5). It follows that $Q_1 \cap \cdots \cap Q_n = Q_1 \cdots Q_n$ (Theorem 17 in Section 7.6) so that $I$ is the product of primary ideals. The $P$-primary ideals of $R$ correspond bijectively with the $PR_P$-primary ideals in the localization $R_P$ (Proposition 42(3) in Section 15.4), and since $R_P$ is a D.V.R. (because (1) implies (2)), it follows from Corollary 6 that if $Q$ is a $P$-primary ideal in $R$ then $Q = P^m$ for some integer $m \geq 1$. Applying this to $Q_i$, $i = 1, \ldots, n$ shows that $I$ is the product of powers of prime ideals, which gives the first implication in (5).

Conversely, suppose that all the nonzero proper ideals of $R$ can be written as a product of prime ideals. We first show for any integral domain that a factorization of an ideal into *invertible* prime ideals is unique, i.e., if $P_1 \cdots P_n = \tilde{P}_1 \cdots \tilde{P}_m$ are two factorizations of $I$ into invertible prime ideals then $n = m$ and the two sets of primes $\{P_1, \ldots, P_n\}$ and $\{\tilde{P}_1, \ldots, \tilde{P}_m\}$ are equal. Suppose $\tilde{P}_1$ is a minimal element in the set $\{\tilde{P}_1, \ldots, \tilde{P}_m\}$. Since $P_1 \cdots P_n \subseteq \tilde{P}_1$, the prime ideal $\tilde{P}_1$ contains one of the primes $P_1, \ldots, P_n$, say $P_1 \subseteq \tilde{P}_1$. Similarly $P_1$ contains $\tilde{P}_i$ for some $i = 1, \ldots, m$. Then $\tilde{P}_i \subseteq P_1 \subseteq \tilde{P}_1$ and by the minimality of $\tilde{P}_1$ it follows that $\tilde{P}_i = P_1 = \tilde{P}_1$, so the factorization becomes $P_1 P_2 \cdots P_n = P_1 \tilde{P}_2 \cdots \tilde{P}_m$. Since $P_1$ is invertible, multiplying by the inverse ideal shows that $P_2 \cdots P_n = \tilde{P}_2 \cdots \tilde{P}_m$ and an easy induction finishes the proof. In particular, the uniqueness statement in (5) now follows from the first statement in (5) since in a Dedekind domain every fractional ideal, in particular every prime ideal of $R$, is invertible.

We next show that *invertible* primes in $R$ are maximal. Suppose then that $P$ is an invertible prime ideal in $R$ and take $a \in R, a \notin P$. We want to show that $P + aR = R$. By assumption, the two ideals $P + aR$ and $P + a^2R$ can be written as a product of prime ideals, say $P + aR = P_1 \cdots P_n$ and $P + a^2R = \tilde{P}_1 \cdots \tilde{P}_m$. Note that $P \subseteq P_i$ for $i = 1, \ldots, n$ and also $P \subseteq \tilde{P}_j$ for $j = 1, \ldots, m$. In the quotient $R/P$, which is an integral domain, we have the factorization $(\bar{a}) = (P_1/P) \cdots (P_n/P)$, and each $P_i/P$ is a prime ideal in $R/P$. Since the product is a principal ideal, each $P_i/P$ is also an invertible $R/P$-ideal (cf. Exercise 2). Similarly, $(\bar{a}^2) = (\tilde{P}_1/P) \cdots (\tilde{P}_m/P)$ is a factorization into a product of invertible prime ideals. Then $(\bar{a})^2 = (P_1/P)^2 \cdots (P_n/P)^2 = (\tilde{P}_1/P) \cdots (\tilde{P}_m/P)$ give two factorizations into a product of invertible prime ideals in the integral domain $R/P$, so by the uniqueness result in the previous paragraph, $m = 2n$ and $\{P_1/P, P_1/P, \ldots, P_n/P, P_n/P\} = \{\tilde{P}_1/P, \ldots, \tilde{P}_m/P\}$. It follows that the set of primes $\tilde{P}_1, \ldots, \tilde{P}_m$ in $R$ consists of the primes $P_1, \ldots, P_n$, each repeated twice. This shows that $P + a^2R = (P + aR)^2$. Since $P \subseteq P + a^2R$ and $(P + aR)^2 \subseteq P^2 + aR$, we have $P \subseteq P^2 + aR$, so every element $x$ in $P$ can be written in the form $x = y + az$ where $y \in P^2$ and $z \in R$. Then $az = x - y \in P$ and since $a \notin P$, we have $z \in P$, which shows that $P \subseteq P^2 + aP$. Clearly $P^2 + aP \subseteq P$ and so $P = P^2 + aP = P(P + aR)$. Since $P$ is assumed invertible, it follows that $R = P + aR$ for any $a \in R - P$, which proves that $P$ is a maximal ideal.

