

Negative microfilm
received from university

65-5275

BROOKS, James Oliver, 1930-
CLASSIFICATION OF REPRESENTATION
MODULES OVER QUADRATIC ORDERS.

The University of Michigan, Ph.D., 1964
Mathematics

University Microfilms, Inc., Ann Arbor, Michigan

CLASSIFICATION OF REPRESENTATION MODULES
OVER QUADRATIC ORDERS

by

James Oliver Brooks

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy in the
University of Michigan
1964

Doctoral Committee:

Professor Donald G. Higman, Chairman
Professor Frederick J. Beutler
Professor Donald J. Lewis
Professor Jack E. McLaughlin
Doctor John H. Smith

ACKNOWLEDGMENTS

I wish to express my deep appreciation to Professor Higman for his suggestion of the topic of this research and for his guidance during the development of the research and the writing of the thesis. I am also much indebted to Dr. David K. Harrison, who suggested the topic of Chapter 5, and who guided my work on it during the year 1961-62 in Philadelphia.

Professor McLaughlin kindly served as second reader of a draft of this thesis.

I am grateful for financial support from the National Science Foundation, both at the University of Michigan, and at the University of Oklahoma during Summer, 1963.

I am appreciative of the support and encouragement from my wife and my mother during the years of graduate study.

TABLE OF CONTENTS

	Page
ACKNOWLEDGMENTS	ii
Chapter	
1. INTRODUCTION	1
1.1 Summary of results	1
1.2 Basic concepts and notations	6
1.3 The elementary ideal invariants and the Steinitz theorem	8
2. ON A THEOREM OF BASS	16
2.1 Introduction	16
2.2 Preparation for the proof of Bass's theorem	16
2.3 Proof of Bass's theorem	18
2.4 Remarks related to Bass's theorem	26
3. ON REPRESENTATION MODULES OVER A QUADRATIC ORDER IN A FIELD	29
3.1 Introduction	29
3.2 The normal form	29
3.3 Invariants	32
3.4 An example	37

Chapter	Page
4. ON REPRESENTATION MODULES OVER A QUADRATIC $\mathbb{Z}$ -ORDER	
WITH ZERO DIVISORS	39
4.1 Introduction	39
4.2 The normal form	41
4.3 Invariants	46
5. ON FIXED-POINT-FREE AUTOMORPHISMS OF MODULES	48
5.1 Introduction	48
5.2 The D-module structure of a finitely generated	
R-module	49
5.3 Conditions for a D-module to admit a fixed-	
point-free automorphism	53
5.4 Further observations	55
BIBLIOGRAPHY	57

CHAPTER 1

INTRODUCTION

1.1 Summary of results

An important general problem in algebra is that of classifying modules over rings. An ideal solution of this problem for a given class of rings and modules provides a canonical form and a complete set of invariants. For finitely generated modules over a Dedekind domain, such a solution is provided by the classical theorem of Steinitz. This theorem asserts that any finitely generated module over a Dedekind domain R is a direct sum of a torsion module and a torsion-free module. The torsion module is uniquely determined and the torsion-free module is determined within isomorphism. The torsion module is a direct sum of cyclic submodules. The torsion-free module is a direct sum of R -ideals. The order ideals of an appropriately chosen decomposition of the torsion part, and the rank and ideal class of the torsion-free part, are a complete set of invariants for the module.

The Steinitz theorem includes in particular the theory of finitely generated modules over a principal ideal domain, and, therefore, the theory of similarity of matrices over a field and the theory of finitely generated abelian groups.

An order over an integral domain D is a ring R which contains D as a subring and which is finitely generated and torsion-free as a D -module. The theory of integral representations deals with those

modules over a D-order R which are finitely generated and torsion-free as D-modules: the so-called R-representation modules. In case D is a principal ideal domain, a D-order R , as well as any R-representation module, has a finite D-basis, and we see that the study of R-representation modules is equivalent to the study of representations of R by matrices with coefficients in D .

Let D be a principal ideal domain. We call a D-order R quadratic if R is a proper ring extension of D generated by a single element which satisfies some quadratic dependence relation over D . We show below in Theorem (1.4) of Section 1.3 that a quadratic D-order R is isomorphic to the D-order

$$(1.1) \quad D[X] / D[X] \cdot f(X)$$

where $f(X)$ is some monic quadratic polynomial in $D[X]$.

In the present study we are concerned with the classification of representation modules over quadratic orders. That problem immediately breaks up into two cases:

Case (A). R is a quadratic order which is an integral domain. Then the polynomial $f(X)$ of (1.1) is irreducible, and R is a D-order in the field $K = k(\theta)$, where k is the quotient field of D , and θ is a root of $f(X)$ over k . Conversely, any D-order R in a quadratic extension field K of k is a quadratic order, for R has a D-basis $\{1, \theta\}$ for some D-integer $\theta \in K$, $\theta \notin k$, and then $R = D[\theta]$. Thus R is of the form (1.1).

Case (B). R is a quadratic order with zero divisors. Then $f(X)$ is reducible, say $f(X) = (X-a)(X-b)$ for some $a, b \in D$. If $a = b$, then R is an order in an algebra with radical; if $a \neq b$, then R is an order

in the semisimple algebra $k \dot{+} k$.

In case (A) we achieve a complete solution of the problem of the classification of R -representation modules, i.e., finitely generated torsion-free R -modules. Let R be a quadratic order with quotient field K . We show, in Theorem (3.1) of Section 3.2, that provided the integral closure of R is a finitely generated R -module, any finitely generated torsion-free R -module M is isomorphic to a module of the form

$$(1.2) \quad R_1 \dot{+} R_2 \dot{+} \dots \dot{+} R_{n-1} \dot{+} \mathcal{O}$$

where the R_i are R -orders in K , $\mathcal{O}$ is an invertible ideal of some R -order R_n in K , and $R_1 \subset R_2 \subset \dots \subset R_n$.

The elementary ideal and ideal class invariants of M determine the form (1.2) essentially uniquely, so that (1.2) is canonical, and the elementary ideal and ideal class invariants are a complete set of invariants (Theorem (3.6) of Section 3.3).

We consider case (B) only for the principal ideal domain $D = Z$, where Z is the ring of rational integers, and only for $a \nmid b$, so that the order is contained in a semisimple algebra. Our solution to the classification problem is incomplete, and is contained in Theorems (4.3) of Section 4.2 and (4.13) of Section 4.3. Let g be the coset of X in (1.1), so that g satisfies $(g-a)(g-b) = 0$. Clearly any Z -matrix representation of R is completely determined by its representation of g . The indecomposable Z -matrix representations of R are of ranks one and two. A complete set of Z -inequivalent indecomposable representations is

$$g \rightarrow T_a = [a], \quad g \rightarrow T_b = [b],$$

$$g \rightarrow T(e) = \begin{bmatrix} a & e \\ 0 & b \end{bmatrix} \quad \text{for } e \in \{1, 2, \dots, \lfloor \frac{|a-b|}{2} \rfloor\}.$$

admits a fixed-point-free automorphism of order q if and only if

- (i) $q-1$ divides the rank of M ,
- (ii) if $D\pi$ is a prime ideal of D which ramifies in R ,
then no power of $D\pi$ occurs as an elementary
divisor of M , and
- (iii) if $D\pi$ is a prime ideal of D which is unramified in R ,
if P is a prime ideal of R which lies over $D\pi$,
and if $f(\pi)$ is the relative degree of P over $D\pi$,
then for each $n = 1, 2, 3, \dots$, the multiplicity of
 $D\pi$ as an elementary divisor of M is a multiple
of $f(\pi)$.

In our solution of case (A) of the classification problem for representation modules over quadratic orders, we make essential use of a theorem of Hyman Bass, which states that if R is an integral domain of altitude one whose integral closure is a finitely generated R -module and in which every ideal can be generated by two elements, then any finitely generated torsion-free R -module is a direct sum of R -ideals. We give an independent proof of this theorem in Section 2.3. In Section 2.4 we give a general class of examples of orders in number fields which do not satisfy the hypothesis of Bass's theorem concerning two element generation of ideals. This means that methods different from ours will have to be introduced to attack the problem of classifying representation modules over general non-maximal orders in number fields of degree greater than two.

In Section 1.2 we define some basic concepts and notations. In Section 1.3 we derive the representation (1.1) of a quadratic order, and we review the theory of elementary ideals, the definition of the ideal class of a module, and the Steinitz theorem.

1.2 Basic concepts and notations

Our notations are generally those of Curtis-Reiner [9]. One important exception is that we denote the basic ring of operators of a module by R instead of G . For general background on modules and representations we refer the reader to [9], especially to Chapter XI; for background on commutative ring theory we refer to Zariski-Samuel [35]; and for background on homological algebra of modules over commutative rings, we refer to Northcott [26], particularly to Chapter 9.

$\mathbb{Z}$ is the ring of rational integers and $\mathbb{Q}$ the rational number field.

A ring is assumed to be commutative with identity. When R and S are rings and $R \subset S$, then the 1 of R is the 1 of S . A module over a ring is assumed to be left unitary. The quotient field of an integral domain R is denoted by K .

The rank of a module M over an integral domain R is the dimension over K of $K \otimes_R M$. The rank of M is the maximal number of R -linearly independent elements of M . If N is a submodule of M , then $\text{rank } M = \text{rank } N + \text{rank } M/N$.

Remark. In places in the literature, including [8] and [11], "rank" has a different meaning than it does here.

The order $\text{ord}(x)$ of an element x of an R -module is the annihilating ideal of x , i.e., the ideal of all $\alpha \in R$ such that $\alpha x = 0$.

If K is an integral domain, an K -ideal is any finitely generated R -submodule of K . R ideals contained in R are integral. Prime, maximal and pairwise comaximal ideals are integral ideals which are prime, maximal, or pairwise comaximal, respectively, in the usual sense.

An integral domain R is of altitude one if every nonzero prime ideal of R is maximal. A domain is also said to be of Krull dimension one if it satisfies that condition.

If R is a domain and $\mathcal{O}$ is a nonzero R -ideal, then

$$\mathcal{O}^{-1} = (R:\mathcal{O}) = \{b \in K : b\mathcal{O} \subset R\}.$$

$\mathcal{O}$ is invertible if $\mathcal{O}\mathcal{O}^{-1} = R$.

Let D be a principal ideal domain and let R be a D -order. We recall that K -representation modules are related to D -matrix representations of R as follows: Any choice of a D -basis for an K -representation module M induces a D -matrix representation of R . If the basis is $\{x_1, \dots, x_n\}$ and if, for $\alpha \in R$,

$$\alpha x_i = \sum a_{ji} x_j \quad \text{for } i = 1, \dots, n, \\ a_{ji} \in D,$$

then the corresponding matrix representation is $T: \alpha \rightarrow T(\alpha)$ defined by $T(\alpha) = (a_{ij})$. Conversely, any D -matrix representation of a D -order R induces an K -representation module. Two R -matrix representations T, U are D -equivalent if there exists an invertible D -matrix S such that

$$U(\alpha) = S^{-1} T(\alpha) S \quad \text{for all } \alpha \in R.$$

Classes of D -equivalent representations correspond in one-to-one fashion with isomorphism classes of K -representation modules.

The internal direct sum of two modules is denoted by $\oplus$ and the external direct sum by $\dot{+}$.

1.3 The elementary ideal invariants and the Steinitz theorem

(a) On quadratic orders.--We first prove the result needed for the description (1.1) of a quadratic order.

(1.4) Theorem. Let D be a principal ideal domain and let R be a quadratic D -order. Then R is isomorphic to the D -order

$$D[X] / D[X] \cdot f(X)$$

for some monic quadratic polynomial $f(X) \in D[X]$.

Proof. Let $g \in R$ such that $R = D[g]$. Then since R is torsion-free as a D -module, R can be embedded in the k -algebra $A = k[g]$, where k is the quotient field of D . Over k , g has some monic minimal polynomial $f(X)$. f is quadratic, since on the one hand some quadratic polynomial annihilates g , and on the other hand A is a proper extension of D . Since $R = D[g]$ is a finitely generated D -module, g is a D -integer, and the coefficients of f lie in D .

