International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

On Algebraic Number Theory domains Dedekind

Ramesh B. Ghadge

Assistant Professor and H.O.D, Department of Mathematics, Kalikadevi Arts, commerce & Science College, Shirur Kasar Tq.shirur kasar Dist. Beed, Sate Maharashtra, India

Abstract:

This article is based on a series talks I gave on the topic mentioned in the title in a Counsellor Seminar at proms'. The exposition till Section is based on and most of the remainder is based on and some notes on Algebraic Number Theory available.

Keywords: The AKLB setup Notation AKLB setup, Dedekind Domains

Fractional ideals field, Number Theory Mathematics.

Introduction:

The purpose of this article is to study the single most important ring that comes up in algebraic Number theory - Dedekind domains. These domains share many properties with Z, and indeed, Z is a Dedekind domain. Moreover, weird rings like Z [−5], which are notorious for not having unique. Prime factorization, are also Dedekind domains. In fact, one of the most beautiful and important facts about these domains is that "unique prime factorization is restored at the ideal level". Thering of integers of any algebraic number field is a Dedekind domain, and so it is a very crucial object to study for number theorists. Furthermore, as Example 1 suggests, they also come up a lot in algebraic geometry. Finally, Dedekind domains are also very fascinating from a purely commutative algebra point of view, and several equivalent characterizations of them are available in literature. Without further ado, let's get started.

Definition 1. An integral domain D is a Dedekind domain if

1. *D* is a No ethereal ring.
2. *D* is integrally closed in its field of fractions.
3. All non-zero prime ideals of *D* are maximal. [1]

Example 1. Easier examples to follow. And this particular example won't be needed anywhere the ring of regular functions of a non-singular at fine curve over an algebraically closed field is a Dedekind domain.

Example 2. The following are some non-examples of Dedekind domains. Here, k denotes a field, and x, y, xi's are in determinates. The proofs of these Statements are elementary exercises in com- mutative algebra.

$K[x]/\langle x^2\rangle$ is not a Dedekind domain as it is not a domain.

$K[x, y]/\langle x^2 - y^3\rangle$ is not a Dedekind domain as it is not integrally closed.

K[x, y] is not a Dedekind domain as the non-zero prime ideal $\langle x\rangle$ of k[x, y] is not maximal.

The next proposition gives a plethora of Dedekind domains:
$K[x_1, x_2 ...]$ is not *a* Dedekind nd doma in as it is *not* Noetherian

Proposition: A principal ideal domain is a Dedekind domain.

Proof: Let *D* be a principal ideal domain (PID). Then it is trivially a Noetherian Ring. Since every principal ideal domain is a unique factorization domain (UFD), and UFDs are inte- grally closed domains, we get that *D* is integrally closed in its field of fractions.
Let $p = (p) = (0)$ be a prime ideal of *D*. Suppose $m = (q)$ is a maximal ideal of *D* prime, *p* is a prime element of *D*, and so it is irreducible, whence either *q* or *d* is a unit. But *q* cannot be a unit since it generates a maximal ideal. Thus, *d* is a unit, and hence, $q = p.d^{-1}$, implying (q) (p). Thus, we have $p = m$, and it follows that every non-zero prime ideal of *D* is maximal.

Fractional ideals:

The study of fractional ideals is one of the key building blocks of the general theory of Dedekind domains. Roughly speaking, fractional ideals are kind of "a fraction times an ideal", and this provides a way to discuss "inevitability" of ideals: just like to discuss inevitability of ordinary integers, one brings in fractions.
In this section, D denotes an integral domain which is not a field, and K its field of fractions.

Definition: A D-sub module M of K of the form $M = cI = \{x \in K \mid x = ca$ for some $a \in I\}$, where $c \in K^*$ and I is a non-zero ideal of D is called a fractional ideal of D, or a fractional D-ideal.

Proposition: Let D be a Noetherian integral domain, then the following conditions on a non-zero D-sub module M of K are equivalent:

M is a fractional ideal of D. M is a finitely generated D-sub module of K.

Proof: Suppose $M = cI$ is a fractional ideal of D, where $c \in K^*$ and I is a D $\sum$ ideal. Let $I = \langle a_1, a_2 ... a_n\rangle$, where each $a_i \in D$.

Then, every element of M can be expressed as

With $d_i \in D$, i.e., M is the D-submodule of K generated by $\{ca_1, ca_2 ... ca_n\}$.

