Let $K/\mathbb{Q}$ be a fin. ext. $[K:\mathbb{Q}] < \infty$

$\mathcal{O}_K := \{ a \in K \mid m_a(x) \in \mathbb{Z}[x] \}$.

Example: If $n \in \mathbb{Z}$ is squarefree, then

$$\mathcal{O}_{\mathbb{Q}(\sqrt{n})} = \begin{cases} \mathbb{Z}[\sqrt{n}] = \mathbb{Z} + \mathbb{Z}\sqrt{n} & \text{if } n \equiv 2 \text{ or } 3 \bmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right] = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{n}}{2} & \text{if } n \equiv 1 \bmod 4. \end{cases}$$

Big Theorem: If $[K:\mathbb{Q}] < \infty$

1) $\mathbb{Q} \cdot \mathcal{O}_K = K$.
2) $\mathcal{O}_K$ is a subring of K

$\Big\} \Rightarrow \mathrm{Frac}(\mathcal{O}_K) = K$

3) $\mathcal{O}_K$ is integrally closed.
4) $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $= [K:\mathbb{Q}]$.

hard part is to see it's finitely generated.

1 is elementary. 2-3 Follow from much more general statements.

4 special to this situation.

Proof of 1: Suppose $\alpha \in K$

$$m_\alpha(x) = x^n + \frac{a_{n-1}}{s}x^{n-1} + \cdots + \frac{a_0}{s}$$

$a_i \in \mathbb{Z}$, $s \in \mathbb{Z}$.

$\beta = s\alpha \longleftrightarrow \alpha = \frac{\beta}{s}$.

β is a root of $m_\alpha\left(\frac{y}{s}\right) = \frac{y^n}{s^n} + \frac{a_{n-1}}{s^n}y^{n-1} + \frac{a_{n-2}}{s^{n-1}} + \cdots + \frac{a_0}{s}$.

$\cdot s^n \downarrow$

$$m_\beta(y) = y^n + a_{n-1}y^{n-1} + \cdots + a_0 s^{n-1}.$$

has integer coeff.

so $\beta \in \mathcal{O}_K$.

Some definitions for integral elements. (Rings are always commutative w/ 1).

Def'n: $R \subseteq S$.

- We say $s \in S$ is integral over R if there is a monic polynomial $f(x) \in R[x]$ s.t. $f(s) = 0$.
- S is integral over R if every $s \in S$ is integral over R.
- R is integrally closed in S if only elements of S integral over R are in R.
  (Integral closure of R in S is R)
- Integral closure of R in S = everything in S integral over R.

For R a domain, we say R is integrally closed if it integrally closed in Frac R.

Example: $\mathbb{Z}$ is integrally closed. If K is a field, $K[x]$ is integrally closed.

In fact, any UFD is integrally closed.

Example: $\mathbb{Z}[\sqrt{5}] \subseteq \mathbb{Q}(\sqrt{5})$ is not integrally closed.

$\frac{1+\sqrt{5}}{2} \notin \mathbb{Z}[\sqrt{5}]$ but is a root of

$x^2 - 2x - 2$. ← coeff. are in $\mathbb{Z}$ so also in $\mathbb{Z}[\sqrt{5}]$.

Example: $R = \mathbb{C}[x,y]/y^2 - x^2(x-1) \subseteq$ Frac R.

$z = \frac{y}{x}$ $\quad z^2 - (x-1)$.

so z is a root of $t^2 - (x-1)$

Integral closure is $\mathbb{C}[x,z]/z^2-(x-1)$, coeff. in $\mathbb{C}[x] \subseteq R$,

$\operatorname{Frac} R = \mathbb{C}(x)\left(\pm\sqrt{x+1}\right) \simeq \mathbb{C}(x)\left(\pm\sqrt{x-1}\right)$.

