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 $\bar{A} = \{ c \in C \mid c \text{ integral over } A \}$ "integral closure"

Our thm. last time: $b_1, \dots, b_n$ integral$/A \iff A[b_1, \dots, b_n]$ fin. gen. A-module ensured $\bar{A}$ is a ring.

Define $\mathcal{O}_K$: ring of ints. of # field K $=$ $\bar{\mathbb{Z}}$ 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 $\bar{A}$ is integral closure of A in B, then $\bar{A}$ is "integrally closed" in B

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

Example: $K = \mathbb{Q}(\sqrt{d})$, d square-free (so $\not\equiv 0 \pmod 4$)

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

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

How to prove this? Exploit Galois symmetry!

pf: σ: non-triv. elt. of $\mathrm{Gal}(K/\mathbb{Q})$ $\sqrt{d} \to -\sqrt{d}$

$x \in \mathcal{O}_K$, then $\sigma(x) \in \mathcal{O}_K \Rightarrow x + \sigma(x), \ x \cdot \sigma(x) \in \mathcal{O}_K$

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

But $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$ (all P.I.D.s int. 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 situation more tailored to our interests:

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

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

(1) Elts in L of form $\beta = \frac{b}{a}$ $b \in B$, $a \in \cancel{B}\ A$ we can conclude this finer statement

because if $a_n \beta^n + \cdots + a_1 \beta + a_0 = 0$ $a_i \in A$

(do this by clearing denoms for eq'n with coeffs in K)

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

$a_n\beta = b$ so $b \in B$,

i.e. $\beta = b/a_n$.

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

not just any polynomial

$\Rightarrow$:

(if β 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 $T_x : \beta \mapsto x\beta$

then we have natural invariants $\operatorname{tr}(T_x)$, $\det(T_x)$ (thinking of L as v.s. $/K$)

$\operatorname{Tr}_{L/K}(x)$ "trace of x" "norm of x" $N_{L/K}(x)$

More generally, we have invariants for each coeff. of char. poly.

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

if $[L:K] = n$

with a_1 : trace a_n : norm

(viewing L as n-dim'l v.s. $/K$, so endomorphism T_x presented in K-coords)

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

$$\mathrm{Tr}_{L/K}(x+y) = \mathrm{Tr}_{L/K}(x) + \mathrm{Tr}_{L/K}(y), \quad N_{L/K}(xy) = N_{L/K}(x)\,N_{L/K}(y).$$

i.e. $\mathrm{Tr}_{L/K} \in \mathrm{Hom}(L, K)$, $N_{L/K} \in \mathrm{Hom}(L^*, K^*)$

---

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

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

(i) $\det(t\cdot I_n - T_x) = \prod_\sigma (t - \sigma x)$

(ii) $\mathrm{Tr}_{L/K}(x) = \sum_\sigma \sigma x$

(iii) $N_{L/K}(x) = \prod_\sigma \sigma x$

$\Big\}$ immediate corollaries of (i).

proof: We show first that $\det(t\cdot I_n - T_x) = p_x(t)^d$ $\quad p_x(t)$ min. poly. of x over K, $d = [L : K(x)]$

Indeed, $1, x, \ldots, x^{m-1}$ is basis for $K(x)/K$ if $\deg(p_x(t)) = m$.

Extend to a basis of L/K using basis $\alpha_1, \ldots, \alpha_d$ of $L/K(x)$.

(take all products of α_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

of form
$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots \\ \vdots \\ 0 & 0 & 0 & \cdots & 0\;1 \\ -c_m & -c_{m-1} & & \cdots & -c_1 \end{pmatrix}$$
so char. poly. has form claimed.

for $\alpha_i, \alpha_i x, \ldots \alpha_i x^{m-1}$ 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 $\mathrm{Hom}_K(L, \bar{K})$ of all K-embeddings of L according to equivalence relation:

$$\sigma \sim \tau \iff \sigma x = \tau x \quad \text{for our fixed elt } x \in L.$$

(m equivalence classes with d elts. each.)

Pick rep's $\sigma_1, \ldots, \sigma_m$ for each equivalence class. Then

$$p_x(t) = \prod_{i=1}^{m} (t - \sigma_i x) \quad \text{so}$$

$$\det(t \cdot I_n - T_x) = \prod_{i=1}^{m} (t - \sigma_i x)^d = \prod_{i=1}^{m} \prod_{\sigma \sim \sigma_i} (t - \sigma x)$$
$$= \prod_{\sigma} (t - \sigma x) \quad //$$

using this interpretation, not hard to show

Cor: If $K \subseteq L \subseteq M$ is a tower of finite, separable extensions, then
$\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} = \mathrm{Tr}_{M/K}$ and $N_{L/K} \circ N_{M/L} = N_{M/K}$

(in fact, same is true even if extensions not separable, since trace/norm are expressible in terms of maximal sep. extension.)

Given a basis $\alpha_1, \dots, \alpha_n$ of separable extension L/K then define the discriminant

$$d(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2 \qquad \sigma_i : K\text{-embeddings of } L \text{ in } \overline{K}$$

In particular, if we take a basis of form,

$1, \theta, \theta^2, \dots, \theta^{n-1}$, and set $\theta_i := \sigma_i(\theta)$ then we must compute the determinant of the Vandermonde matrix

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

so the discriminant is this quantity squared.

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

$$\prod_{i<j} (r_i - r_j)^2 \quad \text{where } r_i : \text{roots of poly.}$$

For example, given finite separable extension of ~~...~~ fields L/K, write

$L = K(\theta)$ with basis $1, \theta, \dots, \theta^{n-1}$

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

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 : separable ext'n of K,

B int. closure of A in L, then know $Tr(x), N(x) \in A$ if $x \in B$

(use characterization in terms of embeddings $x \in B$ ~~...~~, $\sigma(x) \in B$ so $Tr(x) \in B \cap K = A$