Last time, trying to provide general definition for ring of integers of # field.

Given extension of rings $A \subseteq B$, say $b \in B$ is integral if it satisfies monic polynomial with coeffs in $A$. Call the entire ring $B$ integral if all elts $b \in B$ integral. How to make such ring?

Given $A \subseteq C$, let $\overline{A} = \{ c \in C \mid c \text{ integral over } A \}$ "integral closure"

Our then last time: $b, \ldots, b_n$ integral $\iff \overline{A}[b, \ldots, b_n]$ fin gen. $A$-module
ensured $\overline{A}$ is a ring.

Define $\mathcal{O}_K$: ring of ints. of # field $K = \overline{\mathbb{Z}}$ in $K$ (integral closure of $\mathbb{Z}$ in $K$)

Note that if $A \subseteq B \subseteq C$ with $C$ integral over $B$, $B$ integral over $A$,
then $C$ integral over $A$ (owing to fin gen. module criterion)

$\Rightarrow$ if $\overline{A}$ is integral closure of $A$ in $B$, then $\overline{A}$ is "integreally closed" in $B$

i.e. $\overline{A} = \overline{\overline{A}}$.

Example: $K = \mathbb{Q}(\sqrt{d})$, $d$ square-free ($\equiv 0 \pmod{4}$)

then $\mathcal{O}_K = \{ a + b \sqrt{d} \mid a, b \in \mathbb{Z} \}$ if $d \equiv 2, 3 \pmod{4}$

$= \{ a + \frac{b}{2} (1 + \sqrt{d}) \mid a, b \in \mathbb{Z} \}$ if $d \equiv 1 \pmod{4}$

How to prove this?

Exploit Galois symmetry!

pf: $b$: non-triv. elt. of $\text{Gal}(K/\mathbb{Q})$ \quad $\overline{\sqrt{d}} \to -\sqrt{d}$

$x \in \mathcal{O}_K$ , then $b(x) \in \mathcal{O}_K \iff x + b(x), x \cdot b(x) \in \mathcal{O}_K$

so if $x = a + b \sqrt{d}$ then $x + b(x) = 2a$, $x \cdot b(x) = a^2 - db^2 \subseteq \mathbb{Q}$.

But $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$ (all $\mathbb{Q}$-Ds closed in their field of fractions)

so in fact $2a, a^2 - db^2$ must be in $\mathbb{Z}$, also sufficient since $x$ is

a root of $X^2 - 2ax + (a^2 - db^2) = 0$. Now just play with conditions to get result for $d$ mod $4$.
Turning to situations more tailored to our interests:

A: integral domain, \( K \) : field of fractions, \( L/K \) : finite extension which is integrally closed in \( L \)

B: integral closure of \( A \) in \( L \). (now know \( B \) is integrally closed (in \( L \))

1. Elts in \( L \) of form \( \beta = \frac{b}{a} \), \( b \in B \), \( a \in A \)

   because if \( a_n \beta^n + \ldots + a_1 \beta + a_0 = 0 \), \( a_i \in A \)

   (do this by clearing denominators for \( \beta \) with coeffs in \( K \))

   then \( a_n \beta \) is root of monic equation with coeffs in \( A \) (multi. by \( a_n^{-1} \))

   \( \beta \) is an integral over \( A \)

   i.e. \( \beta = \frac{b}{a_m} \). not just any polynomial

2. \( \beta \in L \) is integral over \( A \) \( \iff \) its minimal poly. \( p(x) \) has coeffs. in \( A \)

   \( \Rightarrow \):

   (if \( \beta \) is root of \( g(x) \), monic in \( A[x] \), then \( p(x) \mid g(x) \) in \( K[x] \)

   \( \Rightarrow \) zeros \( \beta_1, \ldots, \beta_n \) of \( p(x) \) are integral over \( A \)

   \( \Rightarrow \) coeffs of \( p(x) \) are integral over \( A \), but \( A \) integrally closed

   so coeffs in \( A \).  \\

Want to define invariants of such rings analogous to the norm function for the Gaussian integers. Just need to think in basis-free way.

Given \( x \in L \) as above, define "translation" endomorphism \( T_x : \beta \mapsto \beta x \)

then we have natural invariants \( \text{Tr}_K(x) \), \( \det(T_x) \)

\( \text{Tr}_K(x) \) "trace of \( x \)" "norm of \( x \)" \( \text{Nuc}_K(x) \)
More generally, we have invariants for each coeff of char. poly.

\[ \text{det} (t \cdot I_n - T_x) = t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n \in K[t] \]

with \( a_1 \): trace \( a_n \): norm 

(\text{viewing } L \text{ as } n\text{-dim} \text{ } \text{v.s.} / K, \text{ so endomorphism } T_x \text{ presented in } K\text{-coords} )

Of course, since trace is additive and det is multiplicative, we have

\[ \text{Tr}_{L/K} (x+y) = \text{Tr}_{L/K} (x) + \text{Tr}_{L/K} (y), \quad N_{L/K} (xy) = N_{L/K} (x) N_{L/K} (y). \]

i.e. \( \text{Tr} \in \text{Hom} (L_1 K), \quad N_{L/K} \in \text{Hom} (L^*, K^*) \)

if \( L/K \) is separable, we can give an alternate definition in terms of Galois theory:

\begin{align*}
(1) & \quad \text{det} (t \cdot I_n - T_x) = \prod_{\sigma} (t - \sigma(x)) \\
(2) & \quad \text{Tr}_{L/K} (x) = \sum_{\sigma} \sigma(x) \\
(3) & \quad N_{L/K} (x) = \prod_{\sigma} \sigma(x) \\
\end{align*}

\text{where } \sigma \text{ varies over all } K \text{ embeddings of } L \text{ in algebraic closure } \overline{K}/K.

