International Journal of Engineering, Science and Mathematics
Vol. 6 Issue 5, September 2017,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

A STUDY ON ROLE OF DEDEKIND DOMAINS IN ALGEBRAIC NUMBER THEORY

Seema
Research Scholar, Calorx Teachers' University
Ahmedabad (Gujarat) - India

ABSTRACT

Current study explains the role of Dedekind Domains in Algebraic Number Theory. Study was based on the literature and descriptive in nature. This paper introduces the important concept of Dedekind domains, which is important to understand the concept of rings of integers. Rings of integers arc an important class of Dedekind domains, but other examples include rings of polynomial functions on smooth algebraic curves. In this study, we prove two fundamental facts about Dedekind domains: every nonzero ideal can be factored uniquely as a product of prime ideals; and the set of 'fractional ideals' form a group under multiplication. 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.

KEYWORDS: Algebraic number, number theory, Dedekind domains, and Rings of integers.

INTRODUCTION TO DEDEKIND DOMAINS

This section introduces the important concept of Dedekind domains, before turning to a more focused study of rings of integers. Rings of integers arc an important class of Dedekind domains, but other examples include rings of polynomial functions on smooth algebraic curves. In this study, we prove two fundamental facts about Dedekind domains: every nonzero ideal can be factored uniquely as a product of prime ideals; and the set of 'fractional ideals' form a group under multiplication. 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.

THE FAILURE OF UNIQUE FACTORIZATION

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 $\mathbb{Z}[\sqrt{-n}]$. However, this is most useful when $\mathbb{Z}[\sqrt{-n}]$ has unique prime factorization, as in the case of $\mathbb{Z}[i]$, where we were able to analyse precisely when p factors. Similarly, we recall that Lame gave a proof of Fcrmat's Last Theorem which mistakenly relied on unique factorization in $\mathbb{Z}[\zeta_p]$
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. Indeed, this was what led Dedekind to introduce the notion and terminology of ideals, in an admittedly primitive form. In order to study irreducibility of elements, it then makes sense to study

the factorizations into prime ideals, and then to analyse when the prime ideals that appear arc principal, leading to factorizations into elements.
A prototypical restatement is the following elementary fact:

1. A prime p is of the form $x^2 + ny^2$ if and only if
2. $p\mathbb{Z}[\sqrt{-n}]$ Factors as pip2 for two (not necessarily distinct) prime ideals of $\mathbb{Z}[\sqrt{-n}];$
3. Both pi, p2 are principal ideals.

PROOF. We already saw that $p = x^2 + ny^2$ if and only if p is reducible in $\mathbb{Z}[\sqrt{-n}],$ and that in this case, both factors would have norm p. Thus, they generate prime ideals, so the Proposition is simply a rephrasing of the result, of the exercise.

We note that this situation doesn't quite fall into the situation of rings of integers or more generally Dedekind domains. However, it will turn out to remain well-behaved for p not dividing 2n.

Factorization into prime ideals turns out to be relatively straightforward; indeed, how to analyse when (i) occurs. However, (ii) is far subtler, and will require the full machinery of class field theory to study effectively. That said, by shifting our attention from elements to ideals, we will ultimately be able to obtain a good answer to our original question. Similarly, by studying the structure of ideals in $\mathbb{Z}[\zeta_p],$ Kummer was able to give his partial results on Format's Last Theorem, and his arguments can be extended to yield an algorithm which allows one to check in finite time, for any fixed prime p, whether or not $x^p + y^p = z^p$ has solutions.

DEDEKIND DOMAINS

Definition "An integral domain A is a Dedekind domain if it satisfies":

1. A is Nocthcrian;
2. Every non-zero prime ideal of A is maximal;
3. S is integrally closed in its field of fractions.

Recall that for A to be Noctherian means that every ascending chain of ideals stabilizes. We will use the following to see that every ring of integers is a Dedekind domain.

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 Nocthcrian 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 bisection with the ideals of A/I. there can only be finitely many such ideals, and any ascending chain containing I stabilizes. Thus, A is Nocthcrian.

