More on Fractional Ideals

As has been our practice so far, $\mathbb{K}$ will be a number field with ring of integers $\mathcal{O}_\mathbb{K}$. The upper case script German ("fraktur") font will be used to denote fractional ideals and the lower case Greek font will be used to denote elements of $\mathbb{K}$.

Recall our big result.

Theorem (Fundamental Theorem)
The set of non-zero fractional ideals of $\mathbb{K}$ is a free abelian group on (generated by) the maximal ideals of $\mathcal{O}_\mathbb{K}$.

In particular, any non-zero ideal $I$ can be expressed uniquely as a product of non-zero prime ideals:

$$I = P_{e_1}^{e_1} \cdots P_{e_r}^{e_r}.$$ 

(1)
More on Fractional Ideals

As has been our practice so far,
As has been our practice so far, $K$ will be a number field with ring of integers $\mathcal{O}_K$. 

Recall our big result.

**Theorem (Fundamental Theorem)**

The set of non-zero fractional ideals of $K$ is a free abelian group on (generated by) the maximal ideals of $\mathcal{O}_K$.

In particular, any non-zero ideal $I$ can be expressed uniquely as a product of non-zero prime ideals:

$$I = P_1^{e_1} \cdots P_r^{e_r}.$$ 

(1)
As has been our practice so far, $K$ will be a number field with ring of integers $\mathfrak{O}_K$. The upper case script German (“fraktur”) font will be used to denote fractional ideals and the lower case Greek font will be used to denote elements of $K$. 

Recall our big result.

**Theorem (Fundamental Theorem)**

The set of non-zero fractional ideals of $K$ is a free abelian group on $(generated by) the maximal ideals of $\mathfrak{O}_K$.

In particular, any non-zero ideal $I$ can be expressed uniquely as a product of non-zero prime ideals:

$$I = \mathfrak{P}_e^1 \cdots \mathfrak{P}_e^r.$$
As has been our practice so far, $K$ will be a number field with ring of integers $\mathcal{O}_K$. The upper case script German (“fraktur”) font will be used to denote fractional ideals and the lower case Greek font will be used to denote elements of $K$.

Recall our big result.
As has been our practice so far, \( K \) will be a number field with ring of integers \( \mathfrak{O}_K \). The upper case script German (“fraktur”) font will be used to denote fractional ideals and the lower case Greek font will be used to denote elements of \( K \).

Recall our big result.

**Theorem (Fundamental Theorem)**

*The set of non-zero fractional ideals of \( K \) is a free abelian group on (generated by) the maximal ideals of \( \mathfrak{O}_K \).*
As has been our practice so far, $K$ will be a number field with ring of integers $\mathcal{O}_K$. The upper case script German (“fraktur”) font will be used to denote fractional ideals and the lower case Greek font will be used to denote elements of $K$.

Recall our big result.

**Theorem (Fundamental Theorem)**

The set of non-zero fractional ideals of $K$ is a free abelian group on (generated by) the maximal ideals of $\mathcal{O}_K$.

In particular, any non-zero ideal $\mathfrak{I}$ can be expressed uniquely as a product of non-zero prime ideals:
More on Fractional Ideals

As has been our practice so far, $K$ will be a number field with ring of integers $\mathcal{O}_K$. The upper case script German (“fraktur”) font will be used to denote fractional ideals and the lower case Greek font will be used to denote elements of $K$.

Recall our big result.

**Theorem (Fundamental Theorem)**

The set of non-zero fractional ideals of $K$ is a free abelian group on (generated by) the maximal ideals of $\mathcal{O}_K$.

In particular, any non-zero ideal $\mathfrak{I}$ can be expressed uniquely as a product of non-zero prime ideals:

$$\mathfrak{I} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}. \quad (1)$$
For two non-zero ideals $\mathfrak{A}$ and $\mathfrak{B}$
For two non-zero ideals $A$ and $B$ we are on firm ground saying $A|B$ if $B = AC$ for some non-zero ideal $C$ by the Fundamental Theorem.
For two non-zero ideals $A$ and $B$ we are on firm ground saying $A|B$ if $B = AC$ for some non-zero ideal $C$ by the Fundamental Theorem. Note that $A|B$ if and only if $A \supseteq B$ as sets.
For two non-zero ideals $A$ and $B$ we are on firm ground saying $A | B$ if $B = AC$ for some non-zero ideal $C$ by the Fundamental Theorem. Note that $A | B$ if and only if $A \supseteq B$ as sets.

**Definition**

For a non-zero fractional ideal $I$ as in (1) above,
For two non-zero ideals $A$ and $B$ we are on firm ground saying $A|B$ if $B = AC$ for some non-zero ideal $C$ by the Fundamental Theorem. Note that $A|B$ if and only if $A \supseteq B$ as sets.

**Definition**

For a non-zero fractional ideal $\mathcal{I}$ as in (1) above, the order of $\mathcal{I}$ at the maximal ideal $\mathfrak{p}_i$ is $e_i$ for $i = 1, \ldots, r$. 
For two non-zero ideals $A$ and $B$ we are on firm ground saying $A|B$ if $B = AC$ for some non-zero ideal $C$ by the Fundamental Theorem. Note that $A|B$ if and only if $A \supseteq B$ as sets.

**Definition**

For a non-zero fractional ideal $I$ as in (1) above, the order of $I$ at the maximal ideal $\mathfrak{p}_i$ is $e_i$ for $i = 1, \ldots, r$. For all other maximal ideals $\mathfrak{p}$,
For two non-zero ideals $A$ and $B$ we are on firm ground saying $A|B$ if $B = A\mathcal{C}$ for some non-zero ideal $\mathcal{C}$ by the Fundamental Theorem. Note that $A|B$ if and only if $A \supseteq B$ as sets.

**Definition**

For a non-zero fractional ideal $\mathcal{I}$ as in (1) above, the order of $\mathcal{I}$ at the maximal ideal $\mathfrak{p}_i$ is $e_i$ for $i = 1, \ldots, r$. For all other maximal ideals $\mathfrak{p}$, the order of $\mathcal{I}$ at $\mathfrak{p}$ is 0.
For two non-zero ideals $A$ and $B$ we are on firm ground saying $A|B$ if $B = AC$ for some non-zero ideal $C$ by the Fundamental Theorem. Note that $A|B$ if and only if $A \supseteq B$ as sets.

**Definition**

For a non-zero fractional ideal $I$ as in (1) above, the order of $I$ at the maximal ideal $P_i$ is $e_i$ for $i = 1, \ldots, r$. For all other maximal ideals $P$, the order of $I$ at $P$ is 0. The order of $\mathcal{O}_K$ at $P$ is 0 for all maximal ideals $P$. 
For two non-zero ideals $A$ and $B$ we are on firm ground saying $A|B$ if $B = AC$ for some non-zero ideal $C$ by the Fundamental Theorem. Note that $A|B$ if and only if $A \supseteq B$ as sets.

**Definition**

For a non-zero fractional ideal $I$ as in (1) above, the order of $I$ at the maximal ideal $\mathfrak{p}_i$ is $e_i$ for $i = 1, \ldots, r$. For all other maximal ideals $\mathfrak{p}$, the order of $I$ at $\mathfrak{p}$ is 0. The order of $\mathcal{O}_K$ at $\mathfrak{p}$ is 0 for all maximal ideals $\mathfrak{p}$. We write $\text{ord}_{\mathfrak{p}}(I)$ for the order of $I$ at $\mathfrak{p}$.
For two non-zero ideals \( A \) and \( B \) we are on firm ground saying \( A \mid B \) if \( B = AC \) for some non-zero ideal \( C \) by the Fundamental Theorem. Note that \( A \mid B \) if and only if \( A \supseteq B \) as sets.

**Definition**

For a non-zero fractional ideal \( I \) as in (1) above, the order of \( I \) at the maximal ideal \( \mathfrak{P}_i \) is \( e_i \) for \( i = 1, \ldots, r \). For all other maximal ideals \( \mathfrak{P} \), the order of \( I \) at \( \mathfrak{P} \) is 0. The order of \( \mathcal{O}_K \) at \( \mathfrak{P} \) is 0 for all maximal ideals \( \mathfrak{P} \). We write \( \text{ord}_{\mathfrak{P}}(I) \) for the order of \( I \) at \( \mathfrak{P} \).

By the Fundamental Theorem, any ideal \( I \) is completely determined by the set of numbers
For two non-zero ideals $A$ and $B$ we are on firm ground saying $A | B$ if $B = AC$ for some non-zero ideal $C$ by the Fundamental Theorem. Note that $A | B$ if and only if $A \supseteq B$ as sets.

**Definition**

For a non-zero fractional ideal $I$ as in (1) above, the order of $I$ at the maximal ideal $\mathfrak{p}_i$ is $e_i$ for $i = 1, \ldots, r$. For all other maximal ideals $\mathfrak{p}$, the order of $I$ at $\mathfrak{p}$ is 0. The order of $\mathcal{O}_K$ at $\mathfrak{p}$ is 0 for all maximal ideals $\mathfrak{p}$. We write $\text{ord}_{\mathfrak{p}}(I)$ for the order of $I$ at $\mathfrak{p}$.

By the Fundamental Theorem, any ideal $I$ is completely determined by the set of numbers

$$\{\text{ord}_{\mathfrak{p}}(I) : \mathfrak{p} \text{ a maximal ideal of } \mathcal{O}_K\}.$$
Definition

Given two non-zero ideals \( \mathfrak{A} \) and \( \mathfrak{B} \),

\[
\text{ord}_P(\gcd(\mathfrak{A}, \mathfrak{B})) = \min\{\text{ord}_P(\mathfrak{A}), \text{ord}_P(\mathfrak{B})\},
\]

\[
\text{ord}_P(\lcm(\mathfrak{A}, \mathfrak{B})) = \max\{\text{ord}_P(\mathfrak{A}), \text{ord}_P(\mathfrak{B})\},
\]

for all maximal ideals \( P \).

We say \( \mathfrak{A} \) and \( \mathfrak{B} \) are relatively prime if their greatest common divisor is \( \mathcal{O}_K \).

We will abuse notation just a bit here and extend all of the above to individual non-zero elements \( \alpha \in K \) via principal ideals. For example,

\[
\text{ord}_P(\alpha) = \text{ord}_P((\alpha)),
\]

where \((\alpha)\) is the principal ideal generated by \( \alpha \).
Definition

Given two non-zero ideals $\mathcal{A}$ and $\mathcal{B}$, we define the greatest common divisor $\gcd(\mathcal{A}, \mathcal{B})$

and least common multiple $\text{lcm}(\mathcal{A}, \mathcal{B})$ as follows:

$$\text{ord}_P(\gcd(\mathcal{A}, \mathcal{B})) = \min\{\text{ord}_P(\mathcal{A}), \text{ord}_P(\mathcal{B})\},$$

$$\text{ord}_P(\text{lcm}(\mathcal{A}, \mathcal{B})) = \max\{\text{ord}_P(\mathcal{A}), \text{ord}_P(\mathcal{B})\},$$

for all maximal ideals $P$.

We say $\mathcal{A}$ and $\mathcal{B}$ are relatively prime if their greatest common divisor is $\mathcal{O}$.

We will abuse notation just a bit here and extend all of the above to individual non-zero elements $\alpha \in \mathcal{O}$ via principal ideals.

For example, $\text{ord}_P(\alpha) = \text{ord}_P((\alpha))$, where $(\alpha)$ is the principal ideal generated by $\alpha$. 
Definition

Given two non-zero ideals \( \mathfrak{A} \) and \( \mathfrak{B} \), we define the greatest common divisor \( \gcd(\mathfrak{A}, \mathfrak{B}) \) and least common multiple \( \operatorname{lcm}(\mathfrak{A}, \mathfrak{B}) \) of \( \mathfrak{A} \) and \( \mathfrak{B} \) as follows:

\[
\operatorname{ord}_P(\gcd(\mathfrak{A}, \mathfrak{B})) = \min\{\operatorname{ord}_P(\mathfrak{A}), \operatorname{ord}_P(\mathfrak{B})\},
\]
\[
\operatorname{ord}_P(\operatorname{lcm}(\mathfrak{A}, \mathfrak{B})) = \max\{\operatorname{ord}_P(\mathfrak{A}), \operatorname{ord}_P(\mathfrak{B})\},
\]
for all maximal ideals \( P \).

We say \( \mathfrak{A} \) and \( \mathfrak{B} \) are relatively prime if their greatest common divisor is \( 0 \). We will abuse notation just a bit here and extend all of the above to individual non-zero elements \( \alpha \in K \) via principal ideals. For example, \( \operatorname{ord}_P(\alpha) = \operatorname{ord}_P((\alpha)) \), where \( (\alpha) \) is the principal ideal generated by \( \alpha \).
Definition

Given two non-zero ideals \( A \) and \( B \), we define the greatest common divisor \( \gcd(A, B) \) and least common multiple \( \text{lcm}(A, B) \) of \( A \) and \( B \) as follows:

\[
\text{ord}_P \left( \gcd(A, B) \right) = \min\{ \text{ord}_P(A), \text{ord}_P(B) \},
\]

for all maximal ideals \( P \).

We say \( A \) and \( B \) are relatively prime if their greatest common divisor is \( O_K \).

