NOTES ON DEDEKIND RINGS

J. P. MAY

Contents

These notes record the basic results about DVR's (discrete valuation rings) and Dedekind rings, with at least sketches of the non-trivial proofs, none of which are hard. This is standard material that any educated mathematician with even a mild interest in number theory should know. It has often slipped through the cracks of Chicago's first year graduate program, but then we would need at least three years to cover all of the basic algebra that every educated mathematician should know.

Throughout these notes, R is an integral domain with field of fractions K.

1. Fractional ideals

Definition 1.1. A *fractional ideal* A of R is a sub R-module of K for which there is a non-zero element d of R such that $dA \subset R$. Define A^{-1} to be the set of all $k \in K$, including zero, such that $kA \subset R$. For fractional ideals A and B define AB to be the set of finite linear combinations of elements ab with $a \in A$ and $b \in B$. Observe that AB and A^{-1} are fractional ideals. The set of isomorphism classes of non-zero fractional ideals is a commutative monoid with unit R under this product. Clearly $AA^{-1} \subset R$. Equality need not hold, and A is said to be invertible if it does. The *class group* $C(R)$ is the Abelian group of isomorphism classes of invertible fractional ideals of R. If this group is finite, its order is the *class number* of R.

Remark 1.2. If there is any B such that $AB = R$, then $B = A^{-1}$.

Lemma 1.3. *Every finitely generated sub R-module of K is a fractional ideal, and the converse holds if R is Noetherian.*

For each non-zero element $k \in K$, kR is an invertible fractional ideal that is isomorphic to R, and $C(R)$ can be identified with the quotient of the Abelian group of all invertible R-modules by its subgroup of principal R-modules. We think of $C(R)$ as measuring by how much ideals can differ from being principal. When R is a Dedekind ring, all non-zero fractional ideals are invertible, and they can all be

generated by two elements. If, further, R is a ring of integers in a number field, then $C(R)$ is finite.

We relate invertibility to projectivity. The following general observation, in which R can be any commutative ring, will make the relationship apparent.

Theorem 1.4 (Dual basis theorem)**.** *An R-module A is projective if and only there is a set of elements a_i of A and a set of R-maps $f_i\colon A \longrightarrow R$ such that the sum $\sum f_i(a)a_i$ is finite and equal to a for each element $a \in A$.*

Proof. Choose a free module F on a basis e_i and an epimorphism $g\colon F \longrightarrow A$. Let $a_i = g(e_i)$. Then A is projective if and only if there is an R-map $f\colon A \longrightarrow F$ such that $g \circ f = \mathrm{id}$. Given f, we can write $f(a) = \sum r_i e_i$ and define $f_i(a) = r_i$. The f_i are R-maps as in the statement. Conversely, given such f_i, we can define f by $f(a) = \sum f_i(a)e_i$. □

There is a related conceptual version that is particularly important.

Corollary 1.5. *Define*

$$\phi\colon Hom_R(A, R) \otimes_R A \longrightarrow Hom_R(A, A)$$

by $\phi(f \otimes b)(a) = f(a)b$. Then A is finitely generated and projective if and only if ϕ is an isomorphism.

Returning to our integral domain R, we have the following result.

Proposition 1.6. *A non-zero fractional ideal A is invertible if and only if it is projective, and it is then finitely generated.*

Proof. If A is invertible, we can write 1 as a finite sum $\sum a_i b_i$, where $a_i \in A$ and $b_i \in A^{-1}$. The a_i generate A, and we can define $f_i\colon A \longrightarrow R$ by $f_i(a) = b_i a$. By the dual basis theorem, A is projective with finite set of generators a_i. Conversely, let A be projective and let $f_i\colon A \longrightarrow R$ and a_i be as in the dual basis theorem. Choose any fixed non-zero $b \in A$ and let $k_i = f_i(b)/b$. Observe that

$$af_i(b) = bf_i(a)$$

for any $a \in A$. This is trivial if $a = 0$. If $a \neq 0$, we can write $a = m/n$ and $b = p/q$ as quotients of non-zero elements of R. Then, since f_i is an R-map,

$$af_i(b)nq = anf_i(bq) = f_i(anbq) = f_i(an)bq = f_i(a)bnq.$$

Dividing by b, $f_i(a) = k_i a$ for all a, hence $k_i A \subset R$. Since $f_i(b) = 0$ for all but finitely many i, $k_i = 0$ for all but finitely many i. For any a,

$$a = \sum f_i(a)a_i = \sum k_i a_i a.$$

Since this is an equation in K, $\sum k_i a_i = 1$. Therefore A is invertible. □

2. The definition of Dedekind rings and DVR's

There are many equivalent definitions of Dedekind rings. We take the following one, at least provisionally.

Definition 2.1. An integral domain R is a *Dedekind ring* (or *Dedekind domain*) if every non-zero ideal of R is invertible. A *discrete valuation ring*, or DVR, is a local Dedekind ring.