Consider the map

$$D[X] / D[X] \cdot f(X) \rightarrow R$$

given by $h(X) + D[X] \cdot f(X) \rightarrow h(g)$, for $h(X) \in D[X]$. That map is clearly onto. Suppose $h(g) = 0$ in R . Then $h(X) \in k[X] \cdot f(X) \cap D[X] = D[X] \cdot f(X)$. Thus the map is one-to-one.

(b) Elementary ideals.--The following development of the elementary ideals and their basic properties follows Fitting [15], pp. 195-199. See also Zassenhaus [38], Chapter III, Sect. 3, pp. 117-121.

Let $\mathfrak{S}$ be an arbitrary finite or infinite set of $n \times n$ matrices with coefficients in a ring R . For each nonnegative integer $i < n$, let $D_i(\mathfrak{S})$ be the R -ideal generated by all minors of order $n-i$ of all the matrices in $\mathfrak{S}$, and for $i = n, n+1, \dots$, let $D_i(\mathfrak{S})$ be the unit ideal R .

Let M be a finitely generated R -module and let $\{x_1, \dots, x_n\}$ be a finite set of generators for M . An $n \times n$ R -matrix $A = (a_{ij})$ annihilates the generator set $\{x_1, \dots, x_n\}$ if $\sum a_{ij} x_j = 0$ for $i = 1, \dots, n$. Let $\mathfrak{S}$ be the set of all R -matrices which annihilate $\{x_1, \dots, x_n\}$. Then the i th elementary ideal $\mathcal{J}_i(M)$ of the module M is $D_i(\mathfrak{S})$, for $i = 0, 1, 2, \dots$. The elementary ideals are invariants of M , independent of n and of the basis $\{x_1, \dots, x_n\}$ used in defining them ([15], Hauptsatz, p. 197).

Basic properties of the elementary ideals are the following:

$$(1.5) \quad \mathcal{J}_i(M) \subset \mathcal{J}_{i+1}(M) \quad \text{for } i = 0, 1, 2, \dots \quad ([15], \text{ Satz 1, p. 199}).$$

If M can be generated by n elements, then $\mathcal{J}_n(M) = R$.

(1.6) If $M = M_1 \dot{+} \dots \dot{+} M_n$ is a direct sum of finitely generated R -modules M_i , then $\mathcal{J}_i(M)$ is the ideal sum of all ideal products of the form

$$\mathcal{J}_{i_1}(M_1) \mathcal{J}_{i_2}(M_2) \cdots \mathcal{J}_{i_n}(M_n)$$

where the integers i_j satisfy the conditions $0 \leq i_j \leq i$ and $\sum i_j = i$, $j = 1, \dots, n$ ([15], Satz 5, p. 201).

The next two propositions are undoubtedly well known, but we cannot cite a reference, and so we include proofs. Regarding the first, see [37], p. 21.

(1.7) If R is a domain, then the rank of a finitely generated R -module M is the smallest integer i such that $\mathcal{J}_i(M) \neq 0$.

Proof. Let $\{x_1, \dots, x_n\}$ be a finite set of generators for M , let F be the free R -module on n generators $\{u_1, \dots, u_n\}$, and let φ be the R -homomorphism $: F \rightarrow M$ which extends the map $u_i \rightarrow x_i$, $i = 1, \dots, n$. Let N be the kernel of φ . With respect to the basis $\{u_1, \dots, u_n\}$ of F , elements of F are represented by n -tuples of elements of R . Also, $\text{rank } N = n - \text{rank } M$.

Suppose $\mathcal{J}_i(M) \neq 0$ for some $i < n$. Then there exists some R -matrix A which annihilates $\{x_1, \dots, x_n\}$ and some nonzero minor of A of order $n-i$. The rows involved in that minor correspond to elements of N which are linearly independent over R . Thus $\text{rank } N \geq n-i$ and so $\text{rank } M \leq i$.

Suppose now that $\mathcal{J}_i(M) = 0$ for some $i < n$. Then any set of $n-i$ elements of N is linearly dependent. Thus $\text{rank } N < n-i$, and $\text{rank } M > i$. This completes the proof.

(1.8) Let D be a principal ideal domain and R a D -order which is a simple ring extension of D , say $R = D[g]$ for some $g \in R$. Let M be an R -representation module, let $\{x_1, \dots, x_n\}$ be a D -basis for M , and let A be the D -matrix representation of g induced by the basis $\{x_1, \dots, x_n\}$. Then

$$\mathcal{J}_i(M) = D_i(A - gI),$$

where I is the identity matrix of degree n .

Proof. Let F be the free $D[X]$ -module on n generators $\{t_1, \dots, t_n\}$, let G be the free R -module on n generators $\{u_1, \dots, u_n\}$, let $\eta: F \rightarrow G$ by $\eta(\sum \phi_i(X)t_i) = \sum \phi_i(g)u_i$ and let $\gamma: G \rightarrow M$ by $\gamma(\sum \phi_i(g)u_i) = \sum \phi_i(g)x_i$. Let N_1 be the kernel of $\gamma\eta$ and let N_2 be the kernel of γ . Thus we have the situation

$$\begin{array}{ccccc} F & \xrightarrow{\eta} & G & \xrightarrow{\gamma} & M \\ \uparrow & & \uparrow & & \uparrow \\ N_1 & \xrightarrow{\quad} & N_2 & \xrightarrow{\quad} & 0 \\ \uparrow & & \uparrow & & \\ 0 & & 0 & & \end{array}$$

Let $v_i = \sum a_{ji}t_j - Xt_i \in F$. Since $\sum a_{ji}x_j - gx_i = 0$ in M , $v_i \in N_1$ for each i . Let N_0 be the submodule of F generated by $\{v_1, \dots, v_n\}$. Since $Xt_i = \sum a_{ji}t_j - v_i \equiv \sum a_{ji}t_j \pmod{N_0}$, any $v \in F$, $v = \sum \phi_i(X)t_i$, is congruent modulo N_0 to some $\sum \rho_i t_i$, $\rho_i \in D$. If $v \in N_1$, then $\sum \rho_i t_i \in N_1$ and $\sum \rho_i x_i = 0$. But $\{x_1, \dots, x_n\}$ is a free D -basis for M , so $\rho_i = 0$ for each i , and $\sum \rho_i t_i = 0$ in F . Thus $v \in N_0$, so $N_1 = N_0$.

Now let $B = (\phi_{ij}(g))$ be any R -matrix which annihilates $\{x_1, \dots, x_n\}$. Then $\beta_i = \sum \phi_{ij}(g)u_j \in N_2$. Since N_2 is the image of $N_1 = N_0$ under η , there exist polynomials $\psi_{ij}(X)$ such that $\beta_i = \sum \psi_{ij}(g)w_j$ where $w_i = \eta(v_i) = \sum a_{ji}u_j - gu_i$. Thus the rows β_i of B are R -linear combinations of the rows of $\begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} = (a_{ji} - g_{ij})$, i.e., of the rows of $A^* - gI$, where $*$ denotes transpose.

On the other hand, $A^* - gI$ is certainly one matrix which annihilates $\{x_1, \dots, x_n\}$. Thus if $\mathfrak{S}$ is the set of all annihilating matrices of the basis $\{x_1, \dots, x_n\}$ for M as an R -module, then $\delta_i(M) = D_i(\mathfrak{S}) = D_i(A^* - gI) = D_i(A - gI)$.

Definition. The order $\text{ord}(M)$ of a finitely generated module M over a ring R is $\delta_0(M)$.

(c) Ideal class.--The next definition follows Kaplansky [22], p. 332. Note that "decomposable" is not the negation of "indecomposable."

Definition. Let R be an integral domain. Then a finitely generated torsion-free R -module M is decomposable if it is isomorphic to a module of the form

$$(1.9) \quad \mathcal{A}_1 \div \dots \div \mathcal{A}_n$$

where the $\mathcal{A}_i$ are R -ideals.

Let $\mathcal{A}_1, \dots, \mathcal{A}_n, \mathcal{B}_1, \dots, \mathcal{B}_n$ be R -ideals and suppose that

$$\mathcal{A}_1 \div \dots \div \mathcal{A}_n \simeq \mathcal{B}_1 \div \dots \div \mathcal{B}_n$$

Then the ideal products $\mathcal{A}_1 \dots \mathcal{A}_n$ and $\mathcal{B}_1 \dots \mathcal{B}_n$ lie in the same ideal class ([22], Lemma 1, p. 328).

Definition. The ideal class of a decomposable R -module M is the common ideal class of all products $\mathcal{A}_1 \dots \mathcal{A}_n$ in any representation of the form (1.9) for M .

(d) The Steinitz theorem.--We recall here those facts about the classification of finitely generated modules over a Dedekind domain which will be of use in our work. For further information, see Steinitz [31], [32]; Fitting [15], Sect. 4, pp. 218-225; Kaplansky [22]; and Curtis-Reiner [9], Sect. 22, pp. 144-155.

Let R be a Dedekind domain, and let M be an R -module. The torsion submodule of M and, for each maximal ideal P of R , the P -primary

submodule of M are well-defined submodules of M .

(1.10) Let M be a finitely generated R -module, and let T be the torsion submodule of M . Then $M = T \oplus U$ for some finitely generated torsion-free R -submodule U of M ([15], Struktursatz, p. 219).

(1.11) Let M be a finitely generated torsion-free R -module of rank n . Then M is decomposable. If $n = 1$, $M \simeq \mathcal{O}$ for some R -ideal $\mathcal{O}$, and if $n > 1$,

$$(1.12) \quad M \simeq \underbrace{R \dot{+} \dots \dot{+} R}_{n-1 \text{ summands}} \dot{+} \mathcal{O}$$

for some ideal $\mathcal{O}$. The ideal class of M is the class of $\mathcal{O}$. The rank and ideal class are a complete set of invariants for finitely generated torsion-free R -modules. The form (1.12) is canonical ([9], Lemma 22.3, Theorem 22.5, Theorem 22.11, and Corollary, pp. 146-150).

In particular, (1.11) implies the following statement.

(1.13) An indecomposable finitely generated torsion-free R -module is of rank one, and is isomorphic to an R -ideal.

(1.14) The elementary ideals of the module (1.12) are $\delta_i = 0$ for $i = 0, 1, \dots, n-1$, and $\delta_i = R$ for $i = n, n+1, \dots$. For finitely generated torsion-free R -modules, the elementary ideals and ideal class are a complete set of invariants ([15], Satz 13, 14, pp. 220-221).

(1.15) Let M be a finitely generated torsion R -module. Then M is a direct sum of cyclic submodules. If $M \neq 0$, there exist nonzero elements $x_1, \dots, x_n$ of M and nonzero proper R -ideals $E_1, \dots, E_n$ such that

$$(1.16) \quad M = Rx_1 \oplus \dots \oplus Rx_n,$$

the order of x_i is E_i , and $E_i \supset E_{i+1}$ for $i = 1, \dots, n-1$.

In any two decompositions of the form (1.16), with ideals E_i and F_i , necessarily $E_i = F_i$ for each i ([15], Hilfssatz 5, p. 212; the result also follows from [9], Theorem 22.12, p. 150).

The E_i are called the invariant factors of the torsion module M .

(1.17) The invariant factors are a complete set of invariants for finitely generated torsion R -modules ([15], p. 214).

The elementary divisors of a finitely generated torsion R -module M are the invariant factors of the P -primary submodules of M , for all maximal ideals P of R .

(1.18) The elementary divisors are a complete set of invariants for finitely generated torsion R -modules.

(1.19) A torsion R -module is indecomposable if and only if it is cyclic and primary ([15], Hilfssatz 3, p. 211).

(1.20) Let M be an arbitrary finitely generated R -module, let T be the torsion submodule of M , and let $M = T \oplus U$. Then the elementary divisors of M (i.e., of T), the rank of M , and the ideal class of M (i.e., of U) are a complete set of invariants.