Similarly, if $\mathfrak{p}$ 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 $\mathfrak{p}$ is maximal. Indeed, let. .4 be a finite integral domain, and $a \in A$ 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 $a^{k_1-k_2} = 1,$ so a is invertible, and .4 is a field.

A ring of integers $\mathcal{O}_K$ 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 non-singular curve. Subrings of rings of integers such as $\mathbb{Z}[\sqrt{-3}]$ arc still curves, but have singularities, and their co-attainment 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

From a number-theoretic point of view, the two most basic properties of Dedekind domains involve the behaviour of their ideals under multiplication. We state the main results, and use them to define the ideal class group. The first is:

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

The second requires a definition:

DEFINITION Let R be an integral domain with fraction field K. We say that $I \subseteq K$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

$$\{\alpha \in L : \alpha = \sum_{\ell} i_\ell j_\ell, i_\ell \in I, j_\ell \in J\}$$

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

THEOREM 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 theorem 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. Specifically:

Let R be an integral domain.

1. If R is Noetherian, then R is a unique factorization domain if and only if every irreducible element is prime.

2. R is a principal ideal domain if and only if R is a Dedekind domain and a unique factorization domain.
Note that although this is intended as motivation for Theorems 4.1 and 4.2, the only part which requires either one is the $\Leftarrow$ direction of (ii); we will use the other statements in the proofs of the theorems.
PROOF. For (i), we have already observed that a UFD has every irreducible element prime, by definition. Conversely, given an element $x \in R,$ we claim we can write x as a product of irreducible: if not, it is clear that we can write $x = x_1 y$, with neither of x_1, y a unit, and where x_1 cannot be written as a product of irreducible.

Repeating this inductively, we obtain a sequence x_i with $x_0 = x,$ and $x_{i+1}|x_i$ for each $i,$ with $\frac{x_{i+1}}{x_i}$ not a unit in R. But then the ideals generated by the x_i form an infinite ascending chain, contradicting the hypothesis that R is Nocthcrian. Thus, x may be factored into irreducible, and it is easy to check inductively that this factorization is unique, using that every irreducible is prime.

For (ii), it follows from Exercise that every PID is Nocthcrian. Next, recall that in a PID. Every irreducible element is prime: if x is irreducible, and m is any prime ideal containing x, because m is principal it must be equal to (x). This shows by (i) that any PID is a UFD. But the same argument, if x is a generator for any non-zero prime ideal, shows that (x) is maximal. We already showed that any UFD is integrally closed, so every PID is also a Dedekind domain, as desired.
For the converse, note that by Theorem 4.1, it suffices to show that every prime ideal is principal. But given a nonzero prime ideal $\mathfrak{p}$, we must have that p contains an irreducible clement (rr), by starting with any non-zero element, factoring it into irreducible, and applying the definition of prime ideal inductively. But then this element, is prime, and since every non-zero prime ideal is maximal, and $(x) \subseteq \mathfrak{p},$ we conclude that $(x) = \mathfrak{p}$, as desired.
Finally, we mention that. Exercises give counter examples to the two theorems for rings which are not Dedekind domains, but which arc relatively close.

DEDEKIND DOMAINS AND DVRS

There are several proofs of Theorems 4.1 and 4.2. The most classical approach only works for rings of integers, and first proves that the ideal class group is finite, and concludes these theorems. A slightly less direct, but more general proof is. We will take a more technology-heavy approach of proving these theorems via study of local rings. This is a bit longer, but has the advantage of introducing local rings and the concept, of constructing global data from local data.

We now explore the properties of local rings of Dedekind domains. Recall the following definitions:

Definition. Let R be an integral domain with field of fractions A", and S a multiplicatively closed subset not containing 0. We define $S^{-1}R \subseteq K$ to be the subring of the form $\{\frac{r}{s} : r \in R, s \in S\}$. If p is a prime ideal of R., we define $R_{\mathfrak{p}}$, the local ring of 'R' at p, to be $S^{-1}R$ with $S = R \setminus \mathfrak{p}$

DEFINITION. An integral domain is said to be a discrete valuation ring or DVR if it is a principal ideal domain with a unique maximal ideal.