Proposition 2.2. *A PID is a Dedekind ring.*

Proof. Immediate from the definition. □

It is clear that every non-zero ideal is invertible if and only if every non-zero fractional ideal is invertible. That is, all non-zero fractional ideals must be in the group $C(R)$. We shall justify the name DVR shortly. Such rings have a very simple ideal structure, and a standard method for proving results about Dedekind rings, such as the following theorem, is to observe them locally and deduce them globally. We state the following theorem now and prove it later. It shows that our definition of a Dedekind ring is equivalent to Dedekind's original one.

Theorem 2.3. *A ring R is a Dedekind ring if and only if R is a Noetherian integrally closed integral domain of (Krull) dimension 1, so that every non-zero prime ideal is maximal.*

Theorem 2.4. *The ring $\mathcal{O}_K$ of integers in an algebraic number field K is Dedekind. More generally, if R is Dedekind, L is a finite extension of K, and S is the integral closure of R in L, then S is Dedekind.*

Proof. The first statement follows from the second since $\mathbb{Z}$ is Dedekind. For the second statement, we use our second characterization of Dedekind rings. Certainly S is integrally closed since it is an integral closure.

First assume that the extension is separable. Then there is a finite basis $\{x_i\}$ for L over K such that S is contained in the sub R-module spanned by the x_i. Since R is Noetherian, this implies that S is finitely R-generated and therefore also Noetherian. Let P be a non-zero prime ideal of S and $\mathfrak{p} = P \cap R$. Then $\mathfrak{p}$ is non-zero since the constant coefficient of a minimal degree equation of integral dependence for $x \neq 0$ in P is non-zero and in (x), hence in $P \cap R$. If $P \subset Q$ is a proper inclusion of prime ideals in S, then, by passing to quotients by P, we deduce that $P \cap R \subset Q \cap R$ is a proper inclusion of non-zero prime ideals in R, which is a contradiction.

In the general case, L is a purely inseparable extension of a separable extension L_s of K. The integral closure R_s of R in L_s is Dedekind, and S is the integral closure of R_s in L. Thus we may assume that L is a purely inseparable finite extension of K. The minimal polynomial of a non-zero x in S is of the form $x^{p^e} - a$, where p is the characteristic and $a \in K$. Since x is integral over R, so is a, and since R is integrally closed, a is in R. Since L is finite over K, the exponents p^e are bounded, say by $q = p^f$, and S is the set of all elements $x \in L$ such that $x^q \in R$. Let K' be the field of qth roots of elements of K and R' the integral closure of R in K'. Then $x \mapsto x^q$ is an isomorphism $K' \longrightarrow K$ that restricts to an isomorphism $R' \longrightarrow R$, so that R' is Dedekind. To show that S is Dedekind, it suffices to show that every non-zero ideal I of S is invertible. Since $R'I$ is invertible in K', $1 = \sum a_i b_i$ with $a_i \in I$ and $b_i \in (R'I)^{-1}$. Then $1 = \sum a_i^q b_i^q$ and $b_i^{q_i}$ in K. Let $c_i = a_i^{q-1} b_i^q$, so that $1 = \sum a_i c_i$ with c_i in L. It is easy to check that $c_i \in I^{-1}$ in L since $b_i \in (R'I)^{-1}$ in K'. Therefore I is invertible. □

The class number of a number ring is finite, but that is not true for a general Dedekind ring R.

3. Characterizations and properties of DVR's

We start over with a new definition of a DVR, and we then prove that the new notion is equivalent to the notion of a local Dedekind ring. Remember that R is an

integral domain with field of fractions K. To avoid trivial cases, it is convenient to require R not to be K.

Definition 3.1. A domain R is a *valuation ring* if it is not a field and $x \in K - R$ implies $x^{-1} \in R$.

Lemma 3.2. *If I and J are ideals in a valuation ring R, then either $I \subset J$ or $J \subset I$. Therefore R is local.*

Proof. Let $x \in I$ and $x \notin J$. For $y \neq 0$ in J, $x/y \notin R$, hence $y/x \in R$ and $y = (y/x)x \in I$. □

Let $R^\times$ denote the subgroup of units in a ring R.

Definition 3.3. A discrete valuation on a field K is a function $\nu\colon K^\times \longrightarrow \mathbb{Z}$ that satisfies the following properties.

(i) ν is surjective.
(ii) $\nu(xy) = \nu(x) + \nu(y)$.
(iii) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$.

It is often convenient to set $\nu(0) = \infty$, which makes sense of (iii) when $x = -y$ and ensures that (ii) and (iii) are valid for all $x, y \in K$. With that convention, for a discrete valuation ν, $R = \{x|\nu(x) \geq 0\}$ is the valuation ring of (K, ν). It is a valuation ring by (ii) and (iii). A *discrete valuation ring* (DVR) is an integral domain R that is the valuation ring of a discrete valuation on its field of fractions.

Lemma 3.4. *Let R be a DVR. Then a non-zero element $u \in R$ is a unit if and only if $\nu(u) = 0$.*

Proof. $\nu(1) = 0$ by (ii) since $1 \cdot 1 = 1$, and then (ii) applied to $u \cdot u^{-1} = 1$ gives that $\nu(u) = 0$ if and only if $\nu(u^{-1}) = 0$, in which case the inverse u^{-1} is in R. □

Note that it suffices to define a discrete valuation ν on R, since if $x = r/s \in K$, then we can and must define $\nu(x) = \nu(r) - \nu(s)$.