\text{Immediate corollaries of (1).}

proof: We show first that \( \text{det} (t \cdot I_n - T_x) = p_x(t)^d \) \( p_x(t) \) min. poly. of \( x \) over \( K \)

indeed, \([1, x, \ldots, x^{m-1}] \) is basis for \( K(x)/K \)

if \( \text{deg} (p_x(t)) = m \).

Extend to a basis of \( L/K \) using basis \( \alpha_i, \ldots, \alpha_d \) of \( L/K(x) \).

( take all products of \( \alpha_i \) and \( x^j \) )

With this "good" basis w.r.t. \( x \), then \( T_x \) looks especially nice:
its matrix consists of \( d \) blocks of size \( m \times m \) along diagonal

\[
\begin{pmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 0
\end{pmatrix}
\]

so char. poly. has form claimed:

\[-c_0 - c_1 t - \cdots - c_d\]

for \( c_0, c_1, \ldots, c_d \) \( x \) since mult. by \( x \) takes \( \alpha_i x^j \to \alpha_i x^{j+1} \)

here we are writing \( p_x(t) = t^m + c_1 t^{m-1} + \cdots + c_m \).

---

To finish the proof of (i), partition the set \( \text{Hom}_K(L, K) \) of all \( K \)-embeddings of \( L \) according to equivalence relation:

\[ b \sim \tilde{b} \iff b x = \tilde{b} x \text{ for our fixed elt } x \in L. \]

( \( m \) equivalence classes w/ \( d \) elts. each. )

Pick reps. \( b_1, \ldots, b_m \) for each equivalence class. Then

\[ p_x(t) = \prod_{i=1}^m (t - b_i x) \]

so

\[ \det (t \cdot I_m - T_x) = \prod_{i=1}^m (t - b_i x)^d = \prod_{i=1}^m \prod_{j=1}^d (t - b_i x) \]

\[
= \prod_{i=1}^m (t - b_i) \prod_{j=1}^d (t - b_i x)
\]

using this interpretation, not hard to show

Cor: If \( K \triangleleft L \triangleleft M \) is a tower of finite, separable extensions, then

\[ \text{Tr}_{K} \cdot \text{Tr}_{M/K} = \text{Tr}_{M} \quad \text{and} \quad \text{Nh}_{K} \cdot \text{Nh}_{M/K} = \text{Nh}_{M/K} \]

( in fact, same is true even if extensions not separable, since trace/norm are expressible in terms of maximal sep. extension.)
Given a basis $\alpha_1, \ldots, \alpha_n$ of separable extension $L/K$, then
define the discriminant

$$d(\alpha_1, \ldots, \alpha_n) = \det (b_i(\alpha_j))^2$$

where $b_i : K$-embeddings of $L$ in $\overline{K}$.

In particular, if we take the basis of form,

$$1, \theta, \theta^2, \ldots, \theta^{n-1},$$

and set $\theta_i = b_i(\theta)$ then

we must compute the determinant of the Vandermonde matrix

$$\det \begin{pmatrix}
1 & \theta_1 & \theta_1^2 & \cdots & \theta_1^{n-1} \\
1 & \theta_2 & \theta_2^2 & \cdots & \theta_2^{n-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \theta_m & \theta_m^2 & \cdots & \theta_m^{n-1}
\end{pmatrix} = \prod_{i<j} (\theta_i - \theta_j)^2$$

so the discriminant is this quantity squared.

If this looks familiar, recall discriminant of monic polynomial is the product:

$$\prod (r_i - r_j)^2$$

where $r_i$ are roots of poly. $i<j$ separable.

For example, given finite extension of fields $L/K$, write

$$L = K(\theta)$$

with basis $1, \theta_1, \ldots, \theta_{n-1}$

and min. poly. $P_\theta(t) = t^n + \cdots + a_n = \prod_{i=1}^n (t - b_i(\theta))$.

In the simplest case where $L$ is Galois, elts permute the roots but still true even if $L/K$ separable.

These definitions make sense for any field extension, but if we assume $A$ int. closed integral domain, $K$ field of fractions, $L$ extn of $K$, $B$ int. closure of $A$ in $L$, then know $\text{Tr}(x), N(x) \in A$.

(Use characterization in terms of embeddings if $x \in B$)

$$x \in B \iff \sum_{x \in B} b(x) = \text{Tr}(x)$$