The following is a special case of (1.20).

(1.21) If R is a principal ideal domain, then the elementary divisors and rank are a complete set of invariants for finitely generated R -modules.

(1.22) Let M be a finitely generated torsion R -module. If M_0 is a submodule of M , then the order of M is equal to the product of the order of M_0 and the order of M/M_0 . The order of M is equal to the product of the invariant factors of M , is equal to the product of the elementary divisors of M , and is equal to the product of the orders of the factors of any normal series for M .

The order of M equals R if and only if $M = 0$ ([15], Satz 10, p. 214; Satz 18, p. 224).

CHAPTER 2

ON A THEOREM OF BASS

2.1 Introduction

In this chapter we give a new proof of the following theorem of Hyman Bass. The theorem will be employed in Chapter 3 in the derivation of a canonical form for representation modules over a quadratic order in a field.

(2.1) Theorem (Bass [4], Sects. 6,7, pp. 17-25). Let R be an integral domain of altitude one such that the integral closure of R in its quotient field is a finitely generated R -module, and such that every R -ideal can be generated by two elements. Let M be a finitely generated torsion-free R -module. Then M is isomorphic to a direct sum of R -ideals.

In Section 2.4 we state for reference a theorem which is implicit in Bass's paper [5], and which contains a converse to Theorem (2.1). Also, we prove a theorem which restricts the class of orders in number fields which satisfy the condition that every ideal can be generated by two elements.

2.2 Preparation for the proof of Bass's theorem

We collect together results which will be used in the proof of Theorem (2.1) in the next section.

(2.2) Lemma ([34], Lemma 3, p. 84). If R is a noetherian domain of altitude one, then for each maximal ideal P , P^{-1} is strictly larger than R .

(2.3) Lemma ([9], Theorem 58.6, p. 396). Let A be a ring which satisfies the minimum condition. Then the following conditions on A are equivalent:

- (i) A is a quasi-Frobenius ring,
- (ii) the dual of an irreducible A -module is an irreducible A -module,
- (iii) A is injective as an A -module.

(2.4) Lemma ([26], Corollary, p. 180). Let a be neither a unit nor a zero divisor in a ring A . Let $\bar{A} = A/Aa$, and let $\bar{M}$ be an arbitrary $\bar{A}$ -module. Then

$$\text{Ext}_A^2(\bar{M}, A) \cong \text{Ext}_{\bar{A}}^1(\bar{M}, \bar{A})$$

as $\bar{A}$ -modules.

(2.5) Lemma ([26], Lemma 1, p. 181). If A is a ring and N a finitely generated A -module, and if $\mathfrak{m}N = N$ for every maximal ideal $\mathfrak{m}$ of A , then $N = 0$.

(2.6) Lemma ([5], Lemma 1.3, p. 321). If $\mathcal{O}_1, \dots, \mathcal{O}_n$ are pairwise comaximal ideals in a ring R , and if $x_1, \dots, x_n$ are elements of an R -module M , then there is an $x \in M$ such that $x \equiv x_i \pmod{\mathcal{O}_i M}$ for $i = 1, \dots, n$.

(2.7) Lemma ([1], Lemma 2.4, p. 6). Let R be a noetherian ring and S a ring containing R which is a flat R -module. Then if A is any finitely generated R -module and B any R -module,

$$S \otimes_R \text{Ext}_R^n(A, B) \simeq \text{Ext}_S^n(S \otimes_R A, S \otimes_R B)$$

for all $n \geq 0$.

(2.8) Lemma ([26], Lemma 2, p. 187). If R is a ring and A is an R -module, and if $A_P = 0$ for every maximal ideal P of R , then $A = 0$.

Let $\text{dh}_R(A)$ denote the homological dimension of an R -module A .

(2.9) Lemma ([26], Theorem 11, p. 188). Let R be a ring and A a finitely generated R -module. Then

$$\text{dh}_R(A) = \sup_P \text{dh}_{R_P}(A_P)$$

where P ranges over all maximal ideals of R .

2.3 Proof of Bass's theorem

We shall prove that under the hypotheses of (2.1), every indecomposable finitely generated torsion-free R -module is of rank one. This is clearly equivalent to the conclusion of (2.1).

Definition. Let (H) be the hypothesis on a ring R that R is an integral domain of altitude one in which every ideal can be generated by two elements.

(2.10) Proposition. If R satisfies the hypothesis (H) , then for each maximal ideal P , P^{-1}/R is an irreducible R -module.

Proof. P^{-1}/R is not the zero module, by (2.2). We claim that there is no R -ideal strictly between R and P^{-1} .

If P is invertible, and if $P^{-1} \supset \mathcal{O} \supset R$ for some ideal $\mathcal{O}$, then multiplying by P , we find that $R \supset P\mathcal{O} \supset P$. Since P is maximal, either $P\mathcal{O} = R$ or $P\mathcal{O} = P$. Then $\mathcal{O} = P^{-1}$ or $\mathcal{O} = R$, respectively.

Suppose P is not invertible. $PP^{-1} \supset PR = P$ so $PP^{-1} = P$. Then the factor module P^{-1}/P is an R -module which is annihilated by P and which can be generated by two elements. Let $k = R/P$, a field. Then P^{-1}/P is an at most two dimensional vector space over k . The dimension is exactly two, since R/P is a proper one-dimensional subspace. Thus

$$P^{-1}/R \simeq \frac{(P^{-1}/P)}{(R/P)}$$

is a one dimensional space, and so P^{-1}/R is irreducible.

Definition. For R an integral domain, the dual M^* of an R -module M is $\text{Hom}_R(M, R)$ made into an R -module under $(rf)(x) = rf(x)$ for $r \in R$, $x \in M$, and $f \in M^*$.

There is a natural homomorphism $d_M: M \rightarrow M^{**}$ of M into its double dual, given by $d_M(x) = g \in M^{**}$ such that $g(f) = f(x)$ for $f \in M^*$. When M is a finitely generated torsion-free R -module, d_M is one-to-one. For let K be the quotient field of R . M can be embedded in a K -vector space V . If $x \neq 0$ in M , then there exists an $f \in \text{Hom}_K(V, K)$ such that $f(x) \neq 0$. Then since M is finitely generated, for an appropriate nonzero multiple g of the function f , $g(M) \subset R$ and $g(x) \neq 0$. Then g restricted to M , call it $\bar{g}$, is an R -homomorphism from M into R and does not vanish on x . Therefore $d_M(x)(\bar{g}) = \bar{g}(x) \neq 0$, and so $d_M(x)$ is not the zero map in M^{**} .

For M a finitely generated and torsion-free R -module, we use d_M to identify M with its isomorphic image $d_M(M)$ contained in M^{**} .

M is called reflexive if d_M is an isomorphism onto M^{**} . (On duals in general, see [2], pp. 476-478.)

(2.11) Proposition. Let A be a local ring which satisfies the hypothesis (H). Let $\mathfrak{m}$ be the maximal ideal of A . Then for any $a \neq 0$ in $\mathfrak{m}$, the ring $\bar{A} = A/aA$ is injective as an $\bar{A}$ -module, and $\text{Ext}_A^1(M, \bar{A}) = 0$ for any $\bar{A}$ -module M .

Proof. aA is an $\mathfrak{m}$ -primary ideal, so A is a primary ring. Since A is noetherian, a power of $\mathfrak{m}$ is contained in aA , and so $\bar{A}$ has minimum condition. The ideal $(0 : \bar{\mathfrak{m}})$ is minimal in $\bar{A}$ since

$$(0 : \bar{\mathfrak{m}}) = aA : \mathfrak{m} / aA \simeq A : \mathfrak{m} / A = \mathfrak{m}^{-1} / A$$

and $\mathfrak{m}^{-1}/A$ is irreducible, by (2.10).

Let M be any irreducible $\bar{A}$ -module. Then $\bar{\mathfrak{m}} M = 0$ and $M \simeq \bar{A}/\bar{\mathfrak{m}}$.

Then

$$(\bar{A}/\bar{\mathfrak{m}})^* = \text{Hom}_{\bar{A}}(\bar{A}/\bar{\mathfrak{m}}, \bar{A}) \simeq (0 : \bar{\mathfrak{m}})$$

under the correspondence $f \leftrightarrow f(1)$. Thus M^* is irreducible.

We now apply the implication (ii) $\Rightarrow$ (iii) of (2.3) to obtain that $\bar{A}$ is injective as an $\bar{A}$ -module.

(2.12) Proposition. If a local ring A satisfies the hypothesis (H), then $\text{Ext}_A^1(M, A) = 0$ for any finitely generated torsion-free A -module M .

Proof. According to (2.4) and (2.11), for any $\bar{A}$ -module $\bar{M}$,

$$\text{Ext}_A^2(\bar{M}, A) \simeq \text{Ext}_{\bar{A}}^1(\bar{M}, \bar{A}) = 0.$$

For M torsion-free, the map $\psi : M \rightarrow M$ given by $\psi(m) = am$ is one-to-one, for $a \neq 0$. Then

$$0 \rightarrow M \xrightarrow{\psi} M \rightarrow M/aM \rightarrow 0$$

is exact and it induces the exact sequence

$$\text{Ext}_A^1(M, A) \xrightarrow{\psi^*} \text{Ext}_A^1(M, A) \rightarrow \text{Ext}_A^2(M/aM, A) = 0$$

$\psi^* = \text{Ext}_A^1(\psi, \text{Id}_A)$ is the map multiplication by a , since ψ is multiplication by a and since A is commutative and Ext is A -linear.

Thus ψ^* is an onto map:

$$\text{Ext}_A^1(M, A) = a \text{Ext}_A^1(M, A) .$$

Then all the more so,

$$\text{Ext}_A^1(M, A) = m \text{Ext}_A^1(M, A) .$$

But M and A are finitely generated A -modules, so $\text{Ext}_A^1(M, A)$ is too, and so by (2.5), $\text{Ext}_A^1(M, A) = 0$.

(2.13) Proposition. A finitely generated torsion-free module over a local ring A which satisfies the hypothesis (H) is reflexive.

Proof. Let M be such a module. By (2.12), $\text{Ext}_A^1(M, A) = 0$.

Let

$$(2.14) \quad 0 \rightarrow K \rightarrow F \rightarrow M \rightarrow 0$$

be exact, for some finitely generated free module F and submodule K .

Then (2.14) induces

$$0 \rightarrow M^* \rightarrow F^* \rightarrow K^* \rightarrow \text{Ext}_A^1(M, A) = 0 .$$

Next, K is a submodule of the finitely generated module F over the noetherian ring A , so is finitely generated. Then K^* is finitely generated also. And for $f \in K^*$, f takes values in the domain A , so if $af = 0$ for a $\neq 0$ in A , then $f = 0$. Thus K^* is also torsion-free, and $\text{Ext}_A^1(K^*, A) = 0$ by (2.12).

Dualizing again, we get

$$(2.15) \quad \begin{array}{ccccccc} 0 & \rightarrow & K & \xrightarrow{j} & F & \xrightarrow{p} & M \rightarrow 0 \\ & & \downarrow d_K & & \downarrow d_F & & \downarrow d_M \\ 0 & \rightarrow & K^{**} & \xrightarrow{j^{**}} & F^{**} & \xrightarrow{p^{**}} & M^{**} \rightarrow 0 \end{array}$$

Now a finitely generated free module is reflexive: if $u_1, \dots, u_n$ is a basis for the module, then $f_1, \dots, f_n$ with $f_i(u_j) = \delta_{ij}$ is a basis for the dual space, as with finite dimensional vector spaces over fields. The diagram (2.15) is commutative since all maps are natural. Also M is finitely generated and torsion-free over the domain A , so d_M is one-to-one, by the earlier remarks. Finally d_M is onto, since $g \in M^{**}$ is the image of an $f \in F^{**}$ which in turn is the image of an $x \in F$, and then $p(x)$ maps onto g under d_M .

