Definition: An integral domain R is a <u>Dedekind domain</u> if

(1) R is a Noetherian ring

(2) R is an integrally closed

(3) Every nonzero prime ideal is maximal

Question: why do we study Dedekind domain?

<u>Ans:</u> We know $\mathbb{Z}$: ED $\Rightarrow$ PID $\Rightarrow$ UFD

However, for a ring of integer $\mathcal{O}_F$, it is not necessarily a UFD!

Can show: ① $\mathcal{O}_F$ are always Dedekind domains

② In a Dedekind domain, the elements are not necessarily factored, but the ideals will always factor.

Let F be a number field. Then $\dim_{\mathbb{Q}} F = [F:\mathbb{Q}]$.

Let $x \in F$, and we define a linear operator

$$T_x : F \to F$$
$$y \mapsto xy.$$

Set: $\mathrm{Tr}_{F/\mathbb{Q}}(x) = \mathrm{tr}(T_x)$ $\qquad N_{F/\mathbb{Q}}(x) = \det(T_x)$

Notice that we are viewing F as a vector space $/\mathbb{Q}$.

T_x corresponds to $n\times n$ matrices $/\mathbb{Q}$ $\quad (n=[F:\mathbb{Q}])$

$\Rightarrow$ $Tr_{F/\mathbb{Q}}(x)$, $N_{F/\mathbb{Q}}(x) \in \mathbb{Q}$, that is,

$$Tr_{F/\mathbb{Q}},\ N_{F/\mathbb{Q}} : F \longrightarrow \mathbb{Q}.$$

Moreover: $Tr_{F/\mathbb{Q}}, N_{F/\mathbb{Q}} : \mathcal{O}_F \to \mathbb{Z}$.

Definition: Let V be a vector space over some field F.

A <u>pairing</u> is a function: $(\ ,\ ) : V\times V \to F$.

A <u>bilinear form</u> B is a pairing $B: V\times V \to F$ s.t.

(1) $B(av_1+bv_2, v_3) = aB(v_1,v_3) + bB(v_2,v_3)$

(2) $B(v_1, av_2+bv_3) = aB(v_1,v_2) + bB(v_1,v_3)$.

for $a,b\in F$ and $v_1,v_2,v_3\in V$.

Given a bilinear form $B: V\times V\to F$. and fix $v\in V$.

We obtain a linear function $B_v : V \to F$

Hom (V,F) $\quad w \mapsto B(v,w)$

Definition: A bilinear form $B: V\times V \to F$ is <u>nondegenerate</u>

if $B_v = 0 \Rightarrow v=0$.

Exercise: Let $B: V \times V \to F$ be a nondegenerate bilinear form

Then for any basis $\{v_1, \cdots v_n\}$ of V, we can find another basis $\{v_1^*, \cdots v_n^*\}$ s.t.

$$B(v_i, v_j^*) = \delta_{ij} = \begin{cases} 1 & \text{if } i=j \\ 0 & \text{otherwise.} \end{cases}$$

Fact: Let F be a number field. Then:

$$(,): F \times F \to \mathbb{Q}$$
$$(x, y) \mapsto \mathrm{Tr}_{F/\mathbb{Q}}(xy)$$

is a nondegenerate bilinear form.

Theorem: Let F be a number field. Then $\mathcal{O}_F$ is a Dedekind domain.

Recall there are 3 conditions for a Dedekind domain.

We will prove them in the following propositions.

Proposition: Let F be a number field. Then $\mathcal{O}_F$ is a Noetherian ring.

Proof: (1) We can find a finitely generated $\mathbb{Z}$-module M s.t. $\mathcal{O}_F$ is a $\mathbb{Z}$-submodule of M

(2) Use (1) to prove the proposition.

(1) F is a number field. $F = \text{span}_{\mathbb{Q}}\{\alpha_1, \cdots \alpha_n\}$

with $n = [F : \mathbb{Q}]$.

Recall, when showing $\text{Frac}(\mathcal{O}_F) = F$, we can find $d \in \mathbb{Z}$ s.t.

$$d\alpha_i \in \mathcal{O}_F$$

Notice $F = \text{span}_{\mathbb{Q}}\{d\alpha_1, \cdots d\alpha_n\}$

Therefore, we can find $\beta_1, \cdots \beta_n \in \mathcal{O}_F$

s.t. $\beta_1, \cdots \beta_n$ is a basis for $F/\mathbb{Q}$.

By the fact, we can find $\beta_1^* \cdots \beta_n^*$, a basis of F,

$$\text{Tr}(\beta_i \beta_j^*) = \delta_{ij}$$

Claim: $\mathcal{O}_F \subseteq M = \text{span}_{\mathbb{Z}}(\beta_1^*, \cdots \beta_n^*)$

Let $\beta \in \mathcal{O}_F$, since $\beta_1^*, \cdots \beta_n^*$ is a basis,

$$\beta = \sum_{j=1}^{n} a_j \beta_j^* \qquad a_j \in \mathbb{Q}$$

It suffices to show: $a_j \in \mathbb{Z}$.

$$\text{Tr}_{F/\mathbb{Q}}(\beta_i \beta) = \text{Tr}_{F/\mathbb{Q}}\left(\beta_i \sum_{j=1}^{n} a_j \beta_j^*\right)$$

$$= \sum_{j=1}^{n} a_j \text{Tr}_{F/\mathbb{Q}}(\beta_i \beta_j^*) = a_i$$

$\beta, \beta_i \in \mathcal{O}_F \Rightarrow Tr_{F/\mathbb{Q}}(\beta_i \beta) \in \mathbb{Z} \Rightarrow a_i \in \mathbb{Z}$.