Lemma 3.5. *If R is a DVR, then $\nu\colon R - 0 \longrightarrow \mathbb{N}$ is a Euclidean norm. Thus R is a Euclidean domain and therefore a PID.*

Proof. Let $x, y \in R - 0$. By (ii), $\nu(x) \leq \nu(xy)$. If $\nu(x) \geq \nu(y)$, then $\nu(x/y) \geq 0$ and $x/y \in R$. The equations $x = (x/y)y + 0$ if $\nu(x) \geq \nu(y)$ and $x = 0y + x$ if $\nu(x) < \nu(y)$ verify the other defining condition for a Euclidean norm: there exist s and r in R such that $x = sy + r$ with either $r = 0$ or $\nu(r) < \nu(y)$. □

Examples 3.6. We exhibit some discrete valuation rings.

(i) For a prime p, the ring $\mathbb{Z}_{(p)}$ of p-local integers is the valuation ring of $\nu_p\colon \mathbb{Q} \longrightarrow \mathbb{Z}$, where $\nu_p(p^n a/b) = n$ if a and b are integers which are prime to p.
(ii) Let F be a field. For an irreducible polynomial $f \in F[x]$, the localization $F[x]_{(f)}$ is the valuation ring of $\nu\colon F(x) \longrightarrow \mathbb{Z}$, where $\nu_f(f^n a/b) = n$ if a and b are polynomials which are prime to f.
(iii) The power series ring $F[[x]]$ is the valuation ring of the valuation ν on the Laurent series ring $F[x, x^{-1}] = F((x))$ specified by $\nu(\sum a_i x^i) = n$ for the smallest n such that $a_n \neq 0$ but $a_i = 0$ for $i < n$.

Definition 3.7. An element t of a DVR R is a *uniformizing parameter*, abbreviated UP, if $\nu(t) = 1$.

Lemma 3.8. *Let R be a DVR with fraction field K and UP t.*

(i) *If $r \neq 0$ in R, then $r = ut^n$ where $u \in R^\times$ and $n = \nu(r) \geq 0$.*
(ii) *If $x \neq 0$ in K, then $x = ut^n$ where $u \in R^\times$ and $n = \nu(x) \in \mathbb{Z}$.*
(iii) *The only non-zero proper ideals of R are (t^n) with $n \geq 1$.*
(iv) *The only non-zero prime ideal of R is the maximal ideal (t), which is the set of elements $a \in R$ such that $\nu(a) > 0$.*
(v) *The only non-zero fractional ideals of R are the (t^n) for $n \in \mathbb{Z}$.*

Proof. For (i) and (ii), $x = ut^n$ where $u = xt^{-n}$ is a unit in R by Lemma 3.4. For (iii), if $I \subset R$ is a non-zero proper ideal and n is minimal such that there exists $a \in I$ with $\nu(a) = n$, then $a = ut^n$ for a unit u and $(t^n) \subset I$. If $b \in I$, then $b = ut^q$ where u is a unit and $q \geq n$, hence $b \in (t^n)$. The rest is clear. □

We now give the basic characterization theorem for DVR's. It is usually stated starting just with a commutative ring, but it seems more convenient to start with an integral domain. It shows in particular that a DVR in the sense of Definition 3.3 is the same as a DVR in the sense of Definition 2.1.

Theorem 3.9. *The following statements are equivalent for an integral domain R which is not a field.*

(i) *R is a DVR (in the sense of Definition 3.3).*
(ii) *R is a local PID.*
(iii) *R is a UFD with a unique irreducible element t (up to associates).*
(iv) *R is a Noetherian local ring with a principal maximal ideal.*
(v) *R is an integrally closed Noetherian local ring of dimension 1.*
(vi) *R is a local ring such that every non-zero ideal of R is invertible.*

Proof. We first show that (i), (ii), and (iii) are equivalent. We have already shown that (i) $\implies$ (ii). Assume (ii) and let the maximal ideal of R be (t). Then t is irreducible, since if $t = xy$ with neither x nor y a unit, we would have $t \in (t^2)$, implying that t is a unit; t is the unique irreducible by the maximality of (t), so that (iii) holds. Assume (iii). The ideal (t) is prime, and it is maximal by the uniqueness of t. For any $r \in R$, there exists n such that $r \in (t^n)$ and $r \notin (t^{n+1})$. We set $\nu(r) = n$ and find that ν induces a valuation on K with valuation ring R, so that (i) holds.

Clearly (ii) implies (iv). The equivalent conditions (i), (ii), and (iii) also imply (v) and (vi) since the only ideals of R are (t^n) for a UP t, and similarly for fractional ideals, and since R is integrally closed by inspection: no element of K not in R can satisfy an equation of integral dependence over R. We shall prove the implications (iv) $\implies$ (ii), (vi) $\implies$ (iv), and (v) $\implies$ (iv).

