Dedekind domains

The notion of Dedekind domain arises from the observation that the proof that the fractional ideals in the maximal order of a number field form a group can apply to other rings that are not related to number theory. In what follows, let R be an integral domain with fraction field K. A fractional ideal of R is an nonzero R-submodule $I \subset K$ such that for αI is an ideal of R for some nonzero $\alpha \in R$. Note any nonzero finitely generated R-module in K is a fractional ideal. A ring S containing R as a subring is said to be integral over R if for each element $z \in S$ the subring $R[z] \subset S$ is a finitely generated R module. This is equivalent to each element z of S is the root of a monic polynomial in $R[x]$, by looking at the characteristic polynomial of multiplication by z on the ring $R[z]$. The integral closure of R in a ring T containing it is the ring of all $t \in T$ such that $R[t]$ is integral over R. The ring R is integrally closed if the integral closure of R in its fraction field is again R.

Recall that we have the following results:

a) Every nonzero simple R-module is isomorphic to R/P for P a maximal ideal of R.
Proof: If M is a nonzero simple R-module, let $m \in M$ be a nonzero element. The map $r \to rm$ gives an R-module map onto M (since its image is nonzero, by simplicity it is all of M) and the kernel P is maximal, again by the fact that M is simple.

b) If I is an ideal of R such that R/I has finite length as an R-module, then there exist maximal ideals $P_1, \ldots, P_t$ of R such that the product $P_1 \cdots P_t \subset I$.
Proof: Since R/I has finite length there are are submodules $I = M_0 \subset M_1 \subset \cdots M_t \subset M_{t+1} = R$ such that M_i/M_{i-1} is simple, and hence by (a) of the form R/P_i. Thus multiplication by P_i annihilates M_i/M_{i-1}, that is $P_i M_i \subset M_{i-1}$ which shows $P_1 \cdots P_t \subset I$.

c) If P is a prime ideal in R and a product of ideals $P_1 \cdots P_t \subset P$ then P contains one of the P_i. If the P_i are maximal, then P equals one of them.
Proof: Reduce modulo P to obtain that the reductions of the P_i have product zero in the domain R/P, hence some P_i is zero when reduced modulo P, hence is contained in P. If all are maximal it must equal P.

d) If P is a prime ideal of R and for some nonzero $\alpha \in P$ the ideal αR contains a product of maximal ideals $P_1 \cdots P_t$, then the set $(R : P) = \{x \in K | xP \subset R\}$ contains elements not in R.
Proof: Since $P_1 \cdots P_t \subset \alpha R \subset P$ by (c) we may assume that $P_1 = P$. Choose the smallest such product which is inside αR, so that $P_2 \cdots P_t \not\subset \alpha R$. Then if y is in $P_2 \cdots P_t$ and not in αR, the element y/α is not in R but is in $(R : P)$.

e) Under the assumptions of d) and assuming P is maximal, either $(R : P)P = R$ or $(R : P) \subset (P : P) = \{x \in K | xP \subset P\}$ and the latter set is a ring which properly contains R.

Proof: Note $P \subset (R : P)P \subset R$, so that either $(R : P)P = R$ or $(R : P) = P$ which together with the result of d) accounts for the two cases.

f) Products of invertible fractional ideals are invertible. If an invertible ideal factors as a product of fractional ideals, each is invertible.

Proof: If $AI = R, BJ = R$ then $ABIJ = R$. If $I = MN$ is invertible, then $I^{-1}MN = R$ showing that M, N are invertible.

g) If an invertible ideal of R factors into a product of prime ideals, then the factorization is unique up to reordering.

Proof: Suppose that $I = \prod_1^s P_i = \prod_1^t Q_j$ with P_i, Q_j prime ideals. By f), if I is invertible, then so are P_i, Q_j. We induct on $k = \max s, t$, the case $k = 1$ being obvious. By forming the domain by the quotient of P_i or Q_j we see that given a prime on one side of the equation, there exists a prime on the other side contained in the first ideal. After reordering assume that P_1 does not contain any P_j properly. Then there is some j such that $Q_j \subset P_1$. Since Q_j contains some P_i, the assumption on P_1 implies $P_1 \subset Q_j \subset P_1$, so $Q_j = P + 1$. By reordering we may assume $P_1 = Q_1$. Since the ideals are invertible we can consider $P_1^{-1}I$ which has two factorizations of shorter length, which agree after reordering by the induction hypothesis.

h) Let R be an integrally closed Noetherian domain with fraction field K and let L/K be a finite degree separable extension. Then the integral closure S of R in L is Noetherian.

