Definition: A <u>number field</u> F is a field satisfying

$$[F:\mathbb{Q}] = \dim_{\mathbb{Q}} F < \infty.$$

Denote by $\mathbb{Z}[x]$ the one variable polynomials with coefficients in $\mathbb{Z}$.

Definition: A polynomial $f(x) \in \mathbb{Z}[x]$ is <u>monic</u> if

$$f(x) = x^n + a_1 x^{n-1} + \cdots a_{n-1} x + a_n. \quad a_1, \cdots a_n \in \mathbb{Z}.$$

Definition: Let F be a number field. $\alpha \in F$ is an <u>algebraic integer</u> if we can find a monic $f(x) \in \mathbb{Z}[x]$ s.t. $f(\alpha) = 0$.

Denote by $\mathcal{O}_F$ the set of all algebraic integers, called <u>ring of integers</u>.

Theorem: $\mathcal{O}_F$ is an integral domain.

Remark: $\mathcal{O}_F \subseteq F$. Therefore, it suffices to show $\mathcal{O}_F$ is a ring.

Proposition: TFAE:

(1) $\alpha \in F$ is an algebraic integer.

(2) There exists a finitely generated $\mathbb{Z}$-module $M \subseteq F$ s.t.

$\alpha M \subseteq M$.

Proof: (1) $\Rightarrow$ (2) α is an algebraic integer. We can find

$$f(x) = x^n + a_1 x^{n-1} + \cdots a_{n-1} x + a_0 \quad \text{s.t. } f(\alpha) = 0.$$

We consider finitely generated $\mathbb{Z}$-module

$$\mathbb{Z}[\alpha] = \text{span}_{\mathbb{Z}} \{1, \alpha, \alpha^2, \cdots \alpha^{n-1}\}$$

We can show $\alpha \cdot \mathbb{Z}[\alpha] \subseteq \mathbb{Z}[\alpha]$

It suffices to show: $\alpha \cdot \{1, \alpha, \alpha^2, \cdots \alpha^{n-1}\} \subseteq \mathbb{Z}[\alpha]$.

The only nontrivial one is $\alpha \cdot \alpha^{n-1} = \alpha^n = -(a_1 \alpha^{n-1} + \cdots a_0)$
$\in \mathbb{Z}[\alpha]$

(2) $\Rightarrow$ (1) M is finitely generated $\mathbb{Z}$-module. We can find the generators

$x_1, \cdots x_m$

$\alpha \in M \Rightarrow \quad \alpha(x_1, \cdots x_m) = (x_1, \cdots x_m) A$.

with $A \in M_{m \times m}(\mathbb{Z})$.

Take $f(x) = \det(x I_m - A)$, the characteristic polynomial.

$f(x) \in \mathbb{Z}[x]$ and monic (by Laplacian expansion)

Then $f(A) = 0$ ← zero matrix

On the other hand,

$$f(\alpha)(x_1, \cdots x_m) = (x_1, \cdots x_m) f(A) = (x_1, \cdots x_m) \cdot 0$$
$$= (0, \cdots 0)$$

This will force $f(\alpha) = 0$. ∎

Proof of Theorem: It suffices to show for $\alpha, \beta \in \mathcal{O}_F$, then $\alpha + \beta \in \mathcal{O}_F$ and $\alpha\beta \in \mathcal{O}_F$.

$\alpha \in \mathcal{O}_F$, can find a finitely generated $\mathbb{Z}$-module $M \leq F$ s.t. $\alpha M \subseteq M$.

$\beta \in \mathcal{O}_F$, can find a finitely generated $\mathbb{Z}$-module $N \leq F$ s.t. $\beta N \subseteq N$.

Set $MN = \{ \sum m_i n_i : \text{finite sums } m_i \in M, n_i \in N \}$

Check: MN is a finitely generated $\mathbb{Z}$-module $(\subseteq F)$

Then $\alpha\beta MN \subseteq (\alpha M)(\beta N) \subseteq MN$

$$(\alpha + \beta) MN \subseteq (\alpha M)N + M(\beta N) \subseteq MN$$

This implies: $\alpha + \beta$ and $\alpha\beta$ are integral over $\mathbb{Z}$ ∎.

Denote by $\mathrm{Frac}(R)$ the field of fraction for an integral domain R.

Proposition: Let F be a number field. Then

$$\mathrm{Frac}(\mathcal{O}_F) = F.$$

Proof: $\mathcal{O}_F \subseteq F \Rightarrow \mathrm{Frac}(\mathcal{O}_F) \subseteq F$. It suffices to show: $F \subseteq \mathrm{Frac}(\mathcal{O}_F)$.