We have already seen in Proposition 4.3 that every PID is Dedekind. So in particular every DVR is Dedekind. It. follows that, the only prime ideals of a DVR are (0) and the maximal ideal.

We next prove two converses to the statement that a DVR is Dedekind. The first is the following.

Any Dedekind domain R' with a unique maximal ideal is a discrete valuation ring. Every non zero ideal of a discrete valuation ring is a power of the maximal ideal.

PROOF. From the definitions, it suffices to check that R' is a PID. We first claim that the maximal ideal m is principal:

Choose $a \in \mathfrak{m}$ non-zero; by Exercise 2.5, $\exists n \in \mathbb{N}$ such that $\mathfrak{m}^n \subseteq (a)$, but $\mathfrak{m}^{n-1} \not\subseteq (a)$. Choose $b \in \mathfrak{m}^{n-1} \setminus (a)$, and consider $x = \frac{a}{b} \in K,$ the field of fractions ofR'. From the construction, we see that $x^{-1} \not\subseteq R',$ but $x^{-1}\mathfrak{m} \subseteq R'$. Now, since R' is integrally closed, we find that x^{-1} is not integral over R', so since m is finitely generated, $x^{-1}\mathfrak{m} \not\subseteq$ m. But $x^{-1}\mathfrak{m} \subseteq R'$ means it is an ideal of R', so if it is not contained in m, it must be equal to R', and we conclude that m = (x).

We next, show that m = (x) implies that every ideal is principal. We first claim that every irreducible element is prime, and more precisely, of the form xu for some unit u. But given $y \in R'$ irreducible, because y is not a unit, $y \subseteq \mathfrak{m}$, so $x|y$, and by the definition of irreducibility, y = xu for some unit u, as desired. By Proposition 4.3 (i), it follows that R' is a UFD and we see that every element of R' may be written as $x^n u$ for some $n \in \mathbb{N} \cup \{0\}$, u a unit. If I is a non-zero ideal of R', let $n \in \mathbb{N} \cup \{0\}$ be $\min_{a \in I}\{n' : a = x^{n'}u\}$; it is then clear that $I = (x)^n$. Thus R' is a DVR as desired.

We have further shown that in R', every non-zero ideal is a power of the maximal ideal, and since we already saw that every DVR is Dedekind, we conclude that this holds in every DVR. We can now prove the following stronger statement, characterizing Dedekind domains in terms of their local rings.

Let R be a Noetherian integral domain which is not afield. Then R is a Dedekind domain if and only if for all non-zero prime ideals $\mathfrak{p}$, the local ring $R_\mathfrak{p}$ is a discrete valuation ring.

We first, give a lemma in more generality than is needed here, for later use. The general form requires the following definition:

Definition. Given a fractional ideal $I \subseteq K$, and p a non-zero prime ideal of R. denote by $I_\mathfrak{p} \subseteq K$ the fractional ideal of $R_\mathfrak{p}$described by $I_\mathfrak{p} = R_\mathfrak{p} I$ (observe that any denominator for I is a denominator for $I_\mathfrak{p}$).

We find that in general, a fractional ideal is determined by its local images.

For an integral domain R, if I is a fractional ideal of R, then $I = \cap_\mathfrak{p} I_\mathfrak{p}$, where the intersection is taken over all prime ideals of R.

PROOF. Take $x = a/b \in \cap_\mathfrak{p} I_\mathfrak{p}$, Let $J = \{y \in R : ya \in bI\}$. This is certainly an ideal of R, and we claim it cannot be contained in any prime ideal $\mathfrak{p}$ of R: indeed, since $x \in I_\mathfrak{p}$, we can write $a/b = c/d$ for some$d \notin \mathfrak{p}$, and $c \in I$, so by definition, we have $d \in J \setminus \mathfrak{p}$. Since J is not contained in any prime ideal, it must be all of R, and in particular, $1 \cdot a \in bI$, so $x = a/b \in I$ We now have all the pieces to prove the proposition.

