Module MA3412: Integral Domains, Modules and Algebraic Integers
Section 5
Hilary Term 2014

D. R. Wilkins

Contents

5 Discrete Valuations and Dedekind Domains **81**
5.1 The Valuation Ring of a Discrete Valuation 81
5.2 Discrete Valuation Rings 84
5.3 Local Domains 86
5.4 Dedekind Domains 87
5.5 Divisibility Of Ideals in Dedekind Domains 87
5.6 Localization in Integral Domains 92
5.7 Factorization of Ideals in Dedekind Domains 97
5.8 Divisibility of Ideals in Integral Domains 100
5.9 Discrete Valuations on Dedekind Domains 104
5.10 Uniqueness of Ideal Factorization in Dedekind Domains 107
5.11 The Class Group of a Dedekind Domain 107
5.12 Fractional Ideals 109
5.13 Characterizations of Dedekind Domains 111

5 Discrete Valuations and Dedekind Domains

5.1 The Valuation Ring of a Discrete Valuation

Definition Let K be a field, and let $\mathbb{Z} \cup \{\infty\}$ be the set obtained from the ring $\mathbb{Z}$ of integers by adding a symbol ∞ with the properties that $\infty + \infty = \infty$, $n + \infty = \infty + n = \infty$, $\infty - n = \infty$ and $\infty > n$ for all integers n. A *discrete valuation* on the field K is a function $\nu: K \to \mathbb{Z} \cup \{\infty\}$ which satisfies the following conditions:

(i) $\nu(a) = \infty$ if and only if $a = 0_K$;

(ii) $\nu(ab) = \nu(a) + \nu(b)$ for all $a, b \in K$;

(iii) $\nu(a + b) \geq \min(\nu(a), \nu(b))$ for all $a, b \in K$.

Example Let p be a prime number. Then, given any non-zero rational number r, there exist integers k, u and v such that $r = p^k uv^{-1}$ and neither u nor v is divisible by p. The integer k is uniquely determined by r, and we define $\nu_{(p)}(r) = k$. We also define $\nu_{(p)}(0) = \infty$. Then the function

$$\nu_{(p)}: \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$$

defined in this fashion is a discrete valuation on the field $\mathbb{Q}$ of rational numbers.

Lemma 5.1 *Let R be an integral domain that is embedded as a subring of its field of fractions K, and let p be a prime element of R. Then p determines a discrete valuation*

$$\nu_{(p)}: K \to \mathbb{Z} \cup \{\infty\}$$

on K such that $\nu_{(p)}(r) \geq 0$ for all $r \in R$, $\nu_{(p)}(p) = 1$ and $\nu_{(p)}(r) = 0$ for all non-zero elements r of R that are not divisible by p.

Proof Let p be a prime element of R. Then, given any non-zero element c of K, there exists a unique integer k_c such that $c = p^{k_c} uv^{-1}$ for some non-zero elements u and v of R that are not divisible by p. Let $\nu_{(p)}(c) = k_c$. Also let $\nu_{(p)}(0_K) = \infty$. We obtain in this fashion a well-defined function $\nu_{(p)}: K \to \mathbb{Z} \cup \{\infty\}$. If c is a non-zero element of R then $c = p^k u$, where k is some non-negative integer and u is some non-zero element of R that is not divisible by p. It follows that $\nu_{(p)}(r) \geq 0$ for all $r \in R$. Also $\nu(p) = 1$, and $\nu(r) = 0$ for all non-zero elements of r that are not divisible by p.

Let c_1 and c_2 be non-zero elements of K. Then there exist integers k_1 and k_2 such that $c_1 = p^{k_1} u_1 v_1^{-1}$ and $c_2 = p^{k_2} u_2 v_2^{-1}$. Then $\nu_{(p)}(c_1) = k_1$ and

$\nu_{(p)}(c_2) = k_2$. Now $c_1c_2 = p^{k_1+k_2}(u_1u_2)(v_1v_2)^{-1}$. Moreover neither u_1u_2 nor v_1v_2 is divisible by p. It follows that

$$\nu_{(p)}(c_1c_2) = k_1 + k_2 = \nu_{(p)}(c_1) + \nu_{(p)}(c_2).$$

Let $k = \min(k_1, k_2)$. Then

$$c_1 + c_2 = p^k(v_2p^{k_1-k}u_1 + v_1p^{k_2-k}u_2)(v_1v_2)^{-1},$$

and therefore

$$\nu_{(p)}(c_1 + c_2) \geq k = \min(\nu(c_1), \nu(c_2)).$$

Thus $\nu_{(p)}\colon K \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation on K with the required properties. ∎

Proposition 5.2 *Let K be a field, let $\nu\colon K \to \mathbb{Z}\cup\{\infty\}$ be a discrete valuation on K, where $\nu(c) \neq 0$ for at least one non-zero element c of K, and let*

$$R = \{c \in K : \nu(c) \geq 0\}.$$

Then R is a subring of K with exactly one maximal ideal M. This maximal ideal M satisfies

$$M = \{c \in K : \nu(c) > 0\}.$$

Moreover the ring R is a principal ideal domain, and, given any non-zero proper ideal I of R, there exists a positive integer k such that $I = M^k$.

Proof The multiplicative identity element 1_K of K satisfies $1_K \neq 0_K$ and $1_K^2 = 1_K$. It follows that $\nu(1_K) \neq \infty$, and therefore $\nu(1_K) \in \mathbb{Z}$ and $\nu(1_K) + \nu(1_K) = \nu(1_K)$. Therefore $\nu(1_K) = 0$, and thus $1_K \in R$. Also $(-1_K)^2 = 1_K$. It follows that $2\nu(-1_K) = 0$, and therefore $-1_K \in R$. If $r \in R$ and $s \in R$ then $\nu(r + s) \geq \min(\nu(r), \nu(s)) \geq 0$ and $\nu(rs) = \nu(r) + \nu(s) \geq 0$, and therefore $r + s \in R$ and $rs \in R$. Also $-r = (-1_K)r$, and therefore $-r$ in R. Thus R is a subring of R. Moreover R is an integral domain, because it is a subring of a field.

Let c be a non-zero element of K. Then $\nu(c^{-1}) + \nu(c) = \nu(c^{-1}c) = \nu(1_K) = 0$, and therefore $\nu(c^{-1}) = -\nu(c)$. It follows that an element u of R is a unit of R if and only if $\nu(u) = 0$.

If a and b are elements of M and if r is an element of R then $\nu(a + b) \geq \min(\nu(a), \nu(b)) > 0$, $\nu(-a) = \nu(-1_K) + \nu(a) = \nu(a) > 0$, and $\nu(ra) = \nu(r) + \nu(a) \geq \nu(a) > 0$, and therefore $a + b \in M$, $-a \in M$ and $ra \in M$. It follows that M is an ideal of R.

If I is an ideal of R, and if $I \not\subset M$, then there exists some element u of I satisfying $\nu(u) = 0$. Then u is a unit of R, and therefore $I = R$. This proves

that M is a maximal ideal of R. Moreover if N is a maximal ideal of R, then $N \subset M$, and therefore $N = M$. Thus M is the only maximal ideal of R.

The value of $\nu(r)$ is a positive integer for all non-zero $r \in M$. It follows that there exists an element p of M such that $\nu(p) \leq \nu(r)$ for all $r \in M$. Then $\nu(p^{-1}r) \geq 0$ for all $r \in M$, and therefore $p^{-1}r \in R$ for all $r \in M$. Thus p divides every element of M in the ring R. It follows that the ideal M is the principal ideal generated by p.

Let K^* be the multiplicative group of non-zero elements of the field K. Then $\nu(K^*)$ is an additive subgroup of $\mathbb{Z}$, because $\nu|K^*: K^* \to \mathbb{Z}$ is a homomorphism of groups. It follows that $\nu(K^*) = d\mathbb{Z}$, where $d = \nu(p)$. Thus $\nu(p)$ divides $\nu(r)$ for all $r \in R$. Let r be a non-zero element of M. Then $\nu(r) = dk$ for some positive integer k. But then $\nu(p^{-k}r) = -kd + \nu(r) = 0$, and thus $p^{-k}r$ is a unit of the integral domain R. Thus $r = p^k u$, where k is a positive integer and u is a unit of R.

Let I be a non-zero proper ideal of R. Then there exists $r_0 \in I$ such that $r_0 \neq 0_R$ and $\nu(r_0) \leq \nu(r)$ for all $r \in I$. Then r_0 divides every element r of I, and thus $I = (r_0)$. Moreover $\nu(r_0) = dk$ for some positive integer k, where $d = \nu(p)$. But then $r_0 = p^k u$ for some unit u of R. It follows that

$$I = (r_0) = (p^k) = (p)^k = M^k.$$

Thus R is a principal ideal domain, and every non-zero proper ideal of R is of the form M^k for some positive integer k, as required. ∎

Definition Let K be a field, and let $\nu: K \to \mathbb{Z} \cup \{\infty\}$ be a discrete valuation on K. The *valuation ring* determined by this valuation is the subring R of K defined such that

$$R = \{c \in K : \nu(c) \geq 0\}.$$

Lemma 5.3 *Let K be a field, and let $\nu: K \to \mathbb{Z} \cup \{\infty\}$ be a discrete valuation on K. Then the valuation ring R of ν is integrally closed.*

Proof Let $f(x)$ be a monic polynomial of degree n with coefficients in R, where $n > 0$. Then there exist elements $a_0, a_1, \ldots, a_{n-1}$ of R such that

$$f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i.$$

Let c be a non-zero element of the field K. Then

$$f(c) - c^n = \sum_{i=0}^{n-1} a_i c^i,$$

and $\nu(a_i) \geq 0$ for $i = 0, 1, \ldots, n-1$. If $\nu(c) < 0$ then

$$\nu(a_i c^i) = \nu(a_i) + i\nu(c) \geq i\nu(c) \geq (n-1)\nu(c)$$

for $i = 0, 1, \ldots, n-1$, and therefore

$$\nu(c^n - f(c)) = \nu(f(c) - c^n) \geq (n-1)\nu(c) > n\nu(c) = \nu(c^n).$$

Thus $\nu(c^n - f(c)) > \nu(c^n)$ whenever $\nu(c) < 0$, and therefore $f(c) \neq 0_K$ whenever $\nu(c) < 0$. It follows that a non-zero element c of K cannot be a root of the polynomial $f(x)$ unless it belongs to the valuation ring R. Thus R is integrally closed. ∎

5.2 Discrete Valuation Rings

Let R be an integral domain embedded in its field of fractions K as a subring of K, and let p be a prime element of R. Then p determines a corresponding valuation $\nu_{(p)}: K \to \mathbb{Z} \cup \{\infty\}$. on the field K. The valuation ring $R_{(p)}$ of the valuation $\nu_{(p)}$ is the subring of K consisting of all elements c of K for which $\nu_{(p)}(c) \geq 0$. It follows that

$$R_{(p)} = \{rs^{-1} : r, s \in R \text{ and } p \text{ does not divide } s\}.$$

Thus the valuation ring $R_{(p)}$ may be regarded as the ring of fractions $S_{(p)}^{-1}R$, where $S_{(p)}$ is the multiplicatively closed subset of R consisting of all elements of R that are not divisible by the prime element p of R.