Proof: L/K separable means that $L \otimes_K \bar{K}$ is a product of fields, and the trace is a sum of embeddings ϕ_i of L/K into $\bar{K}$. Thus, if s is integral over R, so is $\phi_i(s)$ and hence trace S. Thus the bilinear form $< x, y >= tr_{L/K}(xy)$ is nondegenerate and maps SxS to elements integral over R, hence in R, since it clearly is after tensoring with $\bar{K}$. Choose a basis of L/K consisting of elements $b_i \in S$. Let $b_i* \in L$ be the dual basis with respect to $<, >$. Then if $s \in S$ $s = \sum c_i b_i*$ and $tr(ss_j) = c_j$ is in R. So S is an R-submodule of a finitely generated R-module, and is hence Noetherian.

We now determine equivalent conditions on a domain R as above.

Theorem: The following conditions on an integral domain R are equivalent. Such a domain R is called a Dedekind domain.

1) R is integrally closed and for each nonzero ideal I of R, the quotient R/I is a finite length R–module.
2) Every nonzero proper ideal of R factors uniquely as a product of prime ideals.
2') Every nonzero proper ideal of R factors as a product of prime ideals.
3) For each maximal ideal M there is a fractional ideal M^{-1} such that $MM^{-1} = R$ and the nonzero fractional ideals form a group.
4) R is Noetherian, integrally closed and every nonzero prime ideal is maximal (that is R is a dimension 1 ring).

Proof:

$1 \Rightarrow 2$: By (b) above any nonzero ideal contains a product of maximal ideals, and by (c) any nonzero prime ideal is maximal. If the second case of e) happens for a prime ideal P, we have that $R \neq (P : P)$. Observe that if α is a nonzero element of P and $x \in (P : P)$ the submodules $\alpha R \subset \alpha R + x\alpha R \subset \alpha R + x\alpha R + x^2\alpha R \subset \cdots \alpha R + x\alpha R + x^2\alpha R + \cdots + x^m\alpha R \subset R$ can not be all distinct since $R/\alpha R$ has finite length. Thus for any element $x \in (P : P)$ some power is a polynomial in lower powers with coefficients from R, and since we have assumed that R is integrally closed, $x \in R$. This contradiction shows that every prime ideal P has an inverse $P^{-1} = (R : P)$. We show unique factorization of an ideal I in R by induction on the length of R/I. If I is not maximal, there is an ideal J properly containing I with simple quotient annihilated by a maximal ideal P_1. By induction $J = P_2 \cdots P_t$, so $P_1 \cdots P_t \subset I$. We then have $P_1 \subset P_2^{-1} \cdots P_t^{-1} I \subset P_2^{-1} \cdots P_t^{-1} J = R$. Since Since I and J are different, and P_1 is maximal we have that $P_1 = P_2^{-1} \cdots P_t^{-1} I$ which gives the factorization of I. Uniqueness follows by induction on the length of prime factorization using the inverses of the prime ideals and c) above to see that the prime ideals in one factorization must also appear in any other factorization, and multiplication by the inverse of such a prime shows that factorizations are unique up to order of factors.

$2 \Rightarrow 2' \Rightarrow 3$: We first show all invertible prime ideals are maximal under hypothesis $2'$. This is perhaps the most subtle part of the proof of the theorem on equivalences. Let P be an invertible ideal of R and let a be an element of R which is not in P. The goal is to show $P + aR = R$.

Claim: $(P + a^2R) \subset (P + aR)^2$

Proof: This is true if $P + aR = R$. When $P + aR$ is a proper ideal, so is $P + a^2R$ so by $2'$ there exist primes P_i, Q_j such that

$$(P + a^2R) = \prod P_i, (P + aR) = \prod Q_j.$$

All P_i, Q_j contain P and a^2, hence P, a since P_i, Q_j are prime. Let $\phi : R \to R/P$ be the quotient map. Since $\phi(P + aR)^2 = \phi(a)^2 = \phi(P + aR)^2$ is a proper nonzero principal ideal in the domain R/P it is invertible and by g) after reordering we have that $\phi(Q_j)$ appears twice among $\phi(P_i)$. Since ϕ is one to one on ideals containing P, it must be that each Q_j appears twice in the factorization of $(P + a^2R)$ so that $(P + a^2R) \subset (P + aR)^2$.

The claim implies that $P \subset (P + aR)^2$, so given $p \in P$ there exist $x, x', y, y' \in R$ such that $p = (x + ay)(x' + ay') = xx' + az + a^2w$ with $x, x', z, a^2w \in P$. Since $a \notin P$ we have $w \in P$ proving $P \subset aP + P^2$. Multiply by the inverse of P to get that $R = aR + P$ so that all invertible prime ideals are maximal, as desired.

Let Q be any nonzero prime ideal, and let $\alpha \in Q$ be nonzero. By hypothesis $2'$ the invertible ideal αR factors into a product of invertible prime ideals P_i which are maximal ideals by the preceeding. By c) Q equals one of the P_i so Q is maximal and invertible. Hence every nonzero ideal is a product of invertible prime ideals and by f) all nonzero ideals are invertible. For any fractional ideal A,the ideal αA is invertible so A is invertible by f). Thus the nonzero fractional ideals are all invertible, so they form a group under multiplication of ideals.

