Throughout these notes, $K$ denotes 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 $K$.

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

Note that the binary group operation here is multiplication of fractional ideals. Thus, the Fundamental Theorem asserts that any non-zero fractional ideal $I \neq \mathfrak{O}_K$ can be written uniquely

$$ I = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, $$

where the $\mathfrak{P}_i$s are maximal (i.e., non-zero prime) ideals and the $e_i$s are non-zero elements of $\mathbb{Z}$. The identity element of this group is $\mathfrak{O}_K$. The non-zero ideals are the monoid consisting of those $I$ where the corresponding exponents $e_i$ in (1) are all positive, together with $\mathfrak{O}_K$. If necessary, look up the definitions of free abelian group and monoid in any reasonable algebra text.

For two non-zero ideals $\mathfrak{A}$ and $\mathfrak{B}$, we are on firm ground saying $\mathfrak{A}|\mathfrak{B}$ if $\mathfrak{B} = \mathfrak{A}\mathfrak{C}$ for some non-zero ideal $\mathfrak{C}$ by the Fundamental Theorem. Note that $\mathfrak{A}|\mathfrak{B}$ if and only if $\mathfrak{A} \supseteq \mathfrak{B}$ as sets.

**Definitions/Notation:** 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 $\mathfrak{O}_K$ at $\mathfrak{P}$ is 0 for all maximal ideals $\mathfrak{P}$. We write $\text{ord}_\mathfrak{P}(I)$ for the order of $I$ at $\mathfrak{P}$.

Given two non-zero ideals $\mathfrak{A}$ and $\mathfrak{B}$, we define the greatest common divisor and least common multiple of $\mathfrak{A}$ and $\mathfrak{B}$ to be the non-zero ideals $\text{gcd}(\mathfrak{A}, \mathfrak{B})$ and $\text{lcm}(\mathfrak{A}, \mathfrak{B})$ defined by

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

and

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

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

For non-zero $\alpha, \beta \in \mathfrak{O}_K$ we define $\text{ord}_\mathfrak{P}(\alpha) = \text{ord}_\mathfrak{P}(\langle \alpha \rangle)$, where $\langle \alpha \rangle$ is the principal ideal generated by $\alpha$. We define $\text{gcd}(\alpha, \beta) = \text{gcd}(\langle \alpha \rangle, \langle \beta \rangle)$ and $\text{lcm}(\alpha, \beta) = \text{lcm}(\langle \alpha \rangle, \langle \beta \rangle)$. Occasionally it is handy to define $\text{ord}_\mathfrak{P}(0) = \infty$.

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

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

Similarly, the $\text{lcm}(\mathfrak{A}, \mathfrak{B})$ is the largest (set-theoretically) ideal which is contained in both $\mathfrak{A}$ and $\mathfrak{B}$. It isn’t difficult to see that

$$ \text{gcd}(\mathfrak{A}, \mathfrak{B})\text{lcm}(\mathfrak{A}, \mathfrak{B}) = \mathfrak{A}\mathfrak{B}. $$

It’s a simple matter to extend these definitions to any finite collection of ideals, so that

$$ \text{gcd}(\mathfrak{A}_1, \ldots, \mathfrak{A}_r) = \mathfrak{A}_1 + \cdots + \mathfrak{A}_r. $$
**Remarks:** 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 \( \alpha, \beta \in \mathcal{O}_K \). Since \( (\alpha) + (\beta)|(\alpha + \beta) \), we do have

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

You 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 \( \mathfrak{AB} = (\alpha) \) if and only if \( \alpha \in \mathfrak{A} \).

As for proof, by the Fundamental Theorem \( \mathfrak{AB} = (\alpha) \) if and only if \( \mathfrak{B} = (\alpha)\mathfrak{A}^{-1} \), and \( (\alpha)\mathfrak{A}^{-1} \subseteq \mathcal{O}_K \) if and only if \( (\alpha) \subseteq \mathfrak{A} \).

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

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

Define

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

Note that

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

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

\[
(2) \quad \alpha_1 + \cdots + \alpha_r = 1.
\]

Since each \( \alpha_i \in \mathfrak{A}_i \) we have

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

Since \( \text{ord}_{\mathfrak{P}_i}(1) = 0 \) for all maximal ideals \( \mathfrak{P}_i \), the Remarks above together with (2) and (3) implies that

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

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), (4) and the Remarks above show that

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

Since \( \text{ord}_{\mathfrak{P}_i}(\mathfrak{AB}) = 0 \) for all \( \mathfrak{P}_i \) not among \( \mathfrak{P}_1, \ldots, \mathfrak{P}_r \), we have \( \gcd((\alpha), \mathfrak{AB}) = \mathfrak{A} \).

Combining Lemmas 1 and 2 give 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 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 \( \mathcal{O}_K/\mathfrak{A} \).

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 \( \gcd((\alpha), \mathfrak{A}) | (\beta) \).

As for proof, convince yourself that 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.

**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 prove this by induction on \( r \). First assume \( r = 2 \) and write \( 1 = \alpha_1 + \alpha_2 \) with \( \alpha_1 \in \mathfrak{A}_1 \) and \( \alpha_2 \in \mathfrak{A}_2 \). Verify that the map

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

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

\[
\begin{align*}
\alpha_2 & \equiv 1 \mod \mathfrak{A}_1 & \alpha_1 & \equiv 0 \mod \mathfrak{A}_1 \\
\alpha_1 & \equiv 1 \mod \mathfrak{A}_2 & \alpha_2 & \equiv 0 \mod \mathfrak{A}_2.
\end{align*}
\]

For \( r > 2 \), let \( \mathfrak{B} = \mathfrak{A}_1^{-1} \). Then \( \gcd(\mathfrak{B}, \mathfrak{A}_1) = 1 \) and by the induction hypothesis (twice) we have

\[
\mathcal{O}_K/\mathfrak{I} \cong \mathcal{O}_K/\mathfrak{A}_1 \times \mathcal{O}_K/\mathfrak{B} \cong \mathcal{O}_K/\mathfrak{A}_1 \times \mathcal{O}_K/\mathfrak{A}_2 \times \cdots \times \mathcal{O}_K/\mathfrak{A}_r.
\]

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 $\alpha \in \mathfrak{P}^e \setminus \mathfrak{P}^{e+1}$. Then $\text{gcd}((\alpha), \mathfrak{P}^{e+1}) = \mathfrak{P}^e$. 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 is 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 $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ 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 #5 from homework #3.