We will be concerned with the ring of integers $\mathcal{O}_K$ of a number field $K$, but we first recall some more generic facts about commutative rings and ideals.

Given two ideals $A, B \subseteq R$ of a commutative ring $R$ with identity,

$$AB = \{a_1b_1 + \cdots + a_nb_n : a_i \in A, b_i \in B, \ n \geq 1\}.$$  

Clearly $AB \subseteq A \cap B$ is an ideal. This construction works just as well on $R$-modules contained in the quotient field of an integral domain. In this case we may view ideals as just submodules of the ring $R$ viewed as a module over itself. Recall that an ideal $P \subseteq R$ is called prime if, whenever $IJ \subseteq P$, then either $I \subseteq P$ or $J \subseteq P$. Moreover, this is equivalent to saying the quotient ring $R/P$ is an integral domain. An ideal $M \subseteq R$ is called maximal if, whenever $M \subseteq I \subseteq R$ for an ideal $I$, either $I = M$ or $I = R$. This is equivalent to saying the quotient ring $R/M$ is a field. Finally, $R$ is called Noetherian if, given a sequence of ideals $I_1 \subseteq I_2 \subseteq \cdots$, there is an index $n$ such that $I_m = I_n$ for all $m \geq n$. Note that ideals in a Noetherian ring are necessarily finitely generated (any ideal not so clearly gives rise to an infinite ascending sequence of ideals by just using more and more generators).

Now consider the ring of integers $\mathcal{O}_K$ of a number field $K$. By a previous exercise, you showed that the index $N(I) := [\mathcal{O}_K : I]$ of any non-zero ideal $I \subseteq \mathcal{O}_K$ is finite. This gives us two immediate consequences. First, if $\mathfrak{P} \subseteq \mathcal{O}_K$ is a non-zero prime ideal (note the zero ideal is prime since $\mathcal{O}_K$ is an integral domain), then it necessarily is a maximal ideal as well, since $\mathcal{O}_K/\mathfrak{P}$ is a finite integral domain, whence a field. Second, $\mathcal{O}_K$ is Noetherian since given any sequence of ideals $\mathfrak{I}_1 \subseteq \mathfrak{I}_2 \subseteq \cdots$, there is an $n$ such that $N(\mathfrak{I}_n)$ is minimal, whence $\mathfrak{I}_m = \mathfrak{I}_n$ for all $m \geq n$.

We are keenly interested in how rational primes $p \in \mathbb{Z}$ factor in $\mathcal{O}_K$. Of course, we’ve seen that the question is not well-posed in general, since $\mathcal{O}_K$ need not have unique factorization. But if it did, then we would have a factorization of the form

$$p = u\pi_1^{e_1} \cdots \pi_r^{e_r}$$

where $u \in \mathcal{O}_K$ is a unit and the $\pi_i$s are irreducible elements of $\mathcal{O}_K$. As irreducible elements, we see that they generate maximal ideals $\pi_i\mathcal{O}_K$. Note that $p \in \pi_i\mathcal{O}_K$ for all $i$ by the above equation. Now by an exercise $\mathcal{O}_K/\pi_i$ is a finite field with $p^{e_i}$ elements and by another exercise $N_{K/\mathbb{Q}}(\alpha) = N(\alpha\mathcal{O}_K)$ for any non-zero $\alpha \in \mathcal{O}_K$. Setting $n = [K : \mathbb{Q}]$, we now take the norm of both sides of our equation above and then take the logarithm base $p$ to get

$$n = e_1f_1 + \cdots + e_rf_r.$$  

We would like to know if this holds in general, i.e., something akin to this (and applying this in the case where $\mathcal{O}_K$ is a UFD) is true for any number field $K$.

It will be extremely handy to use the following notion.

**Definition:** A (non-zero) fractional ideal of a number field $K$ is a non-zero $\mathcal{O}_K$-module $\mathfrak{I} \subset K$ such that $\alpha\mathfrak{I} \subseteq \mathcal{O}_K$ for some non-zero $\alpha \in \mathcal{O}_K$.

