As always, in what follows $K$ is a number field. Recall from earlier in the semester that for an $\alpha \in K$ of degree $[K : \mathbb{Q}]$, the discriminant of $\alpha$ is, by definition, the discriminant of the $n$-tuple (where $n = [K : \mathbb{Q}]$) $\text{disc}(1, \alpha, \ldots, \alpha^{n-1})$. Further, if $\sigma_1, \ldots, \sigma_n$ denote the embeddings of $K$ into $\mathbb{C}$ (in any order), then

$$\text{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 = (-1)^{n(n-1)/2} N_{K/\mathbb{Q}}(f'(\alpha)),$$

where $f(X) \in \mathbb{Q}[X]$ is the minimal (monic) polynomial for $\alpha$ ($f(X) \in \mathbb{Z}[X]$ if and only if $\alpha \in \mathcal{O}_K$). The principal ideal generated by $f'(\alpha)$ is called the different of $\alpha$ and will be denoted $\mathfrak{d}(\alpha)$. In the case where $\alpha$ has lower degree than $[K : \mathbb{Q}]$ we simply set $\mathfrak{d}(\alpha) = \{0\}$, the zero ideal.

**Theorem 1:** Let $K$ be a number field of degree $n$ and let $\text{Tr}_{K/\mathbb{Q}}$ denote the trace from $K$ to $\mathbb{Q}$. Let $\mathfrak{A} \subseteq \mathcal{O}_K$ be an ideal with $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_n$. The set of $\beta \in K$ for which $\text{Tr}_{K/\mathbb{Q}}(\beta \alpha) \in \mathbb{Z}$ for all $\alpha \in \mathfrak{A}$ forms a fractional ideal $\mathcal{I}(\mathfrak{A})$. Moreover $\mathfrak{A} \mathcal{I}(\mathfrak{A})$ is a fractional ideal independent of $\mathfrak{A}$; it is dependent only on the field $K$ and is the reciprocal of an integral ideal $\mathfrak{d}$. Finally, a $\mathbb{Z}$-basis for $\mathcal{I}(\mathfrak{A})$ is given by $\beta_1, \ldots, \beta_n$ where these $\beta$s satisfy

$$\text{Tr}_{K/\mathbb{Q}}(\beta_i \alpha_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

**Proof:** If $\beta_1, \beta_2 \in \mathcal{I}(\mathfrak{A})$ and $\gamma \in \mathcal{O}_K$, then for any $\alpha \in \mathfrak{A}$

$$\text{Tr}_{K/\mathbb{Q}}((\beta_1 + \beta_2)\alpha) = \text{Tr}_{K/\mathbb{Q}}(\beta_1 \alpha) + \text{Tr}_{K/\mathbb{Q}}(\beta_2 \alpha) \in \mathbb{Z}$$

and $\text{Tr}_{K/\mathbb{Q}}((\beta \gamma)\alpha) = \text{Tr}_{K/\mathbb{Q}}(\beta(\gamma \alpha)) \in \mathbb{Z}$ since $\gamma \alpha \in \mathfrak{A}$. Thus $\mathcal{I}(\mathfrak{A})$ is an $\mathcal{O}_K$-module.

Suppose $\beta \in \mathcal{I}(\mathfrak{A})$ and let $\sigma_1, \ldots, \sigma_n$ be the embeddings of $K$ into $\mathbb{C}$ (in any order). We then have $\text{Tr}_{K/\mathbb{Q}}(\beta \alpha_i) \in \mathbb{Z}$ for all $i = 1, \ldots, n$, which we may interpret as saying the column vector

$$\begin{pmatrix} \sigma_1(\beta) \\ \vdots \\ \sigma_n(\beta) \end{pmatrix}$$

is a solution to the linear system $A \mathbf{x} = \mathbf{z}$ where $\mathbf{z} \in \mathbb{Z}^n$ and $A$ is the $n \times n$ matrix $A = (\sigma_j(\alpha_i))$. By Cramer’s rule, we see that the $\sigma_j(\beta)$s are quotients of determinants. Here the numerator of the quotient is some $\mathbb{Z}$-linear combination of the $\sigma_j(\alpha_i)$s but the denominator is fixed: $\det(A)$. By a previous exercise this denominator is $N(\mathfrak{A}) \sqrt{\Delta(K)}$, whence there is some non-zero $\gamma \in \mathcal{O}_K$ depending only on the $\alpha_i$s such that $\gamma \beta \in \mathcal{O}_K$. In particular, this $\gamma$ so chosen does not depend on the particular $\beta \in \mathcal{I}(\mathfrak{A})$, so that $\gamma \mathcal{I}(\mathfrak{A}) \subseteq \mathcal{O}_K$. Thus $\mathcal{I}(\mathfrak{A})$ is a fractional ideal.