2 = ⇒ 1: Suppose M is generated by

$\{k_1, k_2, ..., k_n\}$, where $k_i = a_i/b_i$, with $a_i, b_i \in D$ and $b_i = 0 \ \forall \ 1 \leq i \leq n$.

Let $M_1 = b_1 I_1$ and $M_2 = b_2 I_2$ (where $b_1, b_2 \in K^*$ and I_1, I_2 are ideals of

People familiar with basic ring theory can easily give an explicit description of this

product, much in lines of the definition of the product of two ideals of a ring.

The multiplication on the set of fractional ideals of D is associative commutative all our rings are commutative! has an identity element can you guess what Thus,the set of fractional ideals of D form a commutative monoid. We will see later that it in fact forms a group when D is a Dedekind domain.

The multiplication also preserves inclusions in the sense that if $M_1 \subseteq M_2$, then $M_1N \subseteq M_2N$, where M_1, M_2 and N are fractional ideals. In particular, we note that if $I \subseteq D$ is an ideal,then $IM \subseteq DM = M$ for all fractional ideals M.

If $a \in K^*$, we write $\langle a \rangle = aD = \{ay \mid y \in D\}$. Any fractional ideal of this form is said to be principal. We clearly have $\langle a \rangle \langle b \rangle = \langle ab \rangle$.

We call a fractional D-ideal M invertible if there exists a fractional D-ideal N such that no the $MN = D$. ^{2}. for any fractional D-ideal M, we write D.

$II^{-1} = \langle x, y \rangle$ Ç D. To see that I is not invertible, refer to Corollary 1 below.

Example: Let, D = k[x, y], where k is a field, and x, y indeterminate.

Consider the ideal $I = \langle x^2, x\, y \rangle \subseteq D$. Note that $1/x \in I^{-1} \setminus D$, so it

is weakly invertible. Let's determine I^{-1}: clearly, $\frac{1}{} D \subseteq I^{-1}$. Also,

$f \in I^{-1} \Longrightarrow f.x^2 = p$ and $f.\, xy = q$ for some $p, q \in D \Longrightarrow p.\, xy$

$= q.x^2 \Longrightarrow x \mid p$

as D is a UFD. Thus, $f = p/x^2 \in \frac{1}{} D$, and so $I^{-1} = \frac{1}{} D$. Finally,

$II^{-1} = \langle x, y \rangle$ Ç D. To see that I is not invertible, refer to Corollary 1 below.

Proposition: Let M be a fractional D-ideal. Then:

1. If $a \in K^*$, then $\langle a \rangle^{-1} = \langle a^{-1} \rangle$.
2. If $a \in M \cap K^*$, then $M^{-1} \subseteq \langle a^{-1} \rangle$.

If D is Noetherian, then M^{-1} is a finitely generated D module is a fractional

D-ideal from Proposition 2.

Proof. **1.** Let $a \in K^*$ be a unit of K. Then,

$$\langle a\rangle^{-1} = \{x \in K \mid x\langle a\rangle \subseteq D\}$$
$$= \{x \in K \mid x\,ay \in D\ \forall\ y \in D\}$$
$$= \{x \in K \mid x\,a \in D\} \qquad \text{[all our rings have units!]}$$
$$= \{a^{-1}y \mid y \in D\}$$
$$= \langle a^{-1}\rangle$$

2. Let $a \in M \cap K^*$, and suppose $x \in M^{-1}$ is any element. Then, we have $xM \subseteq D$ from the very definition of M^{-1}. But then, $x\,M \subseteq D \Rightarrow x\,a \in D \Rightarrow x \in a^{-1}D = \langle a^{-1}\rangle$. As $x \in M^{-1}$ was arbitrary, we conclude that $M^{-1} \subseteq \langle a^{-1}\rangle$.

Corollary: Let M be an invertible fractional D-ideal, and

Suppose $MN = D$. Then, $N = M^{-1}$.

This corollary shows that M is invertible if and only if $MM^{-1} = D$. This indeed justifies the name M^{-1} for the set $\{x \in K \mid xM \subseteq D\}$!

Proof of Corollary 1. Let x N. Then, $x\,MD = x\,M^{-1}$, whence NM^{-1}.