(2.16) Proposition. Let M be a finitely generated torsion-free module over a noetherian domain R . Then M is reflexive if and only if M_P is reflexive as an R_P -module, for each maximal ideal P of R .

Proof. We first observe that localization commutes with the taking of duals: $(M^*)_P \cong (M_P)^*$. This follows from (2.7) for $n = 0$ and $S = R_P$.

If M is reflexive, then $M^{**} = M$, $M_P^{**} = (M^{**})_P = M_P$, so M_P is reflexive for each maximal ideal P . Conversely, let $\{P_i : i \in I\}$ be the family of maximal ideals of R . For any torsion-free R -module M , $M = \bigcap_{i \in I} M_{P_i}$ ($i \in I$). The one inclusion is obvious. For the other, if $x \in M_{P_i}$ for all i , then $x = y_i/s_i$ for some $y_i \in M$, $s_i \in R - P_i$. Let $\mathcal{O}$ be the R -ideal generated by the set of all the s_i . $\mathcal{O}$ is not proper, for if $P_{i_0} \supset \mathcal{O}$ then $s_{i_0} \in P_{i_0}$, a contradiction. Thus $1 = \sum r_i s_i \in \mathcal{O}$ for some $r_i \in R$. Then $x = 1 \cdot x = \sum r_i s_i x = \sum r_i y_i \in M$ since the y_i lie in M .

Suppose now that M is reflexive for all maximal ideals P . Then $M^{**} = \bigcap_P (M^{**})_P = \bigcap_P (M_P)^{**} = \bigcap_P M_P = M$, so M is reflexive.

From now on in this proof, the argument is based directly on Bass [4], p. 20.

Let R be an integral domain, M an R -module, and M^* the dual module of M . Let

$$(2.17) \quad B = B(M) = \sum_{f \in M^*} f(M) \quad .$$

B is an integral R -ideal. Let R' be the integral closure of R in its quotient field K .

(2.18) Lemma. Let R and S be integral domains with the same quotient field, and let $R \subset S$, and suppose that every R -ideal can be generated by k elements. Then every S -ideal can be generated by k elements.

Proof. Any S -ideal $\mathcal{O}$ is an R -ideal. Let $a_1, \dots, a_k$ be a set of R -generators for $\mathcal{O}$. Then the a_i lie in $\mathcal{O}$ and $\mathcal{O} = Ra_1 + \dots + Ra_k \subset Sa_1 + \dots + Sa_k \subset \mathcal{O}$ whence the a_i generate $\mathcal{O}$ as an S -ideal.

(2.19) Proposition. Let M be a nonzero reflexive finitely generated module over a ring R which satisfies the hypothesis (H). Then for $B = B(M)$, B^{-1} is a subring of R' containing R , B^{-1} satisfies the hypothesis (H), and R and M are B^{-1} -modules.

Proof. $M \neq 0$ implies $B \neq 0$. For each $b = \sum f_i(m_i) \in B$ and $x \in B^{-1}$, $f_i(M) \subset B$ so $xf_i(M) \subset R$ and hence $xf_i \in M^*$. Thus $xb = \sum (xf_i)(m_i) \in B$. Thus for $x, y \in B^{-1}$, $xyb \in xB \subset B$ so $xy \in B^{-1}$, and thus B^{-1} is not only an R -module but also a ring.

B is a B^{-1} -module, for as we saw above, for $x \in B^{-1}$, $b \in B$, $xb \in B$. Therefore $M^* = \text{Hom}_R(M, R) = \text{Hom}_R(M, B)$ is a B^{-1} -module.

By hypothesis $M = M^{**}$ so also M is a B^{-1} -module. Since B^{-1} is an R -ideal, it is a finitely generated R -module, and since a ring, it is an R -order in K : $R \subset B^{-1} \subset R'$. Thus B^{-1} is integral over R and so is a domain of altitude one. By (2.18), every ideal of B^{-1} can be generated by two elements.

(2.20) Proposition. Under the conditions of (2.19) on R and M , if $B^{-1} = R$, then M has a nonzero projective rank one direct summand.

Proof. $B^{-1} = R$ implies $R = B = \sum f(M)$ ($f \in M^*$). Let F be the conductor of R in R' and let $P_1, \dots, P_n$ be the maximal ideals of R containing F . For each i , $\sum f(M) \equiv R \pmod{P_i}$ so there exists a $f_i \in M^*$ with $f_i(M) \equiv R \pmod{P_i}$, and then a $y_i \in M$ with $g_i(y_i) \equiv 1 \pmod{P_i}$. Now apply (2.6) to the R -module M to get, for each i , an $x_i \in M$ such that $x_i \equiv y_i \pmod{P_i M}$ and $\equiv 0 \pmod{P_j M}$ for $j \neq i$. Similarly, for each i , get an $f_i \in M^*$ with $f_i \equiv g_i \pmod{P_i M^*}$ and $\equiv 0 \pmod{P_j M^*}$ for $j \neq i$. Let $x = \sum x_i$, $f = \sum f_i$. Then $f(x) = \sum f_i(x_j) \equiv f_k(x_k) \equiv 1 \pmod{P_k}$, for each $k = 1, \dots, n$.

Let $N = Kx \cap M$, the smallest pure submodule of M containing x . The injection of N into M induces an exact sequence

$$(2.21) \quad 0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$$

with M/N torsion-free. Let P be a maximal ideal of R . Then (2.21) localizes to

$$(2.22) \quad 0 \rightarrow N_P \rightarrow M_P \rightarrow (M/N)_P \rightarrow 0,$$

an exact sequence of R_P -modules. N_P is pure in M_P , and $(M/N)_P$ is torsion-free.

If, in particular, P is one of the maximal ideals of R containing the conductor, then N_P equals $R_P x$ and so is a cyclic R_P -module isomorphic

to R_P . For certainly $R_P x \subset N_P$. Conversely, for $(ax/b) \in N_P$, with $a, b \in R$, $(ax/b) = (m/s)$ for some $m \in M$, $s \in R - P$. Then $asx = bm$. Taking the value of f on both sides, $asf(x) = bf(m)$. But $f(m) \in R$ so b divides $asf(x)$. Since $f(x) \equiv 1 \pmod{P}$, by choice of f and x , there exists a $c \in P$ such that $f(x) + c = 1$. Then $asf(x) = as(1-c)$. Since $1-c \in R - P$,

$$\frac{ax}{b} = \left(\frac{as(1-c)}{b} \right) \cdot \left(\frac{x}{s(1-c)} \right) \in R_P x.$$

Now R_P is a local domain which satisfies the hypothesis (H). Then since N_P is cyclic and $(M/N)_P$ is torsion-free, the sequence (2.22) splits by (2.12), and N_P , being isomorphic to R_P , is a projective module.

For a prime P which does not contain F , R_P is a principal ideal domain, and N_P , being pure in M_P , is a direct summand of M_P . N_P is isomorphic to R_P , and so is projective.

Thus the sequence (2.22) splits for all P . Since by (2.7), localization commutes with formation of Ext , and since by (2.8), the module $\text{Ext}_R^1(M/N, N)$ vanishes globally if it vanishes locally for all maximal ideals P , we get that $\text{Ext}_R^1(M/N, N) = 0$. Thus N is a rank one direct summand of M (cf. [5], Lemma 1.9, p. 322).

Finally we come to the proof of the main theorem. We must show that under the hypothesis (H) together with the assumption that R' is a finitely generated R -module, any indecomposable finitely generated torsion-free R -module is of rank one. So suppose that M is a finitely generated torsion-free R -module of rank greater than one. M is reflexive by (2.13) and (2.16), so we may apply (2.20). If M has a proper direct summand, that contradicts indecomposability. Thus

B^{-1} is strictly larger than R . Since B^{-1} satisfies the hypothesis (H), the argument is repeated on B^{-1} . M has the same rank as a B^{-1} -module as it does as an R -module. The integral closure R' is a finitely generated R -module, so after finitely many steps we arrive at R' as the ring of operators of M . This is a contradiction, because R' is Dedekind, and an indecomposable module over a Dedekind domain cannot have rank greater than one, by (1.13).

This completes the proof of Theorem (2.1).

(2.23) Corollary. If R is an order in a quadratic number field, then any R -module is isomorphic to a direct sum of R -ideals.

Proof. An R -ideal $\mathcal{O}$ is generated by two elements over $\mathbb{Z}$, and so also over R .

2.4 Remarks related to Bass's theorem

(a) The number of isomorphism classes of indecomposable modules over a domain R which satisfies the hypotheses of Bass's theorem is equal to the class number of R , since every indecomposable module is of rank one.

(b) The following theorem, which is an immediate derivation from Propositions 1.2 and 1.4 of Bass [5], pp. 320-321, contains a converse to Theorem (2.1).

Theorem. Let k be a positive integer and let R be a noetherian integral domain such that every finitely generated torsion-free R -module is a direct sum of submodules of ranks $\leq k$. Then every R -ideal can be generated by $k+1$ elements.

(c) It would be of interest to be able to describe the class C of orders in number fields which satisfy the condition that every ideal can be generated by two elements.

C includes all principal orders and all quadratic orders. Some orders which are excluded from C are described in the corollary to the next theorem.

(2.24) Theorem. Let K be an algebraic number field of degree n . Let R' be the principal order in K and let p be a rational prime number. Then the subset $R = Z + pR'$ of R' is an order in K , the subset $P = pR'$ is an ideal in R , and P is generated over R by n elements and not by fewer than n elements.

Proof. To show that R is an order, we need only show it is a ring: $(Z + pR')(Z + pR') = Z + pR' + p^2R' = Z + pR'$. Since $RP = (Z + pR')(pR') = P$, P is an R -ideal. It is maximal since R/P is of order p . $P^2 = p^2R' = pP$, so P/P^2 is a vector space of p^n elements over R/P . Thus $\dim_{R/P} (P/P^2) = n$, and any basis for P/P^2 contains n elements. Thus as an R -ideal, P requires n generators.

Corollary. Let K be an algebraic number field of degree ≥ 3 , and let R' be the principal order in K . Then any order R for which every ideal can be generated by two elements is not a subring of any order of the form $Z + pR'$, for any prime number p .

Proof. Apply (2.24) and (2.18).

The following problems are suggested by Theorem (2.1).

1) Exhibit an order in a number field, other than a principal order or a quadratic order, in which every ideal can be generated by two elements. For instance, can every ideal of the order $Z[\sqrt[3]{4}]$ be generated by two elements?

2) Is there a generalization of Theorem (2.1) to the effect that, for orders in number fields, there is a relation between the maximum number of elements needed to generate R -ideals and the maximum rank of indecomposable R -modules, if such a maximum exists?

3) The hypothesis that the integral closure of R be a finitely generated R -module could be dropped for Theorem (2.1) if one could show that for $B = B(M)$ and $S = B^{-1}$, M as an S -module always has a rank one direct summand.

4) In analogy with the Steinitz theorem, what is the structure of a finitely generated torsion module over a ring R which satisfies the hypotheses of Theorem (2.1)? Is the torsion submodule of an arbitrary finitely generated R -module a direct summand?

CHAPTER 3
ON REPRESENTATION MODULES OVER A QUADRATIC ORDER
IN A FIELD

3.1 Introduction

In Theorem (3.1) of Section 3.2 we derive a normal form for a finitely generated torsion-free module over a domain R of altitude one whose integral closure is a finitely generated R -module, and in which every ideal can be generated by two elements.

Under the further assumption that the ring R is a quadratic order in a field, we show in Theorem (3.6) of Section 3.3 that the normal form is canonical and that the elementary ideals and ideal class are a complete set of invariants.

Since a finitely generated torsion-free module over a quadratic order R in a field is precisely an R -representation module (Theorem (3.15)), Theorems (3.1) and (3.6) constitute a complete classification of R -representation modules.

In Section 3.4 we give as an example the rank two modules over the quadratic order $\mathbb{Z}[\sqrt{-72}]$.