Next, suppose $\beta \in \mathcal{I}(\mathfrak{A})$ and let $\alpha \in \mathfrak{A}$. Then $\text{Tr}_{K/\mathbb{Q}}(\beta \alpha \gamma) \in \mathbb{Z}$ for all $\gamma \in \mathcal{O}_K$ since $\alpha \gamma \in \mathfrak{A}$. This shows that $\beta \alpha \in \mathcal{I}(\mathcal{O}_K)$. In particular, this is true for $\alpha = \alpha_1, \ldots, \alpha_n$, so that $\mathcal{I}(\mathfrak{A})\mathfrak{A} \subseteq \mathcal{I}(\mathcal{O}_K)$. On the other hand, if $\beta \in \mathcal{I}(\mathcal{O}_K)$ and $\delta_1, \ldots, \delta_n$ is a $\mathbb{Z}$-basis for $\mathfrak{A}^{-1}$, then $\alpha \delta_i \in \mathcal{O}_K$ for all $\alpha \in \mathfrak{A}$ and $i = 1, \ldots, n$ and so $\text{Tr}_{K/\mathbb{Q}}(\beta \delta_i \alpha) = \text{Tr}_{K/\mathbb{Q}}(\beta \alpha \delta_i) \in \mathbb{Z}$ for all $i$. Thus $\beta \delta_i \in \mathcal{I}(\mathfrak{A})$ for all $i$, so that $\beta \mathfrak{A}^{-1} \subseteq \mathcal{I}(\mathfrak{A})$, i.e., $\beta \in \mathfrak{A} \mathcal{I}(\mathfrak{A})$. This shows that $\mathcal{I}(\mathcal{O}_K) \subseteq \mathfrak{A} \mathcal{I}(\mathfrak{A})$, whence $\mathcal{I}(\mathcal{O}_K) = \mathfrak{A} \mathcal{I}(\mathfrak{A})$.

Clearly $\mathcal{I}(\mathcal{O}_K) = \mathfrak{d}^{-1}$ for some integral ideal $\mathfrak{d}$ since $1 \in \mathcal{I}(\mathcal{O}_K)$. 


Turning to the $\beta_i$’s sought, as above we view these as solutions to a particular system of linear equations. Indeed, if we consider the $n \times n$ matrix $(\sigma_l(\alpha_j))$, we need to show that the inverse of this matrix is such that the $i^{th}$ row is just the conjugates of some $\beta_i \in K$ for all $i$. For notational convenience, for $1 \leq i, j \leq n$ set $e_{i,j} = 1$ if $i = j$ and 0 otherwise. Denote the inverse of the matrix $(\sigma_l(\alpha_j))$ by $(x_{i,l})$, so that
\[ \sum_{l=1}^{n} x_{i,l} \sigma_l(\alpha_j) = e_{i,j}, \quad j = 1, \ldots, n. \]
We have
\[ \sum_{l=1}^{n} \sigma_l(\alpha_k) \sum_{i=1}^{n} x_{i,l} \sigma_j(\alpha_i) = \sum_{i=1}^{n} e_{i,k} \sigma_j(\alpha_i) = \sigma_j(\alpha_k) = \sum_{l=1}^{n} e_{l,j} \sigma_l(\alpha_k). \]
Now equating coefficients yields $\sum_{i=1}^{n} x_{i,l} \sigma_j(\alpha_i) = e_{l,j}$, so that
\[ \sum_{i=1}^{n} x_{i,l} \sigma_j(\alpha_i) = e_{l,j} \sum_{i=1}^{n} \sigma_j(\alpha_i) = \sigma_l(\alpha_k). \]
Thus
\[ \sum_{i=1}^{n} x_{i,l} \text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_k) = \sigma_l(\alpha_k). \]

Now one of these embeddings $\sigma_l$ is simply the identity map, and in this case the equation above has “solutions” $x_{1,l}, \ldots, x_{n,l} \in K$; denote these more simply by $\beta_1, \ldots, \beta_n$ so that
\[ \sum_{i=1}^{n} \beta_i \text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_k) = \alpha_k, \quad k = 1, \ldots, n. \]

Since the coefficients $\text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_k) \in \mathbb{Q}$ here, we may apply any embedding and get $x_{i,l} = \sigma_l(\beta_i)$ always, which is what we needed to show.

