Given integral basis for $B$, integral closure of $A$ (a P.I.D.) in $L/K$,

then $\text{disc}(B) = \text{disc}(\{d_1, \ldots, d_n\}) = \det(\text{Tr}(\theta_i d_j))$

If $L = K(\theta)$ with $\theta \in B$, then $d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2$, where $\theta_i := b_i(\theta)$

But might not be true that $\text{disc}(B) = \text{disc}(\{\theta\})$. Why? Because $1, \theta, \ldots, \theta^{n-1}$ might not be integral basis. Saw this already for $d = 1(4)$ and $Q(\sqrt{-d})$.

There $L \subset L(\sqrt{d \pm \sqrt{d^2 - 4}})$.

We do know $\mathbb{Z}[\theta]$ is submodule of $B$, since $\theta$ integral (even subring) and both free modules of rank $[L : K]$, so using classification of modules over P.I.D.s $B/\mathbb{Z}[\theta]$ is free gp (any quotient of $B$ by submodule with integral basis of size $n$)

How to calculate the integral basis?

idea (See Ch. 6 of Cohen’s “A Course in Computational Algebraic Number Theory”)

enlarge $\mathbb{Z}[\theta]$ for each prime $p$ in $[B : \mathbb{Z}[\theta]]$

In fact we know more:

$\text{disc}(B) = \mathbb{Z} + \mathbb{Z} \theta + \cdots + \mathbb{Z} \theta^{n-1}$

$\text{disc}(\{\theta\}) = \mathbb{Z}[\theta]$

$\theta$ minimal poly. of $\theta$

And if $[B : \mathbb{Z}[\theta]] = f$ then $\text{disc}(\{\theta\}) = \text{disc}(\{\theta\}) \cdot f^2$.

So can look for primes dividing $\text{disc}(\{\theta\})$ to get order $\mathbb{Z}[\theta]$ and enlarge to $\mathbb{Z}[\theta]$ at each such $p$. 
Studying $\mathfrak{O}_k$ : ring of integers of $K/\mathbb{Q}$, have $N_{K/\mathbb{Q}}$, $Tr_{K/\mathbb{Q}}$, $d(\mathfrak{O}_k)$, integral basis as $\mathbb{Z}$-module.

We want to understand how primes decompose in $\mathfrak{O}_k$, but we don't have unique factorization into irreducible elements.

We do have factorizations of any elt. into irreducibles. (follows from existence of norm function)

If $b = b_1 b_2$ then $N(b) = N(b_1) N(b_2)$

with $N(b_1), N(b_2) < N(b)$ (since $b_1, b_2$ non-units)

But, for example in $\mathbb{Z}([\sqrt{-5}])$, we have $\mathfrak{O}_k = \mathbb{Z}([\sqrt{-5}])$ since $-5 \equiv 3 \pmod{4}$

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Are $1 + \sqrt{-5}$ irreducible in $\mathfrak{O}_k$?

$$1 - \sqrt{-5}$$

If not, need to find $a + b\sqrt{-5}$ with

$$N(a + b\sqrt{-5}) = a^2 + 5b^2$$

a proper divisor of 6.

As Neukirch nicely explains, one could hope to work in enlarged domain containing $\mathfrak{O}_k$ where some further divisibility held:

Want some factorization

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

with properties that if $\mathfrak{p} | a, \mathfrak{p} | b \in \mathfrak{O}_k$ then $\mathfrak{p} | a + b$.

Similarly if $\mathfrak{p} | a, a \in \mathfrak{O}_k$ then $\mathfrak{p} | ma$ for any $m \in \mathfrak{O}_k$.

Leads us to the concept of "ideal." Recall that "prime ideal" in $\mathfrak{O}$. Ring $A$ is ideal set. $A/\mathfrak{p}$ is integral domain. For example

if $M$ maximal ideal, then $A/M$ field, so all maximal ideal are prime.
Dedekind realized right set of conditions required for a ring to have unique factorization into product of prime ideals.

"Dedekind domain" - integral domain that is

(i) Noetherian
(ii) integrally closed (in its field of fractions)
(iii) every non-zero prime ideal is maximal.