We will abuse notation just a bit here and extend all of the above to individual non-zero elements \( \alpha \in K \) via principal ideals. For example, \( \text{ord}_P(\alpha) = \text{ord}_P((\alpha)) \), where \((\alpha)\) is the principal ideal generated by \( \alpha \).
Definition

Given two non-zero ideals $\mathcal{A}$ and $\mathcal{B}$, we define the greatest common divisor $\gcd(\mathcal{A}, \mathcal{B})$ and least common multiple $\operatorname{lcm}(\mathcal{A}, \mathcal{B})$ of $\mathcal{A}$ and $\mathcal{B}$ as follows:

\[
\operatorname{ord}_P(\gcd(\mathcal{A}, \mathcal{B})) = \min\{\operatorname{ord}_P(\mathcal{A}), \operatorname{ord}_P(\mathcal{B})\}, \\
\operatorname{ord}_P(\operatorname{lcm}(\mathcal{A}, \mathcal{B})) = \max\{\operatorname{ord}_P(\mathcal{A}), \operatorname{ord}_P(\mathcal{B})\}
\]
Definition

Given two non-zero ideals $\mathfrak{A}$ and $\mathfrak{B}$, we define the greatest common divisor $\gcd(\mathfrak{A}, \mathfrak{B})$ and least common multiple $\lcm(\mathfrak{A}, \mathfrak{B})$ of $\mathfrak{A}$ and $\mathfrak{B}$ as follows:

$$
\text{ord}_\mathfrak{P} (\gcd(\mathfrak{A}, \mathfrak{B})) = \min\{\text{ord}_\mathfrak{P}(\mathfrak{A}), \text{ord}_\mathfrak{P}(\mathfrak{B})\},
$$

$$
\text{ord}_\mathfrak{P} (\lcm(\mathfrak{A}, \mathfrak{B})) = \max\{\text{ord}_\mathfrak{P}(\mathfrak{A}), \text{ord}_\mathfrak{P}(\mathfrak{B})\}
$$

for all maximal ideals $\mathfrak{P}$.

We say $\mathfrak{A}$ and $\mathfrak{B}$ are relatively prime if their greatest common divisor is $\mathcal{O}_K$.
Definition

Given two non-zero ideals \( \mathfrak{A} \) and \( \mathfrak{B} \), we define the greatest common divisor \( \gcd(\mathfrak{A}, \mathfrak{B}) \) and least common multiple \( \lcm(\mathfrak{A}, \mathfrak{B}) \) of \( \mathfrak{A} \) and \( \mathfrak{B} \) as follows:

\[
\ord_{\mathfrak{P}} \left( \gcd(\mathfrak{A}, \mathfrak{B}) \right) = \min \{ \ord_{\mathfrak{P}}(\mathfrak{A}), \ord_{\mathfrak{P}}(\mathfrak{B}) \},
\]
\[
\ord_{\mathfrak{P}} \left( \lcm(\mathfrak{A}, \mathfrak{B}) \right) = \max \{ \ord_{\mathfrak{P}}(\mathfrak{A}), \ord_{\mathfrak{P}}(\mathfrak{B}) \}
\]

for all maximal ideals \( \mathfrak{P} \). We say \( \mathfrak{A} \) and \( \mathfrak{B} \) are relatively prime if their greatest common divisor is \( \mathcal{O}_K \).
Definition

Given two non-zero ideals $\mathfrak{A}$ and $\mathfrak{B}$, we define the greatest common divisor $\gcd(\mathfrak{A}, \mathfrak{B})$ and least common multiple $\lcm(\mathfrak{A}, \mathfrak{B})$ of $\mathfrak{A}$ and $\mathfrak{B}$ as follows:

$$\text{ord}_{\mathfrak{P}}(\gcd(\mathfrak{A}, \mathfrak{B})) = \min\{\text{ord}_{\mathfrak{P}}(\mathfrak{A}), \text{ord}_{\mathfrak{P}}(\mathfrak{B})\},$$

$$\text{ord}_{\mathfrak{P}}(\lcm(\mathfrak{A}, \mathfrak{B})) = \max\{\text{ord}_{\mathfrak{P}}(\mathfrak{A}), \text{ord}_{\mathfrak{P}}(\mathfrak{B})\}$$

for all maximal ideals $\mathfrak{P}$. We say $\mathfrak{A}$ and $\mathfrak{B}$ are relatively prime if their greatest common divisor is $\mathfrak{O}_K$.

We will abuse notation just a bit here and extend all of the above to individual non-zero elements $\alpha \in K$ via principal ideals.
Definition

Given two non-zero ideals \( \mathfrak{A} \) and \( \mathfrak{B} \), we define the greatest common divisor \( \gcd(\mathfrak{A}, \mathfrak{B}) \) and least common multiple \( \lcm(\mathfrak{A}, \mathfrak{B}) \) of \( \mathfrak{A} \) and \( \mathfrak{B} \) as follows:

\[
\text{ord}_\mathfrak{P} \left( \gcd(\mathfrak{A}, \mathfrak{B}) \right) = \min \{ \text{ord}_\mathfrak{P}(\mathfrak{A}), \text{ord}_\mathfrak{P}(\mathfrak{B}) \},
\]

\[
\text{ord}_\mathfrak{P} \left( \lcm(\mathfrak{A}, \mathfrak{B}) \right) = \max \{ \text{ord}_\mathfrak{P}(\mathfrak{A}), \text{ord}_\mathfrak{P}(\mathfrak{B}) \}
\]

for all maximal ideals \( \mathfrak{P} \). We say \( \mathfrak{A} \) and \( \mathfrak{B} \) are relatively prime if their greatest common divisor is \( \mathcal{O}_K \).

We will abuse notation just a bit here and extend all of the above to individual non-zero elements \( \alpha \in K \) via principal ideals. For example, \( \text{ord}_\mathfrak{P}(\alpha) = \text{ord}_\mathfrak{P}((\alpha)) \), where \((\alpha)\) is the principal ideal generated by \( \alpha \).
Note that the $\text{gcd}(A, B)$ is the smallest (set-theoretically) ideal which contains both $A$ and $B$. 

Similarly, the $\text{lcm}(A, B)$ is the largest (set-theoretically) ideal which is contained in both $A$ and $B$. 

It isn't difficult to see that $\text{gcd}(A, B) \cdot \text{lcm}(A, B) = AB$. 
Note that the \( \gcd(A, B) \) is the smallest (set-theoretically) ideal which contains both \( A \) and \( B \). In other words,

\[
\gcd(A, B) = A + B := \{ \alpha + \beta : \alpha \in A, \beta \in B \}.
\]
Note that the \( \gcd(A, B) \) is the smallest (set-theoretically) ideal which contains both \( A \) and \( B \). In other words,

\[
\gcd(A, B) = A + B := \{ \alpha + \beta : \alpha \in A, \ \beta \in B \}.
\]

Similarly, the \( \text{lcm}(A, B) \) is the largest (set-theoretically) ideal which is contained in both \( A \) and \( B \).
Note that the $\text{gcd}(A, B)$ is the smallest (set-theoretically) ideal which contains both $A$ and $B$. In other words,

$$\text{gcd}(A, B) = A + B := \{ \alpha + \beta : \alpha \in A, \beta \in B \}.$$ 

Similarly, the $\text{lcm}(A, B)$ is the largest (set-theoretically) ideal which is contained in both $A$ and $B$. It isn’t difficult to see that $\text{gcd}(A, B) \text{lcm}(A, B) = AB$. 
Clearly $\text{ord}_\mathfrak{p}(\mathfrak{AB}) = \text{ord}_\mathfrak{p}(\mathfrak{A}) + \text{ord}_\mathfrak{p}(\mathfrak{B})$. 
Clearly $\text{ord}_\mathfrak{p}(AB) = \text{ord}_\mathfrak{p}(A) + \text{ord}_\mathfrak{p}(B)$. Since $A + B = \gcd(A, B)$, we have $\text{ord}_\mathfrak{p}(A + B) = \min\{\text{ord}_\mathfrak{p}(A), \text{ord}_\mathfrak{p}(B)\}$. 

Lemma (1)

Let $A$ be a non-zero ideal and $\alpha \in O_K \setminus \{0\}$. Then there is a non-zero ideal $B$ with $AB = (\alpha)$ if and only if $\alpha \in A$. 

Proof: By the Fundamental Theorem $AB = (\alpha)$ if and only if $B = (\alpha)A^{-1}$, and $(\alpha)A^{-1} \subseteq O_K$ if and only if $(\alpha) \subseteq A$. 

Clearly \( \text{ord}_\mathfrak{P}(AB) = \text{ord}_\mathfrak{P}(A) + \text{ord}_\mathfrak{P}(B) \). Since \( A + B = \gcd(A, B) \), we have \( \text{ord}_\mathfrak{P}(A + B) = \min\{\text{ord}_\mathfrak{P}(A), \text{ord}_\mathfrak{P}(B)\} \). However, it is not generally the case that \((\alpha) + (\beta) = (\alpha + \beta)\) for \( \alpha, \beta \in \mathcal{O}_K \).
Clearly $\text{ord}_\mathfrak{p}(AB) = \text{ord}_\mathfrak{p}(A) + \text{ord}_\mathfrak{p}(B)$. Since $A + B = \gcd(A, B)$, we have $\text{ord}_\mathfrak{p}(A + B) = \min\{\text{ord}_\mathfrak{p}(A), \text{ord}_\mathfrak{p}(B)\}$. However, it is not generally the case that $(\alpha) + (\beta) = (\alpha + \beta)$ for $\alpha, \beta \in \mathcal{O}_K$. Since $(\alpha) + (\beta)|(\alpha + \beta)$,
Clearly \( \text{ord}_\mathfrak{p}(AB) = \text{ord}_\mathfrak{p}(A) + \text{ord}_\mathfrak{p}(B) \). Since \( A + B = \gcd(A, B) \), we have \( \text{ord}_\mathfrak{p}(A + B) = \min\{\text{ord}_\mathfrak{p}(A), \text{ord}_\mathfrak{p}(B)\} \). However, it is not generally the case that \((\alpha) + (\beta) = (\alpha + \beta)\) for \( \alpha, \beta \in \mathcal{O}_K \). Since \((\alpha) + (\beta) | (\alpha + \beta)\), we do have

\[
\text{ord}_\mathfrak{p}(\alpha + \beta) \geq \min\{\text{ord}_\mathfrak{p}(\alpha), \text{ord}_\mathfrak{p}(\beta)\}.
\]
Clearly \( \text{ord}_P(AB) = \text{ord}_P(A) + \text{ord}_P(B) \). Since \( A + B = \gcd(A, B) \), we have \( \text{ord}_P(A + B) = \min\{\text{ord}_P(A), \text{ord}_P(B)\} \). However, it is not generally the case that \((\alpha) + (\beta) = (\alpha + \beta)\) for \(\alpha, \beta \in \mathcal{O}_K\). Since \((\alpha) + (\beta)\mid(\alpha + \beta)\), we do have

\[
\text{ord}_P(\alpha + \beta) \geq \min\{\text{ord}_P(\alpha), \text{ord}_P(\beta)\}.
\]

One can check that this is an equality whenever \(\text{ord}_P(\alpha) \neq \text{ord}_P(\beta)\).
Clearly \( \text{ord}_\mathfrak{p}(AB) = \text{ord}_\mathfrak{p}(A) + \text{ord}_\mathfrak{p}(B) \). Since \( A + B = \gcd(A, B) \), we have \( \text{ord}_\mathfrak{p}(A + B) = \min\{\text{ord}_\mathfrak{p}(A), \text{ord}_\mathfrak{p}(B)\} \). However, it is not generally the case that \((\alpha) + (\beta) = (\alpha + \beta)\) for \(\alpha, \beta \in \mathcal{O}_K\). Since \((\alpha) + (\beta) \mid (\alpha + \beta)\), we do have

\[
\text{ord}_\mathfrak{p}(\alpha + \beta) \geq \min\{\text{ord}_\mathfrak{p}(\alpha), \text{ord}_\mathfrak{p}(\beta)\}.
\]

One can check that this is an equality whenever \(\text{ord}_\mathfrak{p}(\alpha) \neq \text{ord}_\mathfrak{p}(\beta)\).

**Lemma (1)**
Clearly \( \text{ord}\_P(\mathfrak{AB}) = \text{ord}\_P(\mathfrak{A}) + \text{ord}\_P(\mathfrak{B}) \). Since \( \mathfrak{A} + \mathfrak{B} = \gcd(\mathfrak{A}, \mathfrak{B}) \), we have \( \text{ord}\_P(\mathfrak{A} + \mathfrak{B}) = \min\{\text{ord}\_P(\mathfrak{A}), \text{ord}\_P(\mathfrak{B})\} \). However, it is not generally the case that \((\alpha) + (\beta) = (\alpha + \beta)\) for \(\alpha, \beta \in \mathfrak{O}_K\). Since \((\alpha) + (\beta) | (\alpha + \beta)\), we do have

\[
\text{ord}\_P(\alpha + \beta) \geq \min\{\text{ord}\_P(\alpha), \text{ord}\_P(\beta)\}.
\]

One can check that this is an equality whenever \(\text{ord}\_P(\alpha) \neq \text{ord}\_P(\beta)\).