**Lemma:** The product of any two fractional ideals is a fractional ideal.

**Proof:** The product of any two modules is another module, so the only thing to check is the existence of the non-zero element of $\mathcal{O}_K$ in the definition. Let $\mathfrak{I}, \mathfrak{J}$ be non-zero fractional ideals and $\alpha_1, \alpha_2$ be non-zero elements of $\mathcal{O}_K$ with $\alpha_i\mathfrak{I}_i \subseteq \mathcal{O}_K$ for $i = 1, 2$. Then $\alpha_1\alpha_2\mathfrak{I}_1\mathfrak{J}_2 \subseteq \mathcal{O}_K$. 

1
Fundamental Theorem: The non-zero fractional ideals of a number field $K$ form an abelian group with identity $\mathcal{O}_K$. Moreover, this is a free group generated by the maximal (i.e., non-zero prime) ideals $\mathfrak{P}$ of $\mathcal{O}_K$. In other words, every non-zero fractional ideal $\mathfrak{I}$ can be uniquely written as a product

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

where the $\mathfrak{P}_i$s are maximal ideals and the $e_i$s are non-zero rational integers. (As usual, the empty product is interpreted to be the identity, $\mathcal{O}_K$.) In particular, every non-zero ideal $\mathfrak{I} \subseteq \mathcal{O}_K$ has such a unique representation where the exponents $e_i$ are all positive.

The last sentence says $\mathcal{O}_K$ is a Dedekind domain. Essentially what we prove here is that an integrally closed Noetherian integral domain where every non-zero prime ideal is maximal is a Dedekind domain. The converse is also true. In fact, there are a plethora of different, equivalent, descriptions/definitions for Dedekind domain. (Hungerford’s text has a list of 9 equivalent conditions!)

The proof of the Fundamental Theorem isn’t particularly short. We’ll break it up into several easier to digest pieces.

First of all, we claim that any non-zero ideal $\mathfrak{I} \subseteq \mathcal{O}_K$ contains some finite product of (not necessarily unique) maximal ideals: $\mathfrak{I} \supseteq \mathfrak{P}_1 \cdots \mathfrak{P}_l$. To see why, consider the set of all counterexamples and suppose this set is not empty. By the Noetherian property of $\mathcal{O}_K$ there must be a maximum counterexample, i.e., a non-zero ideal $\mathfrak{I}$ that doesn’t contain any such finite product of primes and any ideal $\mathfrak{J} \supseteq \mathfrak{I}$ does contain such a product. Now clearly $\mathfrak{I}$ itself can’t be a prime ideal, so get $\alpha, \beta \in \mathcal{O}_K$ with $\alpha \beta \in \mathfrak{I}$ but $\alpha, \beta \notin \mathfrak{I}$. Consider the ideals

$$(\mathfrak{I}, \alpha) = \{\gamma + \delta \alpha : \gamma \in \mathfrak{I}, \delta \in \mathcal{O}_K\}, \quad (\mathfrak{I}, \beta) = \{\gamma + \delta \beta : \gamma \in \mathfrak{I}, \delta \in \mathcal{O}_K\}.$$

These ideals clearly properly contain $\mathfrak{I}$, thus each contain some finite product of primes. But their product is contained within $\mathfrak{I}$ since $\alpha \beta \in \mathfrak{I}$, which implies that $\mathfrak{I}$ contains a finite product of primes.

