International Journal of
Statistics and Applied Mathematics

ISSN: 2456-1452
Maths 2018; 3(1): 218-220
© 2018 Stats & Maths
www.mathsjournal.com
Received: 12-11-2017
Accepted: 17-12-2017

Pawan kumar Gulia
Research Scholar,
Niilm University,
Kaithal, Haryana, India

Dr. Manjeet jakhar
Assistant Professor,
Niilm University Kaithal,
Haryana, India

Correspondence
Pawan kumar Gulia
Research Scholar,
Niilm University,
Kaithal, Haryana, India

Dedekind Domains

Pawan kumar Gulia and Dr. Manjeet jakhar

Abstract

We motivate our results on Dedekind domains by recalling our study of primes of the form x^2+ny^2. We saw that p=x^2+ny^2 if and only if p can be factored in $Z[\sqrt{-n}]$. However, this is most useful when $Z[\sqrt{-n}]$ has unique prime factorization, as in the case of $Z[i]$, where we were able to analyze precisely when p factors. It turns out that unique factorization doesn't hold very often in cither the imaginary quadratic or cyclotomic case. However, if instead of considering factorization of elements, we consider factorization of ideals, we will find that we do have unique factorization into prime ideal in rings of integers. We will discuss the definition, properties and relationship of Dedekind domain with other structures.

Keywords: Dedekind Domains

Introduction

Dedekind Domains

Definition

An integral domain A is a Dedekind domain if it satisfies:
1. A is Noetherian
2. Every non-zero prime ideal of A is maximal;
3. S is integrally closed in its field of fractions.

Proposition

Suppose that A is an integral domain, integrally closed in its field of fractions, and that for any nonzero ideal I. we have that A/1 is finite. Then A is a Dedekind domain.

PROOF. Since.4 is integrally closed by hypothesis, we need only check that it is Noetherian and that every non-zero prime ideal is maximal. But if I is a non-zero ideal, since A/1 is finite, and the ideals of A containing I are in bijection with the ideals of A/I. there can only be finitely many such ideals, and any ascending chain containing I stabilizes. Thus, A is Noetherian.

Similarly, if p is a non-zero prime ideal of A, then A/p is a finite integral domain, and it is a general fact that any finite integral domain is a field, so that p is maximal. Indeed, let..4 be a finite integral domain, and $\alpha \in A$a non-zero element. Then we must have $a^{k_1} = a^{k_2}$for some $k_1 > k_2$,by finiteness. Because A is an integral domain, we find $\underset{a}{k_{1-k_2} = 1,}$so a is invertible, and.4 is a field.

Corollary

A ring of integers O_K is a Dedekind domain.

Algebraic Geometry Remark

Prom an algebraic geometry perspective, we see that the definition of a Dedekind domains means that it has dimension one and is normal; i.e., we can think of it as a nonsingular curve. Subrings of rings of integers such as $Z[\sqrt{-3}]$are still curves, but have singularities, and their con tainment in the ring of integers corresponds to the normalization map. As in the geometric situation, in order to study the singular curve it is frequently helpful to start by studying the normalization, so we focus primarily on the rings of integers themselves.

Properties of Dedekind Domains

1. Every non-zero ideal of a Dedekind domain may be uniquely factored as a product of prime ideals, up to reordering.

Definition

Let R be an integral domain with fraction field K. We say that $1 \subseteq K$ is a fractional ideal of R if it is closed under addition and under scalar multiplication by elements of R, and if there exists a non-zero $d \in R$ such that $dI \subseteq R$. A fractional ideal is principal if it is of the form αR, for some $\alpha \in K$ Given fractional ideals I, J of R, the product IJ is defined to be

$$\{a \in L: \alpha = \sum_{e} i_e j_e \, i_e \in I, j_e \in J\}$$

The product of two fractional ideals is easily seen to be a fractional ideal.

2. The set of fractional ideals of a Dedekind domain R form a group under multiplication, with R as the identity.

However, we observe that the second result may be equivalently stated as saying that for any ideal I of R, there exists another ideal J such that IJ is principal. Equivalently, ideals modulo principal ideals form a group, called the "ideal class group". This is therefore the first step in understanding the relationship between all ideals and principal ideals. However, having gone to the trouble to define fractional ideals, we make the definition as follows:

Definition

Given a Dedekind domain R, the ideal class group of R is defined to be the group of fractional ideals modulo the group of principal fractional ideals.