**Lemma (1)**

*Let \(\mathfrak{A}\) be a non-zero ideal and \(\alpha \in \mathfrak{O}_K \setminus \{0\}\).*
Clearly \( \text{ord}_\mathfrak{P}(AB) = \text{ord}_\mathfrak{P}(A) + \text{ord}_\mathfrak{P}(B) \). Since \( A + B = \gcd(A, B) \), we have \( \text{ord}_\mathfrak{P}(A + B) = \min\{\text{ord}_\mathfrak{P}(A), \text{ord}_\mathfrak{P}(B)\} \). However, it is not generally the case that \((\alpha) + (\beta) = (\alpha + \beta)\) for \( \alpha, \beta \in \mathcal{O}_K \). Since \((\alpha) + (\beta)|(\alpha + \beta)\), we do have

\[
\text{ord}_\mathfrak{P}(\alpha + \beta) \geq \min\{\text{ord}_\mathfrak{P}(\alpha), \text{ord}_\mathfrak{P}(\beta)\}.
\]

One can check that this is an equality whenever \( \text{ord}_\mathfrak{P}(\alpha) \neq \text{ord}_\mathfrak{P}(\beta) \).

**Lemma (1)**

*Let \( \mathfrak{A} \) be a non-zero ideal and \( \alpha \in \mathcal{O}_K \setminus \{0\} \). Then there is a non-zero ideal \( \mathfrak{B} \) with \( \mathfrak{A}\mathfrak{B} = (\alpha) \) if and only if \( \alpha \in \mathfrak{A} \).*
Clearly \( \text{ord}_\mathfrak{p}(AB) = \text{ord}_\mathfrak{p}(A) + \text{ord}_\mathfrak{p}(B) \). Since \( A + B = \gcd(A, B) \), we have \( \text{ord}_\mathfrak{p}(A + B) = \min\{\text{ord}_\mathfrak{p}(A), \text{ord}_\mathfrak{p}(B)\} \). However, it is not generally the case that \((\alpha) + (\beta) = (\alpha + \beta)\) for \( \alpha, \beta \in \mathcal{O}_K \). Since \((\alpha) + (\beta)|(\alpha + \beta)\), we do have

\[
\text{ord}_\mathfrak{p}(\alpha + \beta) \geq \min\{\text{ord}_\mathfrak{p}(\alpha), \text{ord}_\mathfrak{p}(\beta)\}.
\]

One can check that this is an equality whenever \( \text{ord}_\mathfrak{p}(\alpha) \neq \text{ord}_\mathfrak{p}(\beta) \).

**Lemma (1)**

Let \( A \) be a non-zero ideal and \( \alpha \in \mathcal{O}_K \setminus \{0\} \). Then there is a non-zero ideal \( B \) with \( AB = (\alpha) \) if and only if \( \alpha \in A \).

**Proof:**
Clearly $\text{ord}_\mathfrak{p}(\mathfrak{AB}) = \text{ord}_\mathfrak{p}(\mathfrak{A}) + \text{ord}_\mathfrak{p}(\mathfrak{B})$. Since $\mathfrak{A} + \mathfrak{B} = \gcd(\mathfrak{A}, \mathfrak{B})$, we have $\text{ord}_\mathfrak{p}(\mathfrak{A} + \mathfrak{B}) = \min\{\text{ord}_\mathfrak{p}(\mathfrak{A}), \text{ord}_\mathfrak{p}(\mathfrak{B})\}$. However, it is not generally the case that $(\alpha) + (\beta) = (\alpha + \beta)$ for $\alpha, \beta \in \mathfrak{O}_K$. Since $(\alpha) + (\beta)|(\alpha + \beta)$, we do have

$$\text{ord}_\mathfrak{p}(\alpha + \beta) \geq \min\{\text{ord}_\mathfrak{p}(\alpha), \text{ord}_\mathfrak{p}(\beta)\}.$$ 

One can check that this is an equality whenever $\text{ord}_\mathfrak{p}(\alpha) \neq \text{ord}_\mathfrak{p}(\beta)$.

**Lemma (1)**

*Let $\mathfrak{A}$ be a non-zero ideal and $\alpha \in \mathfrak{O}_K \setminus \{0\}$. Then there is a non-zero ideal $\mathfrak{B}$ with $\mathfrak{AB} = (\alpha)$ if and only if $\alpha \in \mathfrak{A}$.***

**Proof:** By the Fundamental Theorem $\mathfrak{AB} = (\alpha)$ if and only if $\mathfrak{B} = (\alpha)\mathfrak{A}^{-1}$,
Clearly \( \text{ord}_P(AB) = \text{ord}_P(A) + \text{ord}_P(B) \). Since \( A + B = \gcd(A, B) \), we have \( \text{ord}_P(A + B) = \min\{\text{ord}_P(A), \text{ord}_P(B)\} \). However, it is not generally the case that \((\alpha) + (\beta) = (\alpha + \beta)\) for \( \alpha, \beta \in \mathcal{O}_K \). Since \((\alpha) + (\beta) \mid (\alpha + \beta)\), we do have

\[
\text{ord}_P(\alpha + \beta) \geq \min\{\text{ord}_P(\alpha), \text{ord}_P(\beta)\}.
\]

One can check that this is an equality whenever \( \text{ord}_P(\alpha) \neq \text{ord}_P(\beta) \).

**Lemma (1)**

Let \( \mathcal{A} \) be a non-zero ideal and \( \alpha \in \mathcal{O}_K \setminus \{0\} \). Then there is a non-zero ideal \( \mathcal{B} \) with \( \mathcal{A}\mathcal{B} = (\alpha) \) if and only if \( \alpha \in \mathcal{A} \).

**Proof:** By the Fundamental Theorem \( \mathcal{A}\mathcal{B} = (\alpha) \) if and only if \( \mathcal{B} = (\alpha)\mathcal{A}^{-1} \), and \( (\alpha)\mathcal{A}^{-1} \subseteq \mathcal{O}_K \) if and only if \( (\alpha) \subseteq \mathcal{A} \).
Lemma (2)

Let $A$ and $B$ be non-zero ideals. Then there is an $\alpha \in A$ with $\gcd((\alpha), AB) = A$.

Proof: This is obvious if $A = O_K$, so assume $A \neq O_K$.

Let $P_1, \ldots, P_r$ be the maximal ideals occurring in the unique factorization of $AB$.

To ease notation here, let $e_i = \text{ord}_{P_i}(A)$ for $i = 1, \ldots, r$.

Define $A_i = AP_1 \cdots P_r P_i^{-e_i-1}$, $i = 1, \ldots, r$.

Note that $\text{ord}_{P_j}(A_i) = \begin{cases} 0 & \text{if } i = j, \\ e_j + 1 & \text{otherwise}. \end{cases}$

Thus, $\gcd(A_1, \ldots, A_r) = O_K$, which implies that there are $\alpha_i \in A_i$ for $i = 1, \ldots, r$ with $\alpha_1 + \cdots + \alpha_r = 1$. (2)
Lemma (2)

Let $\mathfrak{A}$ and $\mathfrak{B}$ be non-zero ideals.

Proof: This is obvious if $\mathfrak{A} = \mathcal{O}_K$ (just use $\alpha = 1$), so assume $\mathfrak{A} \neq \mathcal{O}_K$.

Let $P_1, \ldots, P_r$ be the maximal ideals occurring in the unique factorization of $\mathfrak{A}\mathfrak{B}$.

To ease notation here, let $e_i = \text{ord}_{P_i}(\mathfrak{A})$ for $i = 1, \ldots, r$.

Define $A_i = \mathfrak{A}P_1 \cdots P_r P_i^{-e_i-1}$, $i = 1, \ldots, r$.

Note that $\text{ord}_{P_j}(A_i) = \begin{cases} 0 & \text{if } i = j, \\ e_j + 1 & \text{otherwise}. \end{cases}$

Thus, $\gcd(A_1, \ldots, A_r) = \mathcal{O}_K$, which implies that there are $\alpha_i \in A_i$ for $i = 1, \ldots, r$ with $\alpha_1 + \cdots + \alpha_r = 1$. (2)
Lemma (2)

Let \( \mathcal{A} \) and \( \mathcal{B} \) be non-zero ideals. Then there is an \( \alpha \in \mathcal{A} \) with \( \gcd((\alpha), \mathcal{A}\mathcal{B}) = \mathcal{A} \).
Lemma (2)

Let $\mathcal{A}$ and $\mathcal{B}$ be non-zero ideals. Then there is an $\alpha \in \mathcal{A}$ with $\gcd((\alpha), \mathcal{A}\mathcal{B}) = \mathcal{A}$.

Proof:
Lemma (2)

Let $\mathcal{A}$ and $\mathcal{B}$ be non-zero ideals. Then there is an $\alpha \in \mathcal{A}$ with $\gcd((\alpha), \mathcal{A}\mathcal{B}) = \mathcal{A}$.

Proof: This is obvious if $\mathcal{A} = \mathcal{O}_K$.
Lemma (2)

Let $\mathfrak{A}$ and $\mathfrak{B}$ be non-zero ideals. Then there is an $\alpha \in \mathfrak{A}$ with $\gcd (\langle \alpha \rangle, \mathfrak{AB}) = \mathfrak{A}$.

Proof: This is obvious if $\mathfrak{A} = \mathcal{O}_K$ (just use $\alpha = 1$),
Lemma (2)

Let \( \mathfrak{A} \) and \( \mathfrak{B} \) be non-zero ideals. Then there is an \( \alpha \in \mathfrak{A} \) with \( \gcd (\alpha, \mathfrak{A}\mathfrak{B}) = \mathfrak{A} \).

**Proof:** This is obvious if \( \mathfrak{A} = \mathcal{O}_K \) (just use \( \alpha = 1 \)), so assume \( \mathfrak{A} \neq \mathcal{O}_K \).
Lemma (2)

Let $\mathcal{A}$ and $\mathcal{B}$ be non-zero ideals. Then there is an $\alpha \in \mathcal{A}$ with $\gcd((\alpha), \mathcal{A}\mathcal{B}) = \mathcal{A}$.

Proof: This is obvious if $\mathcal{A} = \mathcal{O}_K$ (just use $\alpha = 1$), so assume $\mathcal{A} \neq \mathcal{O}_K$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the maximal ideals occurring in the unique factorization of $\mathcal{A}\mathcal{B}$.
Lemma (2)

Let $\mathcal{A}$ and $\mathcal{B}$ be non-zero ideals. Then there is an $\alpha \in \mathcal{A}$ with $\gcd((\alpha), \mathcal{AB}) = \mathcal{A}$.

Proof: This is obvious if $\mathcal{A} = \mathcal{O}_K$ (just use $\alpha = 1$), so assume $\mathcal{A} \neq \mathcal{O}_K$. Let $\mathcal{P}_1, \ldots, \mathcal{P}_r$ be the maximal ideals occurring in the unique factorization of $\mathcal{AB}$. To ease notation here, let $e_i = \text{ord}_{\mathcal{P}_i}(\mathcal{A})$ for $i = 1, \ldots, r$. 
Lemma (2)

Let $\mathfrak{A}$ and $\mathfrak{B}$ be non-zero ideals. Then there is an $\alpha \in \mathfrak{A}$ with $\gcd((\alpha), \mathfrak{A}\mathfrak{B}) = \mathfrak{A}$.

Proof: This is obvious if $\mathfrak{A} = \mathcal{O}_K$ (just use $\alpha = 1$), so assume $\mathfrak{A} \neq \mathcal{O}_K$. Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ be the maximal ideals occurring in the unique factorization of $\mathfrak{A}\mathfrak{B}$. To ease notation here, let $e_i = \text{ord}_{\mathfrak{P}_i}(\mathfrak{A})$ for $i = 1, \ldots, r$. Define

$$\mathfrak{A}_i = \mathfrak{A}\mathfrak{P}_1 \cdots \mathfrak{P}_r \mathfrak{P}_i^{-e_i - 1}, \quad i = 1, \ldots, r.$$
Lemma (2)

Let \( \mathcal{A} \) and \( \mathcal{B} \) be non-zero ideals. Then there is an \( \alpha \in \mathcal{A} \) with \( \gcd((\alpha), \mathcal{A}\mathcal{B}) = \mathcal{A} \).

**Proof:** This is obvious if \( \mathcal{A} = \mathcal{O}_K \) (just use \( \alpha = 1 \)), so assume \( \mathcal{A} \neq \mathcal{O}_K \). Let \( \mathfrak{P}_1, \ldots, \mathfrak{P}_r \) be the maximal ideals occurring in the unique factorization of \( \mathcal{A}\mathcal{B} \). To ease notation here, let \( e_i = \text{ord}_{\mathfrak{P}_i}(\mathcal{A}) \) for \( i = 1, \ldots, r \).

Define

\[
\mathcal{A}_i = \mathcal{A}\mathfrak{P}_1 \cdots \mathfrak{P}_r \mathfrak{P}_i^{-e_i-1}, \quad i = 1, \ldots, r.
\]

Note that

\[
\text{ord}_{\mathfrak{P}_j}(\mathcal{A}_i) = \begin{cases} 
0 & \text{if } i = j, \\
e_j + 1 \geq 1 & \text{otherwise}.
\end{cases}
\]
Lemma (2)

Let $\mathcal{A}$ and $\mathcal{B}$ be non-zero ideals. Then there is an $\alpha \in \mathcal{A}$ with $\gcd((\alpha), \mathcal{A}\mathcal{B}) = \mathcal{A}$.