$3 \Rightarrow 4$: Let $x \in K$ satisfy $x^n + a_1x^{n-1} + \cdots + a_0 = 0, a_i \in R$. Then the fractional ideal $A = R + Rx + Rx^2 + \cdots + Rx^{n-1}$ satisfies that $A^2 = A$. If the fractional ideals form a group, $A = R$, the identity of the group, so that $x \in R$. Hence R is integrally closed. If P is a prime ideal of R, then it is contained in a maximal ideal Q. Then $P = Q^{-1}PQ$ and since P is prime either Q or $Q^{-1}P$ is contained in P. In the second case $P = Q^{-1}PQ \subset PQ \subset P$ so all are equal P implying by the group structure that Q=R. Thus P contains a maximal ideal and thus every nonzero prime is maximal. Finally, any ideal J has an inverse J^{-1} so that $J^{-1}J = R$. Hence there are $\alpha_i \in J^{-1}, b_i \in I$ with $1 = \sum_{i=1}^n \alpha_i b_i$. Then if $b \in I, b = \sum_{i=1}^n (\alpha_i b) b_i$ showing that I is finitely generated, so that R is Noetherian.

$4 \Rightarrow 1$: If M is a nonzero ideal in an integrally closed Noetherian ring R then any element of $(M : M) = \{x \in K | xM \subset M\}$ is integral over R, by exactly the same argument as above (looking at nested ideals $mR + xmR + x^2mR + \ldots + x^kmR$) , hence this module is just R. Given any nonzero ideal I in R such that $(R : I) \neq R$, there is a largest ideal M containing I such that $(R : M) \neq R$, since R is Noetherian. We show M is prime by supposing that a,b are elements of R such that $ab \in M, a \notin M$. Let $\gamma \in (R : M)$ but not in R. Since $M + aR$ is larger than M, we cannot have $\gamma(M + aR)$ contained in R, hence $\gamma a \notin R$. But $\gamma a \in (R : M + bR)$ so by the maximality of M we must have $b \in M$. Hence M is prime, and by the dimension 1 condition and remark above, M is invertible ($M \subset (R : M)M \subset R, (R : M) \neq R$ so $(R : M)$ is not in (M:M), thus $(R : M)M \neq M$). If not every ideal factored as a product of primes, by the Noetherian assumption there is an ideal I which does not factor, but any larger ideal does. Every nonzero ideal I is contained in a maximal ideal P, so that $I \subset (R : P)I \subset R$ and by the remark, $(R : P)I \neq I$. Then $(R : P)I = P_1 \cdots P_t$, so multiplying by P gives the factorization of I. The uniqueness of the factorization follows as above using (c). Finally, note that if ideals $A = P_1 \cdots P_t \subset B = Q_1 \cdots Q_r$ then by c) each prime Q_i must appear among the P_i. Multiplying by the inverses of all Q_i gives that $AQ_1^{-1} \cdots Q_r^{-1} \subset R$, a given prime Q_i appears in B no more times than it appears in A. Thus the possible ideals containing A are finite in number, so R/A is a finite length R–module. This establishes 1.

Examples of Dedekind domains

1. An order in a number field is a Dedekind domain if and only if it is the maximal order.
2. Any principal ideal domain is a Dedekind domain.

3. Let $f(x, y)$ be a nonconstant irreducible polynomial with complex coefficients. Suppose that the partial derivatives of f have no simultaneous complex zeros with f. Then $\mathbf{C}[x, y]/(f(x, y))$ is a Dedekind domain.

4. A unique factorization domain is a Dedekind domain if and only if it is a principal ideal domain.

One use of the theorem of equivalences above is in proving certain rings are Dedekind.

Theorem: Let R be a Dedekind domain with fraction field K. Let L/K be separable of finite degree. Then the integral closure S of R in L is a Dedekind domain.

Proof: By h) S is a Noetherian ring with fraction field L and if $z \in L$ is integral over S it is integral over R so $z \in S$. Thus S is integrally closed.

It remains to check that every nonzero prime ideal $P \subset S$ is maximal. For a nonzero element in P, the constant term of its minimal polynomial in $R[x]$ is in $P \cap R$, so the latter ideal is prime and nonzero. If $P \subset Q$ are distinct primes of S then $P \cap R$ does not equal $Q \cap R$ since S/P is integral over $R/(P \cap R)$ and the comment above applies to $(Q \cap R)/(P \cap R)$, so that $P \cap R \neq Q \cap R$. Thus all prime ideals in S are maximal. S satisfies the conditions of part 4) of the theorem giving that S is a Dedekind domain.

This theorem explains example 1 above by starting with the Dedekind domain Z and taking its integral closure in a number field to get the maximal order. In the polynomial case, smoothness is sufficient to show that the ring considered is the integral closure of $F[x]$ in the finite separable field extension $F[x, y]/(f(x, y))$.