Now ~~[illegible]~~ $\mathcal{O}_K/\wp$ integral over $\mathbb{Z}/(p)$, a field, since $\mathcal{O}_K$ integral over $\mathbb{Z}$ $\Rightarrow$ $\mathcal{O}_K/\wp$ a field $\Rightarrow$ $\wp$ maximal.

Every $b \in \mathcal{O}_K/\wp$ satisfies integral equation with coeffs in field $\mathbb{Z}/p\mathbb{Z}$.

so $A[b] = A(b)$ 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 factorization $\mathfrak{a} = \wp_1 \cdots \wp_r$ into non-zero prime ideals.

—

Recall that product of ideals $\mathfrak{a}\mathfrak{b} = \{ \sum_i a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \}$

and similarly $\mathfrak{a} + \mathfrak{b} = \{ a+b \mid a \in \mathfrak{a}, b \in \mathfrak{b} \}$

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

—

Lemma 1: For every non-zero ideal $\mathfrak{a}$ of $\mathcal{O}$, $\exists$ $\wp_1, \ldots, \wp_r$ with $\mathfrak{a} \supseteq \wp_1 \cdots \wp_r$. (Really only uses fact that $\mathcal{O}$ Noetherian)

pf: Let M: 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 $\mathfrak{m}$. (not prime, since in M)

defn $\Rightarrow$ $\exists$ $b_1, b_2 \in \mathcal{O}$ with $b_1 b_2 \in \mathfrak{m}$ but $b_1, b_2 \notin \mathfrak{m}$

Let $\mathfrak{m}_1 = (b_1) + \mathfrak{m}$ so $\mathfrak{m} \subsetneq \mathfrak{m}_i$, $\mathfrak{m}_1 \mathfrak{m}_2 \subseteq \mathfrak{m}$.
$\mathfrak{m}_2 = (b_2) + \mathfrak{m}$ But $\mathfrak{m}_i$ not in M by maximality, so are products of primes $\Rightarrow$ $\mathfrak{m}$ contains product of both $\mathfrak{m}_i$.

Lemma 2 : Let $\mathfrak{p}^{-1} := \{ x \in K \mid x\mathfrak{p} \subseteq \mathcal{O} \}$ $\quad \mathfrak{p}$: prime ideal of Dedekind domain $\mathcal{O}$

for every ideal $\mathfrak{a} \neq 0$, $\mathfrak{a}\mathfrak{p}^{-1} := \{ \sum_i a_i x_i \mid a_i \in \mathfrak{a}, x_i \in \mathfrak{p}^{-1} \} \neq \mathfrak{a}$.

(by constructing elt in $\mathfrak{p}^{-1} \setminus \mathcal{O}$.)

Pf : First show $\mathfrak{p}^{-1} \neq \mathcal{O}$. Let $a \in \mathfrak{p}$. $a \neq 0$. $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$ for some $\mathfrak{p}_i$ with r minimal. (their existence being guaranteed by previous lemma)

Now one of $\mathfrak{p}_i$ is contained in $\mathfrak{p}$ (else we can make product of elts $a_1 \cdots a_r$ with $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$
but $\mathfrak{p}$ prime implies $a_1 \cdots a_r \notin \mathfrak{p}$
while $a_1 \cdots a_r \in \mathfrak{p}_1 \cdots \mathfrak{p}_r$ ↯.)

Again since r minimal, $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (a)$

$\exists \; b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus (a) \iff a^{-1}b \notin \mathcal{O}$ (a^{-1} : inverse of a in K)

But $b\mathfrak{p}_1 = b\mathfrak{p} \subseteq (a) \iff a^{-1}b\mathfrak{p} \subseteq \mathcal{O}$ so by def'n $a^{-1}b \in \mathfrak{p}^{-1}$

so $\mathfrak{p}^{-1} \neq \mathcal{O}$ since $a^{-1}b \in \mathfrak{p}^{-1} \setminus \mathcal{O}$. (Better : $\mathfrak{p}^{-1} \supsetneq \mathcal{O}$)

To show $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$, let $\alpha_1, \dots, \alpha_n$ be generators of $\mathfrak{a}$

If $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$ then for every $x \in \mathfrak{p}^{-1}$, write

$$x \cdot \alpha_i = \sum_j a_{ij} \alpha_j \qquad a_{ij} \in \mathcal{O}$$

i.e. if $A = (x \cdot \delta_{ij} - a_{ij})$ then $A \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0$. $\Rightarrow \det(A) = 0$

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

i.e. $\mathfrak{p}^{-1} = \mathcal{O}$ since x arbitrary. ↯. //

proof of main thm: (Existence of factorization) Let M : set of ideals (non-trivial) which don't have decomposition into prime ideals.

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

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

By Lemma 2, $\mathcal{O} \subseteq \mathfrak{p}^{-1}$ so $\mathfrak{m} \subsetneq \mathfrak{m}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$. (*)

Also (using Lemma 2) $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$ and $\mathfrak{p}$ maximal, so we must have $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.

Finally $\mathfrak{m} \neq \mathfrak{p}$ (else it factors as product of primes) so $\mathfrak{m}\mathfrak{p}^{-1} \subsetneq \mathcal{O}$

That is, we may rewrite (*) as: $\mathfrak{m} \subsetneq \mathfrak{m}\mathfrak{p}^{-1} \subsetneq \mathcal{O}$

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

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

proof of main thm. (uniqueness of factorization)

For prime ideals, $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$.
(analogue of divisibility condition $p \mid ab \Rightarrow p \mid a$ or $p \mid b$)

Given two factorizations of same ideal into primes (note a priori, don't know $r = s$)

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$$

then $\mathfrak{p}_1 \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_s \Rightarrow \mathfrak{p}_1 \supseteq \mathfrak{q}_i$ some i. But $\mathfrak{q}_i$ prime $\Leftrightarrow$ $\mathfrak{q}_i$ maximal so $\mathfrak{p}_1 = \mathfrak{q}_i$.

(w.l.o.g. suppose $i = 1$ as well)

multiplying both sides by $\mathfrak{p}_1^{-1}$ and noting $\mathfrak{p}_1\mathfrak{p}_1^{-1} = \mathcal{O}$

then $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$.

Continue cancelling in this way to see $r = s$ with $\mathfrak{p}_i = \mathfrak{q}_i \ \forall i$ //

just a labeling issue.