Now, sincemultiplication of fractional ideals preserves inclusions, we get:

$D = MN \subseteq MM^{-1} \subseteq D$ [The last containment follows from the definition of M^{-1}]

$$\Rightarrow MM^{-1} = D$$
$$\Rightarrow (NM)M^{-1} = ND = N$$
$$\Rightarrow M^{-1} = N$$

The main theorems:

Theorem: Every fractional ideal of a Dedekind domain is invertible.

Before discussing the proofs of these theorems, let us see an example where Theorem fails ifthe domain is not Dedekind gives a failure of Theorem 2 in arbitrary domains.

Theorem: Unique prime factorization of ideals every non-zero ideal I of a Dedekind domain D can be written as a product $I = p_1p_2...p_n$, where p_i are non-zero prime ideals of D; moreover, this representation is unique up to the order of factors.

Lemma: If all the non-zero prime ideals of an integral domain are maximal,

then an inclusion $p \supseteq p_1p_2...p_n$ where p and all the p_j are non-zero prime ideals, implies that $p = p_i$ for some i. maximal. Suppose the result is true when $n = r$ for some $r \in N$. consider the case $n = r+1$. If $p = p_1$, then we are done. If not, then since our domain has dimension 1, $p_{r+1} \not\subseteq p$. But then, $\exists\ c \in p_{r+1}$ S.t $c \notin$

p. Now, if b is any element of $p_1p_2...p_r$, then b c p, and hence b p. Thus, p

$p_1p_2...p_r$ = p = p_i for some i 1, 2...

Lemma: Let D be a Dedekind domain. Then, a D-ideal I is invertible ⇐ ⇒ I

$= m_1m_2...m_r$,

Where mj are invertible parme ideals of D.

Proof: If I = $m_1m_2...m_r$, where each m_j is an invertible prime idea l of D. Then, m is clearly the inverse of I. suppose that I is an invertible D-ideal. If I = D, we can take I to be the empty productof ideals, so the result is trivially t let I Ç D. Then, as $I^{-1} \geq$ D, and so I is weakly invertible. Thus, I m_1, where m_1 is some maximal weakly-invertible ideal. We thus conclude that Im_1^{-1} $m1m1^{-1}$ = D In turn we get that I I m_1^{-1} D, where the inequality holds since the one given in the proof. we have that Im_1^{-1} Ç $m_1m_1^{-1}$ = D. Now, note that

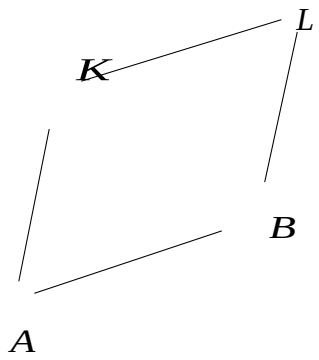
(I m $\overline{1}^{-1}$)(m_{11}^{-1}) = D, Im^{-1} is an If Im^{-1} = D, we have, I= m_1. Otherwise, by repeating the earlier argument multiple times, we obtain IÇ $Im\overline{1}^{1}$ Ç $Im\overline{1}^{1}m_2^{-1}$ Ç Where m_i ' s are maximal weakly invertible ideals. But D is chain stabilizes.

Primes in Dedekind extensions:

The AKLB setup:

Our next goal would be to show that the ring of integers of a finite extension of Q is a Dedekind domain. Not only are the results of this section of utmost importance in number theory, these also give us a way of getting new Dedekind domains from old ones.

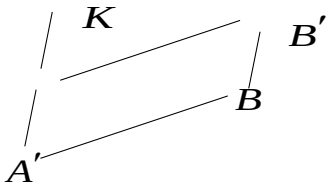
Notation (AKLB setup): Let *A* be a Dedekind domain, *K* its field of fractions, *L* a finite extension of *K*, and *B* the integral closure of *A* in *L*. Pictorially



Proposition: Assume AKLB, and let p be a prime of A. Let S = A\p, and set A′:= $S^{-1}A = A_p$, and B′:= $S^{-1}B$. If q | pB, then we have A′/p A′ ≃ A/p and B′/q B′ ≃ B/q as rings.