Proof: This is obvious if $\mathcal{A} = \mathcal{O}_K$ (just use $\alpha = 1$), so assume $\mathcal{A} \neq \mathcal{O}_K$. Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ be the maximal ideals occurring in the unique factorization of $\mathcal{A}\mathcal{B}$. To ease notation here, let $e_i = \text{ord}_{\mathfrak{P}_i}(\mathcal{A})$ for $i = 1, \ldots, r$. Define

$$\mathcal{A}_i = \mathcal{A}\mathfrak{P}_1 \cdots \mathfrak{P}_r \mathfrak{P}_i^{-e_i-1}, \quad i = 1, \ldots, r.$$ 

Note that

$$\text{ord}_{\mathfrak{P}_i}(\mathcal{A}_i) = \begin{cases} 0 & \text{if } i = j, \\ e_j + 1 \geq 1 & \text{otherwise.} \end{cases}$$

Thus, $\gcd(\mathcal{A}_1, \ldots, \mathcal{A}_r) = \mathcal{O}_K$, 

Lemma (2)

Let $\mathcal{A}$ and $\mathcal{B}$ be non-zero ideals. Then there is an $\alpha \in \mathcal{A}$ with $\gcd((\alpha), \mathcal{A}\mathcal{B}) = \mathcal{A}$.

Proof: This is obvious if $\mathcal{A} = \mathcal{O}_K$ (just use $\alpha = 1$), so assume $\mathcal{A} \neq \mathcal{O}_K$. Let $\mathcal{P}_1, \ldots, \mathcal{P}_r$ be the maximal ideals occurring in the unique factorization of $\mathcal{A}\mathcal{B}$. To ease notation here, let $e_i = \text{ord}_{\mathcal{P}_i}(\mathcal{A})$ for $i = 1, \ldots, r$.

Define

$$\mathcal{A}_i = \mathcal{A}\mathcal{P}_1 \cdots \mathcal{P}_i \mathcal{P}_i^{e_i - 1}, \quad i = 1, \ldots, r.$$  

Note that

$$\text{ord}_{\mathcal{P}_i}(\mathcal{A}_i) = \begin{cases} 0 & \text{if } i = j, \\ e_j + 1 & \geq 1 \text{ otherwise}. \end{cases}$$

Thus, $\gcd(\mathcal{A}_1, \ldots, \mathcal{A}_r) = \mathcal{O}_K$, which implies that there are $\alpha_i \in \mathcal{A}_i$ for $i = 1, \ldots, r$ with

$$\alpha_1 + \cdots + \alpha_r = 1.$$  \hspace{1cm} (2)
Since each $\alpha_i \in A_i$ we have

$$\text{ord}_{\mathfrak{P}_j}(\alpha_i) \geq \text{ord}_{\mathfrak{P}_j}(A_i) = e_j + 1 \geq 1 \quad i \neq j.$$  \hspace{1cm} (3)
Since each $\alpha_i \in \mathcal{A}_i$ we have

$$\text{ord}_{\mathfrak{P}_j}(\alpha_i) \geq \text{ord}_{\mathfrak{P}_j}(\mathcal{A}_i) = e_j + 1 \geq 1 \quad i \neq j.$$  \hfill (3)

Since $\text{ord}_{\mathfrak{P}}(1) = 0$ for all maximal ideals $\mathfrak{P}$,
Since each $\alpha_i \in \mathcal{A}_i$ we have

$$\text{ord}_{\mathcal{P}_j}(\alpha_i) \geq \text{ord}_{\mathcal{P}_j}(\mathcal{A}_i) = e_j + 1 \geq 1 \quad i \neq j.$$ (3)

Since $\text{ord}_{\mathcal{P}}(1) = 0$ for all maximal ideals $\mathcal{P}$, (2) and (3) imply that

$$\text{ord}_{\mathcal{P}_i}(\alpha_i) = 0, \quad i = 1, \ldots, r.$$ (4)
Since each $\alpha_i \in \mathcal{A}_i$ we have
\[ \text{ord}_{\mathfrak{P}_j}(\alpha_i) \geq \text{ord}_{\mathfrak{P}_j}(\mathcal{A}_i) = e_j + 1 \geq 1 \quad i \neq j. \] (3)

Since $\text{ord}_{\mathfrak{P}}(1) = 0$ for all maximal ideals $\mathfrak{P}$, (2) and (3) imply that
\[ \text{ord}_{\mathfrak{P}_i}(\alpha_i) = 0, \quad i = 1, \ldots, r. \] (4)

Now choose $\beta_i \in \mathfrak{P}_i^{e_i} \setminus \mathfrak{P}_i^{e_i+1}$ for all $i = 1, \ldots, r$.
Since each $\alpha_i \in \mathcal{A}_i$ we have

$$\text{ord}_{\mathfrak{p}_j}(\alpha_i) \geq \text{ord}_{\mathfrak{p}_j}(\mathcal{A}_i) = e_j + 1 \geq 1 \quad i \neq j. \quad (3)$$

Since $\text{ord}_{\mathfrak{p}}(1) = 0$ for all maximal ideals $\mathfrak{p}$, (2) and (3) imply that

$$\text{ord}_{\mathfrak{p}_i}(\alpha_i) = 0, \quad i = 1, \ldots, r. \quad (4)$$

Now choose $\beta_i \in \mathfrak{p}_i^{e_i} \setminus \mathfrak{p}_i^{e_i+1}$ for all $i = 1, \ldots, r$ and let

$$\alpha = \alpha_1 \beta_1 + \cdots + \alpha_r \beta_r.$$
Since each $\alpha_i \in A_i$ we have

$$\text{ord}_{\mathfrak{P}_j}(\alpha_i) \geq \text{ord}_{\mathfrak{P}_j}(A_i) = e_j + 1 \geq 1 \quad i \neq j.$$  \hfill (3)

Since $\text{ord}_{\mathfrak{P}}(1) = 0$ for all maximal ideals $\mathfrak{P}$, (2) and (3) imply that

$$\text{ord}_{\mathfrak{P}_i}(\alpha_i) = 0, \quad i = 1, \ldots, r.$$  \hfill (4)

Now choose $\beta_i \in \mathfrak{P}_i^{e_i} \setminus \mathfrak{P}_i^{e_i+1}$ for all $i = 1, \ldots, r$ and let

$$\alpha = \alpha_1 \beta_1 + \cdots + \alpha_r \beta_r.$$

By construction we have $\text{ord}_{\mathfrak{P}_i}(\beta_i) = e_i$ for all $i = 1, \ldots, r$. 

Math 681, Monday, February 1
Since each $\alpha_i \in A_i$ we have
\[
\text{ord}_{\mathfrak{p}_j}(\alpha_i) \geq \text{ord}_{\mathfrak{p}_j}(A_i) = e_j + 1 \geq 1 \quad i \neq j.
\] (3)

Since $\text{ord}_{\mathfrak{p}}(1) = 0$ for all maximal ideals $\mathfrak{p}$, (2) and (3) imply that
\[
\text{ord}_{\mathfrak{p}_i}(\alpha_i) = 0, \quad i = 1, \ldots, r.
\] (4)

Now chose $\beta_i \in \mathfrak{p}_i^{e_i} \setminus \mathfrak{p}_i^{e_i+1}$ for all $i = 1, \ldots, r$ and let
\[
\alpha = \alpha_1 \beta_1 + \cdots + \alpha_r \beta_r.
\]

By construction we have $\text{ord}_{\mathfrak{p}_i}(\beta_i) = e_i$ for all $i = 1, \ldots, r$. This together with (3) and (4) show that
\[
\text{ord}_{\mathfrak{p}_i}(\alpha) = e_i, \quad i = 1, \ldots, r.
\]
Since each $\alpha_i \in \mathfrak{A}_i$ we have

$$\text{ord}_{\mathfrak{P}_j}(\alpha_i) \geq \text{ord}_{\mathfrak{P}_j}(\mathfrak{A}_i) = e_j + 1 \geq 1 \quad i \neq j. \quad (3)$$

Since $\text{ord}_{\mathfrak{P}}(1) = 0$ for all maximal ideals $\mathfrak{P}$, (2) and (3) imply that

$$\text{ord}_{\mathfrak{P}_i}(\alpha_i) = 0, \quad i = 1, \ldots, r. \quad (4)$$

Now choose $\beta_i \in \mathfrak{P}_i^{e_i} \setminus \mathfrak{P}_i^{e_i+1}$ for all $i = 1, \ldots, r$ and let

$$\alpha = \alpha_1 \beta_1 + \cdots + \alpha_r \beta_r.$$

By construction we have $\text{ord}_{\mathfrak{P}_i}(\beta_i) = e_i$ for all $i = 1, \ldots, r$. This together with (3) and (4) show that

$$\text{ord}_{\mathfrak{P}_i}(\alpha) = e_i, \quad i = 1, \ldots, r.$$

Since $\text{ord}_{\mathfrak{P}}(AB) = 0$ for all $\mathfrak{P}$ not among $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$, ...
Since each $\alpha_i \in \mathbb{A}_i$ we have

$$\text{ord}_{\mathfrak{P}_j}(\alpha_i) \geq \text{ord}_{\mathfrak{P}_j}(\mathbb{A}_i) = e_j + 1 \geq 1 \quad i \neq j.$$  \hspace{1cm} (3)

Since $\text{ord}_{\mathfrak{P}_i}(1) = 0$ for all maximal ideals $\mathfrak{P}$, (2) and (3) imply that

$$\text{ord}_{\mathfrak{P}_i}(\alpha_i) = 0, \quad i = 1, \ldots, r.$$ \hspace{1cm} (4)

Now choose $\beta_i \in \mathfrak{P}^{e_i}_i \setminus \mathfrak{P}^{e_i+1}_i$ for all $i = 1, \ldots, r$ and let

$$\alpha = \alpha_1\beta_1 + \cdots + \alpha_r\beta_r.$$

By construction we have $\text{ord}_{\mathfrak{P}_i}(\beta_i) = e_i$ for all $i = 1, \ldots, r$. This together with (3) and (4) show that

$$\text{ord}_{\mathfrak{P}_i}(\alpha) = e_i, \quad i = 1, \ldots, r.$$

Since $\text{ord}_{\mathfrak{P}}(\mathbb{A}\mathbb{B}) = 0$ for all $\mathfrak{P}$ not among $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$, we have $\gcd((\alpha), \mathbb{A}\mathbb{B}) = \mathbb{A}$. 
Combining Lemmas 1 and 2 gives us the following result.
Combining Lemmas 1 and 2 gives us the following result.

**Lemma (3)**

Let \( A \) be a non-zero ideal and let \( \beta \in A \setminus \{0\} \).

Then there is an \( \alpha \in A \) with \( \gcd(\alpha, \beta) = A \).

In particular, all non-zero ideals can be viewed as the greatest common divisor of two algebraic integers.

We can speak of congruences in \( \mathcal{O}_K \) in much the same way we do in \( \mathbb{Z} \).

Specifically, for a non-zero ideal \( A \) and \( \alpha, \beta \in \mathcal{O}_K \), we say \( \alpha \) is congruent to \( \beta \) modulo \( A \) if \( \alpha - \beta \in A \).

We denote this more compactly by writing \( \alpha \equiv \beta \mod A \).

A more "advanced" way to say this is \( \alpha + A = \beta + A \) as elements of the quotient ring \( \mathcal{O}_K / A \).
Combining Lemmas 1 and 2 gives us the following result.

**Lemma (3)**

Let $\mathfrak{a}$ be a non-zero ideal and let $\beta \in \mathfrak{a} \setminus \{0\}$.

Let $\mathfrak{a}$ be a non-zero ideal and let $\beta \in \mathfrak{a} \setminus \{0\}$. Then there is an $\alpha \in \mathfrak{a}$ with $\gcd(\alpha, \beta) = \mathfrak{a}$.

In particular, all non-zero ideals can be viewed as the greatest common divisor of two algebraic integers.

We can speak of congruences in $\mathcal{O}_K$ in much the same way we do in $\mathbb{Z}$.

Specifically, for a non-zero ideal $\mathfrak{a}$ and $\alpha, \beta \in \mathcal{O}_K$, we say $\alpha$ is congruent to $\beta$ modulo $\mathfrak{a}$ if $\alpha - \beta \in \mathfrak{a}$.

We denote this more compactly by writing $\alpha \equiv \beta \mod \mathfrak{a}$.

A more "advanced" way to say this is $\alpha + \mathfrak{a} = \beta + \mathfrak{a}$ as elements of the quotient ring $\mathcal{O}_K / \mathfrak{a}$. 
Combining Lemmas 1 and 2 gives us the following result.

**Lemma (3)**

Let $\mathfrak{A}$ be a non-zero ideal and let $\beta \in \mathfrak{A} \setminus \{0\}$. Then there is an $\alpha \in \mathfrak{A}$ with $\gcd(\alpha, \beta) = \mathfrak{A}$. 

In particular, all non-zero ideals can be viewed as the greatest common divisor of two algebraic integers.