(iv) $\implies$ (ii). Let $M = (t)$ be the maximal ideal of R. We must show that any ideal I is principal. Since I is finitely generated, there is a maximal n such that $I \subset M^n$. For an element a of I that is not in M^{n+1}, $a = ut^n$ for some unit u and thus a is in (t^n). Since this holds for all such a and since $M^{n+1} \subset (t^n)$, $I = (t^n)$.

(vi) $\implies$ (iv). Since invertible ideals are finitely generated, R is Noetherian. We need only show that the maximal ideal M is principal. By Nakayama's lemma $M \neq M^2$. Let $t \in M - M^2$. Since $t \in M$, $tM^{-1} \subset R$, and $tM^{-1} \not\subset M$ since $t \notin M^2$. Therefore $tM^{-1} = R$ and $(t) = M$.

(v) $\implies$ (iv). This is the hardest part, since we must find a way to use the assumption that R is integrally closed. We must prove that the maximal ideal M is

principal. Again, $M \neq M^2$ by Nakayama's lemma, and we can choose $t \in M - M^2$. Clearly $(t) \subset M$, and we claim that equality holds. Since M is the unique non-zero prime ideal, it is the radical of (t). Let n be minimal such that $M^n \subset (t)$. We claim that $n = 1$, and we assume for a contradiction that $n > 1$. Let x be an element of M^{n-1} that is not in (t). Then $xM \subset M^n \subset (t)$. Let $y = x/t \in K$. Then $y \notin R$ since $yt = x \notin (t)$. We claim that y is integral over R and therefore in R, which is a contradiction. Since $xM \subset (t)$, $yM \subset R$ and yM is an ideal. If $yM = R$, say $ym = 1$, then $xm = tym = t$ is in $M^n \subset M^2$, contradicting the choice of t. Thus yM is a proper ideal, $yM \subset M$. This leads to the required equation. Let M be generated by a finite set of elements m_i. Then $ym_j = \sum a_{ij}m_i$ with $a_{ij} \in R$, which can be written

$$\sum(\delta_{ij}y - a_{ij})m_i = 0.$$

Let $d = \det(\delta_{ij}y - a_{ij})$. By Cramer's rule, $dm_i = 0$ for all i and thus $dM = 0$. Since $M \neq 0$, $d = 0$, and this is an equation of integral dependence for y. □

The following corollary shows how little more is needed to ensure that a valuation ring is a DVR.

Corollary 3.10. *A valuation ring R is a DVR if and only if it is Noetherian.*

Proof. A DVR is a PID and is therefore Noetherian. Conversely, let R be a Noetherian valuation ring. An ideal I is generated by finitely many elements a_i. By Lemma 3.2, one of the (a_i) must contain all of the others and therefore must be I. Thus R is a local PID and therefore a DVR by the theorem. □

The following corollary and proposition are useful in local to global arguments.

Corollary 3.11. *If P is a minimal non-zero prime ideal in an integrally closed Noetherian integral domain, then R_P is a DVR.*

Proof. R_P is an integrally closed Noetherian local ring of dimension 1. □

Proposition 3.12. *R is integrally closed if and only if R_P is integrally closed for all prime ideals P or, equivalently, all maximal ideals P.*

Proof. Let $i\colon R \longrightarrow S$ be the inclusion of R in its integral closure in K. Thus R is integrally closed if and only if i is an epimorphism. Of course, K is also the field of fractions of R_P for all primes P, and the integral closure of R_P is $i_P\colon R_P \longrightarrow S_P$. Since i is an epimorphism if and only if i_P is an epimorphism for all prime ideals P or, equivalently, all maximal ideals P, the conclusion follows. □

4. Completions of discrete valuation rings

We assume for now that the reader has seen completions of rings.

Example 4.1. Consider the p-adic integers $\mathbb{Z}_p$ in their fraction field $\mathbb{Q}_p$. This is a local PID with maximal ideal (p), hence a DVR. Any $x \in \mathbb{Q}_p$ is of the form up^n, where u is a unit in $\mathbb{Z}_p$ and n is an integer. The required valuation ν_p is given by $\nu_p(x) = n$.

Clearly the valuations on $\mathbb{Z}_{(p)}$ and $\mathbb{Z}_p$ are related. We make this precise. Let ν be a discrete valuation on a field K. Pick a real number $q > 1$ and define $d(x, y) = ||x - y||$, where $||x|| = q^{-\nu(x)}$. Then K is a metric space with metric d since the following three properties of d are immediate. For (i) we use our convention that $\nu(0) = \infty$ and interpret $q^{-\infty}$ to be zero.

(i) $d(x,y) \geq 0$ with equality if and only if $x = y$.
(ii) $d(x,y) = d(y,x)$
(iii) $d(x,y) \leq \max\{d(x,z), d(z,y)\} \leq d(x,z) + d(z,y)$.

We complete K as a metric space, taking $\hat{K}$ to be the set of equivalence classes of Cauchy sequences, so that Cauchy sequences converge in $\hat{K}$. For definiteness, we add subscripts ν to everything in sight when we want to remember which valuation on K we have in mind.

