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

Then for any basis $\{v_1, \dots v_n\}$ of $V$, we can find another basis $\{v_1^*, \dots v_n^*\}$ 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:

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

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. $F = \text{span}_{\mathbb{Q}}\{\alpha_1, \dots \alpha_n\}$

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

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

s.t. $\beta_1, \dots \beta_n$ 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: $\mathcal{O}_F \subseteq M = \text{span}_{\mathbb{Z}}(\beta_1^*, \dots \beta_n^*)$

Let $\beta \in \mathcal{O}_F$, since $\beta_1^*, \dots \beta_n^*$ 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. □

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

Proof: Let $\alpha \in \mathrm{Frac}(\mathcal{O}_F) = F$. 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 $f(x) = x^n + a_1 x^{n-1} + \cdots a_{n-1} x + a_n \quad a_i \in \mathcal{O}_F$.

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

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

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

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

Proposition: Every nonzero 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 $y \in \mathfrak{p}$ 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 $y \in \mathfrak{p} \subseteq \mathcal{O}_F$

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

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

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

$\Rightarrow$ $\bar{\alpha}$ 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. $\square$

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

Then $R$ is a field. $\square$

Proof: It suffices to show: for any $0 \neq \alpha \in A$, $\alpha^{-1} \in A$.

Then $A \supseteq F[\alpha] \underset{\substack{\uparrow \\ \alpha \text{ is algebraic over } F.}}{=} F(\alpha)$

Therefore $\alpha^{-1} \in A$. $\square$

Let $R$ be a ring. Let $\mathfrak{a}_1, \mathfrak{a}_2$ be two ideals of $R$.

Then we define:

$$\mathfrak{a}_1 \cdot \mathfrak{a}_2 := \left\{ \sum a_i b_i : a_i \in \mathfrak{a}_1, b_i \in \mathfrak{a}_2 \right\}$$

This is an ideal of $R$.

Check: (1) $\mathfrak{a}_1 \cdot \mathfrak{a}_2 = \mathfrak{a}_2 \cdot \mathfrak{a}_1$

(2) $\mathfrak{a}_1 \cdot (\mathfrak{a}_2 \cdot \mathfrak{a}_3) = (\mathfrak{a}_1 \cdot \mathfrak{a}_2) \cdot \mathfrak{a}_3$.

(3) $\mathfrak{a} \cdot R = R \cdot \mathfrak{a} = \mathfrak{a}$.

Theorem: Let $R$ be a Dedekind domain. Then for any ideal $\mathfrak{a} \subseteq R$. $\mathfrak{a}$ can be written as a product of prime ideals, that is,

$$\mathfrak{a} = \mathfrak{P}_1 \mathfrak{P}_2 \cdots \mathfrak{P}_n \qquad \mathfrak{P}_i \text{ prime ideals.}$$

This decomposition is unique up to permutation.

Remark: This will imply:

$$\mathfrak{a} = \mathfrak{P}_1^{r_1} \cdots \mathfrak{P}_s^{r_s} \qquad \mathfrak{P}_i \text{ distinct prime ideal}$$

$\mathfrak{P}_i$ and $r_i$ are uniquely determined.

Definition: A <u>fractional ideal</u> of $F$ is a finitely generated nonzero $\mathcal{O}_F$-module.

Denote by $I(F)$ the set of all fractional ideals.

Example: For $0 \neq a \in F$, we can define a fractional ideal:

$$(a) := \{ ra : r \in \mathcal{O}_F \}$$

Such fractional ideals will be called fractional principal ideals.

Denote by $P(F)$ the set of fractional principal ideals

Then for $M, N \in I(F)$, we can also define

$$M \cdot N := \{ \sum m_i \cdot n_i : m_i \in M, n_i \in N \} \in I(F)$$

Lemma: Let $M \in I(F)$, a fractional ideal. Then we can find $d \in \mathcal{O}_F$ s.t. $dM$ is an ideal of $\mathcal{O}_F$.

Proof: $M \in I(F)$. $\Rightarrow$ $M$ is finitely generated by $x_1, \dots x_n$ with $x_i \in F$.

Notice that $F = \mathrm{Frac}(\mathcal{O}_F)$, we can find $d \in \mathcal{O}_F$ s.t.

$$d x_i \in \mathcal{O}_F.$$

Therefore $dM \subseteq \mathcal{O}_F$

$M$ is a $\mathcal{O}_F$-module $\Rightarrow$ $dM$ is an ideal of $\mathcal{O}_F$.

Let $\mathfrak{p}$ be a prime ideal. We define:

$$\mathfrak{p}^{-1} = \{ x \in F : x\mathfrak{p} \subseteq \mathcal{O}_F \} \in I(F).$$

Lemma: $\mathfrak{p} \subsetneq \mathfrak{p} \cdot \mathfrak{p}^{-1} \subseteq \mathcal{O}_F$. (This implies: $\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathcal{O}_F$)

Proof: ① (Show $\mathcal{O}_F \subsetneq \mathfrak{p}^{-1}$)

We have $\mathcal{O}_F \subseteq \mathfrak{p}^{-1}$ as $\mathcal{O}_F \cdot \mathfrak{p} \subseteq \mathfrak{p} \subseteq \mathcal{O}_F$.