Thus, the ideal class group measures how far a Dedekind domain is from being a principal ideal domain. We claim in our context., this is equivalent to measuring how far away every irreducible element, is from being prime.

Modules over Dedekind Domains (Sketch)

The structure theorem for finitely generated modules over principal ideal domains has an interesting extension to modules over Dedekind domains. Throughout this subsection, A is a Dedekind domain.

First, note that a finitely generated torsion-free.4-module M need not be free. For example, every fractional ideal is finitely generated and torsion-free but it is free if and only if it is principal. Thus the best we can hope for is the following.

* Let A be a Dedekind domain.

1. Every finitely generated torsion-free A-module M is isomorphic to a direct sum of fractional ideals,

$$M \approxeq a_1 \oplus \ldots . \oplus a_m.$$

2. Two finitely generated torsion-free A-modules $M \approxeq a_1 \oplus \ldots . \oplus a_m$. amd
$N \approxeq b_1 \oplus \ldots . \oplus$are isomorphic if and only if
$m = n \wedge \prod a_i \equiv \prod b_i$modulo principal ideals.
Hence, $M \approxeq a_1 \oplus \ldots . \oplus a_m \approxeq A \oplus \ldots \oplus A \oplus a_i \ldots a_m$

Moreover, two fractional ideals a and b of A are isomorphic as A-modules if and only if they define the same element of the class group of A.

The rank of a module M over an integral domain R is the dimension of
$K \otimes_R M$ as a K-vector space, where K is the field of fractions of R. Clearly the rank of $M \approxeq a_1 \oplus \ldots . \oplus a_m$.is m.

These remarks show that the set of isomorphism classes of finitely generated torsion- free A-modules of rank 1 can be identified with the class group of A. Multiplication of elements in Cl(A) corresponds to the formation of tensor product of modules. The Grothendieck group of the category of finitely generated A-modules is CI ($A \oplus Z$.

THEOREM (INVARIANT FACTOR THEOREM) Let $M \supset N$ be finitely generated torsion-free A-modules of the same riuik m. Then there exist elements $e_1 \ldots , e_m$ of M, fractional ideal s$a_1 \ldots , a_m$, and integral ideals
$b_1 \supset b_2 \supset \cdots \supset b_m$such that

$$M = a_1 e_1 \oplus \ldots . \oplus a_m e_m, N = a_1 b_1 e_1 \oplus \ldots . \oplus a_m b_m e_m$$

$$M = a_1 e_1 \oplus \ldots . \oplus a_m e_m, N = a_1 b_1 e_1 \oplus \ldots . \oplus a_m b_m e_m$$

The ideals b_1,b_2,...b_m are uniquely determined by the pair $M \supset N$, and are called the invariant factors of N in M.

The last theorem also yields a description of finitely generated torsion A-modules. For proofs of the above results.

NOTES Let A be a Dedekind domain, and let M be finitely generated torsion-free ^-module. Then A_p⊕M is free, hence projective, forever) nonzero prime ideal p in A (because A_p is principal ideal domain), and this implies that M is projective. Therefore there is a nonzero homomorphism M→A, whose image is an ideal a in A. As a is projective, there exists a section to the map M→a and $M \approxeq a_1 \oplus M_1$so for some submodule Mj of M. Now Mx is projective because it is a direct summand of a projective module, and so we can repeat the argument with M1. This process ends because M is noetherian.

NOTES The Jordan-Holder and Krull-Schmidt theorems both fail for finitely generated projective modules over nonprincipal Dedekind domains. For example, let a be an ideal in A having order 2 in the class group. According to (3.31),$a \oplus a \approxeq A \oplus$A, which contradicts both theorems as $a \not\approxeq A$.

Finding Factorizations

The following result often makes it very easy to factor an ideal in an extension field. Again A is a Dedekind domain with field of fractions K, and B is the integral closure of A in a finite separable extension L of K.

THEOREM 4.6 Suppose that$B = A[\alpha]$, and let f(X) be the minimum polynomial of α over K. Let p be a prime ideal in A. Choose monic polynomials $g_1(X) \ldots . g_r(X) \in A[X]$ that are distinct imd irreducible modulo p, and such that $\overset{X}{f(X)} = \prod g_i^{ei}$ modulo p.