Now the principal ideal (p) generated by the prime element p of R is a prime ideal of R (see Lemma 2.19). The multiplicatively closed subset $S_{(p)}$ is the complement $R \setminus (p)$ of (p) in R. It follows from the definition of localizations of rings at prime ideals that the valuation ring $R_{(p)}$ is the localization of the integral domain R at the prime ideal (p).

The basic properties of the valuation rings determined by discrete valuations on a field K are set out in the statement of Proposition 5.2. That proposition shows in particular that the valuation ring R of a discrete valuation is an integral domain that has a unique maximal ideal M. Moreover every non-zero proper ideal of R is of the form M^k for some positive integer k. We shall show that these properties characterize those rings that are the valuation rings of discrete valuations.

Definition A *discrete valuation ring* is an integral domain R with a unique maximal ideal M whose proper ideals are all of the form M^k for some positive integer k.

Proposition 5.4 *Let R be a discrete valuation ring embedded in its field of fractions K as a subring of K, and let M be the unique maximal ideal of R. If M is the zero ideal then R is a field, and is the valuation ring determined by the trivial valuation on R. If M is not the zero ideal then $M = (p)$ for some prime element p of R. There is then a well-defined discrete valuation $\nu_{(p)}: K \to \mathbb{Z} \cup \{\infty\}$ on K characterized by the property that $\nu_{(p)}(p^k u) = k$ for all integers k and for all units u of R. The ring R is then the valuation ring determined by the discrete valuation $\nu_{(p)}$ on the field of fractions K of R.*

Proof If M is the zero ideal then the only ideals of R are the zero ideal and the whole of R, and therefore R is a field, and thus $R = K$. The valuation ring of a trivial valuation is the whole of the field on which the valuation is defined.

It remains to consider the case where M is a non-zero proper ideal of R. First we show that there exists an element p of R for which $(p) = M$. If there were no element p of M satisfying $(p) = M$ then, given any non-zero element r of M, there would exist some integer k satisfying $k \geq 2$ for which $(r) = M^k$, and therefore $r \in M^2$ for all $r \in M$, and thus $M \subset M^2$. But then $M^2 = M$, and therefore $M^k = M$ for all positive integers k, contradicting the assumption that there is no element p of M for which $M = (p)$. Therefore there must exist some element p of M for which $(p) = M$. Moreover p is a prime element of R, because the ideal (p) is a maximal ideal of R.

The prime element p of R determines a discrete valuation $\nu_{(p)}: K \to \mathbb{Z} \cup \{\infty\}$, where $\nu_{(p)}(p) = 1$ and $\nu_{(p)}(r) = 0$ for all elements r of R that are not divisible by p (see Lemma 5.1). Then $\nu_{(p)}(r) \geq 0$ for all $r \in R$, and $\nu_{(p)}(p^k u) = k$ for all integers k and units u of R.

Let c be a non-zero element of the field of fractions K which satisfies $\nu_{(p)}(c) \geq 0$. Then there exist non-zero elements r and s of R such that $sc = r$. Let $(r) = (p^k)$ and $(s) = (p^l)$. Then there exist units u and v of R such that $r = p^k u$ and $s = p^l v$. It follows that $\nu_{(p)}(r) = k$ and $\nu(p)(s) = l$. Then $c = p^{k-l} u v^{-1}$. Moreover $k - l = \nu_{(p)}(c) \geq 0$. It follows that $c \in R$. Thus R is the valuation ring determined by the discrete valuation $\nu_{(p)}$ on the field of fractions K, as required. ∎

Corollary 5.5 *Every discrete valuation ring is a principal ideal domain.*

Proof Let R be a discrete valuation ring, and let M be the unique maximal ideal of R. It follows from Proposition 5.4 that there exists an element p of M that generates the maximal ideal M. But then $M^k = (p)^k = (p^k)$ for all positive integers k. Thus M^k is a principal ideal for all positive integers k. But the only ideals of the discrete valuation ring R are these ideals M^k. Therefore R is a principal ideal domain. ∎

Corollary 5.6 *Every discrete valuation ring is an integrally-closed domain.*

Proof A discrete valuation ring is the valuation ring of some discrete valuation defined on its field of fractions (Corollary 5.4) But the valuation ring of any discrete valuation is integrally closed (Lemma 5.3). The result follows. ∎

Remark Corollary 5.6 can also be deduced as follows. Every discrete valuation ring is a principal ideal domain (Corollary 5.5). Every principal ideal domain is a unique factorization domain (Lemma 2.23). And every unique factorization domain is integrally closed (Proposition 2.47).

5.3 Local Domains

Definition A unital commutative ring is said to be *local* if it has exactly one maximal ideal.

Definition A *local domain* is an integral domain that has exactly one maximal ideal.

Proposition 5.7 *A local domain is a discrete valuation ring if and only if it is a principal ideal domain.*

Proof A field is a discrete valuation ring, a local domain and a principal ideal domain.

It follows from Corollary 5.5 that every discrete valuation ring is a principal ideal domain.

Let R be a local domain that is not a field but is a principal ideal domain, and let M be the unique maximal ideal of R. Every non-zero prime element of a principal ideal domain generates a maximal ideal of that domain (see Lemma 2.24). Because the local domain R has only one maximal ideal, it follows that all prime elements of R are associates of one another.

Let p be a prime element of R. Then $M = (p)$. Every principal ideal domain is a unique factorization domain (Lemma 2.23). Therefore every element of R factors as a product of prime elements of R. Therefore every non-zero element of R that is not a unit of R can be represented uniquely in the form $p^k u$, where k is a positive integer and u is a unit of R. It follows if I is a non-zero proper ideal of R then I is a principal ideal, and therefore $I = (p^k) = (p)^k = M^k$ for some positive integer. Thus R is a discrete valuation ring. The result follows. ∎

5.4 Dedekind Domains

Definition A *Dedekind domain* is an integrally-closed Noetherian domain in which every non-zero prime ideal is maximal.

It follows from this definition that a unital commutative ring R is a Dedekind domain if and only if it possesses all four of the following properties:

(i) R is an integral domain;

(ii) every ideal of R is finitely generated,

(iii) R is integrally closed in its field of fractions;

(iv) every non-zero prime ideal of R is maximal.

Properties (i) and (ii) characterize Noetherian domains, and property (iii) characterizes integrally-closed domains.

Lemma 5.8 *Every principal ideal domain is a Dedekind domain.*

Proof Let I be an ideal of a principal ideal domain R. Then $I = (r)$ for some $r \in I$, and thus I is finitely generated. Therefore every principal ideal domain is Noetherian domain.

Principal ideal domains are unique factorization domains (Lemma 2.23), and unique factorization domains are integrally closed (Proposition 2.47). Therefore every principal ideal domain is integrally closed.

Every non-zero prime ideal of a principal ideal domain is a maximal ideal (Lemma 2.24). The result follows. ∎

Example It follows from Proposition 4.29 that the ring of integers of any quadratic number field is a Dedekind domain.

The ring of integers of any algebraic number field can be shown to be a Dedekind domain.

5.5 Divisibility Of Ideals in Dedekind Domains

We shall prove that if P is a maximal ideal of a Dedekind domain R, then P divides all ideals contained within it.

Given an ideal I of a unital commutative ring R, and given $a \in R$, we denote by aI the ideal $\{au : u \in I\}$. This ideal aI is the product $(a)I$ of the principal ideal (a) and the ideal I.

Lemma 5.9 *Let R be an integral domain, let a be a non-zero element of R, and let I and J be ideals of R. If $aI \subset aJ$, then $I \subset J$, and if $aI = aJ$ then $I = J$.*

Proof Suppose that $aI \subset aJ$. Then, given any $u \in I$, there exists $v \in J$ such that $au = av$. But then $u = v$, because R is an integral domain and $a \neq 0_R$. It follows that $u \in J$. Thus $I \subset J$ whenever $aI \subset aJ$. It follows that if I and J are ideals of R satisfying $aI = aJ$ then $J \subset I$ and $I \subset J$, and therefore $I = J$, as required. ∎

Lemma 5.10 *Let R be a Noetherian ring. Then any proper ideal of R is contained in a maximal ideal of R.*

Proof Let I be a proper ideal of R, and $\mathcal{C}$ be the collection consisting of all proper ideals J of R satisfying $I \subset J$. This collection has a maximal element M, because R is Noetherian (see Proposition 3.5). Then M is a proper ideal of R that is not contained in any other proper ideal of R. This ideal is thus a maximal ideal of R, and $I \subset M$, as required. ∎

Remark There is an axiom of set theory, known as the Axiom of Choice, which is equivalent to the statement that any Cartesian product of non-empty sets is non-empty. A consequence of this axiom is *Zorn's Lemma*, which is invoked to justify the existence of maximal elements of partially-ordered sets in which every totally-ordered subset is bounded above.

A relation $\preceq$ on a set $\mathcal{S}$ is said to be a *partial order* if it is reflexive, transitive and anti-symmetric. Thus the relation $\preceq$ on $\mathcal{S}$ is a partial order on $\mathcal{S}$ if and only if the following conditions are satisfied: $x \preceq x$ for all $x \in \mathcal{S}$; $x \preceq y$ and $y \preceq z$ together imply $x \preceq z$ for all $x, y, z \in \mathcal{S}$; $x \preceq y$ and $y \preceq x$ together imply $x = y$ for all $x, y \in \mathcal{S}$. A subset $\mathcal{T}$ of a partially-ordered set $\mathcal{S}$ is said to be *totally ordered* if, given $x, y \in \mathcal{T}$, either $x \preceq y$ or $y \preceq x$. An element u of $\mathcal{S}$ is an *upper bound* for a totally-ordered subset $\mathcal{T}$ of $\mathcal{S}$ if $x \preceq u$ for all $x \in \mathcal{T}$. An element x of $\mathcal{S}$ is said to be *maximal* if there does not exist any element y of $\mathcal{S}$ satisfying $x \neq y$ and $x \preceq y$.