3.2 The normal form

(3.1) Theorem. Let R be an integral domain of altitude one such that the integral closure of R in its quotient field is a finitely generated R -module and such that every R -ideal can be generated by two

elements. Let K be the quotient field of R and let R' be the integral closure of R . Then any finitely generated torsion-free R -module is isomorphic to a module of the form

$$(3.2) \quad R_1 + R_2 + \dots + R_{n-1} + \mathcal{L}$$

where the R_i are R -orders in K , $\mathcal{L}$ is an invertible ideal of the R -order $R_n = (\mathcal{L} : \mathcal{L})$, and where $R_1 \subset R_2 \subset \dots \subset R_n$.

We call the set $\{n, R_1, \dots, R_n, \mathcal{L}\}$ the parameters of the form (3.2).

The proof of (3.1) depends on two lemmas. The first is a generalization of a lemma of Grell ([16], Hilfssatz 2, p. 648). His proof goes over immediately to a proof of the present lemma.

(3.3) Lemma. Let R be an integral domain of altitude one and let $\mathcal{O}$ be an invertible integral R -ideal. Then modulo any nonzero ideal $\mathcal{O}_1$ contained in $\mathcal{O}$, $\mathcal{O}$ is principal. Given any integral ideal $\mathcal{B}$, there is an integral ideal $\mathcal{L}$ such that $\mathcal{O}\mathcal{L}$ is principal and $\mathcal{L}$ is relatively prime to $\mathcal{B}$.

(3.4) Lemma. Let R be an integral domain of altitude one, and let M be a decomposable R -module of rank $n \geq 2$, and suppose that

$$M \simeq \mathcal{O} + \mathcal{B}_1 + \mathcal{B}_2 + \dots + \mathcal{B}_{n-1}$$

where $\mathcal{O}$ is an invertible R -ideal and the $\mathcal{B}_i$ are arbitrary nonzero R -ideals. Then

$$M \simeq R + \mathcal{O}\mathcal{B}_1 + \mathcal{B}_2 + \dots + \mathcal{B}_{n-1}$$

Proof. We may assume that $\mathcal{O} \supset R \supset \mathcal{B}_1$. Then by (3.3) there is an ideal $\mathcal{L}$ such that $\mathcal{O}^{-1}\mathcal{L}$ is principal and $\mathcal{L}$ is relatively prime to $\mathcal{B}_1$. If we then show that $\mathcal{L} + \mathcal{B}_1 \simeq R + \mathcal{L}\mathcal{B}_1$, the lemma follows immediately.

Let $c_0 \in \mathcal{L}$, $b_0 \in \mathcal{B}_1$ such that $c_0 - b_0 = 1$. Let
 $\varphi : \mathcal{L} + \mathcal{B}_1 \rightarrow R + \mathcal{L}\mathcal{B}_1$ by

$$\varphi(\gamma, \beta) = (\gamma + \beta, \gamma b_0 + \beta c_0) \quad , \quad \gamma \in \mathcal{L}, \beta \in \mathcal{B}_1.$$

It is easily checked that φ is an R -isomorphism of $\mathcal{L} + \mathcal{B}_1$ onto $R + \mathcal{L}\mathcal{B}_1$ (cf. [9], p. 150).

Proof of (3.1). Since R' is a finitely generated R -module, R'/R has finite length as an R -module. We employ induction on the length of R'/R , and for any fixed ring R , on the rank of an R -module M .

Let M be a finitely generated torsion-free R -module.

If $R = R'$, then R is Dedekind and M is isomorphic to a module of the form

$$(3.5) \quad R + \dots + R + \mathcal{L}$$

where $\mathcal{L}$ is an (invertible) R -ideal, by (1.11). The module (3.5) is then the desired form (3.2) for M .

If $R < R'$, we assume that the theorem holds for any R -order S strictly larger than R . If $B < R$, where $B = B(M)$ as defined in (2.17), then M is a B^{-1} -module and $S = B^{-1}$ is strictly larger than R . As an S -module, M is isomorphic to a module N in the form (3.2). Then N also represents M as an R -module.

If $B(M) = R$ then by (2.20), M has a projective rank one direct summand isomorphic to some R -ideal $\mathcal{O}$. Since R is a domain, $\mathcal{O}$ is invertible ([7], Prop. 3.2, p. 132). If $\text{rank } M = 1$, then $\mathcal{L} = \mathcal{O}$ is of the form (3.2). If $\text{rank } M = n > 1$, then $M \simeq \mathcal{O} + M_0$ for some finitely generated torsion-free R -module M_0 . M_0 is decomposable, by Theorem (2.1), so $M \simeq \mathcal{O} + \mathcal{B}_1 + \dots + \mathcal{B}_{n-1}$ for some R -ideals $\mathcal{B}_i$. Then by (3.4), $M \simeq R + \mathcal{O}\mathcal{B}_1 + \dots + \mathcal{B}_{n-1}$. Let $M_1 = \mathcal{O}\mathcal{B}_1 + \mathcal{B}_2 + \dots + \mathcal{B}_{n-1}$.

Since $\text{rank } M_1 < \text{rank } M$, M_1 is isomorphic to an R -module N in the form (3.2), say with parameters $n-1, R_1, \dots, R_{n-1}, \mathcal{L}$. Then M is isomorphic to $R \oplus N$ which is in the form (3.2) with parameters $n, \tilde{R}_1, \dots, \tilde{R}_n$, given by $\tilde{R}_1 = R$, $\tilde{R}_i = R_{i-1}$ for $i = 2, \dots, n$, and $\tilde{\mathcal{L}} = \mathcal{L}$.

3.3 Invariants

Let D be a principal ideal domain, k the quotient field of D , and K a quadratic extension field of k . Let R be a D -order in K . Since R is an integral extension of D , R has altitude one. Since R has rank 2 as a D -module, any R -ideal can be generated by two elements as a D -module, and so also as an R -module. Assume further that R' is a finitely generated R -module. Then R satisfies the hypotheses on the ring of (3.1).

(3.6) Theorem. Let D be a principal ideal domain, K a quadratic extension field of the quotient field of D , and let R be a D -order in K . Assume that the integral closure of R is a finitely generated R -module. Then the elementary ideals and the ideal class of a finitely generated torsion-free R -module M completely determine the isomorphism class of M . If $\{n, R_1, \dots, R_n, \mathcal{L}\}$ is the set of parameters of a module N in the form (3.2) which is isomorphic to M , then for $i = 1, \dots, n$, R_i is the unique order in the ideal class of $\delta_{2n-i}^{(M)}$, and the class of $\mathcal{L}$ is the class of M . Thus $n, R_1, \dots, R_n$ are uniquely determined by the isomorphism class of M , and the ideal class of $\mathcal{L}$ is determined by that isomorphism class. Except for a choice of the particular ideal $\mathcal{L}$ within its ideal class, the form (3.2) is canonical.

Proof. Let $D, k, R, R',$ and K be as above. Let N be an R -module in the form (3.2). If we show that the parameters $n, R_1, \dots, R_n$ and the ideal class of $\mathcal{L}$ are uniquely determined by the elementary ideals and ideal class of N , then that will demonstrate the completeness of the elementary ideals and ideal class, as well as show (3.2) to be canonical. For then if two modules M_1 and M_2 have the same elementary ideals and ideal class, they are isomorphic to the same N in the form (3.2), and thus are mutually isomorphic.

(3.7) Lemma. Any D -submodule of K of D -rank 2 has a D -basis of the form $\{a, \omega\}$ for some $a \in k$ and $\omega \in K$. Any D -order in K has a basis of the form $\{1, \omega\}$ for some $\omega \in R'$. If S_1 and S_2 are D -orders in K and $S_1 \subset S_2$, and if $\{1, \omega\}$ is a D -basis for S_2 for some $\omega \in R'$, then $\{1, e\omega\}$ is a D -basis for S_1 for some $e \in D$.

Proof. Let $\mathcal{O}$ be a D -submodule of K of D -rank 2. Let $\theta \in K$, $\theta \notin k$, then $\{1, \theta\}$ is a k -basis for K . For some $\lambda \neq 0$ in D , $\lambda \mathcal{O} \subset D + D\theta$. The module $\lambda \mathcal{O}$ then has a D -basis of the form $\{\eta_1, \eta_2\}$ where

$$(3.8) \quad \begin{aligned} \eta_1 &= a_{11} \\ \eta_2 &= a_{21} + a_{22}\theta \end{aligned} \quad a_{ij} \in D, a_{11}a_{22} \neq 0.$$

Then for $a = \eta_1 / \lambda$, $\omega = \eta_2 / \lambda$, $\{a, \omega\}$ is the desired basis for $\mathcal{O}$.

Next, since for a D -order S in K , $S \cap k = D$, if S has a basis of the form $\{a, \omega\}$, then a must be a unit in D and ω a D -integer. Thus we may assume $a = 1$. If $S_1 \subset S_2$, and if $\{1, \omega\}$ is a D -basis for S_2 , then apply the argument leading to (3.8) to the k -basis $\{1, \theta\}$ where $\theta = \omega$. Since $1 \in S_1$, a_{11} is a unit in D and we may take $a_{12} = 0$. Thus for $e = a_{22}$, S_1 has the D -basis $\{1, e\omega\}$.

(3.9) Lemma. If R is as in (3.6), and if $\mathcal{O}$ is an R -ideal,

then $\delta_0(\mathcal{O}) = 0$, $\delta_1(\mathcal{O}) = (\mathcal{O}:\mathcal{O})^{-1}$, and $\delta_2(\mathcal{O}) = R$.

Proof. $\delta_0(\mathcal{O}) = 0$ since $\mathcal{O}$ has positive rank and $\delta_2(\mathcal{O}) = R$ since $\mathcal{O}$ can be generated by two elements.

If $\mathfrak{B}$ is an R -ideal in K and if $\{a_1, \dots, a_n\}$ is a set of elements of $\mathfrak{B}$ which generate $\mathfrak{B}$ as a D -module, then we denote $\mathfrak{B}$ by $(a_1, \dots, a_n)$.

Without loss of generality we may take $\mathcal{O}$ to be integral. Let $\mathcal{O} = (a, \omega)$ for some $a \in D$, $\omega \in R'$. Then ω satisfies a quadratic relation $\omega^2 + b\omega + c = 0$ for some $b, c \in D$. Let $\mathcal{O}' = (a, \omega')$ where ω' is the conjugate of ω over k . Then

$$\mathcal{O}\mathcal{O}' = (a^2, a(\omega + \omega'), a\omega, a\omega') = (a^2, ab, c, a\omega).$$

Let $d = \text{g.c.d.}(a^2, ab, c)$ in D , so $\mathcal{O}\mathcal{O}' = (d, a\omega)$. Let $\theta = a\omega/d$.

θ is a D -integer since $\text{trace}(\theta) = a\omega/d + a\omega'/d = -ab/d \in D$ and $\text{norm}(\theta) = a^2\omega\omega'/d^2 = a^2c/d^2 \in D$. Then $S = (1, \theta)$ is a D -order in K .

One verifies that $\mathcal{O}$ is an S -ideal. Conversely, if $\alpha\mathcal{O} \subset \mathcal{O}$, then $\alpha S = \alpha(\frac{\mathcal{O}\mathcal{O}'}{d}) \subset \mathcal{O}\mathcal{O}'/d = S$, and so $\alpha \in S$. Thus $S = (\mathcal{O}:\mathcal{O})$.

Since $R\mathcal{O} \subset \mathcal{O}$, $R \subset S$ and so S is an R -order in K . Then by (3.7),

$R = (1, e\theta)$ for some $e \in D$. One verifies that

$$(3.10) \quad S^{-1} = eS = (e, e\theta).$$

Since $a\theta = \frac{a^2}{d}\omega$, $\omega\theta = -\frac{c}{d}a - \frac{ab}{d}\omega$, θ is represented

with respect to the D -basis $\{a, \omega\}$ for $\mathcal{O}$ by the matrix

$$B = \begin{bmatrix} 0 & -c/d \\ a^2/d & -ab/d \end{bmatrix}.$$

Hence $e\theta$ is represented by $A = eB$. By proposition (1.8), $\delta_1(\mathcal{O})$ is

the R -ideal generated by all entries of the matrix $A - \theta I$. Thus

$$\delta_1(\mathcal{O}) = e \cdot (-\theta, -c/d, a^2/d, -\theta - ab/d) = e \cdot (1, \theta) = S^{-1}.$$

This completes the proof of (3.9).