Then $\overset{p.g_i(\alpha)\quad ei}{pB = \prod}$ is the factorization of pB into a product of powers of distinct prime ideals. Moreover, the residue field $\frac{B}{p.g_i(\alpha)} \simeq \left(\frac{A}{p}\right)[X]/(\acute{g}_\iota)$, imd so the residue class degree fi is equal to the degree of g_i.

PROOF. Our assumption is that the map X→ α defines an isomorphism
$A\,[X]/\big(f(X)\big) \to B$

When we divide out by p (better, tensor with A/p), this becomes an isomorphism $k\,[X]/\Big(\acute{f}(X)\Big) \to B/pB\,.X \mapsto \alpha$ where k=A/p.

The ring $\overset{\acute{f}}{k\,[X]/}$) has maximal ideals ($\acute{g}_1 \dots.(\acute{g}_r$),and $\acute{g}_\iota\ \overset{ei\ =\ 0}{\prod}$ (but no product with smaller exponents is zero). The ideal $\acute{g}_\iota$)

in $\overset{\acute{f}}{k\,[X]/}$)corresponds to the ideal $\big(g_i(\alpha)\big) + pB \in B/pB$, and this corresponds to the ideal $B_i \overset{\text{def}}{=}$ (p.gi(αin B. Thus B_1.......B_r is the complete set of prime ideals containing pB, and hence is the complete set of prime divisors of p. When we write pB=$\prod B_i^{ei}$, then the are characterized by the fact that pB contains $\prod B_i^{ei}$but it does not contain the product when any e_i is replaced with a smaller value. Thus it follows from the above (parenthetical) statement that e_i is the exponent $\acute{g}_\iota$of occurring in the factorization of $\acute{f}$.

Remark

When it applies the last theorem can be used to prove. For example, m=deg(f), and so the equation $m = \sum e_i f_i$ is simply the equation deg(f)=$\sum e_i.deg(g_i)$. Also,disc(B/A)=disc(f(X)), and this is divisible by p if and only if $\acute{f}(X)$has multiple factors (when regarded as an element of (A/p)[X])i.e., if and only if some ei>0

Conclusion:- In this study, we have discussed sabout Dedekind domains: every nonzero ideal can be factored uniquely as a product of prime ideals and also with the use of invariant factor theorem we have described a close relationship between modules and Dedekind domains. We prove these statements by examining the local structure of Dedekind domains. The group structure allows us to introduce the "ideal class group", which measures how far a Dedekind domain is from being a UFD, and plays a fundamental role throughout algebraic number theory.

Reference

1. Avigad, Jeremy. Methodology and metaphysics in the development of Dedekind's theory of ideals. In: The Architecture of Modern Mathematics. Ed. by Jose Ferreiros and Jeremy Gray. Oxford University Press. 2006; 159(186):8-30.
2. Greaves G. Sieves in Number Theory. Results in Mathematics and Related Areas Springer-Verlag, Berlin, 2001; (3):43.
3. Gabor Ivanyos, Marek Karpinski, Lajos Ronyai, and Nitin Saxena. Trading GRH for algebra: algorithms for factoring polynomials and related structures. CoRR, abs/0811.3165, 2008, 30
4. Cohen H. A course in computational algebraic number theory, Springer-Verlag, Berlin, 1993. MR 94i:11105
5. Berend D, Bilu Y. Polynomials with roots modulo every integer, Proc. Amer. Math. Soc. 1996; 124:1663-1671.
6. Cohen H. A course in computational algebraic number theory, SpringerVerlag, 1996.
7. De Smit B, Lenstra HW. Jr., Linearly equivalent actions of solvable groups, J. Algebra. 2000; 228:270-285.
8. Susan Landau. How to tangle with a nested radical, Math. Intelligencer, 1994; 16:49-55.
9. Lenstra HW. Jr., Algorithms in algebraic number theory, Bulletin of the AMS. 1992; 26:211-244.
10. Bourbaki, Nicolas. Commutative Algebra, Addison-Wesley, 1972.
11. Claborn, Luther, "Dedekind domains and rings of quotients", Pacific J. Math, 1965; 15:59-64, doi:10.2140/pjm.1965.15.59
12. Claborn, Luther, "Every abelian group is a class group", Pacific J Math. 1966; 18(2):219-222, doi:10.2140/pjm.1966.18.219