Take $\alpha \in F$. $[F:\mathbb{Q}] < \infty$. Then we can $g(x) \in \mathbb{Q}[x]$

such that $g(\alpha) = 0$

We write: $g(x) = x^n + a_1 x^{n-1} + \cdots a_{n-1} x + a_n$

with $a_1, \cdots, a_n \in \mathbb{Q}$. Write $a_i = \frac{r_i}{s_i}$ $r_i, s_i \in \mathbb{Z}$
$(r_i, s_i) = 1$

Set $d = \mathrm{l.c.m}[s_0, s_1, \cdots s_n] \in \mathbb{Z}$.

$g(\alpha) = 0 \Rightarrow \alpha^n + a_1 \alpha^{n-1} + \cdots a_{n-1}\alpha + a_n = 0$

Multiply by d^n:

$$(d\alpha)^n + (a_1 d) \cdot (d\alpha)^{n-1} + \cdots a_{n-1} d^{n-1} (d\alpha) + a_n d^n = 0.$$

$a_1 d,\ a_2 d^2, \cdots a_{n-1} d^{n-1},\ a_n d^n \in \mathbb{Z}$.

$\Rightarrow d\alpha \in \mathcal{O}_F \Rightarrow \alpha \in \mathrm{Frac}(\mathcal{O}_F)$. ∎

Let R be an integral domain and $\mathrm{Frac}(R)$ its field of fractions

Take $\alpha \in \mathrm{Frac}(R)$,

Definition: α is integral over R if we can find monic $f(x) \in R[x]$ such that $f(\alpha) = 0$.

Denote by $\overline{R}$ the set of all integral elements over R is $\mathrm{Frac}(R)$.

Definition: An integral domain is integrally closed if $R = \overline{R}$, that is,

$\alpha \in \mathrm{Frac}(R)$ and α integral over $R \Rightarrow \alpha \in R$.

Proposition: Let R be a UFD. Then R is integrally closed.

Proof: Take $\alpha \in \mathrm{Frac}(R)$ and α is integral over R.

Then we have:

$$\alpha^n + a_1 \alpha^{n-1} + \cdots a_{n-1}\alpha + a_n = 0 \qquad a_1, \cdots a_n \in R.$$

$\alpha \in \mathrm{Frac}(R) \Rightarrow \alpha = \frac{a}{b}$ for $a, b \in R$.

$$\Rightarrow \left(\frac{a}{b}\right)^{\alpha} + a_1 \left(\frac{a}{b}\right)^{n-1} + \cdots a_{n-1}\left(\frac{a}{b}\right) + a_n = 0$$

$$\Rightarrow a^{\alpha} + a_1 a^{n-1} b + \cdots a_{n-1} a b^{n-1} + a_n b^n = 0.$$

R is a UFD, we can assume that for every prime element $p \mid b$, $p \nmid a$.

Suppose that such a prime exists, then

$$p \mid a_1 a^{n-1} b, \cdots a_n b^n \quad \text{and} \quad p \mid 0$$

This will force $p \mid a^\alpha$. A contradiction.

Therefore, b is a unit in R and $\alpha = \frac{a}{b} \in R$.

Corollary: $\mathbb{Z}$ is integrally closed. In other words,

$$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}.$$

Proposition: Let F be a number field and $[F:\mathbb{Q}]=2$.

Then we can find a squarefree integer d such that

$$F = \mathbb{Q}(\sqrt{d})$$

Proof: Take $\alpha \in F - \mathbb{Q}$. $[F:\mathbb{Q}]=2$

and $[F:\mathbb{Q}] = [F:\mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha):\mathbb{Q}] \Rightarrow F = \mathbb{Q}(\alpha)$.

On the other hand, $[F:\mathbb{Q}]=2$, we can find

$$f(x) = x^2 + ax + b \quad a,b \in \mathbb{Q} \quad \text{s.t. } f(\alpha)=0.$$

Then $\alpha = \dfrac{-b \pm \sqrt{b^2-4ac}}{2a}$ Set $D = b^2 - 4ac \in \mathbb{Q}$.

Then $F = \mathbb{Q}(\sqrt{D})$.

Then $F = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D'})$ with $D' \in \mathbb{Z}$.

This is because, if $D = \frac{m}{n}$, then

$$\mathbb{Q}(\sqrt{D}) = \mathbb{Q}\left(\sqrt{\tfrac{m}{n}}\right) = \mathbb{Q}\left(\tfrac{1}{n}\cdot\sqrt{mn}\right) = \mathbb{Q}(\underbrace{\sqrt{mn}}_{\sqrt{D'}}).$$

Next, for each integer D', we can write:

$$D' = D_0^2 \cdot d \quad \text{with } d \text{ squarefree.}$$

$$\Rightarrow \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D'}) = \mathbb{Q}(D_0\sqrt{d}) = \mathbb{Q}(\sqrt{d}). \qquad \square$$

Observation: if d is squarefree, then $d \equiv 1,2,3 \pmod 4$.