Next, suppose $\mathfrak{P}$ is a non-zero prime ideal and set

$$\mathfrak{P}^{-1} = \{\alpha \in K : \alpha \mathfrak{P} \subseteq \mathcal{O}_K\}.$$

Obviously $\mathfrak{P}^{-1} \supseteq \mathcal{O}_K$. We claim that it strictly contains $\mathcal{O}_K$, however. To see why, take a non-zero $\alpha \in \mathfrak{P}$ and let $r$ be minimal such that the principal ideal $\alpha \mathcal{O}_K$ contains a product of $r$ maximal ideals (counted with multiplicity):

$$\alpha \mathcal{O}_K = \mathfrak{P}_1 \cdots \mathfrak{P}_r.$$

Since $\mathfrak{P} \supseteq \alpha \mathcal{O}_K$ and is a prime ideal, without loss of generality $\mathfrak{P}_1 = \mathfrak{P}$. (Remember: every non-zero prime ideal is maximal.) By construction, $\alpha \mathcal{O}_K$ does not contain the product $\mathfrak{P}_2 \cdots \mathfrak{P}_r$, so there is a $\beta \in \mathfrak{P}_2 \cdots \mathfrak{P}_r \setminus \alpha \mathcal{O}_K$. Now $\beta \mathfrak{P} \subseteq \mathfrak{P}_1 \cdots \mathfrak{P}_r \subseteq \alpha \mathcal{O}_K$, implying that $\beta \alpha^{-1} \in \mathfrak{P}^{-1}$. But $\beta \alpha^{-1} \notin \mathcal{O}_K$ by construction.

It’s trivial to verify that $\mathfrak{P}^{-1}$ is an $\mathcal{O}_K$-module and even a fractional ideal. We have $\mathfrak{P} \subseteq \mathfrak{P} \mathfrak{P}^{-1} \subseteq \mathcal{O}_K$. Now $\mathfrak{P} \mathfrak{P}^{-1}$, being a product of two fractional ideals, is another fractional ideal. But since it is contained in $\mathcal{O}_K$, it’s just a plain ideal. Now by the maximality of $\mathfrak{P}$, either $\mathfrak{P} \mathfrak{P}^{-1} = \mathfrak{P}$ or $\mathcal{O}_K$. Here is where the notion of “integrally closed” comes in. If $\mathfrak{P} \mathfrak{P}^{-1} = \mathfrak{P}$, then $\mathfrak{P}^{-1}$ leaves the finitely generated $\mathcal{O}_K$ module $\mathfrak{P}$ invariant. In particular, that means all elements of $\mathfrak{P}^{-1}$ are integral over $\mathcal{O}_K$. But (unassigned, whoops!) exercise #4 on page 39 of the textbook shows that any element of $K$ integral over $\mathcal{O}_K$ is in fact an algebraic integer (integral over $\mathbb{Z}$), thus in $\mathcal{O}_K$ by definition. (This is what we mean when we say $\mathcal{O}_K$ is integrally closed in its quotient field.) Since $\mathfrak{P}^{-1} \not\subseteq \mathcal{O}_K$, we conclude that $\mathfrak{P} \mathfrak{P}^{-1} \neq \mathfrak{P}$. The only other option is $\mathfrak{P} \mathfrak{P}^{-1} = \mathcal{O}_K$. Therefore, we have proven that every maximal ideal is “invertible” by a fractional ideal.
We next claim that any non-zero ideal is invertible by a fractional ideal. Indeed, if this were not the case, then by the Noetherian property of $\mathfrak{O}_K$ we can find a maximal counterexample $\mathfrak{I}$ (that is, maximal among the non-empty set of counterexamples). By what we have shown, $\mathfrak{I}$ can’t itself be a maximal ideal; instead, $\mathfrak{I} \subsetneq \mathfrak{P}$ for some maximal ideal $\mathfrak{P}$. Once again we can’t have $\mathfrak{P}\mathfrak{I}^{-1} = \mathfrak{I}$ since $\mathfrak{P}^{-1}$ contains an element not integral over $\mathfrak{O}_K$. On the other hand, we can’t have $\mathfrak{P}\mathfrak{I}^{-1} = \mathfrak{O}_K$ since $\mathfrak{I}$ isn’t invertible by hypothesis. The only remaining option is that $\mathfrak{J} := \mathfrak{P}\mathfrak{I}^{-1}$ is a strictly larger proper ideal. By the maximality of $\mathfrak{I}$, $\mathfrak{J}$ is invertible: $\mathfrak{J}^{-1} \mathfrak{J} = \mathfrak{O}_K$. But now $\mathfrak{P}\mathfrak{I}^{-1} \mathfrak{J}^{-1} = \mathfrak{J}^{-1} = \mathfrak{O}_K$, so that $\mathfrak{I}$ has an inverse after all!

