Recall. In the previous lecture we proved the following important theorem:

**Theorem.** A: Integral domain, Noetherian, dim $A = 1$, Max $A = \mathfrak{m}$. TFAE: (1) $A$ is integrally closed (2) $\mathfrak{m}$ is principal. (3) $\dim_{k(\mathfrak{m})} \mathfrak{m}/\mathfrak{m}^2 = 1$ where $k(\mathfrak{m}) := A/\mathfrak{m}$. (4) For any $0 \neq \mathfrak{a} \leq A$, $\exists i$, $\mathfrak{a} = \mathfrak{m}^i$. (5) $\exists \pi$ s.t. $\forall 0 \neq \mathfrak{a} \leq A$, $\exists i$, $\mathfrak{a} = \langle \pi^i \rangle$. (6) $\exists \nu: \mathbb{F} \to \mathbb{Z} \cup \{\infty\}$ s.t. $\nu(\mathfrak{a}) = \infty \iff \mathfrak{a} = 0$ (Discrete Valuation Ring) $\cdot \nu(\alpha_1, \alpha_2) = \nu(\alpha_1) + \nu(\alpha_2)$ (F: field of frac. of $A$) $\cdot \nu(\alpha_1 + \alpha_2) \geq \min\{\nu(\alpha_1), \nu(\alpha_2)\}$ $\cdot a \in A \iff \nu(a) > 0$.

Next we will see the global analogue of this statement.

**Theorem.** A: integral domain, Noetherian, dim $A = 1$. TFAE: (1) $A$ : integrally closed (2) $A_{\mathfrak{m}}$ : DVR, $\forall \mathfrak{m} \in \text{Max} A$ (3) $\mathfrak{q} \triangleleft A$ primary $\iff \mathfrak{q} = \mathfrak{p}^n$ for some $\mathfrak{p} \in \text{Spec} A$. 
Def: A ring that satisfies the above properties is called a **Dedekind Domain**.

Cor: Suppose \( \mathcal{O}_k \) is the ring of integers of a number field. Then

\[ \mathcal{O}_k \text{ is a Dedekind domain; and so } \forall \neq \mathfrak{a} \neq \mathcal{D}, \]

\[ \mathfrak{a} = \prod_{\mathfrak{p} \in \text{Max } \mathcal{D}} \mathfrak{v}(\mathfrak{a}) \quad \text{and} \quad \mathfrak{v}^{(1)}(\mathfrak{a}) = 0 \text{ except for finitely many } \mathfrak{p}. \]

Pro: We have already proved that \( \mathcal{O}_k \cong \mathbb{Z} \) as an abelian group and in particular it is Noetherian;

\( \mathcal{O}_k \) is the integral closure of \( \mathbb{Z} \) in \( k \); hence it is integrally closed; and \( \dim \mathcal{O}_k = \dim \mathbb{Z} = 1 \).

By the 2nd uniqueness theorem, \( \mathfrak{a} \) has a unique reduced primary decomposition. Since \( \mathcal{O}_k \) is Dedekind, any primary ideal is a power of a prime ideal. Since \( \mathfrak{a} \neq 0 \), \( \text{Ass}(\mathfrak{a}) \subseteq \text{Max}(\mathcal{O}_k) \).

For \( \mathfrak{p} \in \text{Max}(\mathcal{O}_k) \), \( \mathfrak{p} \neq \mathfrak{p}^2 \neq \mathfrak{p}^3 \neq \ldots \); and so by the Chinese Remainder Theorem claim follows.
Proof of Theorem. Let $A_i$ be integrally closed. Thus $A_i$ is integrally closed.

A. Noether, $\dim A = 1 \Rightarrow \dim A_{nr} = 1$ and $A_{nr}$ Noether. Hence $A_{nr}$ is a DVR.

- $\mathfrak{p} \neq 0$ primary $\Rightarrow \sqrt{\mathfrak{p}} = \mathfrak{m} \in \text{Max } A_i$ as $\dim A = 1$; and $\mathfrak{p}_{nr}$ is $nr$-primary $\Rightarrow \mathfrak{p}_{nr} = \mathfrak{m}^n A_{nr}$ for some $n \in \mathbb{Z}^+$ as $A_{nr}$ is a DVR. Since $\mathfrak{m}^n$ is $nr$-primary and $\mathfrak{p}_{nr} = \mathfrak{m}^n$, $\mathfrak{p} = \mathfrak{m}^n$.

- Any non-zero ideal $\mathfrak{a}$ of $A_{nr}$ is $nr$-primary, and so $\exists \mathfrak{q} \subseteq A_i$ $\mathfrak{q}$ : $nr$-primary and $\mathfrak{a} = \mathfrak{q}^n$. By assumption $\mathfrak{q} = \mathfrak{m}^n$; hence $\mathfrak{a} = (\mathfrak{m} A_{nr})^n$. Therefore $A_{nr}$ is a DVR. This implies $A_{nr}$ is integrally closed for any $\mathfrak{m} \in \text{Max } A_i$. Hence $A_i$ is integrally closed. ■