PROOF OF PROPOSITION. Suppose that R is Dedekind and take p a non-zero prime ideal of R. Then by Exercise, we have that $R_\mathfrak{p}$ is Nocthcrian, and moreover the only non-zero prime ideal of $R_\mathfrak{p}$ is necessarily $\mathfrak{p}$, and in particular is maximal. Finally, $R_\mathfrak{p}$must be integrally closed: denote by K the field of fractions of R, and suppose $x \in K$is integral over $R_\mathfrak{p}$. Now x satisfies some mimic poly nominal $x^n + a_{n-1}x^{n-1} + \ldots a_0 = 0$ with each $a_i \in R_\mathfrak{p}$, and we can therefore clear denominators to get an equation $sx^n + a'_{n-1}x^{n-1} + \ldots a'_0 = 0$ where $s \in R \setminus \mathfrak{p}$, and $a'_i \in R$. Multiplying through by s^{n-1} gives that sx is integral over R and hence in R, so x is in $R_\mathfrak{p}$ as desired.

Conversely, let $\mathfrak{p}$ be any non-zero prime ideal of R, and m a maximal ideal containing $\mathfrak{p}$; by hypothesis, $R_\mathfrak{m}$ is a DVR, so $\mathfrak{p} = \mathfrak{m}$ in $R_\mathfrak{m}$ and hence in R by Exercise 2.1. Next, an element $x \in K$ integral over R is integral over every $R_\mathfrak{p}$, so must actually be an element of $R_\mathfrak{p}$ by hypothesis. The previous lemma, in the ease I = R, then completes the proof.

INTEGRAL CLOSURES OF DEDEKIND DOMAINS

We now prove a result that implies that rings of integers in number fields are Dedekind domains, and hence that their ideals factor uniquely into products of prime ideals.

Theorem 3 Let A be a Dedekind domain with field of fractions K. and let B be the integral closure of A in a finite separable extension L of K. Then B is a Dedekind domain.

PROOF. We have to check the three conditions in the definition of a Dedekind domain**.** We first show that B is Noetherian. In (2.29) we showed that B is contained in a finitely generated A-module. It follows that every ideal in B is finitely generated when regarded as an A-module (being a sub module of a Noetherian A-module) and **a fortiori** as an ideal (= A-module). Next, B is integrally closed. It remains to prove that every nonzero prime ideal $\mathfrak{q}$ of B is maximal. Let $\beta \in \mathfrak{q}$, $\beta \neq 0$. Then β is integral over A, and so there is an equation.

$$\beta^n + a_1\beta^{n-1} + \cdots + a_n = 0, \quad a_i \in A$$

Which we may supposed to have the minimum possible degree. Then$a_n \neq 0$. As $a_n \in \beta B \cap A$, we have that$\mathfrak{q} \cap A \neq (0)$. But $\mathfrak{q} \cap A$ is a prime ideal (obviously), and so it is maximal ideal p of A, and $A/\mathfrak{p}$ is a field. We know $B/\mathfrak{q}$ is an integral domain, and the map $a + \mathfrak{p} \mapsto a + \mathfrak{q}$ Identifies $A/\mathfrak{p}$ with a subfield of$B/\mathfrak{q}$. As B is integral over A, $B/\mathfrak{q}$ is algebraic over $A/\mathfrak{p}$ the next lemma shows that $B/\mathfrak{q}$ is a field, and hence that $\mathfrak{q}$ is maximal. Every integral domain B containing a field k and algebraic over k is itself a field.

Let β be a nonzero element of B — we have to prove that it has an inverse in B. Because β is algebraic over k. the ring $k[\beta]$ is finite-dimensional as an A-vector space, and the map $x \mapsto \beta x : k[\beta] \to k[\beta]$ is injective (because B is an integral domain). From linear algebra we deduce that the map is subjective, and so there is an element $\beta' \in k[\beta]$ such that $\beta\beta' = 1$

In fact, Theorem is true without the assumption that L be separable over K —for a proof of the more general result. The added difficulty is that, without the reparability condition. B may fail to be finitely generated as an A module, and so the proof that it is Noetherian is more difficult.