We can speak of congruences in $\mathcal{O}_K$ in much the same way we do in $\mathbb{Z}$.

Specifically, for a non-zero ideal $\mathfrak{A}$ and $\alpha, \beta \in \mathcal{O}_K$, we say $\alpha$ is congruent to $\beta$ modulo $\mathfrak{A}$ if $\alpha - \beta \in \mathfrak{A}$. We denote this more compactly by writing $\alpha \equiv \beta \pmod{\mathfrak{A}}$.

A more "advanced" way to say this is $\alpha + \mathfrak{A} = \beta + \mathfrak{A}$ as elements of the quotient ring $\mathcal{O}_K / \mathfrak{A}$. 
Combining Lemmas 1 and 2 gives us the following result.

**Lemma (3)**

Let $\mathfrak{A}$ be a non-zero ideal and let $\beta \in \mathfrak{A} \setminus \{0\}$. Then there is an $\alpha \in \mathfrak{A}$ with $\gcd(\alpha, \beta) = \mathfrak{A}$. In particular, all non-zero ideals can be viewed as the greatest common divisor of two algebraic integers.
Combining Lemmas 1 and 2 gives us the following result.

**Lemma (3)**

Let $\mathcal{A}$ be a non-zero ideal and let $\beta \in \mathcal{A} \setminus \{0\}$. Then there is an $\alpha \in \mathcal{A}$ with $\gcd(\alpha, \beta) = \mathcal{A}$. In particular, all non-zero ideals can be viewed as the greatest common divisor of two algebraic integers.

We can speak of congruences in $\mathcal{O}_K$ in much the same way we do in $\mathbb{Z}$. 
Combining Lemmas 1 and 2 gives us the following result.

**Lemma (3)**

Let \( \mathfrak{A} \) be a non-zero ideal and let \( \beta \in \mathfrak{A} \setminus \{0\} \). Then there is an \( \alpha \in \mathfrak{A} \) with \( \gcd(\alpha, \beta) = \mathfrak{A} \). In particular, all non-zero ideals can be viewed as the greatest common divisor of two algebraic integers.

We can speak of congruences in \( \mathfrak{O}_K \) in much the same way we do in \( \mathbb{Z} \). Specifically, for a non-zero ideal \( \mathfrak{A} \) and \( \alpha, \beta \in \mathfrak{O}_K \),
Combining Lemmas 1 and 2 gives us the following result.

**Lemma (3)**

Let $\mathfrak{A}$ be a non-zero ideal and let $\beta \in \mathfrak{A} \setminus \{0\}$. Then there is an $\alpha \in \mathfrak{A}$ with $\gcd(\alpha, \beta) = \mathfrak{A}$. In particular, all non-zero ideals can be viewed as the greatest common divisor of two algebraic integers.

We can speak of congruences in $\mathcal{O}_K$ in much the same way we do in $\mathbb{Z}$. Specifically, for a non-zero ideal $\mathfrak{A}$ and $\alpha, \beta \in \mathcal{O}_K$, we say $\alpha$ is congruent to $\beta$ modulo $\mathfrak{A}$ if $\alpha - \beta \in \mathfrak{A}$. 
Combining Lemmas 1 and 2 gives us the following result.

**Lemma (3)**

Let $\mathfrak{A}$ be a non-zero ideal and let $\beta \in \mathfrak{A} \setminus \{0\}$. Then there is an $\alpha \in \mathfrak{A}$ with $\gcd(\alpha, \beta) = \mathfrak{A}$. In particular, all non-zero ideals can be viewed as the greatest common divisor of two algebraic integers.

We can speak of congruences in $\mathcal{O}_K$ in much the same way we do in $\mathbb{Z}$. Specifically, for a non-zero ideal $\mathfrak{A}$ and $\alpha, \beta \in \mathcal{O}_K$, we say $\alpha$ is congruent to $\beta$ modulo $\mathfrak{A}$ if $\alpha - \beta \in \mathfrak{A}$. We denote this more compactly by writing $\alpha \equiv \beta \mod \mathfrak{A}$. 
Combining Lemmas 1 and 2 gives us the following result.

**Lemma (3)**

Let $\mathcal{A}$ be a non-zero ideal and let $\beta \in \mathcal{A} \setminus \{0\}$. Then there is an $\alpha \in \mathcal{A}$ with $\text{gcd}(\alpha, \beta) = \mathcal{A}$. In particular, all non-zero ideals can be viewed as the greatest common divisor of two algebraic integers.

We can speak of congruences in $\mathcal{O}_K$ in much the same way we do in $\mathbb{Z}$. Specifically, for a non-zero ideal $\mathcal{A}$ and $\alpha, \beta \in \mathcal{O}_K$, we say $\alpha$ is congruent to $\beta$ modulo $\mathcal{A}$ if $\alpha - \beta \in \mathcal{A}$. We denote this more compactly by writing $\alpha \equiv \beta \pmod{\mathcal{A}}$. A more “advanced” way to say this is $\alpha + \mathcal{A} = \beta + \mathcal{A}$ as elements of the quotient ring $\mathcal{O}_K/\mathcal{A}$. 
The existence of solutions to linear congruences is very much the same as it is with \( \mathbb{Z} \).
The existence of solutions to linear congruences is very much the same as it is with \( \mathbb{Z} \).

**Lemma (4)**
The existence of solutions to linear congruences is very much the same as it is with \( \mathbb{Z} \).

**Lemma (4)**

Let \( \mathfrak{A} \) be a non-zero ideal and let \( \alpha, \beta \in \mathcal{O}_K \).

**Proof:**

This congruence has a solution if and only if \( \beta \in \mathfrak{A} + (\alpha) \), that is, \( (\beta) \subseteq \gcd((\alpha), \mathfrak{A}) \).
The existence of solutions to linear congruences is very much the same as it is with $\mathbb{Z}$.

**Lemma (4)**

Let $\mathfrak{A}$ be a non-zero ideal and let $\alpha, \beta \in \mathcal{O}_K$. Then the congruence

$$X\alpha \equiv \beta \pmod{\mathfrak{A}}$$

has a solution in $\mathcal{O}_K$ if and only if $\gcd(\alpha, \mathfrak{A}) | \beta$. 

Proof:

This congruence has a solution if and only if $\beta \in \mathfrak{A} + (\alpha)$, that is, $(\beta) \subseteq \gcd(\alpha, \mathfrak{A})$. 

Math 681, Monday, February 1

February 1, 2021
The existence of solutions to linear congruences is very much the same as it is with \( \mathbb{Z} \).

**Lemma (4)**

Let \( \mathfrak{A} \) be a non-zero ideal and let \( \alpha, \beta \in \mathcal{O}_K \). Then the congruence

\[
X \alpha \equiv \beta \quad \text{mod} \quad \mathfrak{A}
\]

has a solution in \( \mathcal{O}_K \) if and only if \( \gcd \left( (\alpha), \mathfrak{A} \right) \mid (\beta) \).
The existence of solutions to linear congruences is very much the same as it is with \( \mathbb{Z} \).

**Lemma (4)**

Let \( \mathfrak{A} \) be a non-zero ideal and let \( \alpha, \beta \in \mathcal{O}_K \). Then the congruence

\[
X \alpha \equiv \beta \mod \mathfrak{A}
\]

has a solution in \( \mathcal{O}_K \) if and only if \( \gcd((\alpha), \mathfrak{A})|\beta \).

**Proof:**
The existence of solutions to linear congruences is very much the same as it is with \( \mathbb{Z} \).

**Lemma (4)**

Let \( \mathcal{A} \) be a non-zero ideal and let \( \alpha, \beta \in \mathcal{O}_K \). Then the congruence

\[
X\alpha \equiv \beta \mod \mathcal{A}
\]

has a solution in \( \mathcal{O}_K \) if and only if \( \operatorname{gcd}((\alpha), \mathcal{A})|(\beta) \).

**Proof:** This congruence has a solution if and only if \( \beta \in \mathcal{A} + (\alpha) \),
The existence of solutions to linear congruences is very much the same as it is with \( \mathbb{Z} \).

**Lemma (4)**

Let \( \mathfrak{A} \) be a non-zero ideal and let \( \alpha, \beta \in \mathcal{O}_K \). Then the congruence

\[
X\alpha \equiv \beta \pmod{\mathfrak{A}}
\]

has a solution in \( \mathcal{O}_K \) if and only if \( \gcd((\alpha), \mathfrak{A}) | (\beta) \).

**Proof:** This congruence has a solution if and only if \( \beta \in \mathfrak{A} + (\alpha) \), that is, \( (\beta) \subseteq \gcd((\alpha), \mathfrak{A}) \).
We also know when we can solve simultaneous congruences.

Theorem (Chinese Remainder Theorem)

Let $A_1, \ldots, A_r$ be non-zero ideals which are pair-wise relatively prime, i.e.,

$$A_i + A_j = \mathbb{O}_K$$

whenever $i \neq j$.

Let $I$ denote the product $A_1 \cdot \cdots \cdot A_r$.

Then $
\mathbb{O}_K/I \cong \mathbb{O}_K/A_1 \times \cdots \times \mathbb{O}_K/A_r
$.

In particular, given $
\beta_1, \ldots, \beta_r \in \mathbb{O}_K
$ there is an
$\alpha \in \mathbb{O}_K$ with

$$\alpha \equiv \beta_i \mod A_i, \quad i = 1, \ldots, r$$

and this $\alpha$ is unique modulo $I$.

Proof:

We prove this by induction on $r$. First assume $r = 2$ and write

$$1 = \alpha_1 + \alpha_2$$

with $\alpha_1 \in A_1$ and $\alpha_2 \in A_2$.
We also know when we can solve simultaneous congruences.

**Theorem (Chinese Remainder Theorem)**

Let $A_1, \ldots, A_r$ be non-zero ideals which are pair-wise relatively prime, i.e., $A_i + A_j = \mathbb{O}_K$ whenever $i \neq j$. Let $I$ denote the product $A_1 \cdots A_r$. Then $\mathbb{O}_K/I \cong \mathbb{O}_K/A_1 \times \cdots \times \mathbb{O}_K/A_r$.

In particular, given $\beta_1, \ldots, \beta_r \in \mathbb{O}_K$ there is an $\alpha \in \mathbb{O}_K$ with $\alpha \equiv \beta_i \text{ mod } A_i$, $i = 1, \ldots, r$ and this $\alpha$ is unique modulo $I$.

**Proof:** We prove this by induction on $r$. First assume $r = 2$ and write $1 = \alpha_1 + \alpha_2$ with $\alpha_1 \in A_1$ and $\alpha_2 \in A_2$. ...
We also know when we can solve simultaneous congruences.

**Theorem (Chinese Remainder Theorem)**

Let $\mathcal{A}_1, \ldots, \mathcal{A}_r$ be non-zero ideals which are pair-wise relatively prime,
We also know when we can solve simultaneous congruences.

**Theorem (Chinese Remainder Theorem)**

Let $\mathcal{A}_1, \ldots, \mathcal{A}_r$ be non-zero ideals which are pair-wise relatively prime, i.e., $\mathcal{A}_i + \mathcal{A}_j = \mathcal{O}_K$ whenever $i \neq j$. 

Then $\mathcal{O}_K / I \cong \mathcal{O}_K / \mathcal{A}_1 \times \cdots \times \mathcal{O}_K / \mathcal{A}_r$.

In particular, given $\beta_1, \ldots, \beta_r \in \mathcal{O}_K$ there is an $\alpha \in \mathcal{O}_K$ with $\alpha \equiv \beta_i \pmod{\mathcal{A}_i}$, $i = 1, \ldots, r$ and this $\alpha$ is unique modulo $I$. 

**Proof:** We prove this by induction on $r$. First assume $r = 2$ and write $1 = \alpha_1 + \alpha_2$ with $\alpha_1 \in \mathcal{A}_1$ and $\alpha_2 \in \mathcal{A}_2$. 
We also know when we can solve simultaneous congruences.

**Theorem (Chinese Remainder Theorem)**

Let \( \mathcal{A}_1, \ldots, \mathcal{A}_r \) be non-zero ideals which are pair-wise relatively prime, i.e., \( \mathcal{A}_i + \mathcal{A}_j = \mathcal{O}_K \) whenever \( i \neq j \). Let \( I \) denote the product \( \mathcal{A}_1 \cdots \mathcal{A}_r \).
We also know when we can solve simultaneous congruences.

**Theorem (Chinese Remainder Theorem)**

Let $\mathfrak{A}_1, \ldots, \mathfrak{A}_r$ be non-zero ideals which are pair-wise relatively prime, i.e., $\mathfrak{A}_i + \mathfrak{A}_j = \mathcal{O}_K$ whenever $i \neq j$. Let $\mathfrak{I}$ denote the product $\mathfrak{A}_1 \cdots \mathfrak{A}_r$. Then

$$\mathcal{O}_K / \mathfrak{I} \cong \mathcal{O}_K / \mathfrak{A}_1 \times \cdots \times \mathcal{O}_K / \mathfrak{A}_r.$$
We also know when we can solve simultaneous congruences.