Now suppose $\mathfrak{I}$ is a non-zero ideal, which we now know has a fractional ideal inverse $\mathfrak{I}^{-1}$. When $\mathfrak{I}$ is a maximal ideal, we have the description of $\mathfrak{I}^{-1}$ above. We assert that this is still the case:

$$\mathfrak{I}^{-1} = \{ \alpha \in K : \alpha \mathfrak{I} \subseteq \mathfrak{O}_K \}.$$ 

Certainly $\mathfrak{I}^{-1}$ is contained in this fractional ideal. On the other hand, if $\alpha \mathfrak{I} \subseteq \mathfrak{O}_K$ then $\alpha \mathfrak{I}^{-1} \subseteq \mathfrak{I}^{-1}$, which implies that $\alpha \in \mathfrak{I}^{-1}$ since $\mathfrak{I}^{-1} = \mathfrak{O}_K$.

Suppose $\mathfrak{I}$ is a non-zero fractional ideal and let $\alpha$ be a non-zero element of $\mathfrak{O}_K$ where $\alpha \mathfrak{I} \subseteq \mathfrak{O}_K$. The ideal $\alpha \mathfrak{I}$ is invertible by what we have shown. Moreover, by the above description of $(\alpha \mathfrak{I})^{-1}$ we readily see that $\alpha (\alpha \mathfrak{I})^{-1} \mathfrak{I} = \mathfrak{O}_K$ so that $\mathfrak{I}$ has an inverse: $\alpha (\alpha \mathfrak{I})^{-1}$. We have thus succeeded in proving that the non-zero fractional ideals form an abelian group.

The heavy lifting being done, we now can complete our proof. We first show that every non-zero ideal is a product of primes. If not, we use the same Noetherian argument to get a maximal counterexample $\mathfrak{J}$ which clearly can’t be a prime (maximal ideal) itself. Get a maximal ideal $\mathfrak{P} \supsetneq \mathfrak{J}$ and consider $\mathfrak{J} = \mathfrak{O}_K \mathfrak{J} \subsetneq \mathfrak{P}^{-1} \mathfrak{J} \subseteq \mathfrak{P}^{-1} \mathfrak{P} = \mathfrak{O}_K$. Once again, though, we can’t have $\mathfrak{P}^{-1} \mathfrak{J} = \mathfrak{J}$. Hence by hypothesis $\mathfrak{P}^{-1} \mathfrak{J}$ is a product of primes. Multiplying this product of primes by $\mathfrak{P}$ gives $\mathfrak{J}$ as a product of primes. The uniqueness of any product of primes is easy. If

$$\mathfrak{P}_1 \cdots \mathfrak{P}_r = \mathfrak{P}_1' \cdots \mathfrak{P}_s'$$

for maximal ideals $\mathfrak{P}_i$ and $\mathfrak{P}_j'$, then $\mathfrak{P}_1$ contains the second product. Since $\mathfrak{P}_1$ is a prime ideal, without loss of generality it contains, whence must be equal to, $\mathfrak{P}_1'$. Now multiply both sides by $\mathfrak{P}_1^{-1}$, rinse and repeat to show uniqueness. Finally, given any non-zero fractional ideal $\mathfrak{J}$, choose a non-zero $\alpha \in \mathfrak{O}_K$ where $\alpha \mathfrak{J}$ is an ideal. Writing this ideal as a product of primes and “dividing” by the principal ideal $\alpha \mathfrak{O}_K$ gives us a representation of $\mathfrak{J}$ as a product of prime powers (just cancel any primes occurring in both $\alpha \mathfrak{J}$ and $\alpha \mathfrak{O}_K$ as necessary).