The symbol " $\sim$ " denotes equivalence of ideals.

(3.11) Lemma. If R is as in (3.6) and if S is an R -order in K , then $S^{-1} \sim S$. If S_1, S_2 are R -orders in K and $S_1 \subset S_2$, then $S_1^{-1} S_2^{-1} \sim S_2$.

Proof. The first statement follows from line (3.10). Then $S_1^{-1} S_2^{-1} \sim S_1 S_2 = S_2$.

(3.12) Lemma. If R and N are as in (3.6), then for each $s = 1, \dots, n$,

$$\mathcal{O}_{2n-s}(N) \sim R_s.$$

Proof. Since R_i is an order, $(R_i : R_i) = R_i$, and so $\mathcal{O}_1(R_i) = R_i^{-1}$ by (3.9). By (1.6), for $s = 1, \dots, n$, $\mathcal{O}_{2n-s}(N)$ is the ideal sum of all products

$$(3.13) \quad \mathcal{O}_{i_1}(R_1) \mathcal{O}_{i_2}(R_2) \cdots \mathcal{O}_{i_{n-1}}(R_{n-1}) \mathcal{O}_{i_n}(L)$$

where $0 \leq i_j \leq 2n-s$ and $\sum i_j = 2n-s$.

If $i_j = 0$ for any j , then the product (3.13) is 0. Thus we need consider only products (3.13) for which $i_j \geq 1$ for all j . At least s factors in such a product must then have $i_j = 1$, for otherwise $\sum i_j > 2(n-s+1) + 1(s-1) = 2n-s+1$. On the other hand, for any choice of exactly s distinct indices $t_1, \dots, t_s$ from among the set $\{1, \dots, n\}$, the product

$$(3.14) \quad \mathcal{O}_1(R_{t_1}) \mathcal{O}_1(R_{t_2}) \cdots \mathcal{O}_1(R_{t_s})$$

is contained in $\mathcal{O}_{2n-s}(N)$. Hence $\mathcal{O}_{2n-s}(N)$ is generated by all products of the form (3.14). Since for any choice of $t_1, \dots, t_s$, $R_1 R_2 \cdots R_s \subset R_{t_1} \cdots R_{t_s}$,

$$\mathcal{O}_1(R_1) \cdots \mathcal{O}_1(R_s) = R_1^{-1} \cdots R_s^{-1} \supset R_{t_1}^{-1} \cdots R_{t_s}^{-1} = \mathcal{O}_1(R_{t_1}) \cdots \mathcal{O}_1(R_{t_s})$$

Thus $\mathcal{O}_{2n-s}(N) = R_1^{-1} \cdots R_s^{-1} \sim R_s$.

We now complete the proof of (3.6). Any ideal class contains at most one order, by [10], Prop. 1.3.3, p. 41. Thus R_s is uniquely determined as the order in the class of $\mathcal{O}_{2n-s}(N)$, by (3.12). Since $(R_1 R_2 \cdots R_{n-1})\mathcal{L} = (R_1 R_2 \cdots R_{n-1})(R_n \mathcal{L}) = (R_1 \cdots R_{n-1} R_n)\mathcal{L} = R_n \mathcal{L} = \mathcal{L}$, the ideal class of $\mathcal{L}$ is precisely the ideal class of N .

(3.15) Theorem. Let D be a principal ideal domain and let R be a quadratic D -order in a field. Then an R -representation module is precisely a finitely generated torsion-free R -module.

Proof. Let M be an R -representation module. Then M is finitely generated as a D -module, and so all the more so as an R -module. Let k be the quotient field of D and let α' be the conjugate over k of an element α of R . $\alpha' = \text{trace}(\alpha) - \alpha$ lies in R . If $\alpha x = 0$ for some $\alpha \neq 0$ in R and some $x \in M$, then $(\alpha' \alpha)x = 0$. Since $\alpha \alpha' = \text{norm}(\alpha)$ is nonzero in D , this implies $x = 0$. Thus M is torsion-free as an R -module.

Conversely, let M be a finitely generated torsion-free R -module. Then M is torsion-free as a D -module. Since R is finitely generated over D , M is finitely generated as a D -module. Thus M is an R -representation module.

(3.16) Corollary. Let D be a principal ideal domain, K a quadratic extension field of the quotient field of D , and R a D -order in K . Assume that the integral closure of R is a finitely generated R -module. Then any D -matrix representation of R is D -equivalent to a direct sum of representations of degree 2. All but one of the summand representations

may be taken to be representations afforded by R-orders in K.

3.4 An example

Let $D = \mathbb{Z}$, let $K = \mathbb{Q}(\sqrt{-2})$, let $\theta = \sqrt{-72}$, and let $R = \mathbb{Z}[\theta]$. Then R is a quadratic order in K . There are four classes of invertible R-ideals, which are represented by the ideals $I_1 = R = (1, \theta)$, $I_2 = (4, 2 + \theta)$, $I_3 = (8, \theta)$, and $I_4 = (8, 4 + \theta)$. There are five classes of non-invertible ideals, which are represented by the ideals $I_5 = (2, \theta)$, $I_6 = (3, \theta)$, $I_7 = (4, \theta)$, $I_8 = (6, \theta)$, and $I_9 = (9, 3 + \theta)$. An R-order in K is of the form $S = (1, \theta/e)$ for $e = 1, 2, 3$, or 6 . Let $S_1 = (1, \theta/2) = \mathbb{Z}[\sqrt{-18}]$, $S_2 = (1, \theta/3) = \mathbb{Z}[\sqrt{-8}]$, and $R' = (1, \theta/6) = \mathbb{Z}[\sqrt{-2}]$. The R-order associated with an ideal $\mathcal{O}$ is $(\mathcal{O}:\mathcal{O})$. In our example, R is the order of each of the invertible ideals $I_1, \dots, I_4$; S_1 is the order of I_5 and I_7 ; S_2 is the order of I_6 and I_9 ; and R' is the order of I_8 . $I_5 \sim S_1$, $I_6 \sim S_2$, and $I_8 \sim R'$.

According to the theory of Sections 3.2 and 3.3, there are 16 isomorphism classes of rank two R-modules. The following is a set of representatives of these classes by modules in canonical form (3.2):

$$\begin{aligned} M_1 &= R \dot{+} R, & M_2 &= R \dot{+} I_2, & M_3 &= R \dot{+} I_3, & M_4 &= R \dot{+} I_4, \\ M_5 &= R \dot{+} S_1, & M_6 &= R \dot{+} I_7, & M_7 &= S_1 \dot{+} S_1, & M_8 &= S_1 \dot{+} I_7, \\ M_9 &= R \dot{+} S_2, & M_{10} &= R \dot{+} I_9, & M_{11} &= S_2 \dot{+} S_2, & M_{12} &= S_2 \dot{+} I_9, \\ M_{13} &= R \dot{+} R', & M_{14} &= S_1 \dot{+} R', & M_{15} &= S_2 \dot{+} R', & M_{16} &= R' \dot{+} R'. \end{aligned}$$

There are 25 isomorphism classes of rank 3 R-modules.

It is clear that the present method of classification of representation modules over quadratic orders in fields does not generalize to the case of representation modules over general orders of higher degree, since it depends essentially on Theorem (2.1), and the theorem of Section 2.4, paragraph (b) shows that the hypothesis of two element generation of ideals in Theorem (2.1) cannot be relaxed.

CHAPTER 4
ON REPRESENTATION MODULES OVER A QUADRATIC Z-ORDER
WITH ZERO DIVISORS

4.1 Introduction

Let R be the Z -order

$$(4.1) \quad Z[X] / Z[X] \cdot (X-a)(X-b)$$

for some $a, b \in Z$ such that $a \neq b$. R is a quadratic Z -order in the semisimple Q -algebra $Q \oplus Q$, since there is an isomorphism of R into $Q[X]/Q[X](X-a)(X-b)$, which is isomorphic to $Q[X]/Q[X](X-a) \oplus Q[X]/Q[X](X-b) \simeq Q \oplus Q$. Let g be the coset of X in (4.1). Then $R = Z[g]$ and $(g-a)(g-b) = 0$.

Any Z -matrix representation of R is completely determined by its representation of g .

Let $g \rightarrow T$ be any Z -matrix representation of g . Then as a Q -matrix representation of g , T has rational invariants u, v where u is the multiplicity of the irreducible representation $g \rightarrow [a]$ in T and v is the multiplicity of the irreducible representation $g \rightarrow [b]$ in T . The degree of T is $n = u+v$. T is Q -equivalent to the completely reduced representation $g \rightarrow \text{diag}(\underbrace{a, \dots, a}_u, \underbrace{b, \dots, b}_v)$, and the parameters u and v completely determine the Q -equivalence class of T .

In Theorem (4.3) of Section 4.2 we give a normal form for a Z -matrix representation of a quadratic order of the form (4.1). In Theorem (4.13) of Section 4.3 we show that for any class $\mathcal{C}$ of Z -matrix

representations for which the multiplicities u and v are unequal, the normal form of Theorem (4.3) is canonical, and the elementary ideals of the R -representation modules induced by representations in $\mathcal{C}$ are a complete set of invariants. We show by an example that when $u = v$, the elementary ideals are not a complete set of invariants.

The following two examples will illustrate the results to be derived.

(a) Let $a = 1$, $b = -1$ so that g satisfies $g^2 - 1 = 0$. Then with respect to multiplication, $\{1, g\}$ is the group of two elements. The Diederichsen-Reiner theorem on integral representations of cyclic groups of prime order ([9], Theorem 74.3, p. 508) asserts that a complete set of indecomposable Z -matrix representations of g is

$$(4.2) \quad g \rightarrow [1], \quad g \rightarrow [-1], \quad g \rightarrow \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix},$$

that any Z -representation of g is a direct sum of a certain number of copies of each of the representations (4.2), and that the number of summands of each type is an invariant of the representation.

(b) Let $a = 0$, $b = 5$ so $g(g-5) = 0$. Consider representations of the form

$$g \rightarrow T(e) = \begin{bmatrix} 0 & e \\ 0 & 5 \end{bmatrix}.$$

One verifies that for any e , $T(e)$ is a Z -matrix representation of g , and that for any e and e' , the representations $T(e)$ and $T(e')$ are Q -equivalent (they both have $u = v = 1$), and that the representations $T(e)$ and $T(e')$ are Z -equivalent if and only if $e' \equiv \pm e \pmod{5}$. Therefore, within Z -equivalence, e may be chosen within the set $\{0, 1, 2\}$, and any two distinct choices of e in this set give Z -inequivalent

representations. Thus there are three Z -equivalence classes of representations in the Q -class of $g \rightarrow \begin{bmatrix} 0 & e \\ 0 & 5 \end{bmatrix}$.

4.2 The normal form

To simplify notation, we first normalize the generator of the quadratic order (4.1). Let $g' = g - a$ and let $m = b - a$. Then $g' - m = g - b$ and $g'(g' - m) = 0$. $R = D[g']$. Any Z -matrix representation of R is determined by its representation of g' . Therefore we will assume henceforth that R is generated over Z by an element g which satisfies the relation $g(g - m) = 0$ for some $m \neq 0$ in Z .