**Definition:** The integral ideal $\mathfrak{d}$ in Theorem 1 above is called the *different* of the field $K$.

**Corollary:** The different and discriminant of a number field $K$ satisfy $N(\mathfrak{d}) = |D(K)|$.

**Proof:** Let $\mathfrak{A}$ be any non-zero fractional ideal and let $\beta_1, \ldots, \beta_n$ be the basis for $\mathfrak{I}(\mathfrak{A})$ as in Theorem 1. Then
\[ \text{disc}(\beta_1, \ldots, \beta_n) = N(\mathfrak{I}(\mathfrak{A}))^2 D(K) = \frac{D(K)}{N(\mathfrak{A})^2} = \frac{D(K)}{N(\mathfrak{A})^2 N(\mathfrak{d})^2} \]
and also
\[ \text{disc}(\beta_1, \ldots, \beta_n) = \frac{1}{\text{disc}(\alpha_1, \ldots, \alpha_n)} = \frac{1}{N(\mathfrak{A})^2 D(K)}. \]

**Lemma 1:** Suppose $\alpha \in \mathfrak{d}^{-1}$. Then for all $\theta \in \mathfrak{D}_K$ of degree $[K : \mathbb{Q}]$ we have $\alpha f'(\theta) \in \mathbb{Z}[\theta]$, where $f(X) \in \mathbb{Z}[X]$ is the minimal polynomial for $\theta$.

**Proof:** Set $n = [K : \mathbb{Q}]$ and let $\sigma_1, \ldots, \sigma_n$ be the embeddings of $K$ into $\mathbb{C}$. Consider the polynomial $g(X) \in \mathbb{C}[X]$ given by
\[ g(X) = f(X) \sum_{i=1}^{n} \frac{\sigma_i(\alpha)}{X - \sigma_i(\theta)}. \]
Note that \( g(X) \in \mathbb{C}[X] \) since \( f(X) = \prod_{i=1}^{n} (X - \sigma_i(\theta)) \). We claim that \( g(X) \in \mathbb{Z}[X] \).

To see why, we look at the polynomial \( f(X)/(X - \theta) \) (a polynomial since \( \theta \) is a root of \( f(X) \) by construction). Write \( f(X) = a_0 + a_1 X + \cdots + X^n \) and set

\[
h(X) = \sum_{i=1}^{n} a_i \sum_{j=0}^{i-1} X^j \theta^{i-j-1}.
\]

We have

\[
(X - \theta)h(X) = \sum_{i=1}^{n} a_i \sum_{j=0}^{i-1} X^j \theta^{i-j-1} - \sum_{i=1}^{n} a_i \sum_{j=0}^{i-1} X^j \theta^{i-j} = \sum_{i=1}^{n} a_i \sum_{j=0}^{i-1} X^j \theta^{i-j} - \sum_{i=1}^{n} a_i X^i \theta^{i-1} = \sum_{i=1}^{n} a_i (X^i - \theta^i) = f(X) - a_0 - (f(\theta) - a_0) = f(X) - f(\theta) = f(X).
\]

Thus \( h(X) = f(X)/(X - \theta) \). We now take traces and get

\[
g(X) = \text{Tr}_{K/\mathbb{Q}}(\alpha h(X)) = \sum_{i=1}^{n} a_i \sum_{j=0}^{i-1} X^j \text{Tr}_{K/\mathbb{Q}}(\alpha \theta^{i-j-1}).
\]

But each \( \theta^{i-j-1} \in \mathcal{O}_K \) here and \( \alpha \in \mathcal{O}^{-1} = \mathcal{J}(\mathcal{O}_K) \) by hypothesis. Thus \( \text{Tr}_{K/\mathbb{Q}}(\alpha \theta^{i-j-1}) \in \mathbb{Z} \), so that \( g(X) \in \mathbb{Z}[X] \) as claimed.

We complete the proof by evaluating \( g(X) \) at \( X = \theta \), giving \( \alpha f'(\alpha) = g(\theta) \in \mathbb{Z}[\theta] \).