Example 4.2. We have the valuation ν_p on $\mathbb{Q}$. Here we take $q = p$ so that $||p^n a/b||_p = p^{-n}$. Then $\hat{\mathbb{Q}} = \mathbb{Q}_p$ and $\hat{\mathbb{Z}}_{(p)} = \mathbb{Z}_p$. One way to think of this is to represent elements of $\mathbb{Q}_p$ as p-adic Laurent series $a = \sum a_i p^i$, $0 \leq a_i < p$, with $\nu_p(a)$ being the minimal n such that $a_n \neq 0$.

Example 4.3. For a field F, the completion of $F(x)$ at ν_x gives $F((x))$, with $F[x]$ completing to $F[[x]]$.

Of course, these completions give the starting point for analytic number theory.

5. Characterizations and properties of Dedekind rings

The global analogue of our characterization theorem for DVR's reads as follows. The equivalence of (i) and (iii) is the promised Theorem 2.3.

Theorem 5.1. *The following statements are equivalent for an integral domain R which is not a field.*

(i) *R is Noetherian, integrally closed, and of dimension 1.*
(ii) *R is Noetherian and each localization R_P at a prime is a DVR.*
(iii) *Every non-zero ideal of R is invertible.*
(iv) *Every non-zero proper ideal of R is a product of maximal ideals.*
(v) *Every non-zero proper ideal of R is a product of prime ideals.*

Moreover, the product decomposition in (iv) is then unique.

Proof. Since primes of R_P correspond to primes contained in P in R, we see that the dimension of R is one if and only if the dimension of each R_P is one. Similarly, the Noetherian property is local, and so is integral closure by Proposition 3.12. Thus (i) is equivalent to (ii) by Theorem 3.9.

By Theorem 3.9 again, to show that (ii) is equivalent to (iii), it suffices to show that every non-zero ideal of R is invertible if and only if every non-zero ideal of each R_P is invertible. In K, which is the field of fractions of R_P,

$$(A^{-1})_P = (A_P)^{-1} \quad \text{and} \quad (AB)_P = A_P B_P$$

for finitely generated fractional ideals A and B of R. Moreover, just as for ideals, each fractional ideal of R_P has the form $R_P A$ for some fractional ideal A of R. Thus, if $AA^{-1} = R$, then $A_P(A_P)^{-1} = R_P$. Since (iii) implies that R is Noetherian, this gives the implication (iii) $\Rightarrow$ (ii). For the converse, if $A_P(A_P)^{-1} = R_P$ for all P, then $(AA^{-1})_P = R_P$ for all P. Taking intersections over P, this gives $AA^{-1} = R$. For a more pedestrian proof, taking A to be an ideal, if AA^{-1} is properly contained in R, then it is contained in some maximal ideal P. Now A_P is principal, say generated by a/s with $a \in A$ and $s \in R - P$. Let I be generated by finitely many elements b_i. Each b_i can be written as $(r_i/s_i)(a/s)$ for some elements $r_i \in R$ and $s_i \in R - P$. Let t be the product of s and all of the s_i. Then $t \in R - P$, and

$t/a \in A^{-1}$ since each $b_i t/a$ is in R. But then $t = a(t/a)$ is in $AA^{-1} \subset P$, which is a contradiction.

There are several ways to prove that (iii) implies (iv). The usual one uses reduced primary decompositions, but a proof that does not assume familiarity with that theory is perhaps preferable. Note again that (iii) implies that R is Noetherian and let $\mathscr{S}$ be the set of all non-zero proper ideals that are not finite products of maximal ideals. If $\mathscr{S}$ is non-empty, it contains a maximal element I. Since I cannot be a maximal ideal, it must be properly contained in some maximal ideal M. Let $J = M^{-1}I$. Then $J \subset R$ and the inclusion is proper. Now $I = MJ \subset J$, and again the inclusion is proper since $MJ = J$ implies $M = R$. By the maximality of I, J must be a product of maximal ideals. But then so is I, which is a contradiction.

Obviously (iv) implies (v). We will complete the proof by showing that (v) $\Rightarrow$ (iii) after giving some corollaries of what has already been proven and proving some preliminary results. □

Corollary 5.2. *A Dedekind ring R is a PID if and only if it is a UFD.*

Proof. Any PID is a UFD. Assume R is a UFD and let P be a prime ideal. Let a be a non-zero element of P. Some irreducible factor t of a is in P and so $(t) \subset P$. Since $\dim(R) = 1$, $(t) = P$. Thus every prime ideal is principal. Since every ideal is a product of prime ideals, every ideal is principal. □

Corollary 5.3. *Let I be a non-zero proper ideal of a Dedekind ring R.*

(i) *There is an ideal J such that IJ is principal.*
(ii) *Every ideal in R/I is principal and R/I is Artinian.*
(iii) *If $I \subset J$, then $J = I + (b)$ for some $b \in R$.*
(iv) *I can be generated by two elements.*

Proof. Let $I = P_1^{r_1} \cdots P_n^{r_n}$, where the P_i are distinct maximal ideals and $r_i > 0$. Distinct maximal ideals P and Q are comaximal, $P + Q = R$, and it follows that any powers P^r and Q^s are also comaximal. Therefore, by the Chinese remainder theorem (CRT), R/I is the product of the $R/P_i^{r_i}$. The CRT also implies that if $b_i \in R - P_i^{r_i+1}$, then there exists an $a \in R$ such that $a \equiv b_i \bmod P_i^{r_i+1}$ for each i. We can choose $b_i \in P^{r_i}$ for each i, and then $a \in I$. We let $J = aI^{-1}$. Then $J \subset R$ and $IJ = (a)$, which proves (i).