(2) Let $\mathfrak{a} \subseteq \mathcal{O}_F$ be an ideal. $\mathcal{O}_F \subseteq M$ as a $\mathbb{Z}$-submodule

Then we can also view $\mathfrak{a}$ as a $\mathbb{Z}$-submodule of M.

M is finitely generated + $\mathbb{Z}$ P.I.D $\Rightarrow$ M is a Neotherian module

$\Rightarrow \mathfrak{a}$ is a finitely generated $\mathbb{Z}$-module

$\Rightarrow \mathfrak{a}$ is a finitely generated ideal. $\square$

Proposition: $\mathcal{O}_F$ is integrally closed.

Proof: Let $\alpha \in Frac(\mathcal{O}_F) = F$. Suppose that we can find monic $f(x) \in \mathcal{O}_F[x]$ s.t. $f(\alpha)=0$

Need to show: $\alpha \in \mathcal{O}_F$.

Write $f(x) = x^n + a_1 x^{n-1} + \cdots a_{n-1}x + a_n \quad a_i \in \mathcal{O}_F$.

$\Rightarrow span_{\mathbb{Z}}(a_1, \cdots a_n)$ is a finitely generated $\mathbb{Z}$-module.

$f(\alpha)=0 \Rightarrow span_{\mathbb{Z}}(a_1, \cdots a_n, \alpha)$ is finitely generated $span_{\mathbb{Z}}(a_1, \cdots a_n)$-module.

$$\begin{array}{lll} \mathbb{Z}[\alpha] \subseteq \mathrm{span}_{\mathbb{Z}}(a_1, \cdots a_n, \alpha) & \left.\right\} \text{finitely generated} & \\ \qquad | & & \Rightarrow \text{finitely generated.} \\ \mathrm{span}_{\mathbb{Z}}(a_1, \cdots a_n) & \left.\right\} \text{finitely generated.} & \\ \qquad | & & \\ \mathbb{Z} & & \end{array}$$

Therefore, $\mathbb{Z}[\alpha]$ is finitely generated as $\mathbb{Z}$-module and α is an algebraic integer $\Rightarrow \alpha \in \mathcal{O}_F$. $\square$

Proposition: Every $\overset{\text{nonzero}}{\vee}$ prime ideal in $\mathcal{O}_F$ is a max'l ideal.

Proof: Let $\mathfrak{P} \subseteq \mathcal{O}_F$ be a prime ideal.

Set $I = \mathfrak{P} \cap \mathbb{Z}$. This is an ideal of $\mathbb{Z}$.

Next, take $x, y \in \mathbb{Z}$, $xy \in I$, $\Rightarrow xy \in \mathfrak{P}$

$\mathfrak{P}$ a prime ideal, $\Rightarrow$ either x or $y \in \mathfrak{P}$ $\underbrace{}_{\text{in } \mathbb{Z}}$

$\Rightarrow$ either x or y in I $\Rightarrow$ I is a prime ideal

Therefore $\mathfrak{P} \cap \mathbb{Z} = (p)$ for some prime number.

Note: $\mathfrak{P} \cap \mathbb{Z}$ is a nonzero ideal in $\mathbb{Z}$: take $y \in \mathfrak{P} \subsetneq \mathcal{O}_F$

can find $y^n + a_1 y^{n-1} + \cdots a_n = 0$ with $a_i \in \mathbb{Z}$ $a_n \neq 0$.

$y \in \mathfrak{P} \Rightarrow a_n \in \mathfrak{P} \cap \mathbb{Z} \Rightarrow \mathfrak{P} \cap \mathbb{Z} \neq \{0\}$

This shows: for $n \in \mathbb{Z} \subseteq \mathcal{O}_F$, the image of n in $\mathcal{O}_F / \mathfrak{P}$ is identified to $\mathbb{Z}/(p)$.

Let $\alpha \in \mathcal{O}_F$ and $\bar{\alpha} \in \mathcal{O}_F/\mathfrak{p}$

$\alpha \in \mathcal{O}_F \Rightarrow \alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots a_n = 0 \quad a_i \in \mathbb{Z}.$

mod $\mathfrak{p} \Rightarrow \bar{\alpha}^n + \bar{a}_1\bar{\alpha}^{n-1} + \bar{a}_2\bar{\alpha}^{n-2} + \cdots \bar{a}_n = 0 \quad \bar{a}_i \in \mathbb{Z}/(p)$

$\Longrightarrow$ $\bar{\alpha}$ is an algebraic number in $\mathbb{Z}/(p)$

This means, for any $\bar{\alpha} \in \mathcal{O}_F/\mathfrak{p}$, $\bar{\alpha}$ is algebraic over a field $\mathbb{Z}/(p) \Rightarrow \mathcal{O}_F/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ is maximal $\square$

Exercise: Let F be a field, R an integral domain and $F \subseteq R$. Suppose that for any $\alpha \in R$, α is algebraic over F, that is, can find $f(x) \in F[x]$ st. $f(\alpha) = 0$

Then R is a field. $\square$