Rings of integers in number fields

K = # field (right now subfield of $\mathbb{C}$ which is finite-dimensional as $\mathbb{Q}$-vector space).

write $\mathcal{O}_K$ for the ~~set~~ ring of algebraic integers in K

i.e. $K \cap \overline{\mathbb{Z}}$

e.g. $K = \mathbb{Q}(\sqrt{-3})$

$$\mathbb{Z}[\sqrt{-3}] \subset \mathcal{O}_K = \mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$$

Ring elements integral over a subring

$A \subset B$ inclusion of rings

$b \in B$ is integral over A if $\exists$ monic poly

$P(x) \in A[x]$ s.t. $P(b) = 0$. ie.

$\exists$ n and $a_1, \dots, a_n \in A$ s.t. $x^n + a_1 x^{n-1} + \cdots + a_n = 0$

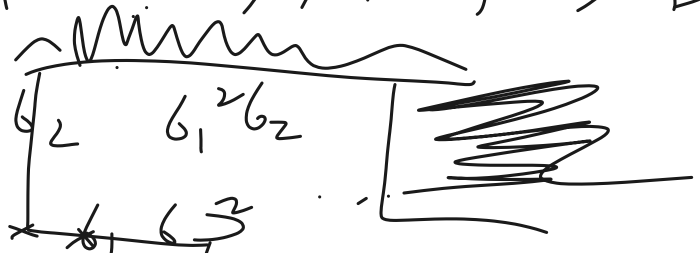
$\Longrightarrow 1, b, \dots, b^{n-1}$ generate $A[b]$ as an A-module

(Note: if A is a field, then can always find the minimal polynomial.)

An approach to integrality via linear algebra

Prop TFAE: i) $b_1, \ldots, b_n$ are all integral over A.
For $b_1 \ldots b_n \in B$ ii) $A[b_1, \ldots, b_n]$ is fin gen as an A-module.

i) $\Rightarrow$ ii)



ii) $\Rightarrow$ i) say $c_1 \ldots c_r \in A[b_1 \ldots b_n]$ is a finite generating set.

For $b \in A[b_1 \ldots b_n]$ $\boxed{b c_i = \sum_{j=1} a_{ij} c_j}$ for some $a_{ij} \in A$.

Define matrix $X = (a_{ij})$; claim $\det(bI_r - X) = 0$.

Cayley–Hamilton th

integral relation.

An approach to integrality via symmetric polynomials

say b_1 P_1 $b_1^{n_1} + a_{11} b_1^{n_1 - 1} + \cdots = 0$

b_2 P_2 $b_2^{n_2} + a_{21} b_2^{n_2 - 1} + \cdots$ $a_{ij} \in A$

are integral over A

Imagine P_1 factors as $\prod_i (X - r_{1i})$

P_2 factors as $\prod_j (X - r_{2j})$

then $a_{11} = -\sum_i r_{1i}$ $a_{12} = \sum_{i_1 < i_2} r_{1 i_1} r_{1 i_2}$

$\vdots$

now $b_1 + b_2$ is a root of

poly $X^{n_1 + n_2} + c_1 X^{n_1 + n_2 - 1} + \cdots$ where ...

Integral closures

the c_i are integer symmetric polynomials in r_{1i} and r_{2j} separately.

e.g. $c_1 = -(\sum r_{1i} + \sum r_{2j})$

$$c_2 = \sum_{i_1 < i_2} r_{1i_1} r_{1i_2} + \sum_{j_1 < j_2} r_{2j_1} r_{2j_2} + \left(\sum_i r_{1i}\right)\left(\sum_j r_{2j}\right)$$

The integral closure of A in B is the ring of all $b \in B$ integral over A. (e.g. $A = \mathbb{Z}$, $B = K$ # field then get $\mathcal{O}_K$

Trace and norm in a field extension

Note: if A is UFD then A is integrally closed in Frac(A)
(rational root theorem!)

Let L/K be a finite extension of fields

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

mult by x

$\mathrm{Norm}_{L/K} : L \to K$

$\mathrm{Norm}(x) = \det(T_x : L \to L)$

if T_x has charpoly $x^n - a_1 x^{n-1} + \dots + (-1)^n a_n$

then $\mathrm{Trace}(x) = a_1$ $\quad$ $\mathrm{Norm}(x) = a_n$

$T_x + T_y = T_{x+y}$ $\quad$ $T_x \circ T_y = T_{xy}$

Trace and norm and eigenvalues

$\mathrm{Trace}_{L/K}(x+y) = \mathrm{Trace}_{L/K}(x) + \mathrm{Trace}_{L/K}(y)$

$\mathrm{Norm}_{L/K}(xy) = \mathrm{Norm}_{L/K}(x)\,\mathrm{Norm}_{L/K}(y)$

$\mathrm{Trace}_{L/K}(x) =$ sum of eigenvalues of T_x
in L

$\mathrm{Norm}_{L/K}(x) =$ product of...

Trace and norm and Galois theory

If L/K is separable and $\sigma : L \hookrightarrow \overline{K}$ varies over K-embeddings of L into a fixed $\overline{K}$,

There are $[L:K]$ of these.

then $\mathrm{Trace}_{L/K}(x) = \sum_\sigma \sigma(x)$

$\mathrm{Norm}_{L/K}(x) = \prod_\sigma \sigma(x)$

b/c the $\sigma(x)$ are the eigenvalues of T_x over $\overline{K}$.

Trace and norm and intermediate field extensions

$M/L/K$ finite extensions

then $\mathrm{Trace}_{M/K} = \mathrm{Trace}_{L/K} \circ \mathrm{Trace}_{M/L}$

$\mathrm{Norm}_{M/K} = \mathrm{Norm}_{L/K} \circ \mathrm{Norm}_{M/L}$