Zorn's Lemma may be stated as follows:

> **Zorn's Lemma.** Let $\mathcal{S}$ be a non-empty partially-ordered set. Suppose that there exists an upper bound for each totally-ordered subset of $\mathcal{S}$. Then $\mathcal{S}$ contains a maximal element.

Let I be a proper ideal of a unital commutative ring R, and let $\mathcal{S}$ be the set of proper ideals J of R that satisfy $I \subset J$. Now set inclusion is a partial order on the set $\mathcal{S}$. Given any totally-ordered subset $\mathcal{T}$ of $\mathcal{S}$, the union of

the proper ideals of R belonging to $\mathcal{T}$ is itself a proper ideal of R, and is an upper bound for $\mathcal{T}$. Assuming Zorn's Lemma, we conclude that the set $\mathcal{S}$ has a maximal element M. This maximal element is a maximal ideal of R, and $I \subset M$. Thus it is a consequence of Zorn's Lemma that every proper ideal of a unital commutative ring R is contained in a maximal ideal of that ring.

Proposition 5.11 *Let R be a Noetherian ring. Then every non-zero ideal of R contains a product of one or more non-zero prime ideals of R.*

Proof Let $\mathcal{C}$ be the collection consisting of all ideals of R that do not contain a product of one or more non-zero prime ideals of R. We must prove that this collection $\mathcal{C}$ is empty.

Suppose that the collection $\mathcal{C}$ were non-empty. Then it would contain a maximal element, because the ring R is Noetherian (Proposition 3.5). Suppose that the ideal I were a maximal element of the collection $\mathcal{C}$. Then I would not itself be a prime ideal, and therefore there would exist ideals J and K such that $J \not\subset I$, $K \not\subset I$ and $JK \subset I$ (see Lemma 2.20). Then $I + J \neq I$, $I + K \neq I$ and $(I + J)(I + K) \subset I$. The maximality of I would ensure that neither $I + J$ nor $I + K$ would belong to the collection $\mathcal{C}$. Therefore there would exist non-zero prime ideals $P_1, P_2, \ldots, P_s$ and $Q_1, Q_2, \ldots, Q_t$ such that

$$P_1P_2 \cdots P_s \subset I + J \quad \text{and} \quad Q_1Q_2 \cdots P_t \subset I + K.$$

But then

$$P_1P_2 \cdots P_sQ_1Q_2 \cdots Q_t \subset I,$$

and therefore the ideal I would not belong to the collection $\mathcal{C}$, contradicting the choice of I as a maximal element of this collection. The result follows. ∎

The following result, applicable to finitely-generated ideals in integrally-closed domains, makes use of the Determinant Trick (Proposition 4.11) that provides a convenient framework for obtaining results concerning finitely-generated ideals and modules that are consequences of the Cayley-Hamilton Theorem (Theorem 4.9).

Proposition 5.12 *Let R be an integrally-closed domain, let J be a finitely-generated non-zero ideal of R, and let r and s be non-zero elements of R. Suppose that $rJ \subset sJ$. Then s divides r in R.*

Proof There is a well-defined R-module endomorphism $\varphi\colon J \to J$ of J defined such that $rv = s\varphi(v)$ for all $v \in J$. It then follows from an application

of the Determinant Trick that there exists a positive integer n and elements $a_0, a_1, \ldots, a_{n-1}$ of R such that

$$\varphi^n(v) + \sum_{k=0}^{n-1} a_k \varphi^k(v) = 0_R$$

for all $v \in J$ (see Corollary 4.15, which is a special case of Proposition 4.11). On multiplying this identity by s^n and applying the definition of φ, we find that

$$r^n v + \sum_{k=0}^{n-1} a_k s^{n-k} r^k v = 0_R$$

for all $v \in J$, and therefore

$$r^n + \sum_{k=0}^{n-1} a_k s^{n-k} r^k = 0_R.$$

Thus the element r/s of the field of fractions of R is integral over R. But R is integrally closed in its field of fractions. It follows that s divides r in R, as required. ∎

Proposition 5.13 *Let R be a Dedekind domain, let P be a maximal ideal of R, let I be a non-zero ideal of R satisfying $I \subset P$, and let*

$$L = \{r \in R : rP \subset I\}.$$

Then $PL = I$.

Proof It follows from the definition of L that $PL \subset I$. We must prove that $I \subset PL$.

Let s be a non-zero element of I, and let $N = \{r \in R : rP \subset (s)\}$. Then N is an ideal of R, $s \in N$ and $sP \subset PN \subset (s)$.

The Dedekind domain R is a Noetherian domain. It follows from Proposition 5.11 that the principal ideal (s) contains some product of non-zero prime ideals of R. Let n be the smallest positive integer such that (s) contains a product of n non-zero prime ideals of R, and let $Q_1, Q_2, \ldots, Q_n$ be non-zero prime ideals of R satisfying

$$Q_1 Q_2 \cdots Q_n \subset (s).$$

Now every maximal ideal of R is a prime ideal (Lemma 2.15). Moreover a product of ideals is contained in a prime ideal if and only if one of the factors

of that product is contained in the prime ideal (see Lemma 2.20). Therefore $Q_i \subset P$ for at least one value of i between 1 and n. We may suppose that $Q_1 \subset P$.

Every non-zero prime ideal of the Dedekind domain R is a maximal ideal. Therefore Q_1 is a maximal ideal of R. It follows that $Q_1 = P$.

If $n = 1$ then $P \subset (s) \subset I \subset P$, and therefore $I = P$, $N = L = R$ and $PL = I$. There is nothing further to prove in this case.

If $n > 1$ then $Q_2 Q_3 \cdots Q_n \subset N$. But $Q_2 Q_3 \cdots Q_n \not\subset (s)$, because the choice of n ensures that no product of fewer than n prime ideals is contained in (s). Therefore $N \not\subset (s)$.

The Dedekind domain R is integrally closed. Moreover the maximal ideal P of R is finitely generated, because R is Noetherian. It follows from Proposition 5.12 that if $r \in R$ satisfies $rP \subset sP$ then s divides r in R, and therefore $r \in (s)$. Now $N \not\subset (s)$. It follows that $PN \not\subset sP$.

Now $PN \subset (s)$, and therefore $PN = sJ$ for some ideal J of R. Also $sP \subset PN$ and $sP \neq PN$, and therefore $P \subset J$ (Lemma 5.9) and $P \neq J$. It follows from the maximality of the ideal P that $J = R$, and therefore $PN = (s)$.

We have now shown that, given any non-zero element s of the ideal I, there exists an ideal N of R such that $PN = (s)$. It follows that $N \subset L$ and $s \in PL$. Therefore $I \subset PL$, and hence $I = PL$, as required. ∎

Proposition 5.14 *Let R be a Noetherian domain, and let P be a maximal ideal of R. Suppose that, given any non-zero ideal I of R contained in P there exists some ideal L of R such that $I = PL$. Then, given any non-zero ideal I of R contained in P, there exists a positive integer k and an ideal H of R such that $H \not\subset P$ and $P^k H = I$.*

Proof Let the ideals $I_0, I_1, I_2, I_3, \ldots$ be defined recursively so that $I_0 = I$ and

$$I_{j+1} = \{r \in R : rP \subset I_j\}$$

for all non-negative integers j. Then $I_j \subset I_{j+1}$ and $PI_{j+1} \subset I_j$ for all non-negative integers j. Then $I_0, I_1, I_2, I_3, \ldots$ is an ascending chain of ideals of R.

Let j be a non-negative integer. Suppose that $I_j \subset P$. Then there exists some ideal L_j of R such that $I_j = PL_j$. But then $L_j \subset I_{j+1}$, and therefore $I_j = PI_{j+1}$. The maximal ideal P of R is a proper ideal of R, and the ideal I_j is finitely generated, because R is a Noetherian domain. A straightforward application of Nakayama's Lemma (Corollary 4.12) shows that $PI_j \neq I_j$ for all non-negative integers j (see Corollary 4.13). It follows that $I_j \neq I_{j+1}$ when $I_j \subset P$.

The Dedekind domain R is Noetherian, and therefore satisfies the Ascending Chain Condition (Proposition 3.5). Therefore there exists some positive integer m such that $I_j = I_m$ whenever $j \geq m$. Then $I_m \not\subset P$.

Now $I_0 \subset P$ and $I_m \not\subset P$. Let k be the smallest positive integer for which $I_k \not\subset P$, and let $H = I_k$. Then $I_j = PI_{j+1}$ whenever $0 \leq j < k$. It follows that $I = I_0 = P^k I_k = PH$ and $H \not\subset P$, as required. ∎

Corollary 5.15 *Let R be a Dedekind domain, let P be a maximal ideal of R, and let I be an non-zero ideal of R satisfying $I \subset P$. Then there exists a positive integer k and an ideal H of R such that $H \not\subset P$ and $P^k H = I$.*

Proof The result follows on combining the results of Proposition 5.13 and Proposition 5.14. ∎

Corollary 5.16 *A local domain is a Dedekind domain if and only if it is a discrete valuation ring.*

Proof Every discrete valuation ring is a principal ideal domain (Corollary 5.5). Moreover every principal ideal domain is a Dedekind domain (Lemma 5.8). Therefore every discrete valuation ring is a Dedekind domain.

Let R be a local domain that is a Dedekind domain, and let M be the unique maximal ideal of R. Then R is a Noetherian domain, and every proper ideal of R is contained in M (Lemma 5.10).