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.

Theorem 4: Let A be a Dedekind domain.

1. Every finitely generated torsion-free A-module M is isomorphic to a direct sum of fractional ideals, $M \approx \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m.$

2. Two finitely generated torsion-free A-modules $M \approx \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m$ and $N \approx \mathfrak{b}_1 \oplus \cdots \oplus$ are isomorphic if and only if $m = n \text{ and } \prod \mathfrak{a}_i = \prod \mathfrak{b}_i$ modulo principal ideals.

Hence, $M \approx \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m \approx A \oplus \cdots \oplus A \oplus \mathfrak{a}_1 \cdots \mathfrak{a}_m.$ 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 $M \approx \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m$ 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 $\mathrm{Cl}(A) \oplus \mathbb{Z}$.

THEOREM 4.5 (INVARIANT FACTOR THEOREM) Let $M \supset N$ be finitely generated torsion-free A-modules of the same ruin m. Then there exist elements $e_1, \ldots, e_m$ of M, fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$, and integral ideals $\mathfrak{b}_1 \supset \mathfrak{b}_2 \supset \ldots \supset \mathfrak{b}_m$ such that

$$M = \mathfrak{a}_1 e_1 \oplus \cdots \oplus \mathfrak{a}_m e_m, \quad N = \mathfrak{a}_1 \mathfrak{b}_1 e_1 \oplus \cdots \oplus \mathfrak{a}_m \mathfrak{b}_m e_m.$$

$$M = \mathfrak{a}_1 e_1 \oplus \cdots \oplus \mathfrak{a}_m e_m, \quad N = \mathfrak{a}_1 \mathfrak{b}_1 e_1 \oplus \cdots \oplus \mathfrak{a}_m \mathfrak{b}_m e_m.$$

The ideals $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_m$ 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.

Let A be a Dedekind domain, and let M be finitely generated torsion-free ^-module. Then $A_\mathfrak{p} \otimes M$ is free, hence projective, forever) nonzero prime ideal $\mathfrak{p}$ in A (because $A_\mathfrak{p}$ is Principal ideal domain), and this implies that M is projective. Therefore there is a nonzero Homomorphism $M \rightarrow A$, whose image is an ideal a in A. As ais projective, there exists a section to the map $M \twoheadrightarrow \mathfrak{a}$, and so $M \approx \mathfrak{a} \oplus M_1$ for some sub module 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.

The Jordan-Holder and Krull-Schmidt theorems both fail for finitely generated projective modules over no principal Dedekind domains. For example, let a be an ideal in A having order 2 in the class group. According to (3.31), $\mathfrak{a} \oplus \mathfrak{a} \approx A \oplus A$., which contradicts both theorems as $\mathfrak{a} \not\approx A$

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.

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

Then $\mathfrak{p}B = \prod(\mathfrak{p}, g_i(\alpha))^{e_i}$ is the factorization of $\mathfrak{p}B$ into a product of powers of distinct prime ideals. Moreover, the residue field $B/(\mathfrak{p}, g_i(\alpha)) \simeq (A/\mathfrak{p})[X]/(\bar{g}_i)$, imd so the residue class degree fi is equal to the degree of g_i .

Our assumption is that the map defines an isomorphism $A[X]/(f(X)) \to B$

When we divide out by $\mathfrak{p}$ (better, tensor with $A/\mathfrak{p}$), this becomes an isomorphism $k[X]/(\bar{f}(X)) \to B/\mathfrak{p}B, \quad X \mapsto \alpha.$ where $k = A/\mathfrak{p}$. The ring $k[X]/(\bar{f})$ has maximal ideals $(\bar{g}_1), \ldots, (\bar{g}_r)$,and $\prod(\bar{g}_i)^{e_i} = 0$ (but no product with smaller exponents is zero). The ideal $(\bar{g}_i)$ in $k[X]/(\bar{f})$ corresponds to the ideal $(g_i(\alpha)) + \mathfrak{p}B$ in $B/\mathfrak{p}B$, and this corresponds to the ideal $\mathfrak{P}_i \overset{\text{def}}{=} (\mathfrak{p}, g_i(\alpha))$ in **B.** Thus $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ is the complete set of prime ideals containing $\mathfrak{p}B$, and hence is the complete set of prime divisors of $\mathfrak{p}$**.** When we write $\mathfrak{p}B = \prod \mathfrak{P}_i^{e_i}$, then they are characterized by the fact that $\mathfrak{p}B$ contains $\prod \mathfrak{P}_i^{e_i}$ 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 of $\bar{g}_i$ occurring in the Factorization of $\bar{f}$.