For (ii), R/I is Noetherian of dimension 0, which is one of the equivalent conditions for a ring to be Artinian. Any one of its factors, R/P^r say, is isomorphic to $R_P/R_P P^r$, which is a quotient of a DVR. Therefore every ideal in R/P^r is principal, and it follows that every ideal in R/I is principal. Comparing with the quotient by I, we see that (iii) is just a reinterpretation of (ii) in R. Finally, for (iv), if a is a non-zero element of I, we can apply (iii) to the inclusion $(a) \subset I$ to obtain b such that $I = (a, b)$. □

We now head towards the proof that (v) $\Longrightarrow$ (iii) in Theorem 5.1. We start with two general observations, the first of which implies the uniqueness statement at the end of that result.

Lemma 5.4. *Let I be an ideal in an integral domain R. If I can be factored as a product of invertible prime ideals, then the factorization is unique.*

Proof. Suppose $P_1 \cdots P_m = Q_1 \cdots Q_n$ are two such factorizations of I. We must show that $m = n$ and, after reordering, $P_i = Q_i$. Take Q_1 to be minimal among the

Q_j, so that $Q_1 \supset Q_j$ implies $Q_1 = Q_j$. Since $I \subset Q_1$, some $P_i \subset Q_1$. Reordering, we can take $P_1 \subset Q_1$. Similarly, $P_1 \supset Q_j$ for some j. But then $Q_j \subset P_1 \subset Q_1$ and these are all equal. Multiplying by Q_1^{-1} we have $P_2 \cdots P_m = Q_2 \cdots Q_n$. The conclusion follows by induction. □

Lemma 5.5. *Let R be an integral domain and let $x \neq 0$ in K. Suppose that $xR = A_1 \cdots A_q$ for fractional ideals A_i. Then each A_i is invertible.*

Proof. The inverse of A_i is $x^{-1}A_1 \cdots A_{i-1}A_{i+1} \cdots A_n$. □

We assume in the following two lemmas that R is an integral domain such that all ideals in R are finite products of prime ideals.

Lemma 5.6. *Every invertible prime ideal P is maximal.*

Proof. Let $a \in R - P$. We claim that $P + (a) = R$. If not, we can write $P + (a)$ and $P + (a^2)$ as products $P_1 \cdots P_m$ and $Q_1 \cdots Q_n$ of prime ideals. Clearly P is contained in each P_i and Q_j. Let b be the image of a in the integral domain R/P and note that b^2 is the image of a^2. Then (b) is the product of the prime ideals P_i/P and (b^2) is the product of the prime ideals Q_j/P. By Lemma 5.5, each P_i/P and Q_j/P is invertible. Clearly

$$(P_1/P)^2 \cdots (P_m/P)^2 = Q_1/P \cdots Q_n/P.$$

By Lemma 5.4, $n = 2m$ and each P_i/P appears twice among the Q_j/P. This proves the equality in the following display, its inclusions being obvious.

$$P \subset P + (a^2) = (P + (a))^2 \subset P^2 + (a).$$

If $x \in P$, then $x = y + ra$ with $y \in P^2$ and $r \in R$, and $ra = x - y$ is in P. Since $a \notin P$, $r \in P$. Thus $P \subset P^2 + aP \subset P$ and $P = P^2 + aP = P(P + (a))$. Since P is invertible, $R = P + (a)$, as claimed. □

Lemma 5.7. *Every non-zero prime ideal P is invertible.*

Proof. Let $a \in P$, $a \neq 0$. Then $(a) = P_1 \cdots P_n$, P_i prime. Each P_i is invertible and therefore maximal, by Lemmas 5.5 and 5.6. Since $(a) \subset P$, $P_i \subset P$ for some i, and then $P = P_i$ is invertible. □

Proof of (v) $\Longrightarrow$ (iii) in Theorem 5.1. Every non-zero ideal is a product of prime ideals and every non-zero prime ideal is invertible. □

Let R be a Dedekind ring in the rest of the section.

Corollary 5.8. *Any non-zero fractional ideal A has a unique factorization*

$$A = P_1^{r_1} \cdots P_q^{r_q},$$

where the P_i are maximal ideals and the r_i are non-zero integers.

Proof. This is clear from Lemma 5.4 if A is an ideal. Applied to (d) and dA where $dA \subset R$, it follows in general. □

We know that the localizations R_P are DVR's, but we can now see this directly.

Definition 5.9. Let $x \in K$, $x \neq 0$, and write $(x) = P_1^{r_1} \cdots P_q^{r_q}$. Let P be a prime and define $\nu_P(x) = r_i$ if $P = P_i$ and $\nu_P(x) = 0$ if P is not one of the P_i.