$y=xz$ ↑

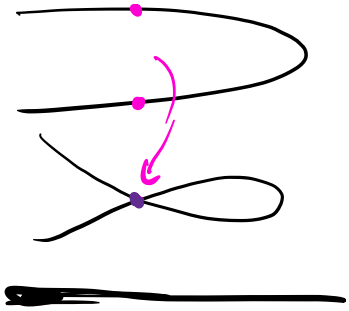
$\mathbb{C}[x,z]/(z^2-(x-1))$

∪

$\mathbb{C}[x,y]/(y^2-x^2(x-1))$

∪

$\mathbb{C}[x]$



Lemma: $R \subseteq S$. Then $s \in S$ is integral $\iff R[s]$ is finite as an R-module.

Proof: $R[s]$ is the image of

$$R[x] \to S$$
$$x \longmapsto s.$$

If s is integral, then $\exists\ f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$, $a_i \in R$ s.t. $f(s) = 0$.

This factors through

$$R[x]/(f(x)) \twoheadrightarrow R[s] \hookrightarrow S$$

$R[x]/(f(x))$ finite as an R-module.

$x^{n-1}, x^{n-2}, \dots, 1 \to s^{n-1}, s^{n-2}, \dots, 1.$

If $R[s]$ is finite, then there are generators $b_1, \dots, b_m$.

↑ each of these is an R-linear combination of powers of s.

only finitely many ⇒

$1, s, s^2, s^3, \ldots, s^N$ is a generating set.

So $s^{N+1} = a_N s^N + a_{N-1} s^{N-1} + \ldots + a_0 \cdot 1$.

for $a_i \in R$ so that gives.

$$\underbrace{s^{N+1} - a_N s^N + a_{N-1} s^{N-1} + \ldots + a_0 = 0}_{\text{monic w/coeff. in } R \text{ satisfied by } s.}$$

So s is integral. ∎

Proposition: $R = \mathbb{Z}$, $S = K$ integral closure is $\mathcal{O}_K$, $[K:\mathbb{Q}] < \infty$ so gives part (2) of main theorem.

1. $R \subseteq S$, integral closure of R in S is a subring of S.
2. $R \subseteq S \subseteq T$, if S is integral over R and $t \in T$ is integral over S, then t is integral over R.

$R = \mathbb{Z}$, $S = \mathcal{O}_K$, $T = K = \mathrm{Frac}(\mathcal{O}_K)$. gives part (3) of $[K:\mathbb{Q}] < \infty$ main theorem.

Proof: Only going to prove (1), proof of (2) same idea.

Step 1: Suppose R is Noetherian

$\tilde{R}$ integral closure of R in S.

$a, b \in \tilde{R}$. $R[a,b]$. ← This a finite R-module generated by $a^k b^l$ $k,l \in \mathbb{N}$

$R[a+b]$ $R[ab]$.

R Noetherian $\Rightarrow$ sub-modules also finite.

So Lemma gives that $a+b$, ab are integral.

Step 2: R not necessarily Noetherian.

$a, b \in \overline{R}$ $\quad f, g \in R[x]$ monic

s.t. $f(a) = 0$ and $g(b) = 0$.

$f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$

$g = x^m + b_{m-1}x^{m-1} + \cdots + b_0$.

$A = \mathbb{Z}[a_0, a_1, \cdots, a_{n-1}, b_0, b_1, \cdots, b_{m-1}]$

$A \subseteq R \subseteq S$, a, b are integral over A.

but A is Noetherian.

So $a+b$, ab are integral over A

$\Rightarrow$ integral over R since $A \subseteq R$.

How to see it $[K:\mathbb{Q}] < \infty$, $\mathcal{O}_K$ is a finite $\mathbb{Z}$-module

This enough for part 4.

Torsion free — structure theorem for modules over a PID says it's free.

Surprisingly subtle!

Suffices to put $\mathcal{O}_K$ inside some finite $\mathbb{Z}$-module inside of K (because $\mathbb{Z}$ is Noetherian).

Philosophy: • In graduate algebra, saw the power of thinking of L/K a field extension as a vector space.

• In graduate NT we'll use that

a (separable) field extension L/K is naturally equipped w/ a non-degenerate bilinear form.

$K/\mathbb{Q}$ a finite extension $\alpha \in K$

$$\alpha \cdot : K \to K$$

is a $\mathbb{Q}$-linear transformation

$Tr_{K/\mathbb{Q}}(\alpha)$ = trace of linear transformation $Tr_{K/\mathbb{Q}} : K \to \mathbb{Q}$.