**Theorem (Chinese Remainder Theorem)**

Let \( \mathcal{A}_1, \ldots, \mathcal{A}_r \) be non-zero ideals which are pair-wise relatively prime, i.e., \( \mathcal{A}_i + \mathcal{A}_j = \mathcal{O}_K \) whenever \( i \neq j \). Let \( \mathcal{I} \) denote the product \( \mathcal{A}_1 \cdots \mathcal{A}_r \). Then

\[
\mathcal{O}_K / \mathcal{I} \cong \mathcal{O}_K / \mathcal{A}_1 \times \cdots \times \mathcal{O}_K / \mathcal{A}_r.
\]

In particular, given \( \beta_1, \ldots, \beta_r \in \mathcal{O}_K \)}
We also know when we can solve simultaneous congruences.

**Theorem (Chinese Remainder Theorem)**

Let $\mathcal{A}_1, \ldots, \mathcal{A}_r$ be non-zero ideals which are pair-wise relatively prime, i.e., $\mathcal{A}_i + \mathcal{A}_j = \mathcal{O}_K$ whenever $i \neq j$. Let $\mathcal{I}$ denote the product $\mathcal{A}_1 \cdots \mathcal{A}_r$. Then

$$\mathcal{O}_K/\mathcal{I} \cong \mathcal{O}_K/\mathcal{A}_1 \times \cdots \times \mathcal{O}_K/\mathcal{A}_r.$$ 

In particular, given $\beta_1, \ldots, \beta_r \in \mathcal{O}_K$ there is an $\alpha \in \mathcal{O}_K$ with

$$\alpha \equiv \beta_i \mod \mathcal{A}_i, \quad i = 1, \ldots, r$$
We also know when we can solve simultaneous congruences.

**Theorem (Chinese Remainder Theorem)**

Let $\mathcal{A}_1, \ldots, \mathcal{A}_r$ be non-zero ideals which are pair-wise relatively prime, i.e., $\mathcal{A}_i + \mathcal{A}_j = \mathcal{O}_K$ whenever $i \neq j$. Let $\mathcal{I}$ denote the product $\mathcal{A}_1 \cdots \mathcal{A}_r$. Then

$$\mathcal{O}_K / \mathcal{I} \cong \mathcal{O}_K / \mathcal{A}_1 \times \cdots \times \mathcal{O}_K / \mathcal{A}_r.$$

In particular, given $\beta_1, \ldots, \beta_r \in \mathcal{O}_K$ there is an $\alpha \in \mathcal{O}_K$ with

$$\alpha \equiv \beta_i \mod \mathcal{A}_i, \quad i = 1, \ldots, r$$

and this $\alpha$ is unique modulo $\mathcal{I}$. 
We also know when we can solve simultaneous congruences.

**Theorem (Chinese Remainder Theorem)**

Let $\mathfrak{A}_1, \ldots, \mathfrak{A}_r$ be non-zero ideals which are pair-wise relatively prime, i.e., $\mathfrak{A}_i + \mathfrak{A}_j = \mathcal{O}_K$ whenever $i \neq j$. Let $\mathfrak{I}$ denote the product $\mathfrak{A}_1 \cdots \mathfrak{A}_r$. Then

$$\mathcal{O}_K / \mathfrak{I} \cong \mathcal{O}_K / \mathfrak{A}_1 \times \cdots \times \mathcal{O}_K / \mathfrak{A}_r.$$ 

In particular, given $\beta_1, \ldots, \beta_r \in \mathcal{O}_K$ there is an $\alpha \in \mathcal{O}_K$ with

$$\alpha \equiv \beta_i \mod \mathfrak{A}_i, \quad i = 1, \ldots, r$$

and this $\alpha$ is unique modulo $\mathfrak{I}$.

**Proof:**
We also know when we can solve simultaneous congruences.

**Theorem (Chinese Remainder Theorem)**

Let \( A_1, \ldots, A_r \) be non-zero ideals which are pair-wise relatively prime, i.e., \( A_i + A_j = \mathcal{O}_K \) whenever \( i \neq j \). Let \( I \) denote the product \( A_1 \cdots A_r \). Then

\[
\mathcal{O}_K/I \cong \mathcal{O}_K/A_1 \times \cdots \times \mathcal{O}_K/A_r.
\]

In particular, given \( \beta_1, \ldots, \beta_r \in \mathcal{O}_K \) there is an \( \alpha \in \mathcal{O}_K \) with

\[
\alpha \equiv \beta_i \mod A_i, \quad i = 1, \ldots, r
\]

and this \( \alpha \) is unique modulo \( I \).

**Proof:** We prove this by induction on \( r \). First assume \( r = 2 \) and write

\( 1 = \alpha_1 + \alpha_2 \) with \( \alpha_1 \in A_1 \) and \( \alpha_2 \in A_2 \).
We readily see that the map

\[ \beta + \mathcal{I} \mapsto (\beta + \mathcal{A}_1, \beta + \mathcal{A}_2) \]
We readily see that the map

\[ \beta + \mathcal{I} \mapsto (\beta + \mathcal{A}_1, \beta + \mathcal{A}_2) \]

gives a well-defined one-to-one ring homomorphism from \( \mathcal{O}_K/\mathcal{I} \) to \( \mathcal{O}_K/\mathcal{A}_1 \times \mathcal{O}_K/\mathcal{A}_2 \).
We readily see that the map

\[ \beta + \mathcal{I} \mapsto (\beta + \mathcal{A}_1, \beta + \mathcal{A}_2) \]

gives a well-defined one-to-one ring homomorphism from \( \mathcal{O}_K/\mathcal{I} \) to \( \mathcal{O}_K/\mathcal{A}_1 \times \mathcal{O}_K/\mathcal{A}_2 \). To see that it is onto, let \( \gamma_1, \gamma_2 \in \mathcal{O}_K \).
We readily see that the map
\[
\beta + \mathcal{I} \mapsto (\beta + \mathcal{A}_1, \beta + \mathcal{A}_2)
\]
gives a well-defined one-to-one ring homomorphism from \(\mathcal{O}_K/\mathcal{I}\) to \(\mathcal{O}_K/\mathcal{A}_1 \times \mathcal{O}_K/\mathcal{A}_2\). To see that it is onto, let \(\gamma_1, \gamma_2 \in \mathcal{O}_K\). Then \(\gamma_1 \alpha_2 + \gamma_2 \alpha_1 + \mathcal{I}\) is mapped to \((\gamma_1 + \mathcal{A}_1, \gamma_2 + \mathcal{A}_2)\).
We readily see that the map

$$\beta + \mathcal{I} \mapsto (\beta + \mathcal{A}_1, \beta + \mathcal{A}_2)$$

gives a well-defined one-to-one ring homomorphism from $\mathcal{O}_K/\mathcal{I}$ to $\mathcal{O}_K/\mathcal{A}_1 \times \mathcal{O}_K/\mathcal{A}_2$. To see that it is onto, let $\gamma_1, \gamma_2 \in \mathcal{O}_K$. Then $\gamma_1 \alpha_2 + \gamma_2 \alpha_1 + \mathcal{I}$ is mapped to $(\gamma_1 + \mathcal{A}_1, \gamma_2 + \mathcal{A}_2)$ since

$$\alpha_2 \equiv 1 \mod \mathcal{A}_1, \quad \alpha_1 \equiv 0 \mod \mathcal{A}_1$$
We readily see that the map

$$\beta + I \mapsto (\beta + A_1, \beta + A_2)$$

gives a well-defined one-to-one ring homomorphism from $O_K/I$ to $O_K/A_1 \times O_K/A_2$. To see that it is onto, let $\gamma_1, \gamma_2 \in O_K$. Then $\gamma_1 \alpha_2 + \gamma_2 \alpha_1 + I$ is mapped to $(\gamma_1 + A_1, \gamma_2 + A_2)$ since

$$\alpha_2 \equiv 1 \mod A_1, \quad \alpha_1 \equiv 0 \mod A_1$$

$$\alpha_1 \equiv 1 \mod A_2, \quad \alpha_2 \equiv 0 \mod A_2.$$
We readily see that the map

$$\beta + \mathcal{I} \mapsto (\beta + \mathcal{A}_1, \beta + \mathcal{A}_2)$$

gives a well-defined one-to-one ring homomorphism from $\mathcal{O}_K/\mathcal{I}$ to $\mathcal{O}_K/\mathcal{A}_1 \times \mathcal{O}_K/\mathcal{A}_2$. To see that it is onto, let $\gamma_1, \gamma_2 \in \mathcal{O}_K$. Then $\gamma_1\alpha_2 + \gamma_2\alpha_1 + \mathcal{I}$ is mapped to $(\gamma_1 + \mathcal{A}_1, \gamma_2 + \mathcal{A}_2)$ since

$$\alpha_2 \equiv 1 \mod \mathcal{A}_1, \quad \alpha_1 \equiv 0 \mod \mathcal{A}_1$$

$$\alpha_1 \equiv 1 \mod \mathcal{A}_2, \quad \alpha_2 \equiv 0 \mod \mathcal{A}_2.$$

For $r > 2$, let $\mathcal{B} = \mathcal{I}\mathcal{A}_1^{-1}$. 
We readily see that the map

$$\beta + I \mapsto (\beta + A_1, \beta + A_2)$$

gives a well-defined one-to-one ring homomorphism from $O_K/I$ to $O_K/A_1 \times O_K/A_2$. To see that it is onto, let $\gamma_1, \gamma_2 \in O_K$. Then $\gamma_1 \alpha_2 + \gamma_2 \alpha_1 + I$ is mapped to $(\gamma_1 + A_1, \gamma_2 + A_2)$ since

$$\alpha_2 \equiv 1 \mod A_1, \quad \alpha_1 \equiv 0 \mod A_1$$
$$\alpha_1 \equiv 1 \mod A_2, \quad \alpha_2 \equiv 0 \mod A_2.$$

For $r > 2$, let $B = IA_1^{-1}$. Then $\gcd(B, A_1) = 1$. 
We readily see that the map

$$\beta + I \mapsto (\beta + A_1, \beta + A_2)$$

gives a well-defined one-to-one ring homomorphism from $\mathcal{O}_K/I$ to $\mathcal{O}_K/A_1 \times \mathcal{O}_K/A_2$. To see that it is onto, let $\gamma_1, \gamma_2 \in \mathcal{O}_K$. Then $\gamma_1 \alpha_2 + \gamma_2 \alpha_1 + I$ is mapped to $(\gamma_1 + A_1, \gamma_2 + A_2)$ since

$$\alpha_2 \equiv 1 \mod A_1, \quad \alpha_1 \equiv 0 \mod A_1$$

$$\alpha_1 \equiv 1 \mod A_2, \quad \alpha_2 \equiv 0 \mod A_2.$$

For $r > 2$, let $B = IA_1^{-1}$. Then $\gcd(B, A_1) = 1$ and by the induction hypothesis (twice) we have
We readily see that the map

\[ \beta + \mathcal{I} \mapsto (\beta + A_1, \beta + A_2) \]

gives a well-defined one-to-one ring homomorphism from \( \mathcal{O}_K/\mathcal{I} \) to \( \mathcal{O}_K/A_1 \times \mathcal{O}_K/A_2 \). To see that it is onto, let \( \gamma_1, \gamma_2 \in \mathcal{O}_K \). Then \( \gamma_1 \alpha_2 + \gamma_2 \alpha_1 + \mathcal{I} \) is mapped to \( (\gamma_1 + A_1, \gamma_2 + A_2) \) since

\[
\begin{align*}
\alpha_2 &\equiv 1 \mod A_1, & \alpha_1 &\equiv 0 \mod A_1 \\
\alpha_1 &\equiv 1 \mod A_2, & \alpha_2 &\equiv 0 \mod A_2.
\end{align*}
\]

For \( r > 2 \), let \( \mathcal{B} = \mathcal{I}A_1^{-1} \). Then \( \gcd(\mathcal{B}, A_1) = 1 \) and by the induction hypothesis (twice) we have

\[
\mathcal{O}_K/\mathcal{I} \cong \mathcal{O}_K/A_1 \times \mathcal{O}_K/\mathcal{B} \cong \mathcal{O}_K/A_1 \times \mathcal{O}_K/A_2 \times \cdots \times \mathcal{O}_K/A_r.
\]
Since the norm of a non-zero ideal $\mathcal{I}$ is the index $[\mathcal{O}_K : \mathcal{I}]$, we get the following.

**Corollary**

Let $A_1, \ldots, A_r$ be pair-wise relatively prime non-zero ideals. Then

$$N(A_1 \cdots A_r) = N(A_1) \cdots N(A_r).$$

**Lemma (5)**

Let $P$ be a maximal ideal and $e$ be a non-negative integer. Then

$$[P^e : P^{e+1}] = N(P).$$

Thus,

$$N(P^e) = N(P)^e.$$
Since the norm of a non-zero ideal $\mathcal{I}$ is the index $[\mathcal{O}_K : \mathcal{I}]$, which is simply the cardinality of the quotient ring,
Since the norm of a non-zero ideal $\mathcal{I}$ is the index $[\mathcal{O}_K : \mathcal{I}]$, which is simply the cardinality of the quotient ring, we get the following.