Before proving the above proposition, let us note that in the above setup, A′*KLB*′ also falls in the "AKLB" setup. Checking that A' and B' are Dedekind domains are very simple arguments centering properties of localizations and integral extensions. Also, note that $B' = S^{-1}B$ is the integral closure of

$A' = S^{-1}A$ in $S^{-1}L = L$ because integral closures respect a field; refer



Proof : Let, $A'/p\,A' = S^{-1}A/S^{-1}p \cong A/p$ [as p is maximal; use the last lemma]. Note that $q \cap S = \varphi$. Indeed,

$$X \in q \cap S$$

$$= \Rightarrow x \in q \text{ and } x \in A \setminus p$$

$$= \Rightarrow x \in q \cap A \text{ and } x \notin p$$

$$= \Rightarrow x \in p \text{ and } x \notin p, \quad \text{a contradiction}$$

another application of the last lemma yields $B'/q\,B' = S^{-1}B/S^{-1}q$

Properties of Dedekind domains:

The remainder of this article, *D* denotes a Dedekind domain (unless otherwise specified) which is not a field, and *K* its field of fractions.
From Theorem 2, we see that the set of fractional *D*-ideals, endowed with multiplication, forms an abelian group, which we denote by I_D.
Let $M = \langle b \rangle^{-1} I$ be a fractional D-ideal, then we may express both $\langle b \rangle$ and I as a product of prime

(i) If M and N are fractional D-ideals, then we immediately deduce from the definition that
$V_p(M\,N) = v_p(M) + v_p(N)$

(ii) As $v_p(D) = 0$, and as every fractional ideal M of D is invertible, we conclude $v_p(MM^{-1}) =$
$V_p(D) = 0$, whence $v_p(M^{-1}) = -v_p(M)$

(iii) M is a D-ideal if and only if $v_p(M) \geq 0\ \forall\ p$ (why?).

(iv) We say that a fractional ideal M divides a fractional ideal N, written M N, if N = MI for some D-ideal I.

(v) **(**division $\Leftarrow \Rightarrow$ containment**)** If M and N are fractional ideals of a Dedekind domain D, then $M \mid N \Leftarrow \Rightarrow v_p(M) \leq v_p(N)\ \forall\ p \Leftarrow \Rightarrow M \supseteq N$. Indeed, the first equivalence follows from (iii). To prove that division implies containment, observe that if M | N, then $N = MI \subseteq MD = M$. And to show that containment implies division, note that if $N \subseteq M$, then $NM^{-1} \subseteq MM^{-1} = D$. Thus, M | M (NM^{-1}) (as $NM^{-1} \subseteq D$ means it s a D-ideal), or, M | N.

(vi) **(lcm of two I deals)** We have $v_p(M \cap N) = \sup(v_p(M$

$V_{p\,(N\,Q)}) \forall$ p. fractional

That $p^{u}p \subseteq M \cap N$ division $\Leftarrow \Rightarrow$ containment. ,

$M \cap N \subseteq M$ and $M \cap N \subseteq N$

$= \Rightarrow M \mid (N \cap M)$ and $N \mid (N \cap M)$

$= \Rightarrow v_p(M \cap N) \geq v_p(M)$ and $v_p(M \cap N) \geq v_p(N) \forall p$

$= \Rightarrow v_p(M \cap N) \geq \sup(v_p(M), v_p(N)) \forall p$

$= \Rightarrow p^{u}p \mid (M \cap N)$

$= \Rightarrow p^{u}p \supseteq M \cap N$

Thus, we get $Q\ p^{u}p = M \cap N$.

(g .c .d of two fractional ideals)

We have $v_p(M + NQ) \quad \inf(v_p(M), PQ(N)) \forall p$.

$M + N \subseteq Q\ p^{w}p$ division $\Leftarrow \Rightarrow$ containment on the other hand,

$M \subseteq M + N$ and $N \subseteq M + N$

$= \Rightarrow (M + N) \mid M$ and $(M + N) \mid N$

$= \Rightarrow v_p(M + N) \leq v_p(M)$ and $v_p(M + N) \leq v_p(N) \forall p$

$= \Rightarrow v_p(M + N) \leq \inf(v_p(M), v_p(N)) \forall p$

$= \Rightarrow (M + N) \mid p^{w}p$

$= \Rightarrow p^{w}p \subseteq M + N$

$P\ p^{u}p = M + N\ p$

(vii) **(g c d. l c m = product)** If M and N are two fractional D-ideals, then (M N) (M +N) = MN. Indeed, we have $V_p(MN)$

$= v_p(M) + v_p(N)$ [from (i)]

$= \sup(v_p(M), v_p(N)) + \inf(v_p(M), v_p(N))$ (why?)

$= v_p(M \cap N) + v_p(M + N)$.

The rest follows from the aforementioned properties of p-adic valuations.