The following result is immediate from the definition.

Proposition 5.10. *ν_p is a valuation on K with valuation ring R_P.*

6. Ideals and fractional ideals in Dedekind rings

The theory above sets up the starting point for algebraic number theory. It allows us to manipulate ideals and prime ideals exactly as if they were numbers and prime numbers. We illustrate by giving ideal versions of standard terminology and results for integers. Let A and B be fractional ideals (in any integral domain R). We say that B divides A, $B|A$, if there is an ideal I such that $A = IB$. Clearly this implies $A \subset B$. When R is Dedekind, as we assume throughout this section, the converse holds. If $A \subset B$ and we define $I = AB^{-1}$, then $I \subset BB^{-1} = R$ and $IB = A$. We define the greatest common divisor $D = (A, B)$ to be a divisor of A and B such that any C that divides both A and B divides D.

Proposition 6.1. *Let $I = P_1^{r_1} \cdots P_q^{r_q}$ and $J = P_1^{s_1} \cdots P_q^{s_q}$ be ideals, where $r_i \geq 0$ and $s_j \geq 0$.*

(i) *$I \subset J$ if and only if $J|I$ if and only if $s_i \leq r_i$ for $1 \leq i \leq n$.*

(ii) *$I + J = (I, J) = P_1^{t_1} \cdots P_q^{t_q}$, where $t_i = min(r_i, s_i)$.*

Proof. For (i), note that $I = HJ$, where $H = P_1^{r_1 - s_1} \cdots P_q^{r_q - s_q}$. For (ii), note that $P_1^{t_1} \cdots P_q^{t_q}$ is the smallest ideal that contains both I and J. □

For fractional ideals in general, we have the following result.

Proposition 6.2. *For fractional ideals A and B, there are elements x and y in K such that xA and yB are relatively prime ideals.*

Proof. Multiplying by suitable elements of R, we may assume without loss of generality that A and B are ideals in R. Let $A = P_1^{r_1} \cdots P_q^{r_q}$ and $B = P_1^{s_1} \cdots P_q^{s_q}$, where $r_i \geq 0$ and $s_j \geq 0$. We can find an ideal I and an element b of R such that $AI = (b)$, and we can then find an ideal J and an element a of R such that $IJ = (a)$. We may take I to be a product of powers of prime ideals Q_j distinct from the P_i and J to be a product of prime ideals distinct from the P_i and Q_j. Then $(a/b)A = (IJ)(I^{-1}A^{-1})A = J$, which is relatively prime to B. □

This result has interesting implications about sums of fractional ideals that will lead to a classification of finitely generated torsion free R-modules.

Lemma 6.3. *Fractional ideals A and B are isomorphic if and only if $A = xB$ for some non-zero $x \in K$.*

Proof. Clearly $x\colon B \longrightarrow xB$ is an isomorphism with inverse x^{-1}. Conversely, $A \cong B$ implies $R \cong B^{-1}A$, and the image of 1 gives an element $x \in B^{-1}A$ such that $B^{-1}A = xR$, hence $A = xB$. □

Proposition 6.4. *For fractional ideals $A_1, \cdots, A_n$,*

$$A_1 \oplus \cdots \oplus A_n \cong R^{n-1} \oplus A_1 \cdots A_n.$$

Proof. By a quick induction, it suffices to prove the result when $n = 2$ and we are dealing with fractional ideals A and B. Multiplying by suitable elements x and y of K, we may assume that A and B are relatively prime ideals in R. Define $\pi\colon A \oplus B \longrightarrow R$ by $\pi(a, b) = a + b$. The kernel of π is $A \cap B = AB$. Since A and B are relatively prime, π is an epimorphism. The short exact sequence

$$0 \longrightarrow AB \longrightarrow A \oplus B \xrightarrow{\pi} R \longrightarrow 0$$

splits since R is free, and this gives the conclusion. □

There is a boring plebian proof and an elegant proof of the following result. Of course, we will not be plebian, but that means that we must assume familiarity with the theory of determinants of modules. The following three results hold for any integral domain R.

Proposition 6.5. *Let A and B be fractional ideals. Then*

$$R^m \oplus A \cong R^n \oplus B$$

if and only if $m = n$ and $A \cong B$.

Proof. In one direction this is trivial. Assume we have the displayed isomorphism. For any fractional ideal A, $A \otimes_R K \cong K$. Therefore, applying $(-) \otimes_R K$ to our isomorphism, we obtain isomorphic vector spaces of dimensions $m+1$ and $n+1$, so $m = n$. Now apply the $(n+1)$st exterior power, that is, the determinant, to our isomorphism. Since the determinant carries sums to tensor products, our given isomorphism becomes an isomorphism $A \cong B$. □

Corollary 6.6. *If $I \oplus R^m \cong R^{m+1}$, then $I \cong R$ is principal.*

Definition 6.7. Two finitely generated modules over a ring are said to be *stably isomorphic* if they become isomorphic after taking direct sums with a finitely generated free R-module.

Corollary 6.8. *If an ideal in an integral domain is stably free, then it is principal.*

Returning to our Dedekind ring, we obtain the following conclusion.

