Now $\mathcal{O}/\mathfrak{p}$ integral over $\mathcal{O}/(\mathfrak{p})$, a field, since $\mathcal{O}$ integral over $\mathcal{O}/\mathfrak{p}$ a field $\Rightarrow$ $\mathfrak{p}$ maximal.

Every $b \in \mathcal{O}/\mathfrak{p}$ satisfies integral equation with coeffs in field $\mathcal{O}/\mathfrak{p}$.

so $\mathcal{A}[b] = \mathcal{A}(b)$ i.e. $b$ invertible. (use division algorithm for polynomial rings)

Main theorem: Every non-trivial ideal $\mathfrak{a}$ in Dedekind domain $\mathcal{O}$ has a unique factorisation $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ into non-zero prime ideals.

Recall that product of ideals $\mathfrak{a} \mathfrak{b} = \sum \mathfrak{a}_i \mathfrak{b}_i$ where $\mathfrak{a}_i \in \mathfrak{a}$, $\mathfrak{b}_i \in \mathfrak{b}$.

and similarly $\mathfrak{a} + \mathfrak{b} = \sum (\mathfrak{a} + \mathfrak{b})$ where $\mathfrak{a} \in \mathfrak{a}$, $\mathfrak{b} \in \mathfrak{b}$.

Sometimes write $\mathfrak{a} \mid \mathfrak{b}$ for $\mathfrak{b} \subseteq \mathfrak{a}$ (just think about integers $7 \mid 14 \Rightarrow 14 \subseteq (7)$).

Lemma 1: For every non-zero ideal $\mathfrak{a}$ of $\mathcal{O}$, $\exists \mathfrak{p}_1, \ldots, \mathfrak{p}_r$ with

$\mathfrak{a} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$. (Really only uses fact that $\mathcal{O}$ Noetherian)

Pf: Let $M$ be set of ideals for which desired property fails.

Then order these ideals by inclusion. Since $\mathcal{O}$ Noetherian, every ascending chain stabilizes, so $\exists$ maximal elt. in $M$, call it $M$. (not prime, since in $M$)

$\Rightarrow \exists b_1, b_2 \in \mathcal{O}$ with $b_1 b_2 \notin M$ but $b_1 b_2 \in M$.

Let $M_1 = (b_1) + M$ so $M \not\supset M_1$, $M_1 M_2 \subseteq M$.

$M_2 = (b_2) + M$ But $M_1$ not in $M$ by maximality, so are products $M$ contain product of both $b_i$. if primes $\Rightarrow$
Lemma 2. Let \( \mathfrak{g}^{-1} := \{ x \in K \mid \forall g \in \mathfrak{g} \forall \alpha \neq 0, \alpha x^{-1} := \{ \sum_{i} a_i x_i \mid a_i \in \alpha, x_i \in g^{-1} \} \neq \alpha \} \) be the set of inverses of \( \mathfrak{g} \) in \( K \), where \( g \) is a prime ideal of \( K \).

For every ideal \( \alpha \neq 0 \), \( \alpha g^{-1} := \{ \sum_{i} a_i x_i \mid a_i \in \alpha, x_i \in g^{-1} \} \neq \alpha \).

(by construction all \( g^{\prime}/\alpha \))

If: First show \( g^{-1} \neq 0 \). Let \( a \in g \), \( a \neq 0 \). \( g_1 \ldots g_r \in (a) \leq g \) for some \( g_i \) with \( r \) minimal. (Their existence being guaranteed by previous lemma.) Now one of \( g_i \) is contained in \( \mathfrak{g} \) (else we can make product of \( a \)'s with \( a_i \in g_i \) or \( \mathfrak{g} \)), while \( \mathfrak{g} \) is prime implies \( a_1 \ldots a_r \in g_i \).

Again since \( r \) minimal, \( g_2 \ldots g_r \in (a) \).

If \( b \in g_2 \ldots g_r \setminus (a) \) \( \Rightarrow a^{-1} b \notin \mathfrak{g} \) (\( a^{-1} \) : inverse of \( a \) in \( K \)).

But \( b g_i = b g \in (a) \) \( \Rightarrow a^{-1} b g \leq g \) so by definition \( a^{-1} b \in g^{-1} \).

So \( g^{-1} \neq 0 \) since \( a^{-1} b \in g^{-1} \setminus \Theta \). (Better: \( g^{-1} \neq 0 \).

