$ 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 a Dedekind domain \( R \), \( I \) is a product of prime ideals. If otherwise, find a maximal counterexample which cannot be prime. So, \( x \in R \) s.t. \( xy \in I \), \( x + I \neq I \).