Example: $Tr_{K/\mathbb{Q}}(\alpha+\beta) = Tr_{K/\mathbb{Q}}(\alpha) + Tr_{K/\mathbb{Q}}(\beta)$

$Tr_{K/\mathbb{Q}}(c\alpha) = c\, Tr_{K/\mathbb{Q}}(\alpha)$ if $c \in \mathbb{Q}$.

(Just write down a basis!)

$$Tr_{K/\mathbb{Q}}(1) = Tr(Id : K \to K) = [K:\mathbb{Q}].$$

ξ symmetric

I get a $\mathbb{Q}$-bilinear form on K with values in $\mathbb{Q}$.

$$(\alpha, \beta) := Tr_{K/\mathbb{Q}}(\alpha\beta).$$

Non-degenerate $\Longleftrightarrow$ ξ

$$\left(\alpha, \frac{\alpha^{-1}}{[K:\mathbb{Q}]}\right) = Tr_{K/\mathbb{Q}}\left(\frac{1}{[K:\mathbb{Q}]}\right)$$

$$= \frac{1}{[K:\mathbb{Q}]} Tr_{K/\mathbb{Q}}(1)$$

$$= \frac{[K:\mathbb{Q}]}{[K:\mathbb{Q}]} = 1.$$

$$K \longrightarrow K^* = Hom_{\mathbb{Q}}(K, \mathbb{Q})$$

$$\alpha \longmapsto (\alpha, -) : \beta \to (\alpha, \beta).$$

is injective thus an isomorphism

(because same dimension)

Take a basis $e_1, \dots, e_n$ for K as a $\mathbb{Q}$-vector space.

by part (1) of main theorem, can assume $e_i \in \mathcal{O}_K$.

Let f_i be the dual basis.

$f_i \in K$ s.t.

$$(f_i, e_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

Claim: $\mathcal{O}_K \subseteq \mathbb{Z} f_1 + \mathbb{Z} f_2 + \dots + \mathbb{Z} f_n$.

For $\alpha \in K$, $\alpha = \sum (e_i, \alpha) f_i$.

$= \sum \mathrm{Tr}(e_i \alpha) f_i$.

If $\alpha \in \mathcal{O}_K$, $e_i \alpha \in \mathcal{O}_K$ because $e_i \in \mathcal{O}_K$ and $\mathcal{O}_K$ is a ring.

$\Rightarrow \mathrm{Tr}(e_i \alpha) \in \mathbb{Z}$. which is what we needed.

Finishes part (4) of the main theorem

V is a f.d. $\mathbb{Q}$-vector space with a non-degenerate bilinear pairing $(,)$.

$M \subseteq V$ is a $\mathbb{Z}$-lattice = free (finite rank) $\mathbb{Z}$-module that generates V

$M^* = \{ f \in V \text{ s.t. } (f, m) \in \mathbb{Z} \ \forall \ m \in M \}$.

Interesting to think about $M \subseteq M^*$

and $|M^*/M|$ a positive integer.

Apply this to $\mathcal{O}_K \subseteq K$

$\subseteq$ lattice in K.

$\mathcal{O}_K \subseteq (\mathcal{O}_K)^*$ ...

$$|\mathcal{O}_K^* / \mathcal{O}_K| = |\operatorname{disc}(\mathcal{O}_K/\mathbb{Z})| \cdot |\operatorname{disc}(K/\mathbb{Q})|.$$

$\mathcal{O}_K$ is a free $\mathbb{Z}$-module $n = [K:\mathbb{Q}]$.

choose a basis $e_1, \dots, e_n$.

$f_1, \dots, f_n$ dual basis.

$$\mathcal{O}_K^* = \mathbb{Z} f_1 + \mathbb{Z} f_2 + \dots + \mathbb{Z} f_n.$$

$|\mathcal{O}_K^*/\mathcal{O}_K| = |$ det of change of basis matrix from f_i to e_i $|$.

// disc.

$\det(\operatorname{Tr}(e_i e_j))$. For any basis.