Let I be a non-zero proper ideal of R. Then $I \subset M$. It follows from Corollary 5.15 that there exists some positive integer k and some ideal H of R such that $H \not\subset M$ and $I = M^k H$. But then H is not a proper ideal of R, and therefore $H = R$ and $I = M^k$. Thus every non-zero proper ideal of R is of the form M^k for some positive integer k, and therefore R is a discrete valuation ring, as required. ∎

5.6 Localization in Integral Domains

Let R be an integral domain embedded in its field of fractions K as a subring of K. A subset S of R is multiplicatively closed if and only if $1_R \in S$ and $uv \in S$ for all $u, v \in S$. Given any multiplicatively-closed subset S of R whose elements are all non-zero, there is a well-defined subring $S^{-1}R$ of the field of fractions K of R consisting of those elements of K that can be represented in the form rs^{-1} for some $r \in R$ and $s \in S$.

Given any prime ideal P of R, the complement $R \setminus P$ of P in R is a multiplicatively-closed subset of R whose elements are all non-zero. Let $R_P = (R \setminus P)^{-1}R$. Then R_P is a well-defined subring of the field of fractions K. An element c of K belongs to the ring R_P if and only if there exist elements r

and s of R such that $c = rs^{-1}$ and $s \notin P$. This subring R_P is the *localization* of the integral domain R at the prime ideal P.

Let P be a prime ideal of R. Given any ideal I of R, we denote by I_P the ideal of the localization R_P of R at P generated by I. The ideal I_P consists of all elements of R_P that can be represented in the form as^{-1} for some $a \in I$ and $s \in R \setminus P$. If X is a subset of I that generates I as an ideal of R, then X also generates I_P as an ideal of R_P. Also

$$I_P \cap R = \{r \in R : sr \in I \text{ for some } s \in R \setminus P\}.$$

Let E be an ideal of the localization R_P of the integral domain R at the prime ideal P. Then the intersection $E \cap R$ is an ideal of R. Moreover $E = (E \cap R)_P$. Indeed $(E \cap R)_P \subset E$, and given any element e of E, there exist $r \in R$ and $s \in R \setminus P$ such that $se = r$. But then $r \in E \cap R$, and therefore $e \in (E \cap R)_P$.

The localization R_P of the integral domain R at a prime ideal P of R is a local domain whose unique maximal ideal is P_P. The elements of R_P that do not belong to P_P are units of R_P.

We now prove a series of results that establish relationships between an integral domain and its localizations at prime ideals of that domain.

Lemma 5.17 *Let R be an integral domain, let I and J be ideals of R, let P be a prime ideal of R, let R_P be the localization of R at the prime ideal P of R, and let I_P, J_P and $(IJ)_P$ be the ideals of R_P generated by I, J and IJ respectively. Then $(IJ)_P = I_P J_P$.*

Proof We consider the integral domain and its localizations to be embedded as subrings of the field of fractions K of R. Then $I \subset I_P$ and $J \subset J_P$. An element of IJ can be represented in the form

$$u_1 v_1 + \cdots + u_k v_k,$$

and all such elements belong to $I_P J_P$. It follows that $(IJ)_P \subset I_P J_P$. Let $a \in I_P$ and and $b \in J_P$. Then there exist $u \in I$, $v \in J$ and $s, t \in R \setminus P$ such that $a = us^{-1}$ and $b = vt^{-1}$. Then $ab = uvs^{-1}t^{-1}$, and therefore $ab \in (IJ)_P$. Moreover $I_P J_P$ is the ideal of R_P generated by products of the form ab where $a \in I_P$ and $b \in J_P$. It follows that $I_P J_P \subset (IJ)_P$. Thus $(IJ)_P = I_P J_P$, as required. ∎

Lemma 5.18 *Let R be an Noetherian domain embedded in its field of fractions K as a subring of K, let P be a prime ideal of R, and let R_P be the subring of K that is the localization of R at the prime ideal P. Then R_P is a Noetherian domain.*

Proof Let E be an ideal of R_P. Then $E \cap R$ is an ideal of R. But every ideal of R is finitely generated, because R is a Noetherian domain. Let $b_1, b_2, \ldots, b_n$ be elements of R that generate $E \cap R$ as an ideal over R. Then these elements also generate E as an ideal over R_P, and therefore E is finitely generated. The result follows. ∎

Lemma 5.19 *Let R be an integral domain embedded in its field of fractions K as a subring of K, let P be a prime ideal of R, and let R_P be the subring of K that is the localization of R at the prime ideal P. Let Q be a prime ideal of R satisfying $Q \subset P$. Then Q_P is a prime ideal of R_P, and $Q = Q_P \cap R$.*

Proof No element of $R \setminus P$ belongs also to Q, because $Q \subset P$, and therefore $1_K \notin Q_P$. Thus Q_P is a proper ideal of R_P.

Clearly $Q \subset Q_P \cap R$. Let $r \in Q_P \cap R$. Then there exist $q \in Q$ and $s \in R$ such that $sr = q$ and $s \notin P$. Then $sr \in Q$ and $s \notin Q$. It follows from the definition of prime ideals that $r \in Q$. Thus $Q_P \cap R = Q$.

Let r_1, r_2, s_1 and s_2 be elements of R, where $s_1 \notin P$ and $s_2 \notin P$. Suppose that $r_1 s_1^{-1} \notin Q_P$ and $r_2 s_2^{-1} \notin Q_P$. Then $r_1 \notin Q_P \cap R$ and $r_2 \notin Q_P \cap R$, and therefore $r_1 \notin Q$ and $r_2 \notin Q$. But then $r_1 r_2 \notin Q$, because Q is a prime ideal of R, and therefore $r_1 r_2 s_1^{-1} s_2^{-1} \notin Q_P$. It follows that Q_P is a prime ideal of R_P, as required. ∎

Lemma 5.20 *Let R be an integral domain that is integrally closed in its field of fractions K. Then the localization R_P of R at any prime ideal P of R is integrally closed in K.*

Proof Let P be a prime ideal of R, and let c be an element of R_P that is the root of a monic polynomial

$$x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$$

whose coefficients $a_0, a_1, \ldots, a_{n-1}$ belong to R_P. Then there exists $s \in R \setminus P$ such that $sa_i \in R$ for $i = 0, 1, \ldots, n-1$. But then

$$(sc)^n + b_{n-1}(sc)^{n-1} + \cdots b_1(sc) + b_0 = 0_R,$$

where $b_i = s^{n-i}a_i$ for $i = 0, 1, \ldots, n-1$. But then $b_i \in R$ for $i = 1, 2, \ldots, n-1$, and therefore sc is integral over R. It follows that $sc \in R$, and therefore $c \in R_P$. Thus R_P is integrally closed for each prime ideal P of R, as required. ∎

Proposition 5.21 *Let R be a Noetherian domain embedded in its field of fractions K as a subring of K, and, for each maximal ideal P of R, let R_P be the subring of K that is the localization of R at the maximal ideal P. Let I be an ideal of R, and, for each maximal ideal P of R, let I_P be the ideal of R_P generated by the ideal I of R. Then*

$$I = \bigcap\nolimits_{P \in \mathrm{Max}(R)} I_P,$$

where $\mathrm{Max}(R)$ *denotes the set of maximal ideals of R.*

Proof Clearly $I \subset \bigcap_{P \in \mathrm{Max}(R)} I_P$. Let $c \in \bigcap_{P \in \mathrm{Max}(R)} I_P$. Then $c \in I_P$ for all maximal ideals P of R. Thus, for each maximal ideal P of R, there exist $a_P \in I$ and $s_P \in R \setminus P$ such that such that $s_P c = a_P$. The elements s_P of R generate an ideal H of R. Now $s_P \in H$ and $s_P \notin P$ for all maximal ideals P of P. Thus H is not contained in any maximal ideal of R. It follows that $H = R$ (Lemma 5.10), and thus $1_R \in H$. It follows that there exist maximal ideals $P_1, P_2, \ldots, P_k$ of R and elements $t_1, t_2, \ldots, t_k$ of R such that $1_R = \sum_{i=1}^{k} t_i s_{P_i}$. But then

$$c = \sum_{i=1}^{k} t_i s_{P_i} c = \sum_{i=1}^{k} t_i a_{P_i},$$

and therefore $c \in I$. The result follows. ∎

Corollary 5.22 *Let R be a Noetherian domain embedded in its field of fractions K as a subring of K, and, for each maximal ideal P of R, let R_P be the subring of K that is the localization of R at the maximal ideal P. Then*

$$R = \bigcap\nolimits_{P \in \mathrm{Max}(R)} R_P,$$

where $\mathrm{Max}(R)$ *denotes the set of maximal ideals of R.*

Proof The result follows immediately on applying Proposition 5.21 to the particular case where the ideal in the statement of that proposition is the integral domain itself. ∎

Corollary 5.23 *Let R be a Noetherian domain embedded in its field of fractions K as a subring of K, and, for each maximal ideal P of R, let R_P be the subring of K that is the localization of R at the maximal ideal P. Let I and J be an ideals of R, and, for each maximal ideal P of R, let I_P and J_P be the ideals of R_P generated by the ideal I and J respectively of R. Then $I \subset J$ if and only if $I_P \subset J_P$ for all maximal ideals P of R. Also $I = J$ if and only if $I_P = J_P$ for all maximal ideals P of R.*

Proof If $I \subset J$ then $I_P \subset J_P$ for all maximal ideals P of R. Conversely if $I_P \subset J_P$ for all maximal ideals P of R then

$$I = \bigcap_{P \in \mathrm{Max}(R)} I_P \subset \bigcap_{P \in \mathrm{Max}(R)} J_P = J,$$

where $\mathrm{Max}(R)$ denotes the set of maximal ideals of R, and thus $I \subset J$. Furthermore $I = J$ if and only if $I \subset J$ and $J \subset I$. The result follows. ∎

Proposition 5.24 *An integral domain R is a Dedekind domain if and only if R is Noetherian and the localization R_P of R at every maximal ideal P of R is a Dedekind domain.*

Proof Let the integral domain R be embedded in its field of fractions K as a subring of K. Then the localization R_P of P at each maximal ideal P of R consists of those elements of K that can be represented in the form rs^{-1} for some $r \in R$ and $s \in R \setminus P$.

