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

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

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

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

where the $P_i$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 $\mathcal{O}_K$. The non-zero ideals are the monoid consisting of those $I$ where the corresponding exponents $e_i$ in (1) are all positive, together with $\mathcal{O}_K$. If necessary, look up the definitions of free abelian group and monoid in any reasonable algebra text.

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.

**Definitions/Notation:** 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 $P$. We write $\text{ord}_P(I)$ for the order of $I$ at $P$.

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

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

and

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

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

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

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

$$\gcd(A, B)\lcm(A, B) = AB.$$ 

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

$$\gcd(A_1, \ldots, A_r) = A_1 + \cdots + A_r.$$
Remarks: Clearly \( \text{ord}_P(\mathfrak{A}\mathfrak{B}) = \text{ord}_P(\mathfrak{A}) + \text{ord}_P(\mathfrak{B}) \). Since \( \mathfrak{A} + \mathfrak{B} = \text{gcd}(\mathfrak{A}, \mathfrak{B}) \), 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 \( \alpha, \beta \in \mathcal{O}_K \). Since \( (\alpha) + (\beta)|(\alpha + \beta) \), we do have

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

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

As for proof, by the Fundamental Theorem \( \mathfrak{A}\mathfrak{B} = (\alpha) \) 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 \( \text{gcd}( (\alpha), \mathfrak{AB} ) = \mathfrak{A} \).

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

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

Note that

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

Thus, \( \text{gcd}(\mathfrak{A}_1, \ldots, \mathfrak{A}_r) = \mathcal{O}_K \), 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 \( \text{ord}_{\mathfrak{P}_i}(\mathfrak{A}\mathfrak{B}) = 0 \) for all \( \mathfrak{P}_i \) not among \( \mathfrak{P}_1, \ldots, \mathfrak{P}_r \), we have \( \gcd((\alpha), \mathfrak{A}\mathfrak{B}) = \mathfrak{A} \).

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 $\mathcal{I}$ denote the product $\mathfrak{a}_1 \cdots \mathfrak{a}_r$. Then

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

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 $\mathcal{I}$.

**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

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

gives a well-defined one-to-one ring homomorphism from $\mathcal{O}_K/\mathcal{I}$ 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 $\gamma_1 \alpha_2 + \gamma_2 \alpha_1 + \mathcal{I}$ is mapped to $(\gamma_1 + \mathfrak{a}_1, \gamma_2 + \mathfrak{a}_2)$ since

$$\alpha_2 \equiv 1 \mod \mathfrak{a}_1 \quad \alpha_1 \equiv 0 \mod \mathfrak{a}_1$$
$$\alpha_1 \equiv 1 \mod \mathfrak{a}_2 \quad \alpha_2 \equiv 0 \mod \mathfrak{a}_2.$$  

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

$$\mathcal{O}_K/\mathcal{I} \cong \mathcal{O}_K/\mathfrak{a}_1 \times \mathcal{O}_K/\mathfrak{B} \cong \mathcal{O}_K/\mathfrak{a}_1 \times \mathcal{O}_K/\mathfrak{a}_2 \times \cdots \times \mathcal{O}_K/\mathfrak{a}_r.$$  

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

**Corollary:** Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ 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 \( \gcd((\alpha), \mathfrak{P}^{e+1}) = \mathfrak{P}^e \). By Lemma 4, for any \( \beta \in \mathfrak{P}^e \) we can solve the congruence \( \chi \alpha \equiv \beta \mod \mathfrak{P}^{e+1} \). 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 \( \chi \alpha \equiv \beta \mod \mathfrak{P}^{e+1} \) 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

\[
[\mathfrak{O}_K : \mathfrak{P}^e] = [\mathfrak{O}_K : \mathfrak{P}] [\mathfrak{P} : \mathfrak{P}^2] \cdots [\mathfrak{P}^{e-1} : \mathfrak{P}] = N(\mathfrak{P})^e.
\]

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

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

for all non-zero fractional ideals \( \mathfrak{J} \) 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 \( p \in \mathbb{Z} \), we apply the Fundamental Theorem to the principal ideal generated by \( p \) in \( \mathfrak{O}_K \),

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

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

\[ [K : \mathbb{Q}] = n = e_1 f_1 + \cdots + e_r f_r. \]

**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.