Take $a \in \mathfrak{p}$. Then $\mathfrak{p} \supseteq (a) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$.

Claim: by arranging $\mathfrak{p}_1, \cdots \mathfrak{p}_r$, we can assume that

$\mathfrak{p}_1 \subseteq \mathfrak{p}$. $\Rightarrow$ $\mathfrak{p}_1 = \mathfrak{p}$ since $\mathcal{O}_F$ is a Dedekind domain.

(Otherwise, we can find $a_i \in \mathfrak{p}_i - \mathfrak{p}$.

Then $a_1 \cdots a_r \in \mathfrak{p}$ A contradiction)

$$(a) = \mathfrak{p} \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq \mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

Moreover, by the unique factorization,

$$(a) \subsetneq \mathfrak{p}_2 \cdots \mathfrak{p}_r$$

Take $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r - (a)$. $\Rightarrow$ $b \notin a \cdot \mathcal{O}_F$.

that is: $a^{-1}b \notin \mathcal{O}_F$.

However, $a^{-1}b\,\mathfrak{p} \subseteq a^{-1}\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq a^{-1}(a) \subseteq \mathcal{O}_F$.

$\Rightarrow a^{-1}b \in \mathfrak{p}^{-1}$

② Suppose that $\mathfrak{p} = \mathfrak{p}^{-1} \cdot \mathfrak{p}$.

Take $x \in \mathfrak{p}^{-1}$, $\mathfrak{p}$ is finitely generated by $x_1, \cdots x_n$

Then $$x(x_1, \cdots x_n) = (x_1, \cdots x_n) \cdot M$$

with $M$ being a $n \times n$ matrices with coefficients in $\mathcal{O}_F$.

Then taking $f(X) = \det(I_n \cdot X - M)$ $f(x) = 0$.

This means: $x$ is integral over $\mathcal{O}_F$.

$\mathcal{O}_F$ integrally closed $\Rightarrow$ $x \in \mathcal{O}_F$ $\Rightarrow \mathfrak{p}^{-1} \subseteq \mathcal{O}_F$.

A contradiction! $\square$

<u>Proposition</u>: (1) $(I(F), \cdot)$ is a abelian group.

(2) $P(F)$ is a subgroup of $I(F)$.

Proof: Check: (1) $M \cdot N = N \cdot M$

(2) $M_1 \cdot (M_2 \cdot M_3) = (M_1 \cdot M_2) \cdot M_3$

(3) $M \cdot \mathcal{O}_F = \mathcal{O}_F \cdot M = M$.

Therefore, it suffices to find $M^{-1}$ for $M \in I(F)$

Claim: $M^{-1} = \{ x \in F : xM \subseteq \mathcal{O}_F \}$

① Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$. Then $\mathfrak{p} \in I(F)$.

By definition: $\mathfrak{p} \cdot \mathfrak{p}^{-1} \subseteq \mathcal{O}_F$.

Lemma: $\mathfrak{p} \subsetneq \mathfrak{p} \cdot \mathfrak{p}^{-1}$ ( Prove later).

Sime $\mathcal{O}_F$ is a Dedekind domain and $\mathfrak{p}$ prime $\Rightarrow$ $\mathfrak{p}$ is maxl

This will force $\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathcal{O}_F$

② Let $\mathfrak{a}$ be an ideal. Then $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$

Then $\mathfrak{a} \cdot (\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_n^{-1}) = \mathcal{O}_F$.

Next, we show: $\mathfrak{a}^{-1} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_n^{-1}$

By the definition of $\mathfrak{a}^{-1}$, $\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_n^{-1} \subseteq \mathfrak{a}^{-1}$

Then take $x \in \mathfrak{a}^{-1}$, $x\mathfrak{a} \subseteq \mathcal{O}_F$

$x\mathfrak{a} \cdot \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_n^{-1} \subseteq \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_n^{-1}$

Sime $\mathfrak{a} \cdot \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_n^{-1} = \mathcal{O}_F$, take $1 \in \mathfrak{a}\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_n^{-1}$

$\Rightarrow x \cdot 1 \in \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_n^{-1}$

③. Let be a fractional ideal. Then we can find $c \in \mathcal{O}_F$ s.t. $c \cdot M \subseteq \mathcal{O}_F$. and $c \cdot M$ is an ideal of $\mathcal{O}_F$.

$(c \cdot M) \cdot (c \cdot M)^{-1} = \mathcal{O}_F$.

We can show: $(c \cdot M)^{-1} = c^{-1} M^{-1}$

This implies: $M \cdot M^{-1} = \mathcal{O}_F$.

(2) This is easy since $(c)^{-1} = (c^{-1})$.

Definition: Let $F$ be a number field. The class group

$$H(F) := I(F)/P(F).$$

Theorem: $H(F)$ is a finite abelian group.

Set: $h(F) := \# H(F)$, the class number.