Lemma:

1. $I + J = D$
2. $I \cap J = IJ$
3. $V_p(I) \cdot v_p(J) = 0 \ \forall \ p$

Proof. 1 $\Leftarrow\Rightarrow$ 2:

$I + J = D$

$\Leftarrow\Rightarrow V_p(I + J) = 0 \ \forall \ p$

$\Leftarrow\Rightarrow \inf(v_p(I), v_p(J)) = 0 \ \forall \ p$

$\Leftarrow\Rightarrow \text{Sup}\ (v_p(I), v\,p\,(J)) = v\,p\,(I) + V_p(J) \ \forall \ p$

$\Leftarrow\Rightarrow I \cap J = IJ$ [from (vi)]

$I \cap J = IJ$

$\Leftarrow\Rightarrow \inf(v_p(I), v_p(J)) = 0 \ \forall \ p$ [as seen above]

$\Leftarrow \ \Rightarrow v_p(I).v_p(J) = 0 \ \forall \ p$

Example: Assume AKLBG. If [L: K] is prime, exactly one of the three possibilities can hold for any prime p of A: totally ramify in B, completely split in B, or remain inert in B.

Theorem: (**Cyclotomic reciprocity law**) let p be an odd prime. Suppose p n and let f be the smallest positive integer such that $p^f \equiv 1 (\text{mod } n)$. Then, p decomposes into $g = \varphi^{(n)}$ distinct primes in Z [ζ_n], each of which has residue degree f.

Proof. Let p be a prime in Z [ζ_n] which lies over p. We claim that Z[ζ_n]/p is a splitting field of x^n 1 over F_p technically speaking, our base field is the image of F_p under the map ϕ as defined the polynomial is $x^n - (1 + p))$. Indeed, from Lemma we know that $\zeta^i + p$ /= $\zeta^{j/} + p$ if
1 = j, and each of them are a root of x^n 1 in Z [ζ_n]/p. Thus, x^n 1 splits completely in Z [ζ_n]/p, and the claim follows since the field is generated by $\zeta_n + p$ over $\phi(F_p)$.

Thus, Lemma shows that [Z [ζ_n]/p: Z/p Z] = f. On the other hand, by definition, [Z [ζ_n]/p: Z/p Z]is the residue degree f_p. Thus, f_p = f.As, p ‡ n, we have e_p = 1 from we have $e_p f_p g_p$ = [Q (ζ_n): Q] = φ (n), where the last inequality $g_p = g = \frac{\varphi(n)}{}$, and we are do

References:

[1] Atiyah, M. F.; Macdonald, I. G. Introduction to commutative algebra. Student economy edition. For the 1969 original see [MR0242802]. Addison-Wesley Series in Mathematics. Westview Press, Boulder, CO, 2016. Ix+128 pp. ISBN: 978-0-8133-5018-9; 0-201-00361-9;

0-201-40751-5.

[2] Taylor, M. J. Algebraic Cambridge mastics, 27. Cambridge University Press, Cambridge, 1993. Xiv+355 pp. ISBN: 0-521-43834-9

[3] Clark, Pete L. Elliptic Dedekind domains revisited. Enseign. Math. (2) 55 (2009), no. 3-4, 213–225.

[4] May, J.P. Article on Notes on *Dedekind domains*.

[5] Koyama, Toshiko; Nishi, Mieo; Yanagihara, Hiroshi. On characterizations of Dedekind domains. Hiroshima Math. J. 4 (1974), 71–74.

[6] Samuel, Pierre. Algebraic theory of numbers. Translated from the French by Allan J. SulzbergerHoughton Mifflin Co., Boston, Mass. 1970 109 pp.

[7] Neukirch, Jürgen. Algebraic number theory. Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder. Grundlehren der Mathematis-chen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322. Springer-Verlag, Berlin, 1999. Xviii+571 pp. ISBN: 3-540-65399-6

[8] Ash, Robert B. A course in algebraic number theory. Dover Publications, Inc., Mineola, N Y, 2010. Viii+112 pp. ISBN: 978-0-486-47754-1; 0-486-47754-1

[9] Sutherland, Andrew. Lecture Notes on *Number Theory I*

[10] Milne, J.S. Lecture notes on Algebraic *Number Theory.*

[11] Washington, Lawrence C. Introduction to cyclotomic fields. Second edition. Graduate Texts in Mathematical 83. Springer-Verlag, New York, 1997. Xiv+487 pp. ISBN: 0-387-94762-0.