Suppose that R is an Dedekind domain. Let P be a maximal ideal of R. The Dedekind domain R is a Noetherian domain. It follows from Lemma 5.18 that R_P is a Noetherian domain. The Dedekind domain R is integrally closed in its field of fractions K. It follows from Lemma 5.20 that R_P is integrally closed in K. Let L be a non-zero prime ideal of R_P. Then $L \cap R \subset P$, because L is a proper ideal of R_P and every element of $R \setminus P$ is a unit of R_P. Also $L \cap R \neq \emptyset$, $1_R \in R \setminus (L \cap R)$, and $uv \in R \setminus (L \cap R)$ for all $u, v \in R \setminus (L \cap R)$. It follows that $L \cap R$ is a non-zero prime ideal of R. But every non-prime ideal of the Dedekind domain R is a maximal ideal of R. It follows that $L \cap R = P$, and therefore $L = (L \cap R)_P = P_P$. Thus every non-zero prime ideal of the integrally-closed Noetherian domain R_P is a maximal ideal. It follows that R_P is a Dedekind domain.

We have now shown that if R is a Dedekind domain, then R_P is a Dedekind domain for each maximal ideal P of R.

Now suppose that R is a Noetherian domain and that the localization R_P of R at every maximal ideal of R is a Dedekind domain. Then R_P is integrally closed in K for each maximal ideal P of R. It follows that if some element c of K is a root of a monic polynomial with coefficients in R then $c \in R_P$ for all maximal ideals P of R. But the intersections of the localizations R_P of R at the maximal ideals P of R is the integral domain R itself (Corollary 5.22). It follows that $c \in R$. Thus R is integrally closed in its field of fractions.

Let Q be a non-zero prime ideal of R. Then $Q \subset P$ for some maximal ideal P of R (Lemma 5.10). It follows from Lemma 5.19 that Q_P is a prime ideal of R_P and $Q = Q_P \cap P$. Thus Q_P is a non-zero prime ideal of the Dedekind domain R_P. It follows that $Q_P = P_P$, and therefore $Q = P$.

We have thus shown that every non-zero prime ideal of the integrally-closed Noetherian domain R is a maximal ideal of R. It follows that R is a Dedekind domain, as required. ∎

Theorem 5.25 *An integral domain R is a Dedekind domain if and only if R is Noetherian and the localization R_P of R at every maximal ideal P of R is a discrete valuation ring.*

Proof An integral domain R is a Dedekind domain if and only if R is Noetherian and the localization R_P of R at every maximal ideal P of R is a Dedekind domain (Theorem 5.24). But the localization R_P of R at each maximal ideal of R is a local domain, and a local domain is a Dedekind domain if and only if it is a discrete valuation ring (Corollary 5.16). The result follows. ∎

5.7 Factorization of Ideals in Dedekind Domains

We shall prove that an integral domain is a Dedekind domain if and only if every non-zero proper ideal of that domain factors as a product of one or more maximal ideals of the domain.

Lemma 5.26 *Let R be a Dedekind domain, and let I be a non-zero proper ideal of R. Then the number of maximal ideals P of R satisfying $I \subset P$ is finite.*

Proof Every non-zero ideal of a Dedekind domain contains a product of one or more non-zero prime ideals (Proposition 5.11). But all non-zero prime ideals of a Dedekind domain are maximal ideals. It follows that the non-zero proper ideal I of R contains a product $Q_1Q_2\cdots Q_n$ of maximal ideals of R.

Let P be a maximal ideal of R for which $I \subset P$. Then

$$Q_1Q_2\cdots Q_n \subset I \subset P.$$

The maximal ideal P is a prime ideal of R (Lemma 2.15), and a product of ideals is contained in a prime ideal if and only one of the factors of that product is contained in the prime ideal (see Lemma 2.20). It follows that $Q_i \subset P$ for at least one value of i between 1 and n. But if $Q_i \subset P$ then $Q_i = P$, because Q_i is a maximal ideal and P is a proper ideal. The result follows. ∎

Lemma 5.27 *Let R be an integral domain that is not a field, and let*

$$I = P_1^{k_1}P_2^{k_2}\cdots P_m^{k_m},$$

where $P_1, P_2, \ldots, P_m$ are distinct maximal ideals of R, and $k_1, k_2, \ldots, k_m$ are positive integers. Let P be a maximal ideal of R, and let R_P be the localization of R at P. If $P = P_i$ then $I_P = P_P^{k_i}$, where P_P is the maximal ideal of R_P. If P is distinct from $P_1, P_2, \ldots, P_m$ then $I_P = R_P$.

Proof Let i be an integer between 1 and m. If P is a maximal ideal distinct from P_i then P_i contains elements of $R \setminus P$, and those elements are units of R_P. It follows that $(P_i)_P = R_P$ when P is distinct from P_i. Also it follows from Lemma 5.17 that

$$I_P = (P_1)_P^{k_1}(P_2)_P^{k_2} \cdots (P_m)_P^{k_m}$$

for all maximal ideals P of R. It follows that $I_{P_i} = (P_i)_{P_i}^{k_i}$ for $i = 1, 2, \ldots, m$, and $I_P = R_P$ for all maximal ideals P that are distinct from $P_1, P_2, \ldots, P_m$. The result follows. ∎

Lemma 5.28 *Let R be an integral domain, let P be a maximal ideal of R, and let I and J be ideals of R satisfying $I \subset J$ that are contained in the maximal ideal P. Suppose that the localization R_P of R at the maximal ideal P is a discrete valuation ring. Let $I_P = P_P^k$ and $J_P = P_P^j$. Then $j \leq k$.*

Proof Every discrete valuation ring is a principal ideal domain (Corollary 5.5). The maximal ideal P_P of R_P is therefore generated by a prime element p of R_P. Then $P_P^n = (p^n)$ for all positive integers n. Moreover p^j does not divide p^k unless $j \leq k$. Thus if $I \subset J$ then $P_P^k \subset P_P^j$, and therefore $j \leq k$, as required. ∎

Lemma 5.29 *Let R be an integral domain. Suppose that every non-zero proper ideal of R factors as a product of one or more maximal ideals of R. Then the localization of R at every maximal ideal of R is a discrete valuation ring.*

Proof Let P be a maximal ideal of R, let E be a non-zero proper ideal of R_P and let $I = E \cap R$. Then I is a non-zero proper ideal of R, and $E = I_P$. Every non-zero proper ideal of R factors as a product of one or more maximal ideals of R. Therefore there exist distinct maximal ideals $P_1, P_2, \ldots, P_m$ and positive integers $k_1, k_2, \ldots, k_m$ such that

$$I = P_1^{k_1} P_2^{k_2} \cdots P_m^{k_m}.$$

It follows from Lemma 5.27 that $E = I_P = P_P^{k_i}$ if $P = P_i$ and $E = I_P = R_P$ if P is distinct from $P_1, P_2, \ldots, P_m$. We have thus shown that every proper ideal of R_P is of the form P_P^k for some positive integer k. Therefore R_P is a discrete valuation ring, as required. ∎

Lemma 5.30 *Let R be an integral domain. Suppose that every non-zero proper ideal of R factors as a product of one or more maximal ideals of R. Let I be a non-zero proper ideal of R. Then there are only finitely many ideals J of R satisfying $I \subset J$.*

Proof Let I be a non-zero proper ideal of R. Then there exist distinct maximal ideals $P_1, P_2, \ldots, P_m$ and positive integers $k_1, k_2, \ldots, k_m$ such that

$$I = P_1^{k_1} P_2^{k_2} \cdots P_m^{k_m}.$$

Let P be a maximal ideal of R. It follows from Lemma 5.27 that $I_P = P_P^{k_i}$ if $P = P_i$ and $I_P = R_P$ if P is distinct from $P_1, P_2, \ldots, P_m$. Let J be a non-zero proper ideal of R satisfying $I \subset J$, let n be the number of maximal ideals of R that contain the ideal J, and let the prime ideals $P_1, P_2, \ldots, P_m$ be ordered so that $J \subset P_i$ for $i = 1, 2, \ldots, n$ and $J \not\subset P_i$ when $n < i \leq m$. Then there exist integers $j_1, j_2, \ldots, j_n$ such that $J_P = P_P^{j_i}$ when $P = P_i$ for some integer i between 1 and n. Also $J_P = R_P$ when P is a maximal ideal distinct from $P_1, P_2, \ldots, P_n$. Then

$$J = P_1^{j_1} P_2^{j_2} \cdots P_n^{j_n}.$$

Now the localization R_P of R at each maximal ideal P of R is a discrete valuation ring (Lemma 5.29). It follows from Lemma 5.28 that $j_i \leq k_i$ for $i = 1, 2, \ldots, n$. The result follows. ∎

Lemma 5.31 *Let R be an integral domain. Suppose that every non-zero proper ideal of R factors as a product of one or more maximal ideals of R. Then R is a Noetherian domain.*

Proof Let $\mathcal{C}$ be a non-empty collection of ideals of R. If all ideals in $\mathcal{C}$ are the zero ideal of R then $\mathcal{C}$ the zero ideal is a maximal element of the collection $\mathcal{C}$. If R belongs to $\mathcal{C}$ then R is a maximal element of the collection $\mathcal{C}$. In all other cases, the collection $\mathcal{C}$ contains a non-zero proper ideal I. It follows from Lemma 5.30 that there exist only finitely many ideals J of R satisfying $I \subset J$. If I is not itself a maximal element of $\mathcal{C}$ then one of the ideals J of R satisfying $I \subset J$ must be a maximal element of $\mathcal{C}$. Thus the integral domain R satisfies the Maximal Condition. It is therefore a Noetherian domain (see Proposition 3.5). ∎

Theorem 5.32 *An integral domain R is a Dedekind domain if and only if every non-zero proper ideal of R factors as a product of one or more maximal ideals of R.*

Proof Let R be an integral domain. Suppose that every non-zero proper ideal of R factors as a product of one or more maximal ideals of R. Then R is a Noetherian domain (Lemma 5.31), and the localization of R at each maximal ideal of R is a discrete valuation ring (Lemma 5.29). It follows from Theorem 5.25 that R is a Dedekind domain.

We now prove the converse. Let R be a Dedekind domain, and let I be a non-zero proper ideal of R. If P is a maximal ideal of R for which $I \subset P$ then the localization R_P of R at the maximal ideal P is a discrete valuation ring (Theorem 5.25). The unique maximal ideal of R_P is P_P. It follows that if P is a maximal ideal of R and if $I \subset P$ then $I_P = P_P^k$ for some positive integer k.