To show \( \alpha g^{-1} \neq 0 \), let \( a_1, \ldots, a_n \) be generators of \( \alpha \).

If \( \alpha g^{-1} = \alpha \) then for every \( x \in g^{-1} \), write

\[ x \cdot d_i = \sum_{j} a_{ij} d_j \]  

\( \forall \alpha \neq 0 \), \( a_{ij} \in \Theta \).

i.e. if \( A = (a_{ij}) \), then \( A \cdot (d_1, \ldots, d_n) = 0 \) \( \Rightarrow \) \( \det(A) = 0 \).

But \( \det(X \delta_{ij} - a_{ij}) \) is monic poly. in \( X \) with root \( x \), so \( x \in \Theta \).

i.e. \( g^{-1} = 0 \) since \( x \) arbitrary. Y. \( \alpha \).
proof of main theorem: Let \( M \) be the set of ideals (non-trivial) which don't have decomposition into prime ideals.

(Existence of factorization) \( M \) contains maximal elt. \( M \) (just as in Lemma 1). ordering by inclusion.

Since \( M \) Noetherian, \( M \) contains maximal elt. \( \mathfrak{m} \) (just as in Lemma 1). ordering by inclusion.

Now \( M \) is contained in maximal (= prime) ideal \( \mathfrak{p} \).

By Lemma 2, \( \mathfrak{p} \subseteq \mathfrak{p}^{-1} \) so \( \mathfrak{p} \not\subseteq \mathfrak{p}^{-1} \in \mathfrak{p}^{-1} \subseteq \mathfrak{p} \). (*)

Also \( \mathfrak{p} \not\subseteq \mathfrak{p}^{-1} \in \mathfrak{p} \) and \( \mathfrak{p} \) maximal, so we must have \( \mathfrak{p} \mathfrak{p}^{-1} = \mathfrak{p} \).

(Using Lemma 2.) Finally \( \mathfrak{m} \not\subseteq \mathfrak{p} \) (else it factors as product of primes) so \( \mathfrak{m} \mathfrak{p}^{-1} \not\subseteq \mathfrak{p} \).

That is, we may rewrite (*) as: \( \mathfrak{m} \not\subseteq \mathfrak{p} \mathfrak{p}^{-1} \not\subseteq \mathfrak{p} \).

By maximality of \( \mathfrak{m} \), \( \mathfrak{m} \mathfrak{p}^{-1} \) is factorizable, but if so, then \( \mathfrak{m} \) factorizable as product of primes \( \mathfrak{n} \).

(e.g. \( \mathfrak{m} \mathfrak{p}^{-1} = \mathfrak{n}_1 \cdots \mathfrak{n}_r \) then \( \mathfrak{m} = \mathfrak{n}_1 \mathfrak{n}_2 \cdots \mathfrak{n}_r \).

proof of main theorem: For prime ideals, \( \alpha \beta \subseteq \mathfrak{p} \Rightarrow \alpha \subseteq \mathfrak{p} \) or \( \beta \subseteq \mathfrak{p} \).

(uniqueness of factorization) (analogue of divisibility condition \( \gcd(ab) = \gcd(a) \cdot \gcd(b) \))

For prime ideals, \( \alpha \beta \subseteq \mathfrak{p} \Rightarrow \alpha \subseteq \mathfrak{p} \) or \( \beta \subseteq \mathfrak{p} \).

Given two factorizations of some ideal into primes

\[ \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s \]

(note a priori, don't know \( r = s \))

then \( \mathfrak{p}_1 \cdots \mathfrak{p}_r \Rightarrow \mathfrak{q}_i \subseteq \mathfrak{p}_i \).

But \( \mathfrak{q}_i \) prime \( \Rightarrow \)

\( \mathfrak{q}_i \) maximal

so \( \mathfrak{p}_i = \mathfrak{q}_i \).

(If \( \mathfrak{p}_i \neq \mathfrak{q}_i \),

\( i = 1 \) as well)

just a labeling issue.

multiplying both sides by \( \mathfrak{p}_i^{-1} \) and noting \( \mathfrak{p}_1 \mathfrak{p}_i^{-1} = \mathfrak{p} \)

then \( \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s \).

Continue cancelling in this way to see \( r = s \)

with \( \mathfrak{q}_i = \mathfrak{p}_i \).