Proposition: For $F = \mathbb{Q}(\sqrt{d})$,

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

Notice, in this case, $\mathbb{Z}[\alpha] = \mathrm{span}_{\mathbb{Z}}\{1,\alpha\}$
$= \{a + b\alpha : a, b \in \mathbb{Z}\}$

Definition: For $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, we define:

$$\bar{\alpha} = a - b\sqrt{d}$$

$$\mathrm{Tr}(\alpha) = \alpha + \bar{\alpha} \quad \text{and} \quad N(\alpha) = \alpha\bar{\alpha}$$

Check: (1) $\mathrm{Tr}(\alpha)$, $N(\alpha) \in \mathbb{Q}$

Indeed, $Tr(\alpha) = (a+b\sqrt{d}) + (a-b\sqrt{d}) = 2a. \in \mathbb{Q}.$

$N(\alpha) = (a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - db^2 \in \mathbb{Q}.$

(2) If $\alpha \in \mathcal{O}_F$, so will $\bar{\alpha}$.

Observation: $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$

Proof of Prop: Let $\alpha = a+b\sqrt{d} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

Then $\bar{\alpha}$ is an algebraic integer

$\Rightarrow Tr(\alpha) \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ and $N(\alpha) \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$

On the other hand, $Tr(\alpha), N(\alpha) \in \mathbb{Q}$

Therefore, $Tr(\alpha), N(\alpha) \in \mathbb{Z}$ since $\mathbb{Z}$ is integrally closed.

This implies: $Tr(\alpha) = 2a \in \mathbb{Z}$ $N(\alpha) = a^2 - db^2 \in \mathbb{Z}$.

$2a \in \mathbb{Z} \Rightarrow a$ is an integer or a half integer.

Case I: (a is an integer) $a^2 - db^2 \in \mathbb{Z} \Rightarrow db^2 \in \mathbb{Z}$.

This will force $b \in \mathbb{Z}$ since d is squarefree.

(If $b = \frac{m}{n}$ with $n > 1$, then $p \mid n$ for some prime.

$db^2 = \frac{dm^2}{n^2} \in \mathbb{Z} \Rightarrow p^2 \mid d$. A contradiction!)

Case II: $\left(a = \frac{n}{2}\text{, a half integer}\right)$ We can assume that n is odd.

Then $a^2 - db^2 = \frac{n^2}{4} - db^2 \in \mathbb{Z}$.

n odd $\Rightarrow n^2 \equiv 1 \pmod 4) \Rightarrow \frac{1}{4} - db^2 \in \mathbb{Z}$.

Write $b = \frac{m}{m'}$.

① Similar to Case I: if $p > 2$, then $p \nmid m'$

②. $m' = \pm 2$, otherwise, b is an integer.

and we never have $\frac{1}{4} - db^2 \in \mathbb{Z}$.

This also forces m_1 to be an odd integer.

Therefore, $b = \frac{m}{2}$ with m odd.

Case I + Case II implies: $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ $\alpha = \frac{n}{2} + \frac{m}{2}\sqrt{d}$

with m, n and $m \equiv n \pmod 2$.

Then $\alpha = \frac{n-m}{2} + m \cdot \frac{1+\sqrt{d}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$

We have: $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \subseteq \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$

Next, $\alpha = a + b\sqrt{d} \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] - \mathbb{Z}[\sqrt{d}]$

Then $\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d}$ with m, n being odd.

$$= \frac{1}{2} + \frac{1}{2}\sqrt{d} + \left(\frac{n-1}{2} + \frac{m-1}{2}\sqrt{d}\right)$$

m, n odd $\Rightarrow \frac{n-1}{2} + \frac{m-1}{2}\sqrt{d} \in \mathbb{Z}[\sqrt{d}] \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$

Therefore: $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ iff $\frac{1}{2} + \frac{1}{2}\sqrt{d} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

Since we are choosing α randomly,

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } \frac{1+\sqrt{d}}{2} \notin \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } \frac{1+\sqrt{d}}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \end{cases}$$

When $d \equiv 1 \pmod 4$: can show:

$f(x) = x^2 - x + \frac{1-d}{4} \in \mathbb{Z}[x]$, monic and

$f\left(\frac{1}{2} + \frac{1}{2}\sqrt{d}\right) = 0$

This shows: $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$

When $d \equiv 2, 3 \pmod 4$:

Recall $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \Rightarrow N(\alpha) \in \mathbb{Z}$

$N\left(\frac{1+\sqrt{d}}{2}\right) = \frac{1-d}{4} \notin \mathbb{Z} \Rightarrow \frac{1+\sqrt{d}}{2} \notin \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$

This shows: $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$.