We can define the norm and trace of an element \( \alpha \in \mathcal{O}_K \):

\[
N_{K/Q}(\alpha) = \prod_{i} \Phi_i(\alpha), \text{ where } \{\Phi_i, \ldots, \Phi_d\} \text{ are the homs. } \Phi_i : K \to \mathbb{C}.
\]

\[
N_{K/Q}(\alpha) = \prod_{\sigma \in \mathcal{G}(\alpha)}^m \text{ if } K/Q \text{ is Galois, where } \mathcal{G} = \text{Gal} (K/Q), \text{ where } m = [K : \mathbb{Q}(\alpha)].
\]

\[
N_{\mathbb{Q}}(2) = 2.
\]

\[
N_{\mathbb{Q}(\sqrt{2})}(2) = 2 \cdot 2 = 4.
\]

In general, \( N_K(2) = 2^d \), where \( d = [K : \mathbb{Q}] \).

Even more generally, if \( [L : K] = m \), then \( N_L(\alpha) = N_K(\alpha)^m \).

Note \( |N_K(\alpha)| = N(\alpha \mathcal{O}_K) \), and \( N_K(\alpha) \in \mathbb{Z} \), if \( \alpha \in \mathcal{O}_K \).

Also, \( N_K(\alpha) = (-1)^d \alpha_0^{\frac{m}{d}} \), where \( \alpha_0 = \text{const. coeff. in monic min. poly. for } \alpha/\mathbb{Q} \), \( d = [\mathbb{Q}(\alpha) : \mathbb{Q}] \), \( m = [K : \mathbb{Q}] \).

Finally, note \( N_K(\alpha) = \pm 1 \) if \( \alpha \in \mathcal{O}_K^* \), provided \( \alpha \in \mathbb{Q} \).
If $N_k(a) = \pm 1$, then say $\Phi(a) = \pm 1$. Then
\[
\prod_{i=2}^d \Phi_i(a) = \pm 1 \in \Theta_k^*, \text{ so } a \in \Theta_k^*, \text{ with inverse }
\prod_{i=2}^d \Phi_i(a).
\]

If $a \in \Theta_k^*$, then $a\beta = 1$ for some $\beta \in \Theta_k$. Then
\[
1 = N(1) = N(a\beta) = N(a)N(\beta), \text{ so } N(a) \in \mathbb{Z} \text{ is a unit, and so } N(a) = \pm 1.
\]

$Tr_k(a) = \sum \Phi_i(a)$. Note $Tr(a) \in \mathbb{Z}$ if $a \in \Theta_k$, and $Tr(a + \beta) = Tr(a) + Tr(\beta)$.

$Tr_k(a) = mTr_k(\bar{a})$, where $m = [L : K]$.

**Quest:** Compute the norm and trace of $\sqrt{2} + \sqrt{3}$, in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Compute $N_k(\sqrt{2})$, where $K = \mathbb{Q}(\sqrt{2}) + \sqrt{3} = e^{\frac{2\pi i}{4}}$.

Compute $Tr_k(\sqrt{2})$.

**Solv:** The norm of $\sqrt{2}$ is always 1, because $N_k(\sqrt{2}) = \prod_{a=1}^n \sqrt{2}$. This product is a product of factors of the form $\sqrt{2}, \sqrt{3} = \pm 1$. So $N(\sqrt{2}) = 1$. 
as long as \( n \geq 3 \).

If \( \mathfrak{p} \subset \mathcal{O}_K \) is a prime ideal, then \( N(\mathfrak{p}) = \mathfrak{p}^f \) for some integer \( f \geq 1 \). Then \( f \) is called the inertial degree of \( \mathfrak{p} \), written \( F_K(\mathfrak{p}) \).

Write \( \mathfrak{p} \mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \) for prime ideals \( \mathfrak{p}_i \subset \mathcal{O}_K \). Then \( e_i = e_K(\mathfrak{p}_i) \) = ramification index of \( \mathfrak{p}_i \) in \( \mathcal{O}_K \). And \( g_K(\mathfrak{p}) \) = decomposition number of \( \mathfrak{p} \) in \( K \).