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 $\deg(f) = \sum e_i \cdot \deg(g_i)$. Also, $\operatorname{disc}(B/A) = \operatorname{disc}(f(X))$, and this is divisible by p if and only if $\bar{f}(X)$ has multiple factors (when regarded as an element of $(A/\mathfrak{p})[X]$), i.e., if and only if some $e_i > 0$

The conclusion of the theorem holds for a particular prime of A under the following weaker hypothesis: $D(1, \alpha, \ldots, \alpha^{m-1}) = \mathfrak{a} \cdot \operatorname{disc}(B/A)$ with a an ideal of A not divisible by $\mathfrak{p}$. To prove this, invert any element of a not in $\mathfrak{p}$, and apply the theorem to the new ring and its integral closure.

REFERENCES

- Avigad, Jeremy (2006). 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, pp.159 {186 (cit. on pp. 8, 30).
- G.Greaves, Sieves in Number Theory. Results in Mathematics and Related Areas (3), 43. Springer-Verlag, Berlin, 2001.
- 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
- H. Cohen, A course in computational algebraic number theory, Springer-Verlag, Berlin, 1993. MR 94i:11105 150
- H.P.F. Swinnerton-Dyer. A Brief Guide to Algebraic Number Theory. University Press of Cambridge, 2001.
- Harper, M., and Murty, R., Euclidean rings of algebraic integers, Canadian Journal of Mathematics, **56**(1), (2004), 71-76.
- J. A. Buchmann and H. W. Lenstra, Jr., Approximating rings of integers in number fields, J. Th_eor. Nombres Bordeaux 6 (1994), no. 2, 221{260. MR 1360644 (96m:11092)
- J.W.S. Cassels, Global fields, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 42{84.
- Kimball Martin. Nonunique factorization and principalization in number fields. Proc. Amer. Math. Soc. 139, No. 9: 3025-3038, 2011.
- Lawrence C. Washington, Introduction to cyclotomic fields, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR 1421575 (97h:11130)
- M.Artin, Algebra, Prentice Hall Inc., Englewood Clients, NJ, 1991. MR 92g:00001
- Michael Atiyah and Ian G. Macdonald. Introduction to Commutative Algebra. Addison-Wesley, 1969.
- Mollin, Richard: Algebraic Number Theory. Chapman and Hall/CRC Press. 1999
- Murty, R., Problems in Analytic Number Theory, GTM/RIM 206, Springer-Verlag, 2001
- Ono, Takashi: An Introduction to Algebraic Number Theory. Plenum Publishing Corporation. 1990
- S. Lang, Algebraic numbers, Addison-Wesley Publishing Co., Inc., Reading, Mass.-Palo Alto-London, 1964. MR 28 #3974
- Schwermer, Joachim (2007). Minkowski, Hensel, and Hasse: On the Beginnings of the Local-Global Principle". In: Episodes in the History of Modern Algebra (1800-1950).
- Serge Lang. Algebra revised 3rd ed. Springer-Verlag, 2002.
- Serge Lang. Algebra. Springer-Verlag, New York Inc., third edition, 2002. 11
- Steve Chien and Alistair Sinclair. Algebras with Polynomial Identities and Computing the Determinant. In FOCS, pages 352{361, 2004. 82
- Victor Shoup. A Computational Introduction to Number Theory and Algebra. Cambridge University Press, New York, 2009. Available from http://shoup.net/ntb/.
- W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (1997), no. 3{4, 235{265, Computational algebra and number theory (London, 1993). MR 1 484478