Corollary

Let $A_1, \ldots, A_r$ be pair-wise relatively prime non-zero ideals. Then

$$N(A_1 \cdots A_r) = N(A_1) \cdots N(A_r).$$

Lemma (5)

Let $P$ be a maximal ideal and $e$ be a non-negative integer. Then

$$[P^e : P^{e+1}] = N(P).$$

Thus,

$$N(P^e) = N(P)^e.$$
Since the norm of a non-zero ideal \( \mathcal{I} \) is the index \( [\mathcal{O}_K : \mathcal{I}] \), which is simply the cardinality of the quotient ring, we get the following.

**Corollary**

Let \( A_1, \ldots, A_r \) be pair-wise relatively prime non-zero ideals. Then \( N(A_1 \cdots A_r) = N(A_1) \cdots N(A_r) \).

Lemma (5)

Let \( P \) be a maximal ideal and \( e \) be a non-negative integer. Then \( [P^e : P^{e+1}] = N(P) \).

Thus, \( N(P^e) = N(P)^e \).
Since the norm of a non-zero ideal $\mathfrak{I}$ is the index $[\mathcal{O}_K : \mathfrak{I}]$, which is simply the cardinality of the quotient ring, we get the following.

**Corollary**

Let $\mathfrak{A}_1, \ldots, \mathfrak{A}_r$ be pair-wise relatively prime non-zero ideals.
Since the norm of a non-zero ideal $I$ is the index $[\mathcal{O}_K : I]$, which is simply the cardinality of the quotient ring, we get the following.

**Corollary**

Let $\mathfrak{A}_1, \ldots, \mathfrak{A}_r$ be pair-wise relatively prime non-zero ideals. Then

$$N(\mathfrak{A}_1 \cdots \mathfrak{A}_r) = N(\mathfrak{A}_1) \cdots N(\mathfrak{A}_r).$$
Since the norm of a non-zero ideal $\mathcal{I}$ is the index $[\mathcal{O}_K : \mathcal{I}]$, which is simply the cardinality of the quotient ring, we get the following.

**Corollary**

Let $\mathcal{A}_1, \ldots, \mathcal{A}_r$ be pair-wise relatively prime non-zero ideals. Then

$$N(\mathcal{A}_1 \cdots \mathcal{A}_r) = N(\mathcal{A}_1) \cdots N(\mathcal{A}_r).$$

**Lemma (5)**

Let $\mathcal{P}$ be a maximal ideal and $\mathcal{P}^e$ be a non-negative integer. Then

$$[\mathcal{P}^e : \mathcal{P}^{e+1}] = N(\mathcal{P}).$$

Thus,

$$N(\mathcal{P}^e) = N(\mathcal{P})^e.$$
Since the norm of a non-zero ideal $\mathcal{I}$ is the index $[\mathcal{O}_K : \mathcal{I}]$, which is simply the cardinality of the quotient ring, we get the following.

**Corollary**

Let $\mathcal{A}_1, \ldots, \mathcal{A}_r$ be pair-wise relatively prime non-zero ideals. Then

$$N(\mathcal{A}_1 \cdots \mathcal{A}_r) = N(\mathcal{A}_1) \cdots N(\mathcal{A}_r).$$

**Lemma (5)**

Let $\mathfrak{p}$ be a maximal ideal and $e$ be a non-negative integer.
Since the norm of a non-zero ideal \( \mathcal{I} \) is the index \([\mathcal{O}_K : \mathcal{I}]\), which is simply the cardinality of the quotient ring, we get the following.

**Corollary**

Let \( \mathcal{A}_1, \ldots, \mathcal{A}_r \) be pair-wise relatively prime non-zero ideals. Then

\[
N(\mathcal{A}_1 \cdots \mathcal{A}_r) = N(\mathcal{A}_1) \cdots N(\mathcal{A}_r).
\]

**Lemma (5)**

Let \( \mathfrak{m} \) be a maximal ideal and \( e \) be a non-negative integer. Then

\[
[\mathfrak{m}^e : \mathfrak{m}^{e+1}] = N(\mathfrak{m}).
\]
Since the norm of a non-zero ideal $\mathfrak{I}$ is the index $[\mathcal{O}_K : \mathfrak{I}]$, which is simply the cardinality of the quotient ring, we get the following.

**Corollary**

Let $\mathfrak{A}_1, \ldots, \mathfrak{A}_r$ be pair-wise relatively prime non-zero ideals. Then

$$N(\mathfrak{A}_1 \cdots \mathfrak{A}_r) = N(\mathfrak{A}_1) \cdots N(\mathfrak{A}_r).$$

**Lemma (5)**

Let $\mathfrak{P}$ be a maximal ideal and $e$ be a non-negative integer. Then

$$[\mathfrak{P}^e : \mathfrak{P}^{e+1}] = N(\mathfrak{P}).$$

Thus,

$$N(\mathfrak{P}^e) = N(\mathfrak{P})^e.$$
Proof:

Let $\alpha \in \mathbb{P} \setminus \mathbb{P} + 1$. Then $\gcd((\alpha), \mathbb{P} + 1) = \mathbb{P}$. By Lemma 4, for any $\beta \in \mathbb{P}$ we can solve the congruence $X \equiv \beta \pmod{\mathbb{P} + 1}$. Moreover, $\gamma_1 \alpha \equiv \gamma_2 \alpha \pmod{\mathbb{P} + 1}$ if and only if $\mathbb{P} \mid (\gamma_1 - \gamma_2)(\alpha)$, which is true if and only if $\mathbb{P} \mid (\gamma_1 - \gamma_2)$. In other words, the solutions to the congruence $X \alpha \equiv \beta \pmod{\mathbb{P} + 1}$ are all congruent modulo $\mathbb{P}$. Thus, there are precisely $N(\mathbb{P})$ elements of $\mathbb{P}$ which are incongruent modulo $\mathbb{P}$. Finally, we have $[\mathbb{O}_K : \mathbb{P}] = [\mathbb{O}_K : \mathbb{P}] [\mathbb{P} : \mathbb{P}^2] \cdots [\mathbb{P}^{e-1} : \mathbb{P}^e] = N(\mathbb{P})^e$. 

Math 681, Monday, February 1
Proof: Let $\alpha \in \mathbb{P}^e \setminus \mathbb{P}^{e+1}$.
Proof: Let $\alpha \in \mathcal{P}^{e} \setminus \mathcal{P}^{e+1}$. Then $\gcd((\alpha), \mathcal{P}^{e+1}) = \mathcal{P}^{e}$.
Proof: Let $\alpha \in \mathcal{P}^e \setminus \mathcal{P}^{e+1}$. Then $\gcd((\alpha), \mathcal{P}^{e+1}) = \mathcal{P}^e$. By Lemma 4, for any $\beta \in \mathcal{P}^e$ we can solve the congruence $X \alpha \equiv \beta \mod \mathcal{P}^{e+1}$. 

Moreover, $\gamma_1 \alpha \equiv \gamma_2 \alpha \mod \mathcal{P}^{e+1}$ if and only if $\mathcal{P}^{e+1} | (\gamma_1 - \gamma_2) \alpha$, which is true if and only if $\mathcal{P} | (\gamma_1 - \gamma_2)$. In other words, the solutions to the congruence $X \alpha \equiv \beta \mod \mathcal{P}^{e+1}$ are all congruent modulo $\mathcal{P}^{e+1}$. Thus, there are precisely $N(\mathcal{P})$ elements of $\mathcal{P}^e$ which are incongruent modulo $\mathcal{P}^{e+1}$. 

Finally, we have $[\mathcal{O}_K] : [\mathcal{O}_K] : [\mathcal{P}] : \cdots : [\mathcal{P}^{e-1}] = N(\mathcal{P})^e$. 


Proof: Let $\alpha \in \mathcal{P}^e \setminus \mathcal{P}^{e+1}$. Then $\gcd((\alpha), \mathcal{P}^{e+1}) = \mathcal{P}^e$. By Lemma 4, for any $\beta \in \mathcal{P}^e$ we can solve the congruence $X \alpha \equiv \beta \mod \mathcal{P}^{e+1}$. Moreover, $\gamma_1 \alpha \equiv \gamma_2 \alpha \mod \mathcal{P}^{e+1}$ if and only if $\mathcal{P}^{e+1}|(\gamma_1 - \gamma_2)(\alpha)$.
Proof: Let $\alpha \in \mathcal{P}^e \setminus \mathcal{P}^{e+1}$. Then $\gcd((\alpha), \mathcal{P}^{e+1}) = \mathcal{P}^e$. By Lemma 4, for any $\beta \in \mathcal{P}^e$ we can solve the congruence $X\alpha \equiv \beta \mod \mathcal{P}^{e+1}$. Moreover, $\gamma_1\alpha \equiv \gamma_2\alpha \mod \mathcal{P}^{e+1}$ if and only if $\mathcal{P}^{e+1}|(\gamma_1 - \gamma_2)(\alpha)$, which it true if and only if $\mathcal{P}|(\gamma_1 - \gamma_2)$. 
Proof: Let $\alpha \in \mathcal{P}^e \setminus \mathcal{P}^{e+1}$. Then $\gcd ((\alpha), \mathcal{P}^{e+1}) = \mathcal{P}^e$. By Lemma 4, for any $\beta \in \mathcal{P}^e$ we can solve the congruence $X \alpha \equiv \beta \mod \mathcal{P}^{e+1}$. Moreover, $\gamma_1 \alpha \equiv \gamma_2 \alpha \mod \mathcal{P}^{e+1}$ if and only if $\mathcal{P}^{e+1} | (\gamma_1 - \gamma_2)(\alpha)$, which it true if and only if $\mathcal{P} | (\gamma_1 - \gamma_2)$. In other words, the solutions to the congruence $X \alpha \equiv \beta \mod \mathcal{P}^{e+1}$ are all congruent modulo $\mathcal{P}$. 
Proof: Let $\alpha \in \mathcal{P}^{e} \setminus \mathcal{P}^{e+1}$. Then $\gcd ((\alpha), \mathcal{P}^{e+1}) = \mathcal{P}^{e}$. By Lemma 4, for any $\beta \in \mathcal{P}^{e}$ we can solve the congruence $X\alpha \equiv \beta \mod \mathcal{P}^{e+1}$. Moreover, $\gamma_{1}\alpha \equiv \gamma_{2}\alpha \mod \mathcal{P}^{e+1}$ if and only if $\mathcal{P}^{e+1}|(\gamma_{1} - \gamma_{2})(\alpha)$, which it true if and only if $\mathcal{P}|(\gamma_{1} - \gamma_{2})$. In other words, the solutions to the congruence $X\alpha \equiv \beta \mod \mathcal{P}^{e+1}$ are all congruent modulo $\mathcal{P}$. Thus, there are precisely $N(\mathcal{P})$ elements of $\mathcal{P}^{e}$ which are incongruent modulo $\mathcal{P}^{e+1}$. 

**Proof:** Let $\alpha \in \mathfrak{p}^e \setminus \mathfrak{p}^{e+1}$. Then $\text{gcd} \left((\alpha), \mathfrak{p}^{e+1}\right) = \mathfrak{p}^e$. By Lemma 4, for any $\beta \in \mathfrak{p}^e$ we can solve the congruence $X\alpha \equiv \beta \mod \mathfrak{p}^{e+1}$.

Moreover, $\gamma_1\alpha \equiv \gamma_2\alpha \mod \mathfrak{p}^{e+1}$ if and only if $\mathfrak{p}^{e+1}|(\gamma_1 - \gamma_2)(\alpha)$, which it true if and only if $\mathfrak{p}|(\gamma_1 - \gamma_2)$. In other words, the solutions to the congruence $X\alpha \equiv \beta \mod \mathfrak{p}^{e+1}$ are all congruent modulo $\mathfrak{p}$. Thus, there are precisely $N(\mathfrak{p})$ elements of $\mathfrak{p}^e$ which are incongruent modulo $\mathfrak{p}^{e+1}$.

Finally, we have

$$[\mathcal{O}_K : \mathfrak{p}^e] = [\mathcal{O}_K : \mathfrak{p}][\mathfrak{p} : \mathfrak{p}^2] \cdots [\mathfrak{p}^{e-1} : \mathfrak{p}^e] = N(\mathfrak{p})^e.$$
Combining the Corollary to the Chinese Remainder Theorem with Lemma 5 gives the following.

Theorem
For any maximal ideals \(P_1, \ldots, P_r\) and non-negative integers \(e_1, \ldots, e_r\) we have
\[
N(P_1^{e_1} \cdots P_r^{e_r}) = N(P_1)^{e_1} \cdots N(P_r)^{e_r}.
\]

Given this, it is natural to extend the definition of norm to all non-zero fractional ideals by defining
\[
N(I) = N(P_1)^{e_1} \cdots N(P_r)^{e_r}
\]
for all non-zero fractional ideals \(I\) as in (1).

With this extended definition the norm is a group homomorphism from the non-zero fractional ideals to the positive rational numbers. Moreover, it “does the right thing” in regards to indices and quotient rings. See exercise #2 from homework #4.
Combining the Corollary to the Chinese Remainder Theorem with Lemma 5 gives the following.

**Theorem**

For any maximal ideals $P_1, \ldots, P_r$ and non-negative integers $e_1, \ldots, e_r$ we have

\[
N(P_1^{e_1} \cdots P_r^{e_r}) = N(P_1)^{e_1} \cdots N(P_r)^{e_r}.
\]

Given this, it is natural to extend the definition of norm to all non-zero fractional ideals by defining

\[
N(I) = N(P_1)^{e_1} \cdots N(P_r)^{e_r}
\]

for all non-zero fractional ideals $I$ as in (1).