We now show that every nonzero prime ideal is invertible. If $P$ is a nonzero prime ideal, let $a$ be any nonzero element in $P$. By assumption, $Ra = P_1 \cdots P_n$ can be written as a product of prime ideals, and $P_1, \ldots, P_n$ are invertible since their product is principal (by Exercise 2 again). Since $P_1 \cdots P_n = Ra \subseteq P$, the prime ideal $P$ contains $P_i$ for some $1 \leq i \leq n$. Since $P_i$ is maximal by the previous paragraph, it follows that

$P = P_i$ is invertible.

Finally, since every nonzero proper ideal of $R$ is a product of prime ideals, it follows that every nonzero ideal of $R$ is invertible, and since every fractional ideal of $R$ is of the form $(d^{-1})I$ for some ideal in $R$, also every fractional ideal of $R$ is invertible. This proves that (5) implies (3), and complete the proof of the theorem.

The following corollary follows immediately from Proposition 14:

**Corollary 16.** If $\mathcal{O}_K$ is the ring of integers in an algebraic number field $K$ then every nonzero ideal $I$ in $\mathcal{O}_K$ can be written uniquely as the product of powers of distinct prime ideals:

$$I = P_1^{e_1} P_2^{e_2} \cdots P_n^{e_n},$$

where $P_1, \ldots, P_n$ are distinct prime ideals and $e_i \geq 1$ for $i = 1, \ldots, n$.

*Remark:* The development of Dedekind Domains given here reverses the historical development. As mentioned in Section 9.3, the unique factorization of nonzero *ideals* into a product of prime *ideals* replaces the failure of unique factorization of nonzero *elements* into products of prime *elements* in rings of integers of number fields. This property of rings of integers in Corollary 16 is what led originally to the definition of an ideal, and Dedekind originally defined what we now call Dedekind Domains by property 5 in Theorem 15. It was Noether who observed that they can also be characterized by property (1), which we have taken as the initial definition of a Dedekind Domain.

The unique factorization into prime ideals in Dedekind Domains can be used to explicitly define the valuations $v_P$ on $R$ with respect to which the valuation rings are the localizations $R_P$ in Theorem 15(2) (cf. Exercise 6). We now indicate how unique factorization for ideals can be used to define a divisibility theory for ideals similar to the divisibility of integers in $\mathbb{Z}$.

**Definition.** If $A$ and $B$ are ideals in the integral domain $R$ then $B$ is said to *divide* $A$ (and $A$ is *divisible by* $B$) if there is an ideal $C$ in $R$ with $A = BC$.

If $B$ divides $A$ then certainly $A \subseteq B$. If $R$ is a Dedekind Domain, the converse is true: $A \subseteq B$ implies $C = AB^{-1} \subseteq BB^{-1} = R$ so $C$ is an ideal in $R$ with $BC = A$.

We can also define the notion of the *greatest common divisor* $(A, B)$ of two ideals $A$ and $B$: $(A, B)$ divides both $A$ and $B$ and any ideal dividing both $A$ and $B$ divides $(A, B)$. The second statement in the next proposition shows that this greatest common divisor always exists for integral ideals in a Dedekind Domain and gives a formula for it similar to the formula for the greatest common divisor of two integers.