Now there exist distinct maximal ideals $P_1, P_2, \ldots, P_m$ such that $I \subset P_i$ for $i = 1, 2, \ldots, m$ and $I \not\subset P$ for all maximal ideals P distinct from $P_1, P_2, \ldots, P_m$. Let $k_1, k_2, \ldots, k_m$ be the positive integers determined such that $I_{P_i} = (P_i)_{P_i}^{k_i}$, and let

$$J = P_1^{k_1} P_2^{k_2} \cdots P_m^{k_m}.$$

It follows from Lemma 5.27 that $J_{P_i} = (P_i)_{P_i}^{k_i} = I_{P_i}$ for $i = 1, 2, \ldots, m$.

If P is a maximal ideal of R that is distinct from $P_1, P_2, \ldots, P_m$ then $I \not\subset P$. But then I contains units of R_P and therefore $I_P = R_P$. It follows that $J_P = R_P = I_P$ for all maximal ideals P that are distinct from $P_1, P_2, \ldots, P_m$. Therefore $I_P = J_P$ for all maximal ideals P of R. It follows from Corollary 5.23 that $I = J$. The result follows. ∎

5.8 Divisibility of Ideals in Integral Domains

Lemma 5.33 *Let R be an integral domain that is not a field. Suppose that every non-zero proper ideal of R factors as a product of one or more maximal ideals of R. Then, given any maximal ideal P of R, there exists a non-zero ideal H of R such that PH is a principal ideal of R.*

Proof The zero ideal is not a maximal ideal of R, because R is not a field. Let P be a maximal ideal of R, and let s be a non-zero element of P. Then there exist maximal ideals $Q_1, Q_2, \ldots, Q_n$ of R such that

$$(s) = Q_1 Q_2 \cdots Q_n.$$

Every maximal ideal of R is a prime ideal, and a product of ideals is contained in a prime ideal if and only one of the factors of that product is contained in the prime ideal (see Lemma 2.20). It follows that $Q_i \subset P$ for at least one value of Q between 1 and n. It then follows from the maximality of Q_i

that $Q_i = P$. We may suppose that $Q_1 = P$. Let $H = R$ if $n = 1$, and $H = Q_2 Q_3 \cdots Q_n$ if $n > 1$. Then $PH = (s)$. Morever H is a non-zero ideal because s is a non-zero element of R. The result follows. ∎

Proposition 5.34 *Let R be an integral domain. Suppose that every non-zero proper ideal of R factors as a product of one or more maximal ideals of R. Then, given any non-zero proper ideal I of R, there exists a non-zero ideal L of R for which IL is a principal ideal of R.*

Proof If R is a field then R has no non-zero proper ideals, and there is nothing to prove. Therefore we may assume that R is not a field.

Let I be a non-zero proper ideal of R. Then there exist maximal ideals $P_1, P_2, \ldots, P_n$ of R such that $I = P_1 P_2 \cdots P_n$. It follows from Lemma 5.33 that there exist non-zero ideals $H_1, H_2, \ldots, H_n$ of R and non-zero elements $s_1, s_2, \ldots, s_n$ of R such that $P_i H_i = (s_i)$ for $i = 1, 2, \ldots, n$. Let $L = H_1 H_2 \cdots H_n$ and $s = s_1 s_2 \cdots s_n$. Then s is a non-zero element of R, because any product of non-zero elements of an integral domain is non-zero. Also $IL = (s)$. But then L is a non-zero ideal and IL is a principal ideal. The result follows. ∎

Lemma 5.35 *Let R be an integral domain, and let I, J_1 and J_2 be ideals of R satisfying $IJ_1 = IJ_2$. Suppose that I is a non-zero proper ideal of R, and that there exists some non-zero ideal L of R for which IL is a principal ideal. Then $J_1 = J_2$.*

Proof The ideal IL is a non-zero principal ideal, and thus there exists a non-zero element s of R such that $IL = (s)$. Then $sJ_1 = LIJ_1 = LIJ_2 = sJ_2$. It follows from Lemma 5.9 that $J_1 = J_2$, as required. ∎

Lemma 5.36 *Let R be an integral domain, and let I and J be ideals satisfying $J \subset I$. Suppose that I is a non-zero proper ideal of R, and that there exists some non-zero ideal L of R for which IL is a principal ideal. Then there exists some ideal N of R such that $J = IN$.*

Proof The ideal IL is a non-zero principal ideal, and thus there exists a non-zero element s of R such that $IL = (s)$. Then $JL \subset IL = (s)$, and therefore there exists some ideal N of R such that $JL = sN$. Then $sJ = JIL = sIN$, and therefore $J = IN$ (see Lemma 5.9). ∎

Definition Let R be an integral domain, and let I and J be ideals of R. The ideal I is said to *divide* the ideal J in R if there exists some ideal N of R such that $J = IN$.

When an ideal I divides an ideal J in an integral domain R, we can denote this relation by writing $I|J$.

If I and J are ideals of an integral domain R, and if I divides J in R then $J \subset I$.

A non-zero ideal I of an integral domain R divides some non-zero principal ideal of I if and only if there exists some non-zero ideal L of I for which IL is a principal ideal of R.

Proposition 5.37 *Let R be an integral domain, and let I be a non-zero ideal of R. Suppose that there exists a non-zero ideal L of R for which IL is a principal ideal. Then the ideal I is finitely generated.*

Proof Let L be a non-zero ideal of R for which IL is a principal ideal, and let s be an element of R that generates the principal ideal IL. Then s is non-zero and $IL = (s)$. It follows that there exist elements $v_1, v_2, \ldots, v_m$ of I and $w_1, w_2, \ldots, w_m$ of L such that

$$s = v_1 w_1 + v_2 w_2 + \cdots + v_m w_m.$$

We show that I is generated by $v_1, v_2, \ldots, v_m$.

Let a be an element of the ideal I. Then $aL \subset (s)$, and therefore there exist elements $r_1, r_2, \ldots, r_m$ of R such that $aw_i = sr_i$ for $i = 1, 2, \ldots, m$. Then

$$s \sum_{i=1}^{m} r_i v_i = a \sum_{i=1}^{m} v_i w_i = sa,$$

and therefore $a = \sum_{i=1}^{m} r_i v_i$. Thus the elements $v_1, v_2, \ldots, v_m$ of I generate the ideal I, as required. ∎

Corollary 5.38 *Let R be an integral domain. Suppose that every non-zero ideal of R divides some non-zero principal ideal of R. Then R is a Noetherian domain.*

Proof Proposition 5.37 ensures that all ideals of R are finitely generated. ∎

Proposition 5.39 *Let R be a Noetherian domain. Suppose that each maximal ideal of R divides all ideals contained within it. Then R is a Dedekind domain.*

Proof We show that the localization R_P of R at each maximal ideal P of R is a discrete valuation ring. Let E be a proper ideal of R_P and let $I = E \cap R$. Then $I \subset P$ and $E = I_P$. The maximal ideal P divides all

ideals contained within it. It follows from Proposition 5.14 that there exists a positive integer k and an ideal H of R such that $H \not\subset P$ and $I = P^k H$. Then $H_P = R_P$, because H contains units of R_P. Also the ideal of R_P generated by a product of ideals of R is the product of the corresponding ideals of R_P (Lemma 5.17). Therefore $E = I_P = P_P^k H_P = P_P^k$. Thus every proper ideal of the local ring R_P is of the form P_P^k for some positive integer k, and therefore R_P is a discrete valuation ring. The integral domain R is thus a Noetherian domain whose localization at every maximal ideal is a discrete valuation ring. It follows from Theorem 5.25 that R is a Dedekind domain, as required. ∎

Theorem 5.40 *An integral domain R is a Dedekind domain if and only if every ideal of R divides all ideals contained within it.*

Proof Suppose that R is a Dedekind domain. It follows from Theorem 5.32 that every non-zero proper ideal of R factors as a product of one or more maximal ideals of R. It then follows from Proposition 5.34 that every non-zero proper ideal of R divides some non-zero principal ideal of R. It then follows from Lemma 5.36 that every ideal of R divides all ideals contained within it.

Conversely suppose that R is an integral domain and that every ideal of R divides all ideals contained within it. If I is a non-zero ideal of R, and if s is a non-zero element of I, then there exists a non-zero ideal L of R such that $IL = (s)$. It then follows from Proposition 5.37 that the ideal I is finitely generated. Therefore the integral domain R is a Noetherian domain. Also every maximal ideal of R divides all ideals contained within it. It follows from Proposition 5.39 that R is a Dedekind domain, as required. ∎

Corollary 5.41 *An integral domain R is a Dedekind domain if and only if every non-zero ideal of R divides some non-zero principal ideal of R.*

Proof The result follows on combining Lemma 5.36 and Theorem 5.40. ∎

Example It follows from the Hilbert Basis Theorem that the ring $\mathbb{Q}[x, y]$ of polynomials in two independent indeterminates x and y with rational coefficients is a Noetherian domain (see Theorem 3.8 and Corollary 3.10). The ideal (x, y) generated by polynomials x and y contains the ideal (x) generated by the polynomial x. But the ideal (x, y) does not divide the ideal (x). Indeed let L be an ideal of $\mathbb{Q}[x, y]$ with the property that $(x) \subset (x, y)L$. Then there exist polynomials $f(x, y)$ and $g(x, y)$ belonging to the ideal L such that $x = xf(x, y) + yg(x, y)$. But then $g(x, y) = 0$ and $f(x, y) = 1$, and therefore $L = \mathbb{Q}[x, y]$. Thus there is no ideal L of $\mathbb{Q}[x, y]$ for which $(x) = (x, y)L$, and therefore the ideal (x, y) does not divide the ideal (x) in $\mathbb{Q}[x, y]$.

5.9 Discrete Valuations on Dedekind Domains

Let R be a Dedekind domain embedded in its field of fractions K as a subring of K, and let P be a maximal ideal of R. We regard the localizations R_P of R at each maximal ideal of R as subrings of the field of fractions K of R. Then R is the intersection of the local domains R_P as P ranges over all maximal ideals of R (Corollary 5.22). The ideal P_P of R_P generated by the maximal ideal P of R is the unique maximal ideal of the local domain R_P.

Lemma 5.42 *Let R be a Dedekind domain embedded in its field of fractions K as a subring of K. Then each maximal ideal P of R determines a corresponding discrete valuation ν_P on K which is the unique discrete valuation on K satisfying the following conditions:*

(i) $\nu_P(r) = 0$ *for all* $r \in R \setminus P$;

(ii) $\nu_P(r) = k$ *for all elements* r *of* $P^k \setminus P^{k+1}$.