**Lemma 2** (Lagrange Interpolation Formula): Suppose \( f(X) = (X - \rho_1) \cdots (X - \rho_n) \in \mathbb{C}[X] \) with distinct roots \( \rho_1, \ldots, \rho_n \). Then

\[
\sum_{i=1}^{n} \frac{\rho_i^{j+1}}{f'(\rho_i)} f(X) = \begin{cases} X^{j+1} & \text{for } j = 0, \ldots, n-2, \\ X^n - f(X) & \text{for } j = n-1. \end{cases}
\]

**Proof:** Fix a \( j \) between 0 and \( n-1 \) for the moment and consider the polynomial

\[
g(X) = X^{j+1} - \sum_{i=1}^{n} \frac{\rho_i^{j+1}}{f'(\rho_i)} f(X).
\]

Note that this is indeed a polynomial since \( (X - \rho_i)|f(X) \) for each \( i \) and \( f'(\rho_i) \neq 0 \) since each \( \rho_i \) is a simple root. We note that \( g(\rho_i) = 0 \) for all \( i \), so that \( g(X) \) has at least \( n \) roots. On the other hand, it’s clear from the definition that the degree of \( g(X) \) is at most the maximum of \( j + 1 \) and \( n - 1 \). This shows that \( g(X) \) is identically 0 if \( j < n - 1 \). In the case \( j = n - 1 \), the polynomials \( g(X) \) and \( f(X) \) share the exact same roots, so that their quotient is a constant; say \( g(X) = \epsilon f(X) \). Since

\[
\lim_{x \to x} \frac{g(X)}{f(X)} = \lim_{x \to x} \frac{X^n}{f(X)} - \sum_{i=1}^{n} \frac{\rho_i^n}{f'(\rho_i)(X - \rho_i)} = 1 - 0,
\]

3
we see that \( g(X) = f(X) \) when \( j = n - 1 \).

**Lemma 3:** With the hypotheses in Lemma 1, for all \( \beta \in \mathbb{Z}[\theta] \) we have \( \text{Tr}_{K/Q}(\beta/f'(\theta)) \in \mathbb{Z} \).

**Proof:** By hypothesis \( \mathbb{Z}[\theta] \) is a \( \mathbb{Z} \)-module with basis \( 1, \ldots, \theta^{n-1} \), so it suffices to prove the lemma for just those elements of \( \mathbb{Z}[\theta] \). We apply Lemma 2 to \( f(X) \) and set \( X = 0 \) to get

\[
\text{Tr}_{K/Q}(\theta^j/f'\theta) = \sum_{i=1}^{n} \frac{\sigma_i(\theta)^j}{f'(\sigma_i(\theta))} = \begin{cases} 
0 & \text{if } 0 \leq j < n - 1, \\
1 & \text{if } j = n - 1.
\end{cases}
\]

For \( \theta \in \mathcal{O}_K \) as in Lemma 1, we see that the principal ideal generated by \( f'(\theta) \), i.e., the different \( \mathfrak{d}(\theta) \), satisfies \( \mathfrak{d}^{-1}\mathfrak{d}(\theta) \subseteq \mathbb{Z}[\theta] \subseteq \mathcal{O}_K \), so that \( \mathfrak{d}(\theta) = \mathfrak{d}f(\theta) \) for some ideal \( f(\theta) \). This ideal is called the **conductor** of the element \( \theta \).

**Theorem 2:** Let \( K \) be a number field and let \( \theta \in \mathcal{O}_K \) be of degree \( [K: Q] \). Then the conductor \( f(\theta) \subseteq \mathbb{Z}[\theta] \) and any ideal \( \mathfrak{A} \subseteq \mathbb{Z}[\theta] \) is divisible by the conductor \( f(\theta) \).

**Proof:** Suppose \( \beta \in f(\theta) \). Then \( \alpha = \beta/f'(\theta) \in \mathfrak{d}^{-1} \), so by Lemma 1 \( \beta = \alpha f'\theta \in \mathbb{Z}[\theta] \).

Now suppose \( \mathfrak{A} \) is an ideal contained in \( \mathbb{Z}[\theta] \). Then \( \text{Tr}_{K/Q}(\alpha/f'(\theta)) \in \mathbb{Z} \) for all \( \alpha \in \mathfrak{A} \) by Lemma 3. This implies by Theorem 1 that \( 1/f'(\theta) \in \mathcal{I}(\mathfrak{A}) = (\mathfrak{d}\mathcal{O})^{-1} \). Thus the principal ideal generated by \( 1/f'(\theta) \) is contained in \( (\mathfrak{A}\mathcal{O})^{-1} \), so that taking inverses yields \( f(\theta)\mathfrak{d} \supseteq \mathfrak{A}\mathcal{O} \). Therefore \( \mathfrak{A} \) is divisible by the conductor of \( \theta \).

**Theorem 3:** For any number field \( K \) the different \( \mathfrak{d} \) is the greatest common divisor of the differentials \( \mathfrak{d}(\theta) \) of all integers \( \theta \in \mathcal{O}_K \).

