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 L/K finite field extension

$\mathrm{Trace}_{L/K} : L \to K$ $\quad \mathrm{Trace}_{L/K}(x) = \mathrm{Trace}(T_x : L \to L)$

What if $K = \mathbb{Q}$, $x \in \mathcal{O}_L$?

Then $\mathrm{Trace}_{L/K}(x) \in \mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$.

The trace pairing L/K finite field extension

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

K-bilinear map $L \times L \to K$

<u>Prop</u> if L/K is <u>separable</u> (and $\alpha_1 \dots \alpha_n$ is a basis of L/K) then $\langle x, y \rangle$ is <u>(perfect) nondegenerate</u>, i.e. $L \xrightarrow[\langle , \rangle]{\sim} L^\vee = \mathrm{Hom}_K(L, K)$

$$x \longrightarrow y \mapsto \langle x, y \rangle$$

<u>Pf</u>: write $L = K(\theta)$, use basis $1, \theta, \dots, \theta^{n-1}$

compute det of pairing matrix (Vandermonde)

Integral bases

Corollary: If L is a number field then $\mathcal{O}_L$ is finite free $\mathbb{Z}$-module of rank $= [L:\mathbb{Q}]$ (i.e. a lattice in L as a $\mathbb{Q}$-vector space).

Pf: Pick a basis of $L/\mathbb{Q}$ consisting of elements of $\mathcal{O}_L$ $\alpha_1 \ldots \alpha_n$. Then for any $\beta \in \mathcal{O}_L$, $\langle \alpha_i, \beta \rangle \in \mathbb{Z}$. This gives an upper bound on $\mathcal{O}_L$ b/c pairing is perfect.

Ideals in rings of integers

L = # field

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

Kummer: fix this by adding "ideal numbers"

ie. $\gcd(2, 1+\sqrt{-5})$

Dedekind: instead, consider set of multiples

R = ring, $I \subset R$ is an ideal if
- $x, y \in I \Rightarrow x+y \in I$
- $x \in I$, $y \in R \Rightarrow xy \in I$

prev slide $\Rightarrow$

$\mathcal{O}_L$ is noetherian (ACC)

Dedekind domains

An integral domain R is a <u>Dedekind domain</u> if:

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

Recall: $I \subset R$ is <u>prime</u> if $\forall x, y \in R$, if $xy \in I$
ideal
then $x \in I$ or $y \in I$.

(e.g. $\mathbb{Z}$)

Rings of integers are Dedekind domains

$\Leftarrow$ # field

<u>Theorem</u> $\mathcal{O}_L$ is a Dedekind domain.

$\alpha \neq 0$, $\alpha \in I$ (e.g. $\mathrm{Norm}_{L/\mathbb{Q}}(\alpha)$)

- noetherian ✓
- integrally closed

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

The ring $x \in \mathcal{O}_L/I$ is finite over $\mathbb{Z}/(p) = \mathbb{F}_p$ & is integral domain, so a field:

$$x^n + a_1 x^{n-1} + \dots + a_n = 0 \qquad -a_n = x(x^{n-1} + a_1 x^{n-2} + \dots)$$

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 $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are nonzero prime ideals, which is unique up to order.

\mathfrak

(Note: no units!)

A lemma on products of prime ideals

R = Dedekind domain

Lemma: For every nonzero ideal I in R,

$\exists$ $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ nonzero prime ideals s.t. $I \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$.

Pf otherwise find a maximal counterexample which cannot be prime. so $\exists$ $x, y \in R$ s.t. $xy \in I$, but $x+I, y+I \neq I$..

$$x+I \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r \qquad y+I \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_s \qquad I \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s \cdots$$

$\Rightarrow \cancel{\Leftarrow}$.