Corollary 6.9. *For fractional ideals $A_1, \cdots, A_m$ and $B_1, \cdots B_n$,*

$$A_1 \oplus \cdots \oplus A_m \cong B_1 \oplus \cdots \oplus B_n$$

if and only if $m = n$ and $A_1 \cdots A_n = xB_1 \cdots B_n$ for some $x \in K$.

Proof. The displayed isomorphism is equivalent to an isomorphism

$$R^{m-1} \oplus A_1 \cdots A_m \cong R^{n-1} \oplus B_1 \cdots B_n,$$

which in turn is equivalent to $m = n$ and an isomorphism $A_1 \cdots A_n \cong B_1 \cdots B_n$, which, finally, is equivalent to $m = n$ and $A_1 \cdots A_n = xB_1 \cdots B_n$. □

7. The structure of modules over a Dedekind ring

We explain how the classical classification of finitely generated modules over a PID extends to Dedekind rings. Remember that an invertible fractional ideal over an integral domain R is a finitely generated projective R-module.

Definition 7.1. The torsion submodule, $\mathrm{Tor}(M)$, of an R-module M is the set of elements m such that $rm = 0$ for some non-zero $r \in R$. Equivalently, it is the kernel of $M \longrightarrow M \otimes_R K$. M is torsion free if $\mathrm{Tor}(M) = 0$, and $M/\mathrm{Tor}(M)$ is torsion free for any M. If M is finitely generated, the rank of M, $\mathrm{rank}(M)$, is the dimension over K of $M \otimes_R K$.

Observe that M cannot be projective if it has a torsion element m, $rm = 0$, because m is in the kernel of any homomorphism from M to a free R-module. Assume that R is Dedekind in the rest of the section.

Theorem 7.2. *A finitely generated R-module M is projective if and only if it is torsion free, and this holds if and only if $M \cong R^{n-1} \oplus I$, where $n = rank(M)$ and I is an ideal. Thus M is stably isomorphic to I.*

Proof. If M is projective, then it is a direct summand of a free R-module and is therefore torsion free. Assume that M is torsion free and proceed by induction on the rank n of M. If $n = 1$, then M is a sub R-module of $M \otimes_R K \cong K$ and is therefore isomorphic to a fractional ideal. By choosing $n-1$ elements of M that span a vector space of that dimension in $M \otimes_R K$, we can construct a sub R-module N of rank $n-1$. The exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

remains exact upon tensoring with K, hence M/N has rank 1. Thus M/N is projective and the sequence splits. Since any fractional ideal is isomorphic to an ideal, the conclusion follows from the inductive hypothesis and Proposition 6.4. □

This leads to the structure theorem for finitely generated R-modules.

Theorem 7.3. *Let M be a finitely generated R-module. Then*

$$M \cong Tor(M) \oplus M/Tor(M);$$

$M/Tor(M)$ is stably isomorphic to an ideal I, uniquely determined up to isomorphism, and

$$Tor(M) \cong R/P_1^{r_1} \oplus \cdots \oplus R/P_q^{r_q}$$

for uniquely determined prime ideals P_i and positive integers r_i.

Proof. Since $M/\mathrm{Tor}(M)$ is torsion free, it is projective and the short exact sequence

$$0 \longrightarrow \mathrm{Tor}(M) \longrightarrow M \longrightarrow M/\mathrm{Tor}(M) \longrightarrow 0$$

splits. In view of the previous result, it remains to consider the structure of finitely generated torsion modules N. Let J be the annihilator of N, $J = \{r|rN = 0\}$. Let $J = P_1^{s_1} \cdots P_q^{s_q}$ be its prime factorization. Then

$$R/J \cong R/P_1^{s_1} \times \cdots \times R/P_q^{s_q}.$$

Therefore, as an R/J-module,

$$N \cong N/P_1^{s_1}N \times \cdots \times N/P_q^{s_q}N,$$

where each $N/P_i^{s_i}N$ can be identified with the P_i-torsion summand $\{n|P^{s_i}n = 0\}$. Thus it remains to study finitely generated modules Q over the Artinian quotient ring $R/P^s \cong R_P/P_P^s$ for a prime ideal P. The following result gives the conclusion. □

Proposition 7.4. *Let M be a finitely generated module over a quotient ring $R/(t^s)$, where R is a DVR with UP t. Then M is isomorphic to a direct sum of modules $R/(t^r)$, where $1 \le r \le s$. Let d_i be the dimension of the vector space $t^iM/t^{i+1}M$ over $R/(t)$. Then the number of summands of type $R/(t^r)$ appearing in the decomposition of M is $d_{r-1} - d_r$.*

Proof. The quotient ring $Q = R/(t^s)$ is self-injective (that is, Q is a quasi-Frobenius ring). We may as well assume that there exists $m \in M$ such that $t^{s-1}m \neq 0$, since otherwise M is a module over $R/(t^{s-1})$. Then $Qm \cong Q$ and the inclusion $Qm \subset M$ splits, so that $M \cong Qm \oplus N$ where N has one fewer generator than M. The conclusion follows by induction. □