As we have seen before $O_k$ is not necessarily a PID. Next we want to have a way of saying how "badly" $O_k$ is failing of being a PID.
Def. A: integral domain ; \( F \): field of fractions;

\[
\text{Frac}(A) := \{ M \subseteq F \mid \exists \alpha \in F^x, \alpha M \subseteq A \},
\]

\[
\text{Prin}(A) := \{ \alpha \in A \mid \alpha \in F^x \},
\]

\[\text{Lemma.} \quad M_1, M_2 \in \text{Frac}(A) \Rightarrow M_1 M_2 \in \text{Frac}(A),\]

where \( M_1 M_2 := \sum_{m_1 \in M_1} \sum_{m_2 \in M_2} A m_1 m_2 \).

\[
\text{\bullet} \quad M \in \text{Frac}(A) \Rightarrow M : A = A : M = M.
\]

\[
\text{\bullet} \quad (\text{Prin}(A), \cdot) \text{ is a group.}
\]

\[\text{Proof.} \quad \text{Clear.} \quad \blacksquare\]

\[\text{Lemma.} \quad \text{For } M \in \text{Frac}(A), \quad (A : M) := \{ \alpha \in F \mid \alpha M \subseteq A \} \in \text{Frac}(A),\]

and \( M \) has an inverse in \( \text{Frac}(A) \) if and only if \( (A : M) M = A \).

\[\text{Proof.} \quad (A : M) \text{ is a submodule of } F \text{ and, for } \beta \in M \setminus \{0\},\]

\[
\beta (A : M) \subseteq A; \text{ and so } (A : M) \in \text{Frac}(A).
\]

\[
\text{Proof.} \quad (A : M) M = A, \text{ then } M \text{ is invertible in } \text{Frac}(A) \text{ by definition.}
\]

\[
\text{Proof.} \quad \text{If } M' M = A \text{ for some } M' \in \text{Frac}(A), \text{ then } M' \subseteq (A : M); \text{ and so}\]

\[
A \subseteq (A : M) M \subseteq A; \text{ and claim follows.} \quad \blacksquare
\]
Proposition. TFAE: (1) $M \subseteq \text{Frac}(A)$ is invertible.

(2) $M$ is f.g. and $\forall p \in \text{Spec}(A), M_p \subseteq \text{Frac}(A_p)$ is invertible.

(3) $M$ is f.g. and $\forall \mathfrak{m} \in \text{Max}(A), M_{\mathfrak{m}} \subseteq \text{Frac}(A_{\mathfrak{m}})$ is invertible.

Proof: (1) $\Rightarrow$ (2). $MM' = A$ implies $\exists m_i \in M, m'_i \in M'$ s.t. $\sum_{i=1}^{k} m_i m'_i = 1$.

Then, for any $x \in \text{Max}(A)$, $x = x \cdot 1 = \sum_{i=1}^{n} (x m'_i) m_i \in \langle m_1, ..., m_k \rangle$.

And so $M = \langle m_1, ..., m_k \rangle$ is a f.g. $A_{\mathfrak{m}}$-mod.

(2) $\Rightarrow$ (3) is clear.

(3) $\Rightarrow$ (1). To show $(A : M)M = A$, it is enough to show for any $\mathfrak{m} \in \text{Max}(A)$, $(A : M)_{\mathfrak{m}} M = A_{\mathfrak{m}}$. It is clear that $(A : M)_{\mathfrak{m}} M = (A : M)_{\mathfrak{m}} M_{\mathfrak{m}}$. We also have

$$(A_{\mathfrak{m}} : M_{\mathfrak{m}}) = \{ x \in F \mid x M_{\mathfrak{m}} \subseteq A_{\mathfrak{m}} M_{\mathfrak{m}} \} = \{ x \in F \mid x M \subseteq A_{\mathfrak{m}} M \}$$

where $M = \langle x_1, ..., x_k \rangle$.

$$= \{ x \in F \mid x = q_1 s_1 + ..., x = q_k s_k \text{ for some } q_i e A, s_i e A_{\mathfrak{m}} \}$$

$$= \{ x \in F \mid \exists s e A_{\mathfrak{m}} \setminus \mathfrak{m}, s x_i e A_{\mathfrak{m}} \} \quad (s = s_1 s_2 \ldots s_k)$$

$$(A : M)_{\mathfrak{m}}; \text{ and claim follows}.$$
Corollary. If $A$ is a Dedekind domain $\Rightarrow$ all elements of $\text{Frac}(A)$ are invertible.

**Proof.** $A$ is a Dedekind domain $\Rightarrow$ $\forall \mathfrak{m} \subseteq \text{Max} A$, $A_{\mathfrak{m}}$ is a DVR.

and, if $\alpha M \subseteq A$, implies $\alpha M$ is f.g. as $A$ is Noether.

And so $M$ is f.g.

Let $N$ be a f.g. $A_{\mathfrak{m}}$-submod of $F$. Suppose

$$N = A_{\mathfrak{m}} \alpha_1 + \ldots + A_{\mathfrak{m}} \alpha_k \quad \text{and} \quad \alpha_i = u_i \pi^{n_i} \quad u(c_i) = 0,$$

$$u(c) = 1.$$ Then $N = A_{\mathfrak{m}} \pi^{\min(n_1, \ldots, n_k)}$; and so

$$(A_{\mathfrak{m}} : N) = \pi^{\min(n_1, \ldots, n_k)} A_{\mathfrak{m}}$$ which implies

$$(A_{\mathfrak{m}} : N) N = A_{\mathfrak{m}}. \quad \Box$$

**Def.** The class group of $A$ is $\text{Cl}(A) = \text{Frac}(A) / \text{Prin}(A)$.

**Cor.** $\text{Cl}(A) = 0 \iff A$ is a PID.