(4.3) Theorem. Let R be the Z -order $Z[X]/Z[X] \cdot X(X - m)$ for some $m \neq 0$ in Z and let g be the coset of X in R . Then a complete set of indecomposable Z -matrix representations of g is

$$(4.4) \quad \begin{aligned} g &\rightarrow T_0 = [0], & g &\rightarrow T_m = [m], \\ g &\rightarrow T(e) = \begin{bmatrix} 0 & e \\ 0 & m \end{bmatrix} & \text{for } e \in \{1, 2, \dots, \lfloor \frac{|m|}{2} \rfloor\}. \end{aligned}$$

Let T be an arbitrary Z -matrix representation of g . Let u be the multiplicity of the irreducible representation T_0 in T and let v be the multiplicity of the irreducible representation T_m in T . We may assume that $u \geq v$. Then T is Z -equivalent to a representation of the form

$$(4.5) \quad g \rightarrow \begin{bmatrix} 0 & 0 & 0 & & & & 0 \\ & 0 & 0 & & & & \\ & & 0 & e_1 & & & \\ & & 0 & m_1 & & & \\ & & & 0 & e_2 & & \\ & & & 0 & m_2 & & \\ & & & & \dots & & \\ & & & & & 0 & e_v \\ & & & & & 0 & m_v \\ 0 & & & & & & \end{bmatrix}$$

in which there are $u-v$ 1×1 blocks $[0]$ and v 2×2 blocks $\begin{bmatrix} 0 & e_i \\ 0 & m^i \end{bmatrix}$ on the diagonal, and in which the e_i are positive integers which satisfy the conditions

$$(4.6) \quad \begin{aligned} e_i & \mid e_{i+1} & i = 1, \dots, v-1, \\ e_{v-1} & \mid m, & e_v \leq m. \end{aligned}$$

Further, if u is strictly greater than v , then e_v is also required to satisfy the condition

$$(4.7) \quad e_v \mid m.$$

Proof. Let T be a Z -matrix representation of g with rational invariants u, v . Let M be the R -representation module induced by T . Let $M_1 = \{ x \in M : gx = 0 \}$. The Z -rank of M_1 is u . For $x \in M_1$, $gx = 0$, so multiplication by g effects the zero map on M_1 . For $x \in M$, $(g-m)x \in M_1$, so multiplication by g effects the map m times the identity on the factor module M/M_1 . Choose a Z -basis for M_1 and extend it to a basis for M . With respect to this basis, g is represented by the matrix

$$(4.8) \quad U = \begin{bmatrix} O_u & L \\ 0 & mI_v \end{bmatrix}$$

where O_u is the $u \times u$ zero matrix, I_v is the $v \times v$ identity matrix, and L is a $u \times v$ Z -matrix. Thus T is Z -equivalent to a matrix of the form (4.8).

Let U, U' be two Z -matrix representations of g in the form (4.8) which are Z -equivalent. Then there exists a unimodular Z -matrix W which intertwines U and U' , say $WU' = UW$. We partition W in accord with U and U' , so

$$(4.9) \quad WU' = \begin{bmatrix} W_{11} & W_{12} \\ W_{21} & W_{22} \end{bmatrix} \cdot \begin{bmatrix} 0 & L' \\ 0 & mI \end{bmatrix} = \begin{bmatrix} 0 & L \\ 0 & mI \end{bmatrix} \cdot \begin{bmatrix} W_{11} & W_{12} \\ W_{21} & W_{22} \end{bmatrix} = UW$$

It follows from (4.9) that $W_{21} = 0$ and that W_{11} and W_{22} are unimodular. Then $L' = W_{11}^{-1} L W_{22} - m W_{11}^{-1} W_{12}$. Thus if U and U' are Z -equivalent representations of g , there exist Z -matrices P and Q of appropriate sizes such that $L' \equiv P L Q \pmod{m}$.

Conversely, if $L' \equiv P L Q \pmod{m}$, then $L' - PLQ = mB$ for some Z -matrix B , and so with $W_{11} = P^{-1}$, $W_{22} = Q$, and $W_{12} = W_{11}B$, the matrix $W = \begin{bmatrix} W_{11} & W_{12} \\ 0 & W_{22} \end{bmatrix}$ is unimodular, and it intertwines U and U' .

Definition. Two $u \times v$ Z -matrices L and L' are m -equivalent if there exists a unimodular $u \times u$ matrix P and a unimodular $v \times v$ matrix Q such that $L' \equiv P L Q \pmod{m}$.

We call a matrix L related to U as in (4.8) the binding matrix of U . The discussion above shows that two representations U, U' are Z -equivalent if and only if their binding matrices are m -equivalent.

For any sequence $s = (e_1, \dots, e_v)$ of integers, we define diag(s) to be the $u \times v$ Z -matrix whose i, i entry is e_i , $i = 1, \dots, v$, and whose other entries are zero.

We next develop a reduction process for $u \times v$ matrices of the form diag(s) for some sequence s .

Let Σ be the set of all sequences of positive integers of length v . For s, s' in Σ , let $s' \prec s$ if s' strictly precedes s in the lexicographical ordering of Σ . We define four types of substitution.

If one of these substitutions is applicable to a given sequence

$s = (e_1, \dots, e_v)$ of Σ , then we replace s by a new sequence $s' = (e'_1, \dots, e'_v)$ with the properties that (i) diag(s') is m -equivalent to diag(s), and (ii) $s' \prec s$. Because of property (i), the Z -matrix representation U whose binding matrix is diag(s) is then Z -equivalent to a new

representation U' whose binding matrix is $\text{diag}(s')$.

Substitutions:

- (a) If $e_i > m$ for some i , then let $e_i' = e_i - m$, $e_k' = e_k$ for $k \neq i$.
 (b) If $e_i \nmid e_{i+1}$ for some $1 \leq i \leq v-1$, then let $d = \text{g.c.d.}(e_i, e_{i+1})$,
 let $e_i' = d$, $e_{i+1}' = e_i e_{i+1} / d$, $e_k' = e_k$ for $k \neq i, i+1$.

Since there exist unimodular matrices P, Q such that
 $\text{diag}(s') = P \text{diag}(s) Q$, we see that $\text{diag}(s')$ is indeed
 m -equivalent to $\text{diag}(s)$.

- (c) Suppose $e_{v-1} \mid e_v$ and $e_{v-1} \nmid m$. Let $d = \text{g.c.d.}(e_{v-1}, m)$.
 Then since $e_{v-1} \mid e_v$, $d = \text{g.c.d.}(e_{v-1}, e_v + m)$. The matrix
 $D = \text{diag}(e_1, \dots, e_{v-1}, e_v + m)$ is m -equivalent to $\text{diag}(s)$.
 Then by substitution (b), there is some e_v' such that for
 the sequence $s' = (e_1, \dots, e_{v-2}, d, e_v')$, $\text{diag}(s')$ is m -equivalent
 to D . Then s' is the desired final sequence of this
 substitution.

- (d) Suppose that $u > v$ and $e_v \nmid m$. For notational simplicity,
 let $f = e_v$. Let $d = \text{g.c.d.}(f, m)$, $f = df_1$, $m = dm_1$, and
 let $l = f_1 s + m_1 t$ for some $s, t \in \mathbb{Z}$. $\text{Diag}(s)$ is m -equivalent
 to the matrix

$$D = \begin{pmatrix} e_1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & e_{v-1} & 0 \\ 0 & \dots & 0 & f \\ 0 & \dots & 0 & m \\ \vdots & & \vdots & \vdots \\ 0 & & 0 & 0 \end{pmatrix} \left. \vphantom{\begin{pmatrix} e_1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & e_{v-1} & 0 \\ 0 & \dots & 0 & f \\ 0 & \dots & 0 & m \\ \vdots & & \vdots & \vdots \\ 0 & & 0 & 0 \end{pmatrix}} \right\} \begin{matrix} v\text{th and } (v+1)\text{st} \\ \text{rows} \end{matrix}$$

Let P be the $u \times u$ matrix

$$\begin{pmatrix} 1 & & & & & & 0 \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & s & t & & \\ & & & -m_1 & f_1 & & \\ & & & & & 1 & \\ 0 & & & & & & 0 \end{pmatrix}$$

in which the indicated 2×2 block occurs in the v th and $(v+1)$ st rows and columns. P is unimodular. The product PD is the same as D except that in PD the 2×2 block $\begin{bmatrix} 0 & f \\ 0 & m \end{bmatrix}$ of D is replaced by

$$\begin{bmatrix} s & t \\ -m_1 & f_1 \end{bmatrix} \begin{bmatrix} 0 & f \\ 0 & m \end{bmatrix} = \begin{bmatrix} 0 & sf+tm \\ 0 & -fm_1+f_1m \end{bmatrix} = \begin{bmatrix} 0 & d \\ 0 & 0 \end{bmatrix}.$$

The sequence s' defined by $e_v' = d$ and $e_k' = e_k$ for $k \neq v$ is to be the final sequence of this substitution.

Repeated application of the four types of substitution transforms an original sequence s into a new one s' which is capable of no further reduction, and so which satisfies the conditions (4.6), if $u = v$, and (4.6) together with (4.7), if $u > v$.

Now let T be a $\mathbb{Z}$ -matrix representation of g with rational invariants $u, v, u \geq v$. T is $\mathbb{Z}$ -equivalent to a matrix U of the form (4.8). The binding matrix L of U is equivalent to a matrix $\text{diag}(s)$ for some sequence $s = (e_1, \dots, e_v)$ of nonnegative integers e_i . We add m to any of the entries e_i which are 0. Thus L is m -equivalent to a matrix $\text{diag}(s')$ for some sequence s' of positive integers. Next we apply the reduction process above to conclude that $\text{diag}(s')$ is m -equivalent to the matrix $\text{diag}(s'')$ of a sequence s'' whose entries satisfy the conditions (4.6), or (4.6) and (4.7) if $u > v$. Embed $\text{diag}(s'')$ as a binding matrix in a matrix U' of the form (4.8). Then conjugation of U' by an obvious permutation matrix gives the desired form (4.5) of a matrix $\mathbb{Z}$ -equivalent to T .

From the normal form (4.5), it is clear that indecomposable representations of g can only be of degrees one and two. It is easily checked that the representations (4.4) are a complete set of indecomposable representations.

The conclusion of the lemma follows immediately by considering the two cases $t < v$ and $t = v$.

(4.13) Theorem. Let T be a Z -matrix representation of g in normal form (4.5). Then the entries $e_1, e_2, \dots, e_{v-1}$ of T and the number $e_0 = \text{g.c.d.}(e_v, m)$ are uniquely determined by the elementary ideals of the R -representation module induced by T , and hence by the Z -equivalence class of T . Thus, if $u > v$, the form (4.5), subject to the conditions (4.6) and (4.7) on the e_i , is canonical, and the elementary ideals are a complete set of invariants.

Proof. T represents the generator g of R on a Z -basis for the R -representation module M which it induces. Thus by (1.8), the elementary ideals δ_i of M may be computed according to the formula $\delta_i = D_i(T - gI) = D_i(B)$, where B is the matrix (4.11).

By Lemma (4.10), for $t < v$, $\mathcal{O}_t = (e_1 e_2 \dots e_t, g e_1 \dots e_{t-1})$, and $\mathcal{O}_v = (e_1 e_2 \dots e_{v-1} e_0, g e_1 \dots e_{v-1})$. Thus

$$\mathcal{O}_t \cap Z = \begin{cases} Ze_1 \dots e_t, & t < v, \\ Ze_1 \dots e_{v-1} e_0, & t = v. \end{cases}$$

Hence $Ze_i = (\mathcal{O}_i \cap Z) : (\mathcal{O}_{i-1} \cap Z) = (\delta_{n-i} \cap Z) : (\delta_{n-i+1} \cap Z)$, $i < v$,

and $Ze_0 = (\mathcal{O}_v \cap Z) : (\mathcal{O}_{v-1} \cap Z) = (\delta_{n-v} \cap Z) : (\delta_{n-v+1} \cap Z)$.

Thus the $e_1, \dots, e_{v-1}, e_0$ are uniquely determined as the positive generators of the ideals Ze_i and Ze_0 , respectively.

The following example (example (b) of Section 4.1) shows that when $u = v$, the elementary ideals do not in general completely determine the Z -equivalence class of a representation.