With this extended definition the norm is a group homomorphism from the non-zero fractional ideals to the positive rational numbers. Moreover, it "does the right thing" in regards to indices and quotient rings. See exercise #2 from homework #4.
Combining the Corollary to the Chinese Remainder Theorem with Lemma 5 gives the following.

**Theorem**

For any maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and non-negative integers $e_1, \ldots, e_r$ we have

$$N(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}) = N(\mathfrak{p}_1^{e_1}) \cdots N(\mathfrak{p}_r^{e_r}).$$

Given this, it is natural to extend the definition of norm to all non-zero fractional ideals by defining

$$N(I) = N(\mathfrak{p}_1^{e_1}) \cdots N(\mathfrak{p}_r^{e_r})$$

for all non-zero fractional ideals $I$ as in (1).

With this extended definition the norm is a group homomorphism from the non-zero fractional ideals to the positive rational numbers. Moreover, it "does the right thing" in regards to indices and quotient rings. See exercise #2 from homework #4.
Combining the Corollary to the Chinese Remainder Theorem with Lemma 5 gives the following.

**Theorem**

For any maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and non-negative integers $e_1, \ldots, e_r$ we have

$$N(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r}.$$
Combining the Corollary to the Chinese Remainder Theorem with Lemma 5 gives the following.

**Theorem**

For any maximal ideals \( \mathfrak{p}_1, \ldots, \mathfrak{p}_r \) and non-negative integers \( e_1, \ldots, e_r \) we have

\[
N(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r}.
\]

Given this, it is natural to extend the definition of norm to all non-zero fractional ideals by defining
Combining the Corollary to the Chinese Remainder Theorem with Lemma 5 gives the following.

**Theorem**

For any maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and non-negative integers $e_1, \ldots, e_r$ we have

\[ N(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r}. \]

Given this, it is natural to extend the definition of norm to all non-zero fractional ideals by defining

\[ N(\mathfrak{I}) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r} \]

for all non-zero fractional ideals $\mathfrak{I}$ as in (1).
Combining the Corollary to the Chinese Remainder Theorem with Lemma 5 gives the following.

**Theorem**

For any maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and non-negative integers $e_1, \ldots, e_r$ we have

$$N(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r}.$$ 

Given this, it is natural to extend the definition of norm to all non-zero fractional ideals by defining

$$N(I) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r}$$

for all non-zero fractional ideals $I$ as in (1). With this extended definition the norm is a group homomorphism from the non-zero fractional ideals to the positive rational numbers.
Combining the Corollary to the Chinese Remainder Theorem with Lemma 5 gives the following.

**Theorem**

For any maximal ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ and non-negative integers $e_1, \ldots, e_r$ we have

$$N(\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}) = N(\mathfrak{P}_1)^{e_1} \cdots N(\mathfrak{P}_r)^{e_r}.$$ 

Given this, it is natural to extend the definition of norm to all non-zero fractional ideals by defining

$$N(I) = N(\mathfrak{P}_1)^{e_1} \cdots N(\mathfrak{P}_r)^{e_r}$$

for all non-zero fractional ideals $I$ as in (1). With this extended definition the norm is a group homomorphism from the non-zero fractional ideals to the positive rational numbers. Moreover, it “does the right thing” in regards to indices and quotient rings.
Combining the Corollary to the Chinese Remainder Theorem with Lemma 5 gives the following.

**Theorem**

For any maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and non-negative integers $e_1, \ldots, e_r$ we have

$$N(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r}.$$ 

Given this, it is natural to extend the definition of norm to all non-zero fractional ideals by defining

$$N(\mathfrak{I}) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r}$$

for all non-zero fractional ideals $\mathfrak{I}$ as in (1). With this extended definition the norm is a group homomorphism from the non-zero fractional ideals to the positive rational numbers. Moreover, it “does the right thing” in regards to indices and quotient rings. See exercise #2 from homework #4.
Given a prime number \( p \in \mathbb{Z} \),
Given a prime number $p \in \mathbb{Z}$, we apply the Fundamental Theorem to the principal ideal generated by $p$ in $\mathcal{O}_K$:

$$p \mathcal{O}_K = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}.$$ (5)

Note that the non-zero prime ideals $\mathcal{P}_1, \ldots, \mathcal{P}_r$ here are precisely those prime ideals of $\mathcal{O}_K$ that contain the prime number $p$.

We say these prime ideals lie above $p$.

An earlier exercise showed that $\mathcal{O}_K/\mathcal{P}_i$ was a finite field of characteristic $p$, thus is the finite field with $p^{f_i}$ elements for some positive integer $f_i$.

Another exercise applied to the principal ideal $p \mathcal{O}_K$ showed that $N(p \mathcal{O}_K) = |N_{K/Q}(p)| = p^n$, where $n = [K:Q]$.

Therefore by the Theorem above and equation (5),

$$[K:Q] = n = e_1 f_1 + \cdots + e_r f_r.$$
Given a prime number $p \in \mathbb{Z}$, we apply the Fundamental Theorem to the principal ideal generated by $p$ in $\mathcal{O}_K$:

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}. \quad (5)$$
Given a prime number $p \in \mathbb{Z}$, we apply the Fundamental Theorem to the principal ideal generated by $p$ in $\mathcal{O}_K$:

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}. \quad (5)$$

Note that the non-zero prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ here are precisely those prime ideals of $\mathcal{O}_K$ that contain the prime number $p$. 
Given a prime number $p \in \mathbb{Z}$, we apply the Fundamental Theorem to the principal ideal generated by $p$ in $\mathcal{O}_K$:

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}. \quad (5)$$

Note that the non-zero prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ here are precisely those prime ideals of $\mathcal{O}_K$ that contain the prime number $p$. We say these prime ideals lie above $p$. 
Given a prime number \( p \in \mathbb{Z} \), we apply the Fundamental Theorem to the principal ideal generated by \( p \) in \( \mathcal{O}_K \):

\[
p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.
\]  

(5)

Note that the non-zero prime ideals \( \mathfrak{P}_1, \ldots, \mathfrak{P}_r \) here are precisely those prime ideals of \( \mathcal{O}_K \) that contain the prime number \( p \). We say these prime ideals lie above \( p \). An earlier exercise showed that \( \mathcal{O}_K/\mathfrak{P}_i \) was a finite field of characteristic \( p \),
Given a prime number $p \in \mathbb{Z}$, we apply the Fundamental Theorem to the principal ideal generated by $p$ in $\mathcal{O}_K$:

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}. \quad (5)$$

Note that the non-zero prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ here are precisely those prime ideals of $\mathcal{O}_K$ that contain the prime number $p$. We say these prime ideals lie above $p$. An earlier exercise showed that $\mathcal{O}_K / \mathfrak{P}_i$ was a finite field of characteristic $p$, thus is the finite field with $p^{f_i}$ elements for some positive integer $f_i$. 
Given a prime number $p \in \mathbb{Z}$, we apply the Fundamental Theorem to the principal ideal generated by $p$ in $\mathcal{O}_K$:

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}. \quad (5)$$

Note that the non-zero prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ here are precisely those prime ideals of $\mathcal{O}_K$ that contain the prime number $p$. We say these prime ideals lie above $p$. An earlier exercise showed that $\mathcal{O}_K/\mathfrak{P}_i$ was a finite field of characteristic $p$, thus is the finite field with $p^{f_i}$ elements for some positive integer $f_i$. Another exercise applied to the principal ideal $p\mathcal{O}_K$ showed that $N(p\mathcal{O}_K) = |N_{K/\mathbb{Q}}(p)| = p^n$, where $n = [K : \mathbb{Q}]$. 
Given a prime number \( p \in \mathbb{Z} \), we apply the Fundamental Theorem to the principal ideal generated by \( p \) in \( \mathcal{O}_K \):

\[
p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.
\]  

(5)

Note that the non-zero prime ideals \( \mathfrak{P}_1, \ldots, \mathfrak{P}_r \) here are precisely those prime ideals of \( \mathcal{O}_K \) that contain the prime number \( p \). We say these prime ideals \emph{lie above} \( p \). An earlier exercise showed that \( \mathcal{O}_K/\mathfrak{P}_i \) was a finite field of characteristic \( p \), thus is the finite field with \( p^{f_i} \) elements for some positive integer \( f_i \). Another exercise applied to the principal ideal \( p\mathcal{O}_K \) showed that \( N(p\mathcal{O}_K) = |N_{K/\mathbb{Q}}(p)| = p^n \), where \( n = [K : \mathbb{Q}] \). Therefore by the Theorem above and equation (5),
Given a prime number $p \in \mathbb{Z}$, we apply the Fundamental Theorem to the
principal ideal generated by $p$ in $\mathcal{O}_K$:

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$  \hspace{1cm} (5)

Note that the non-zero prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ here are precisely those
prime ideals of $\mathcal{O}_K$ that contain the prime number $p$. We say these prime
ideals lie above $p$. An earlier exercise showed that $\mathcal{O}_K/\mathfrak{P}_i$ was a finite field
of characteristic $p$, thus is the finite field with $p^{f_i}$ elements for some
positive integer $f_i$. Another exercise applied to the principal ideal $p\mathcal{O}_K$
showed that $N(p\mathcal{O}_K) = |N_{K/Q}(p)| = p^n$, where $n = [K : \mathbb{Q}]$. Therefore by
the Theorem above and equation (5),

$$[K : \mathbb{Q}] = n = e_1 f_1 + \cdots + e_r f_r.$$
The exponents $e_i$ in (5) are called the \textit{ramification indices} of the prime ideals $P_i$.

If $e_i > 1$ for any $i$, we say the prime number $p$ \textit{ramifies} in the number field $K$.

The positive integers $f_i$ are called the \textit{residue class degrees} or \textit{inertial degrees} of the prime ideals $P_i$.

Obviously an important task is to determine the ramification indices and residue class degrees.

We'll work hard to show that the prime numbers $p$ that ramify are precisely the primes dividing the discriminant. Thus the ramification index is equal to 1 with finitely many exceptions.
Definition

The exponents $e_i$ in (5) are called the *ramification indices* of the prime ideals $\mathfrak{p}_i$. 

If $e_i > 1$ for any $i$ we say the prime number $p$ ramifies in the number field $K$. The positive integers $f_i$ are called the *residue class degrees* or *inertial degrees* of the prime ideals $\mathfrak{p}_i$.

Obviously an important task is to determine the ramification indices and residue class degrees. We'll work hard to show that the prime numbers $p$ that ramify are precisely the primes dividing the discriminant. Thus the ramification index is equal to 1 with finitely many exceptions.
Definition

The exponents $e_i$ in (5) are called the *ramification indices* of the prime ideals $\mathfrak{P}_i$. If $e_i > 1$ for any $i$ we say the prime number $p$ *ramifies* in the number field $K$. Obviously an important task is to determine the ramification indices and residue class degrees. We'll work hard to show that the prime numbers $p$ that ramify are precisely the primes dividing the discriminant. Thus the ramification index is equal to 1 with finitely many exceptions.
Definition

The exponents $e_i$ in (5) are called the *ramification indices* of the prime ideals $\mathfrak{P}_i$. If $e_i > 1$ for any $i$ we say the prime number $p$ *ramifies* in the number field $K$. The positive integers $f_i$ are called the *residue class degrees* or *inertial degrees* of the prime ideals $\mathfrak{P}_i$. Obviously an important task is to determine the ramification indices and residue class degrees.

We'll work hard to show that the prime numbers $p$ that ramify are precisely the primes dividing the discriminant. Thus the ramification index is equal to 1 with finitely many exceptions.
Definition

The exponents $e_i$ in (5) are called the *ramification indices* of the prime ideals $\mathfrak{p}_i$. If $e_i > 1$ for any $i$ we say the prime number $p$ *ramifies* in the number field $K$. The positive integers $f_i$ are called the *residue class degrees* or *inertial degrees* of the prime ideals $\mathfrak{p}_i$.

Obviously an important task is to determine the ramification indices and residue class degrees.
**Definition**

The exponents $e_i$ in (5) are called the *ramification indices* of the prime ideals $\mathfrak{p}_i$. If $e_i > 1$ for any $i$ we say the prime number $p$ *ramifies* in the number field $K$. The positive integers $f_i$ are called the *residue class degrees* or *inertial degrees* of the prime ideals $\mathfrak{p}_i$.

Obviously an important task is to determine the ramification indices and residue class degrees.

We’ll work hard to show that the prime numbers $p$ that ramify are precisely the primes dividing the discriminant.
Definition

The exponents $e_i$ in (5) are called the *ramification indices* of the prime ideals $\mathfrak{P}_i$. If $e_i > 1$ for any $i$ we say the prime number $p$ *ramifies* in the number field $K$. The positive integers $f_i$ are called the *residue class degrees* or *inertial degrees* of the prime ideals $\mathfrak{P}_i$.

Obviously an important task is to determine the ramification indices and residue class degrees.

We’ll work hard to show that the prime numbers $p$ that ramify are precisely the primes dividing the discriminant. Thus the ramification index is equal to 1 with finitely many exceptions.