**Theorem:** \( \sum_{\mathfrak{p} \mid \mathfrak{p}} e_K(\mathfrak{p}) F_K(\mathfrak{p}) = [K: \mathbb{Q}] \).

(The sum is over all prime ideals of \( \mathcal{O}_K \) that contain \( \mathfrak{p} \).)

**Proof:** Write \( \mathfrak{p} \mathcal{O}_K = (\mathfrak{p}) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \). Then

\[
E_K = N(\mathfrak{p} \mathcal{O}_K) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_g)^{e_g} = (\mathfrak{p}_1^{e_1})^{e_1} \cdots (\mathfrak{p}_g^{e_g})^{e_g}
\]

so \( [K: \mathbb{Q}] = e_1 f_1 + \cdots + e_g f_g \), as desired. \( \square \)
We say that \( p \) ramifies in \( K \) iff \( e_K(p) \geq 2 \) for some ideal \( P \) containing \( p \). Otherwise, we say that \( p \) is unramified.

Note that \( p \) ramifies in \( K \) (say \( \mathcal{O}_K = \mathbb{Z}[\alpha] \)) iff \( m(x) \) has a multiple factor mod \( p \), where \( m(x) \) is the monic min. poly. For \( \mathbb{F}_p(x) \), which happens iff \( p \in (m(x), m'(x)) \subset \mathbb{Z}[x] \), iff \( p \) divides \( \text{disc}(m(x)) = \text{disc}(\mathbb{Z}[\alpha]) \).

In general, \( p \) ramifies in \( K \) iff \( p \mid \text{disc}(K) \).

**Question:** Let \( d \) be a squarefree integer, \( d \neq 1 \). Which primes ramify in \( \mathbb{Q}(\sqrt{d}) \)?

**DVRs:** (Discrete Valuation Rings)

A DVR is a Noetherian local domain \( D \) with a principal max. ideal \( P \).
If \( P = (t) \), then \( t \) is called a uniformiser for \( D \).

Every element of \( D \) can be written in the form \( ut^a \) for \( u \in D^* \), \( a \in \mathbb{Z} \), \( a \geq 0 \).

Every element of \( K(D) \) (frac. field) can be written as \( ut^a \) for \( u \in D^* \), \( a \in \mathbb{Z} \).

The ideals of \( D \) are exactly \((t^a)\) for \( a \in \mathbb{Z} \), \( a \geq 0 \).

In PM 441/641, our DVRs are local rings of Dedekind domains at a prime ideal \( P \):

\[
D_P = \left\{ \frac{a}{b} \mid a, b \in D, b \not\in P \right\}
\]

\[
D_P^* = \left\{ \frac{a}{b} \mid a, b \in D, a, b \not\in P \right\}.
\]

Ex: \( \mathbb{Z}_{(5)} = \left\{ \frac{a}{b} \mid b \not\in (5) \right\} \)

\( \mathbb{Z}_{(5)}^* = \left\{ \frac{a}{b} \mid a, b \not\in (5) \right\} \).

\( P = 5 \mathbb{Z}_{(5)} = \left\{ \frac{a}{b} \mid b \not\in (5), a \in (5) \right\} \).
So $\mathcal{S}$ is a uniformiser for $\mathbb{Z}_{15}$.

$\mathcal{S} = \mathbb{Z}(\sqrt{15})$ is also a uniformiser for $\mathbb{Z}_{15}$, because $24 \in \mathbb{Z}^{*}_{15}$.

Example: $D = \mathbb{Z}(\sqrt{10})$, $p = (5, \sqrt{10})$. Then $\sqrt{10}$ is a uniformiser for $D_p$, because:

$PD_p = (5, \sqrt{10})D_p = (\frac{\sqrt{10}}{5}, \sqrt{10})D_p = \sqrt{10}D_p$.

If $p = (a_1, \ldots, a_n)$ as an ideal of $D$, then for some $i$, $PD_p = a_iD_p$.

Proof: Write $a_i = u_i + r_i$ for $u_i \in D_p^*$, $r_i \in \mathbb{Z}$ ($r_i \geq 0$), $\mathcal{S} + \alpha$ a uniformiser.

Then $PD_p = (u_1 + r_1, \ldots, u_n + r_n)D_p = (r_1, \ldots, r_n)D_p = (r)D_p$, where $r = \min(r_i)$.

If wlog $r_i = r$, then $PD_p = (a_1)D_p$. 