To show
(1) \( \Omega_k \) is Dedekind domain
(2) Any Dedekind domain has unique factorization of non-trivial ideal into product of prime ideals.

Proposition: \( \Omega_k \) is Dedekind domain.

Proof: (iii) follows by definition. For (i), we use the fact that \( \mathbb{Z} \), as P.I.D., is Noetherian (as \( \mathbb{Z} \)-module, every increasing sequence is stationary).
and \( \Omega_k \) is finitely generated over \( \mathbb{Z} \), so also Noetherian.
( in general \( E' \leq E \) are \( A \)-modules, then \( E \) Noetherian \( \iff \) \( E' \), \( E/E' \) Noetherian)

So left to show if \( \mathfrak{g} \neq 0 \) is prime ideal, then \( \mathfrak{g} \) maximal:
we have \( \mathfrak{g} \cap \mathbb{Z} \) is prime ideal of \( \mathbb{Z} \), say \( (p) \), because \( \mathfrak{g} \cap \mathbb{Z} \) is kernel of \( \mathbb{Z} \rightarrow \Omega_k \rightarrow \Omega_k/\mathfrak{g} \) so have injective hom \( \mathbb{Z}/(\mathfrak{g} \cap \mathbb{Z}) \rightarrow \Omega_k/\mathfrak{g} \)
so \( \mathbb{Z}/(\mathfrak{g} \cap \mathbb{Z}) \) is subring of integral domain.

Given \( x \in \mathfrak{g} \), \( x \neq 0 \) with min. poly \( x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0 \)
and to see else this wasn't min. poly, b/c we can factor out \( x \).

Now \( an \in \Omega_k \cdot x \cap \mathbb{Z} \subset \mathfrak{g} \cap \mathbb{Z} = (p) \Rightarrow p \neq 0. \) (which we didn't know a priori)
\[ \mathbb{O}_k / \mathfrak{p} \text{ integral over } \mathbb{Z}/(p), \text{ a field, since } \mathbb{O}_k \text{ integral over } \mathbb{Z} \Rightarrow \mathbb{O}_k / \mathfrak{p} \text{ a field } \Rightarrow \mathfrak{p} \text{ maximal.} \]

Every \( \mathfrak{b} \in \mathbb{O}_k / \mathfrak{p} \) satisfies integral equation with coeffs in field \( \mathbb{Z}/(p) \).

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

---

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

Recall that product of ideals \( \mathfrak{a} \mathfrak{b} = \mathfrak{z} \sum a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \)

and similarly \( \mathfrak{a} + \mathfrak{b} = \mathfrak{z} \sum a_i + b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \)

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

---

Lemma 1: For every non-zero ideal \( \mathfrak{a} \) of \( \mathbb{O} \), \( \mathbb{O} \subseteq \mathfrak{a} \cdots \mathfrak{a} \) write

\[ \mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_r. \]

(Really only uses fact that \( \mathbb{O} \) Noetherian)

---

If: Let \( M \) set of ideals for which desired property fails.

Then order these ideals by inclusion. Since \( \mathbb{O} \) Noetherian, every ascending chain stabilizes, so \( \mathfrak{I} \) maximal elt. in \( M \), call it \( \mathfrak{I}_0 \). (not prime, since in \( M \))

def: \( \mathfrak{J} = \mathfrak{b}_1, \mathfrak{b}_2 \in \mathfrak{O} \) with \( \mathfrak{b}_1, \mathfrak{b}_2 \neq M \) but \( \mathfrak{b}_1, \mathfrak{b}_2 \notin \mathfrak{M} \)

Let \( \mathfrak{M}_1 = (\mathfrak{b}_1) + M \) so \( \mathfrak{M}_1 \notin \mathfrak{M}_0 \), \( \mathfrak{M}_1 \mathfrak{M}_2 \leq \mathfrak{M} \).

Let \( \mathfrak{M}_2 = (\mathfrak{b}_2) + M \) But \( \mathfrak{M}_1 \) not in \( M \) by maximality, so are products \( \mathfrak{M} \) contains product of both \( \mathfrak{M}_1 \) of primes \( \mathfrak{p}_0 \).