The valuation ring of the discrete valuation ν_P is the localization R_P of R at the maximal ideal P of R.

Proof The localization R_P of R at each maximal ideal P of R is a discrete valuation ring, because R is a Dedekind domain (Theorem 5.25). It follows that R_P is the valuation ring of a discrete valuation $\nu_P \colon K \to \mathbb{Z} \cup \{\infty\}$ on K which maps the multiplicative group K^* of non-zero elements of K surjectively onto the group $\mathbb{Z}$ of integers under addition. Then $\nu_P(r) = 0$ for all $r \in R \setminus P$, and $\nu_P(r) = k$ for all positive integers k and elements r of $P^k \setminus P^{k+1}$.

We now prove that ν_P is the unique discrete valuation on K satisfying conditions (i) and (ii). Let $\nu \colon K \to \mathbb{Z} \cup \{\infty\}$ be a discrete valuation on K. Suppose that $\nu(r) = 0 = \nu_P(r)$ for all elements r of $R \setminus P$, and $\nu(r) = k = \nu_P(r)$ for all positive integers k and elements r of $P^k \setminus P^{k+1}$. Every element of R that is not in $R \setminus P$ belongs to $P^k \setminus R^{k+1}$ for some positive integer k. Therefore $\nu(r) = \nu_P(r)$ for all $r \in R$. Every non-zero element of the field of fractions K of R can be expressed as a quotient of the form rs^{-1}, where r and s are non-sero elements of R. Then $\nu(rs^{-1}) = \nu(r) - \nu(s) = \nu_P(r) - \nu_P(s) = \nu_P(rs^{-1})$. It follows that $\nu(c) = \nu_P(c)$ for all $c \in K$, as required. ∎

Definition Let R be a Dedekind domain embedded in its field of fractions K as a subring of K, and let P be a maximal ideal of R. We define the discrete valuation $\nu_P \colon K \to \mathbb{Z} \cup \{\infty\}$ *determined* by the maximal ideal P to be the unique discrete valuation on K characterized by the following properties:

(i) $\nu_P(r) = 0$ for all $r \in R \setminus P$;

(ii) $\nu_P(r) = k$ for all elements r of $P^k \setminus P^{k+1}$.

Proposition 5.43 *Let R be a Dedekind domain embedded in its field of fractions K as a subring of K, and, for each each maximal ideal P of R, let $\nu_P : K \to \mathbb{Z} \cup \{\infty\}$ be the discrete valuation on K determined by P. Then*

$$R = \{c \in K : \nu_P(c) \geq 0 \text{ for all } P \in \mathrm{Max}(R)\},$$

where $\mathrm{Max}(R)$ *is the set of maximal ideals of R.*

Proof It follows from Corollary 5.22 that $R = \bigcap_{P \in \mathrm{Max}(R)} R_P$. The result follows. ∎

Corollary 5.44 *Let R be a Dedekind domain embedded in its field of fractions K as a subring of K, and, for each each maximal ideal P of R, let $\nu_P : K \to \mathbb{Z} \cup \{\infty\}$ be the discrete valuation on K determined by P. Let r and s be non-zero elements of R. Then r divides s in R if and only if $\nu_P(r) \leq \nu_P(s)$ for all maximal ideals P of R.*

Proof Let r and s be non-zero elements of R. If r divides s in R then there exists $t \in R$, such that $s = rt$. It follows that $\nu_P(s) = \nu_P(r) + \nu_P(t) \geq \nu_P(r)$ for all maximal ideals P of R. Conversely if $\nu_P(s) \geq \nu_P(r)$ for all maximal ideals of R then $\nu_P(sr^{-1}) \geq 0$ for all maximal ideals of R. It then follows from Proposition 5.43 that $sr^{-1} \in R$, and thus r divides s in R, as required. ∎

Proposition 5.45 *Let R be a Dedekind domain embedded in its field of fractions K as a subring of K, and, for each each maximal ideal P of R, let $\nu_P : K \to \mathbb{Z} \cup \{\infty\}$ be the discrete valuation on K determined by P. Let r be a non-zero element of R. Then there are only finitely many maximal ideals P of R for which $\nu_P(r) \neq 0$.*

Proof Let r be a non-zero element of R, and let P be a maximal ideal of R. Then $\nu_P(r) \neq 0$ if and only if $(r) \subset P$. The result therefore follows directly from Lemma 5.26. ∎

Let R be a Dedekind domain embedded in its field of fractions K as a subring of K, and, for each each maximal ideal P of R, let $\nu_P : K \to \mathbb{Z} \cup \{\infty\}$ be the discrete valuation on K determined by P. Let I be an ideal of R. If I is the zero ideal of R then we define $\nu_P(I) = \infty$. If I is a non-zero ideal, then we define

$$\nu_P(I) = \inf\{\nu_P(r) : r \neq 0_R \text{ and } r \in I\}.$$

Then $\nu_P(I)$ is a non-negative integer, and is the minimum value taken on by $\nu_P(r)$ on the set of non-zero elements of the ideal I. It follows from the definition of $\nu_P(I)$ that $\nu_P(I) \leq \nu_P(r)$ for all $r \in I$.

Lemma 5.46 *Let R be a Dedekind domain embedded in its field of fractions K as a subring of K, and, for each each maximal ideal P of R, let $\nu_P: K \to \mathbb{Z} \cup \{\infty\}$ be the discrete valuation on K determined by P. Let I be a non-zero ideal of R. Then $\nu_P(I)$ is non-zero for at most finitely many maximal ideals P of R.*

Proof Let r be a non-zero element of I. Then $0 \leq \nu_P(I) \leq \nu_P(r)$ for all maximal ideals of R. The result therefore follows from Proposition 5.45. ∎

Proposition 5.47 *Let R be a Dedekind domain embedded in its field of fractions K as a subring of K, and, for each each maximal ideal P of R, let $\nu_P: K \to \mathbb{Z} \cup \{\infty\}$ be the discrete valuation on K determined by P. Let I be an ideal of R. Then*

$$I = \{r \in R : \nu_P(r) \geq \nu_P(I) \text{ for all } P \in \mathrm{Max}(R)\},$$

where $\mathrm{Max}(R)$ *denotes the set of maximal ideals of R.*

Proof The ideal I_P of R_P generated by I satisfies

$$I_P \cap R = \{r \in R : \nu_P(r) \geq \nu_P(I)\}.$$

Moreover $I = \bigcap_{P \in \mathrm{Max}(R)} I_P$ (Proposition 5.21). It follows that

$$I = \{r \in R : \nu_P(r) \geq \nu_P(I) \text{ for all } P \in \mathrm{Max}(R)\},$$

as required. ∎

Proposition 5.48 *Let R be a Dedekind domain embedded in its field of fractions K as a subring of K, and, for each each maximal ideal P of R, let $\nu_P: K \to \mathbb{Z} \cup \{\infty\}$ be the discrete valuation on K determined by P. Let I and J be non-zero ideals of R. Then $\nu_P(IJ) = \nu_P(I) + \nu_P(J)$ for all maximal ideals I and J of R.*

Proof The localization of R at a maximal ideal P is the valuation ring of the valuation ν_P. Moreover the unique maximal ideal of R_P is the ideal P_P generated by the maximal ideal P in R_P. It follows that

$$\begin{aligned} I_P &= \{c \in K : \nu_P(c) \geq \nu_P(I)\} = P_P^{\nu_P(I)}, \\ J_P &= \{c \in K : \nu_P(c) \geq \nu_P(J)\} = P_P^{\nu_P(J)}. \end{aligned}$$

But then $(IJ)_P = I_P J_P = P_P^{\nu_P(I)+\nu_P(J)}$ (see Lemma 5.17). It follows that $\nu_P(IJ) = \nu_P(I) + \nu_P(J)$, as required. ∎

5.10 Uniqueness of Ideal Factorization in Dedekind Domains

Proposition 5.49 *Let R be a Dedekind domain, and let $P_1, P_2, \ldots, P_k$ and $Q_1, Q_2, \ldots, Q_l$ be maximal ideals of R. Suppose that*

$$P_1 P_2 \cdots P_k = Q_1 Q_2, \cdots Q_l,$$

Then $k = l$, and there exists some permutation σ of the set $\{1, 2, \ldots, k\}$ such that $Q_i = P_{\sigma(i)}$ for $i = 1, 2, \ldots, k$.

Proof We may assume without loss of generality that $l \geq k$. Corollary 5.41 ensures that there exist non-zero ideals $L_1, L_2, \ldots, L_k$ and non-zero elements $b_1, b_2, \ldots, b_k$ of R such that $P_i L_i = b_i$ for $i = 1, 2, \ldots, k$.

The product of the maximal ideals $Q_1, Q_2, \ldots, Q_l$ is contained in the maximal ideal P_1. All maximal ideals are prime ideals (Lemma 2.15). Moreover if a product of ideals is contained in a prime ideal then at least one of the factors must be contained in that prime ideal (see Lemma 2.20). It follows that at least one of the ideals $Q_1, Q_2, \ldots, Q_s$ is contained in P_1. We may therefore reorder $Q_1, Q_2, \ldots, Q_s$ to ensure that $Q_1 \subset P_1$. It then follows from the maximality of Q_1 that $Q_1 = P_1$.

Suppose that $k = 1$. Then $L_1 P_1 = (b_1)$. If it were the case that $l > 1$ then the maximal ideals $Q_2, \ldots, Q_k$ would satisfy $(b_1) = L_1 P_1 Q_2 \cdots Q_k = b_1 Q_2 \cdots Q_k$ But that would imply that $Q_2 \cdots Q_k = R$, which is impossible, because maximal ideals of R are proper ideals of R. Therefore $l = k = 1$ and $P_1 = Q_1$ in the case when $k = 1$.