**Proposition 17.** Suppose $R$ is a Dedekind Domain and $A$, $B$ are two nonzero ideals in $R$, with prime ideal factorizations $A = P_1^{e_1} \cdots P_n^{e_n}$ and $B = P_1^{f_1} \cdots P_n^{f_n}$ (where $e_i, f_i \geq 0$ for $i = 1, \ldots, n$). Then

**(1)** $A \subseteq B$ if and only if $B$ divides $A$ (i.e., "to contain is to divide") if and only if $f_i \leq e_i$ for $i = 1, \ldots, n$,

(2) $A + B = (A, B) = P_1^{\min(e_1, f_1)} \cdots P_n^{\min(e_n, f_n)}$, so in particular $A$ and $B$ are relatively prime, $A + B = R$, if and only if they have no prime ideal factors in common.

*Proof:* We proved the first statement in (1) above. If each $f_i \leq e_i$, then taking $C = P_1^{e_1 - f_1} \cdots P_n^{e_n - f_n} \subseteq R$ shows that $B$ divides $A$. Conversely, if $B$ divides $A$, then writing $C$ as a product of prime ideals in $A = BC$ shows that $f_i \leq e_i$ for all $i$, which proves all of (1). Since $A + B$ is the smallest ideal containing both $A$ and $B$, (2) now follows from (1).

**Proposition 18.** *(Chinese Remainder Theorem)* Suppose $R$ is a Dedekind Domain, $P_1, P_2, \ldots, P_n$ are distinct prime ideals in $R$ and $a_i \geq 0$ are integers, $i = 1, \ldots, n$. Then

$$R/P_1^{a_1} \cdots P_n^{a_n} \cong R/P_1^{a_1} \times R/P_2^{a_2} \times \cdots \times R/P_n^{a_n}.$$

Equivalently, for any elements $r_1, r_2, \ldots, r_n \in R$ there exists an element $r \in R$, unique up to an element in $P_1^{a_1} \cdots P_n^{a_n}$, with

$$r \equiv r_1 \bmod P_1^{a_1}, \quad r \equiv r_2 \bmod P_2^{a_2}, \quad \ldots, \quad r \equiv r_n \bmod P_n^{a_n}.$$

*Proof:* This is immediate from Theorem 17 in Section 7.6 since the previous proposition shows that the $P_i^{a_i}$ are pairwise comaximal ideals.

**Corollary 19.** Suppose $I$ is an ideal in the Dedekind Domain $R$. Then

(1) there is an ideal $J$ of $R$ relatively prime to $I$ such that the product $IJ = (a)$ is a principal ideal,

(2) if $I$ is nonzero then every ideal in the quotient $R/I$ is principal; equivalently, if $I_1$ is an ideal of $R$ containing $I$ then $I_1 = I + Rb$ for some $b \in R$, and

(3) every ideal in $R$ can be generated by two elements; in fact if $I$ is nonzero and $0 \neq a \in I$ then $I = Ra + Rb$ for some $b \in I$.

*Proof:* Suppose $I = P_1^{e_1} \cdots P_n^{e_n}$ is the prime ideal factorization of $I$ in $R$. For each $i = 1, \ldots, n$, let $r_i$ be an element of $P_i^{e_i} - P_i^{e_i+1}$. By the proposition, there is an element $a \in R$ with $a \equiv r_i \bmod P_i^{e_i+1}$ for all $i$. Hence $a \in P_i^{e_i} - P_i^{e_i+1}$ for all $i$, so the power of $P_i$ in prime ideal factorization of $(a)$ is precisely $e_i$ by (1) of Proposition 17:

$$(a) = P_1^{e_1} \cdots P_n^{e_n} P_{n+1}^{e_{n+1}} \cdots P_m^{e_m}$$

for some prime ideals $P_{n+1}, \ldots, P_m$ distinct from $P_1, \ldots, P_n$. Letting $J = P_{n+1}^{e_{n+1}} \cdots P_m^{e_m}$ gives (1). For (2), by the Chinese Remainder Theorem it suffices to prove that every ideal in $R/P^m$ is principal in the case of a power of a prime ideal $P$, and this is immediate since $R/P^m \cong R_P/P^m R_P$ and the localization $R_P$ is a P.I.D. Finally, (3) follows from (2) by taking $I = Ra$.

The first statement in Corollary 19 shows that there is an integral ideal $J$ relatively prime to $I$ lying in the inverse class of $I$ in the class group of $R$. One can even impose additional conditions on $J$, cf. Exercise 11.