**Proof:** Fix a prime \( \mathfrak{P} \). We will show that there is a \( \theta \in \mathcal{O}_K \) of degree \( [K: Q] \) whose conductor is not divisible by \( \mathfrak{P} \). This implies that the greatest common divisor of the conductors is \( \mathcal{O}_K \), whence \( \mathfrak{d} \) is the greatest common divisor of all the differentials \( \mathfrak{d}(\theta) \).

The field \( \mathcal{O}_K/\mathfrak{P} \), being finite, has the property that the multiplicative group of non-zero elements is cyclic. In other words, there is an element \( \theta \in \mathcal{O}_K \) such that

\[
\mathcal{O}_K/\mathfrak{P} = \{0 + \mathfrak{P}, \theta + \mathfrak{P}, \ldots, \theta^{N(\mathfrak{P})-1} + \mathfrak{P}\}.
\]

Set

\[
S_0(\theta) = \{0, \ldots, \theta^{N(\mathfrak{P})-1}\}.
\]

Obviously such an element \( \theta \) is not itself in \( \mathfrak{P} \) and is only unique modulo \( \mathfrak{P} \). We will use this flexibility to choose such an element with particular attributes.

First, we may choose \( \theta \) such that \( \theta^{N(\mathfrak{P})} - \theta \not\in \mathfrak{P}^2 \). Indeed, if our original choice of \( \theta \) doesn’t fit the bill, then simply adding an element of \( \mathfrak{P} \setminus \mathfrak{P}^2 \) to it works. Moreover, adding any element of \( \mathfrak{P}^2 \) to our desired choice does no harm here.

Next, let \( p \) be the rational prime element of \( \mathfrak{P} \) and write \( p\mathcal{O}_K = \mathfrak{P}^e \mathfrak{A} \) where \( \mathfrak{A} \) is relatively prime to \( \mathfrak{P} \). By adding a suitable element of \( \mathfrak{P}^2 \) to our \( \theta \) if necessary, we may assume further that \( \theta \in \mathfrak{A} \) and the degree of \( \theta \) is \( [K: Q] \). For any positive integer \( l \) set

\[
S_l(\theta) = \{\gamma_0 + \gamma_1 \alpha + \cdots + \gamma_l \alpha^l: \alpha = \theta^{N(\mathfrak{P})} - \theta, \, \gamma_i \in S_0(\theta)\} \subseteq \mathbb{Z}[\theta].
\]

Then

\[
(*) \quad \mathcal{O}_K/\mathfrak{P}^l = \{\delta + \mathfrak{P}^l: \delta_i \in S_l(\theta)\}.
\]
We claim that \( f(\theta) \) is not divisible by \( \mathfrak{P} \). To see why, write \( N(\mathfrak{a}f(\theta)) = p^k a \) for some rational integer \( a \) relatively prime to \( p \) and some non-negative integer \( k \). Given any \( \beta \in \mathcal{O}_K \), via (*) with \( l = e_\mathfrak{P} k \), there is a \( \rho \in \mathbb{Z}[\theta] \) such that \( \beta - \rho \in \mathfrak{P}^{e_\mathfrak{P} k} \). Now

\[
\frac{(\beta - \rho)a^k}{f'(\theta)} = \frac{(\beta - \rho)a^k N(\mathfrak{a}f(\theta))}{\mathfrak{a}f(\theta)p^k} = \frac{N(\mathfrak{a}f(\theta))}{\mathfrak{a}f(\theta)} \frac{(\beta - \rho)a^k}{\mathfrak{P}^{e_\mathfrak{P} k} \mathfrak{a}^k}.
\]

(Here individual elements are to be interpreted as the corresponding principal fractional ideal.) We thus see that \( (\beta - \rho)a^k / f'(\theta) \in \mathcal{O}_K \subseteq \mathfrak{d}^{-1} \). By Lemma 1

\[
\frac{(\beta - \rho)a^k}{f'(\theta)} = \frac{\rho'}{f'(\theta)}
\]

for some \( \rho' \in \mathbb{Z}[\theta] \). In particular, \( \beta - \rho = \frac{\rho'}{a^k} \). But now \( a\theta^k \beta = a\theta^k \rho + \rho' \in \mathbb{Z}[\theta] \). The upshot is that, since \( \beta \) was arbitrary, the entire principal ideal \( a\theta^k \mathcal{O}_K \subseteq \mathbb{Z}[\theta] \). Finally, by Theorem 2 we see that \( f(\theta) \) is not divisible by \( \mathfrak{P} \), since neither \( a \) nor \( \theta \) are elements of \( \mathfrak{P} \).