Now suppose that $k > 1$. Then

$$b_1 P_2 P_3 \cdots P_k = L_1 P_1 P_2 P_3 \cdots P_k = L_1 P_1 Q_2 Q_3 \cdots Q_l = b_1 Q_2 Q_3 \cdots Q_l,$$

and therefore $P_2 P_3 \cdots P_k = Q_2 Q_3 \cdots Q_l$. Thus if the result holds for ideals that factor as products of $k-1$ maximal ideals, then it must also hold ideals that factor as products of k maximal ideals. The result therefore follows by induction on the number of maximal ideals $P_1, P_2, \ldots, P_k$. ∎

5.11 The Class Group of a Dedekind Domain

Lemma 5.50 *Let R be an integral domain, let $\mathcal{A}$ be the set of non-zero ideals of R, and let $\sim$ be the relation on $\mathcal{A}$ defined so that non-zero ideals I and J of R satisfy $I \sim J$ if and only if there exist non-zero elements a and b of R such that $aI = bJ$. Then $\sim$ is an equivalence relation on the set $\mathcal{A}$. Moreover if I, J H and L are non-zero ideals of R, and if $I \sim H$ and $J \sim L$ then $IJ \sim HL$.*

Proof The relation $\sim$ on $\mathcal{A}$ is clearly reflexive and symmetric. Let I, J and L be non-zero ideals of R where $I \sim J$ and $J \sim L$. Then there exist non-zero elements a, b, c and d of R such that $aI = bJ$ and $cJ = dL$. Then ac and bd are non-zero elements of R and $acI = bcJ = bdL$. It follows that $I \sim L$. Thus the relation $\sim$ on $\mathcal{A}$ is transitive. It is thus an equivalence relation.

Let I, J, H and L be non-zero ideals of R, where $I \sim H$ and $J \sim L$. Then there exist non-zero elements a, b, c and d of R such that $aI = bH$ and $cJ = dL$. Then ac and bd are non-zero elements of R, and $acIJ = bdHL$. It follows that $IJ \sim HL$, as required. ∎

Given a non-zero ideal I of an integral domain R, we denote by $[I]$ the equivalence class of I with respect to the relation $\sim$ on the set $\mathcal{A}$ of non-zero ideals of R defined in the statement of Lemma 5.50. This equivalence class $[I]$ is referred to as the *ideal class* of the ideal I. Non-zero ideals I and J of R thus satisfy $[I] = [J]$ if and only if there exist non-zero elements a and b of R such that $aI = bJ$. It follows from Lemma 5.50. that if I, J, H and L are non-zero ideals of R, and if $[I] = [H]$ and $[J] = [L]$ then $[IJ] = [HL]$. There is thus a well-defined multiplication operation defined on the set of ideal classes of an integral domain, where the product $[I][J]$ of ideal classes $[I]$ and $[J]$ is the ideal class $[IJ]$ of the product ideal IJ.

The ideal classes of an arbitrary integral domain need not constitute a group with respect to this operation of multiplication of ideal classes. But the ideal classes of a Dedekind domain do constitute a group.

Proposition 5.51 *Let R be a Dedekind domain. Then the set of ideal classes of non-zero ideals of R is an Abelian group, where multiplication of ideal classes is defined such that $[I][J] = [IJ]$ for all non-zero ideals I and J of R.*

Proof Multiplication of ideals is associative and commutative, and therefore multiplication of ideal classes is associative and commutative. Also $[R][I] = [RI] = [I]$ for all non-zero ideals I of R, and therefore the ideal class $[R]$ is an identity element for multiplication of ideal classes. Corollary 5.41 ensures that, given any non-zero ideal I of the Dedekind domain R, there exists a non-zero ideal L for which IL is a principal ideal of R. Then $[I][L] = [R]$. It follows that every ideal class of R has an inverse with respect to the operation of multiplication defined on ideal classes of R. Therefore the set of ideal classes of R is an Abelian group with respect to the specified operation of multiplication of ideal classes. ∎

Definition Let R be a Dedekind domain. The *class group* of R is the Abelian group whose elements are ideal classes of non-zero ideals of R, with

multiplication of ideal classes defined such that $[I][J] = [IJ]$ for all ideals I and J of R.

Proposition 5.52 *An integral domain is a Dedekind domain if and only if its ideal classes constitute a group with respect to the operation of multiplication defined on ideal classes so that* $[I][J] = [IJ]$ *for all non-zero ideals* I *and* J *of* R.

Proof This result follows directly from Corollary 5.41. ∎

Definition Let R be a Dedekind domain whose class group is finite. The *class number* of R is the order of the class group of R.

Let R be a Dedekind domain whose class group is finite, and let h be the class number of R. Then I^h is a principal ideal of R for all non-zero ideals I of R. This result follows from the basic result of group theory which states that the order of any element of a finite group divides the order of the group.

5.12 Fractional Ideals

Let R be an integral domain, and let K be its field of fractions. We identify R with the subring of K that corresponds to it under the natural embedding of the integral domain R in its field of fractions. Thus R is considered to be a subring of K.

Definition A *fractional ideal* of R is a subset of the field K of fractions of R that is of the form cI, where c is a non-zero element of K and I is an ideal of R.

A fractional ideal of R is not an ideal of R unless it is contained in R. If R is not itself a field, then the field K of fractions of K will contain fractional ideals of R that are not ideals of R. Indeed, given any element c of $K \setminus R$, the subset cR of K is a fractional ideal of K, where $cR = \{cr : r \in R\}$, but it is not an ideal of R. However any fractional ideal of R that is contained in R is an ideal of R.

Definition A *principal fractional ideal* of an integral domain R is an ideal of the form cR, where c is an element of the field of fractions of R.

If R is not a field, then the only fractional ideal of R that is an ideal of K is the zero ideal. When R is itself a field, the only fractional ideals of R are the zero ideal and the whole of R, and these are ideals of R.

A fractional ideal of an integral domain R is an R-module, and is isomorphic as an R-module to some ideal of R. Indeed, given a fractional ideal M of R contained in the field of fractions of R, there exists a non-zero element a of R for which $aM \subset R$. Then aM is an ideal of R, and multiplication by a provides an isomorphism of R-modules between the fractional ideal M of R and the ideal aM of R.

Let M and N be fractional ideals of the integral domain R. Then there exist non-zero elements c and d of K and ideals I and J of R such that $M = cI$ and $N = dJ$. We define $MN = cdIJ$. Then MN consists of those elements of K that can be expressed in the form

$$a_1b_1 + a_2b_2 + \cdots + a_kb_k,$$

where $a_1, a_2, \ldots, a_k \in M$ and $b_1, b_2, \ldots, b_k \in N$. We define the ideal class $[M]$ of the fractional ideal M to be the ideal class $[I]$ of the ideal I, where $M = cI$. Then $[M][N] = [MN]$ for all fractional ideals M and N of R.

Let I be an non-zero ideal of R. Suppose that there exists a non-zero ideal L of R for which IL is a principal ideal of R. Then there exists a non-zero element a of R such that $IL = (s)$. Let $M = s^{-1}L$. Then M is a fractional ideal of R, and $IM = R$. If N is a fractional ideal of R satisfying $IN = R$ then $N = RN = (IM)N = (IN)M = RM = M$. Therefore M is the unique fractional ideal of M for which $MI = R$. This ideal is referred to as the *inverse* of the ideal I, and is denoted by I^{-1}.

Lemma 5.53 *Let R be an integral domain, and let I be an non-zero ideal of R. Then the ideal I divides some non-zero principal ideal of R if and only if there exists some fractional ideal I^{-1} of R for which $II^{-1} = R$. Moreover if such a fractional ideal I^{-1} exists, then it is the unique fractional ideal of R for which $II^{-1} = R$.*

The following result follows from Corollary 5.41, and is essentially a restatement of that corollary.

Proposition 5.54 *An integral domain R is a Dedekind domain if and only if its non-zero fractional ideals constitute an Abelian group under the operation of multiplication of fractional ideals.*

The class group of a Dedekind domain R is isomorphic to the quotient of the group G of non-zero fractional ideals of R by the subgroup consisting of the non-zero principal fractional ideals of R.

5.13 Characterizations of Dedekind Domains

Proposition 5.55 *Let R be an integral domain. Then the following conditions are equivalent, and if the integral domain R satisfies any one of these conditions, then it satisfies all of them, and is a Dedekind domain:*

(i) *R is an integrally-closed Noetherian domain in which every non-zero prime ideal is maximal;*

(ii) *R is a Noetherian domain, and the localization of R at every maximal ideal of R is a Dedekind domain;*

(iii) *R is a Noetherian domain, and the localization of R at every maximal ideal of R is a principal ideal domain;*

(iv) *R is a Noetherian domain, and the localization of R at every maximal ideal of R is a discrete valuation ring;*

(v) *every non-zero proper ideal of R factors as a product of one or more maximal ideals;*

(vi) *given any ideals I and J of R satisfying $J \subset I$, there exists an ideal N of R such that $J = IN$;*

(vii) *given any non-zero ideal I of R, there exists a non-zero ideal L of R for which IL is a principal ideal;*

(viii) *the fractional ideals of R constitute a group with respect to the operation of multiplication of fractional ideals;*

(ix) *R is a Noetherian domain, and each maximal ideal of R divides the ideals contained within it;*

(x) *R is a Noetherian domain, and, given any maximal ideal P of R, there exists a non-zero ideal L of R for which PL is a principal ideal of R;*

Proof Corollary 5.16 ensures that a local domain is a Dedekind domain if and only if it is a discrete valuation ring. Proposition 5.7 ensures that a local domain is a discrete valuation ring if and only if it is a principal ideal domain. Lemma 5.8 ensures that every principal ideal domain is a Dedekind domain. It follows that conditions (ii), (iii) and (iv) are equivalent.

Theorem 5.25 ensures that an integral domain R is a Dedekind domain if and only if R is Noetherian and the localization R_P of R at every maximal ideal P of R is a discrete valuation ring. It follows that (i) is equivalent to (ii), (iii) and (iv).

Theorem 5.32 ensures that an integral domain is a Dedekind domain if and only if every non-zero proper ideal factors as a product of maximal ideals. It follows that (i) and (v) are equivalent.

Theorem 5.40 ensures that an integral domain R is a Dedekind domain if and only if every ideal of R divides all ideals contained within it. Also Lemma 5.36 ensures that a non-zero ideal divides all ideals contained within it if and only if it divides some non-zero principal ideal. It follows that (i) and (vi) and (vii) are equivalent.

Condition (viii) is essentially a restatement of (vii), and is therefore equivalent to (i) (Proposition 5.54).

Lemma 5.36 ensures that (ix) and (x) are equivalent to one another. Conditions (i) and (vi) are equivalent and imply (ix). Moreover Proposition 5.39 ensures that condition (ix) implies condition (i). Therefore conditions (i), (vi), (ix) and (x) are equivalent. Therefore all the conditions listed in the statement of the proposition are equivalent. ∎