Let $m = 5$, $T(1) = \begin{bmatrix} 0 & 1 \\ 0 & 5 \end{bmatrix}$, $T(2) = \begin{bmatrix} 0 & 2 \\ 0 & 5 \end{bmatrix}$. These two representations are Z -inequivalent, but both associated representation modules have elementary ideals $\delta_0 = 0$ and $\delta_i = R$ for $i \geq 1$.

CHAPTER 5

ON FIXED-POINT-FREE AUTOMORPHISMS OF MODULES

5.1 Introduction

An automorphism α of a group G is fixed-point-free if $\alpha g = g$ for $g \in G$ implies that g is the identity element of G . An automorphism α of a module M is fixed-point-free if $\alpha x = x$ for $x \in M$ implies $x = 0$. The order of α is the order of α in the group of all automorphisms of the module.

Fixed-point-free automorphisms of groups are of interest in connection with Frobenius groups, and a result of John Thompson [33] states that a finite group with a fixed-point-free automorphism of prime order is nilpotent. Other results on algebraic systems with fixed-point-free automorphisms have been obtained by Neumann [25], G. Higman [19], and Patterson [28].

Under certain restrictions on a principal ideal domain D and rational prime number q , we establish here two basic results. Let θ be a q th root of unity over the quotient field of D , and let $R = D[\theta]$. Then under certain conditions on the module M , we determine in Theorem (5.3) of Section 5.2 the D -module structure of a finitely generated R -module M . This theorem is used in the proof of Theorem (5.6) of Section 5.3, which gives necessary and sufficient conditions for a finitely generated D -module M to admit a fixed-point-free automorphism of order q .

The restrictions on the principal ideal domain D and prime number q are satisfied for any q when $D = \mathbb{Z}$. Thus Theorem (5.6) without restriction determines necessary and sufficient conditions for a finitely generated abelian group to admit a fixed-point-free automorphism.

5.2 The D -module structure of a finitely generated R -module

Definition. Let us call a pair (D, q) consisting of a principal ideal domain D and a rational prime number q compatible if D and q satisfy the following two conditions, in which k is the quotient field of D :

(i) the cyclotomic polynomial Φ_q of order q is irreducible over

k , and

(ii) $D[\theta]$ is integrally closed, where θ is a root of Φ_q over k .

Throughout this chapter, whenever (D, q) is a compatible pair, the symbols R , K , P and (π) have the following meanings: $R = D[\theta]$ and $K = k(\theta)$. If P is a prime ideal of R , then (π) is the contraction of P in D .

Since K over k is a normal extension, the primes of R which lie over (π) are all conjugate and we may unambiguously write $f(\pi)$ for the relative degree of P over (π) ([35], Theorem 22, p. 289).

K is also a separable extension of k , R is the ring of D -integers in K , and R has a D -basis $\{1, \theta, \dots, \theta^{q-2}\}$. R is Dedekind. The different $\mathcal{D}_{R/D}$ of R over D is Rq^{q-2} by [35], Theorem 29, p. 303, and the computation on p. 314. Thus a prime ideal P of R is ramified if and only if $q \in P$ ([35], Corollary, p. 303).

(5.1) Theorem. Let (D, q) be a compatible pair and let P be a prime ideal of R which does not contain q . Then $M = R/P^n$ considered as a D -module is isomorphic to the direct sum of $f(\pi)$ copies of $D/(\pi)^n$.

Proof. Let $x \in R$. Then $\pi^n x \in P^n x \subset P^n$ so the order of the coset $\bar{x}$ of x in R/P^n divides $(\pi)^n$.

Lemma. Let $u_1, \dots, u_f$ be elements of R whose cosets in R/P are linearly independent over $D/(\pi)$. Then for any $m = 1, 2, 3, \dots$, if $\sum a_i u_i \equiv 0 \pmod{P^m}$ for some $a_i \in D$, then necessarily $a_i \equiv 0 \pmod{\pi^m}$ for each $i = 1, \dots, f$.

Proof. For $m = 1$ this follows from the choice of the u_i . Suppose the lemma is true for an integer m , $m > 1$, and let $\sum a_i u_i \equiv 0 \pmod{P^{m+1}}$. Then $\sum a_i u_i \equiv 0 \pmod{P^m}$ whence $a_i \equiv 0 \pmod{\pi^m}$ for each i . Let $a_i = \pi^m b_i$ for some $b_i \in D$. Then $\sum a_i u_i = \pi^m \sum b_i u_i \equiv 0 \pmod{P^{m+1}}$. Thus since P is unramified over (π) , P^m exactly divides π^m and thus $\sum b_i u_i \equiv 0 \pmod{P}$. Let $b_i = \pi c_i$ for some $c_i \in D$. Then $a_i = \pi^{m+1} c_i \equiv 0 \pmod{\pi^{m+1}}$, for each $i = 1, \dots, f$.

We continue with the proof of the theorem. Let $u_1, \dots, u_f$ be elements of R whose cosets in R/P are linearly independent over $D/(\pi)$. For $u \in R$, let $\bar{u}$ be the coset of u in R/P^n . Let $M_0 = R\bar{u}_1 + \dots + R\bar{u}_f$. Then

$$(5.2) \quad M_0 \simeq \sum D/(\pi)^n \quad (\text{direct sum of } f \text{ copies}).$$

By (5.2) the invariant factors of M_0 are $(\pi)^n$, repeated f times. Thus, by (1.22), the order of M_0 as a D -module is $(\pi)^{fn}$. On the other hand, a normal series for the D -module M is

$$M = R/P^n \supset P/P^n \supset \dots \supset P^n/P^n = 0$$

The i th factor module of this series is

$$(P^{i-1}/P^n)/(P^i/P^n) \simeq P^{i-1}/P^i \simeq R/P.$$

There are n such factors, and $\text{ord}(R/P) = (\pi)^f$. Thus $\text{ord}(M) = (\pi)^{fn} = \text{ord}(M_0)$. Since $M_0 \subset M$, this implies $M = M_0$. This completes the proof of (5.1).

(5.3) Theorem. Let (D, q) be a compatible pair and let M be a finitely generated D -module. Then M admits the structure of an R -module for which the P -primary submodule is 0 for any ramified prime ideal P of R , if and only if the D -module structure of M satisfies the following three conditions:

- (i) $q-1$ divides the rank of M ,
- (ii) if π is an irreducible element of D and if (π) ramifies in R , then no power of (π) occurs as an elementary divisor of M ,
- (iii) if π is an irreducible element of D and if (π) is unramified in R , and if $f(\pi)$ is the relative degree of any prime ideal of R lying over (π) , then for each $n = 1, 2, 3, \dots$, the number of times that $(\pi)^n$ occurs as an elementary divisor of M is a multiple of $f(\pi)$.

Proof. Suppose M admits the structure of an R -module for which the P -primary submodule is 0 for any ramified prime ideal P of R . Then as an R -module M is isomorphic to a direct sum of indecomposable R -modules, i.e., of R -ideals and of cyclic primary torsion R -modules, by (1.10), (1.13), and (1.19).

A decomposition of M as a direct sum of indecomposable D -modules is obtained from a decomposition of M as a direct sum of R -modules by decomposing the R -module summands. Clearly R -ideals and only R -ideals contribute free D -summands. For each prime ideal (π) of D , P -primary summands for all primes P of R which lie over (π) , and only such R -module summands, contribute to the (π) -primary submodule of M as a D -module.

An R -ideal $\mathcal{O}$ is a free D -module of rank $q-1$. Hence $q-1$ divides the rank of M as a D -module.

If (π) ramifies in R , then the P -primary submodule of M as an R -module is 0, for any prime P which lies over (π) , and thus the (π) -primary submodule of M as a D -module is 0. This proves (ii).

If (π) is unramified in R , then each R -module of the form R/P^n contributes $f(\pi)$ summands each with order $(\pi)^n$. This holds for all P lying over (π) . Thus the total number of summands of order $(\pi)^n$, which is to say, the number of times $(\pi)^n$ occurs as an elementary divisor of M as a D -module, is a multiple of $f(\pi)$.

Conversely, if the D -module invariants of M satisfy the conditions (i), (ii), (iii), then one may collect together sets of $q-1$ free cyclic summands, and to each set assign the structure of an R -ideal. One collects together sets of $f(\pi)$ summands of order $(\pi)^n$, and assigns the structure of R/P^n for some prime P which lies over (π) . The action of θ on the total module is defined componentwise. Since no summands $D/(\pi)^n$ occur in M as a D -module for any prime (π) of D which ramifies in R , then for any P of R which is ramified, the P -primary submodule of M as an R -module is zero.

5.3 Conditions for a D-module to admit a fixed-point-free automorphism

We recall that if R is a ring and M is an R -module, an element $\beta \in R$ is a zero divisor with respect to M if $\beta x = 0$ for some $x \neq 0$ in M .

(5.4) Theorem. Let (D, q) be a compatible pair and let M be a nonzero finitely generated D -module. Then M admits a fixed-point-free automorphism of order q if and only if M admits the structure of an R -module for which $1-\theta$ is not a zero divisor with respect to M .

Proof. $\Rightarrow$: Let α be a fixed-point-free automorphism of M of order q . Let $D[X]$ be the polynomial domain in one indeterminate over D . We make M into a $D[X]$ -module by defining $f(X) \cdot m = f(\alpha)m$ for $f(X) \in D[X]$ and $m \in M$. Since α is fixed-point-free, if $(1-X)m = 0$ for some $m \in M$, then $m = 0$. Thus for any $m \in M$, $(1-X)\bar{\Phi}_q(X)m = (1-X^q)m = 0$ and so $\bar{\Phi}_q(X)m = 0$. Thus $\bar{\Phi}_q(X)$ annihilates M . Thus M is a module over $D[X]/D[X] \cdot \bar{\Phi}_q(X) \simeq D[\theta]$ under the definition

$$\theta \cdot m = \{X + D[X] \cdot \bar{\Phi}_q(X)\} \cdot m = Xm.$$

Then also if $(1-\theta)m = 0$ for some $m \in M$, then $m = 0$. Thus $1-\theta$ is not a zero divisor with respect to M .

$\Leftarrow$: Let M be an R -module for which $1-\theta$ is not a zero divisor with respect to M . Let $\alpha \in \text{Hom}_D(M, M)$ be defined by $\alpha \cdot m = \theta m$ for $m \in M$. Then $\alpha^q m = \theta^q m = 1 \cdot m = m$ for any $m \in M$ so α^q is the identity automorphism of M . Let $m \neq 0$ in M . Then $(1-\theta)m \neq 0$ so $\alpha m \neq m$. Thus α is fixed-point-free and has order q .

If an R -module M is a direct sum of R -submodules M_i , and if $\beta \in R$, then β is a zero divisor with respect to M if and only if it is a zero divisor with respect to M_i for some i .

(5.5) Lemma. Let (D, q) be a compatible pair and let P be a prime ideal of R . Then $(1 - \theta)$ is a zero divisor with respect to the R -module R/P^n if and only if $q \in P$.

Proof. We first observe that $q = \prod_{i=1}^{q-1} (1 - \theta^i) = u(1 - \theta)^{q-1}$ where u is a unit of R ([35], p. 314). Thus $q \in P$ if and only if $1 - \theta \in P$.

The order of any nonzero element of R/P^n as an R -module is a power of P . If $\bar{x} \neq 0$ in R/P^n and $(1 - \theta)\bar{x} = 0$ then $1 - \theta \in \text{ord}(\bar{x})$ and so $1 - \theta \in P$. Hence $q \in P$.

If $q \in P$ then $1 - \theta \in P$. Let $x \in P^{n-1}$, $x \notin P^n$. Then $\bar{x} \neq 0$ in R/P^n but $(1 - \theta)\bar{x} = 0$, so $1 - \theta$ is a zero divisor with respect to R/P^n .

(5.6) Theorem. Let (D, q) be a compatible pair and let M be a nonzero finitely generated D -module. Then M admits a fixed-point-free automorphism of order q if and only if the D -module structure of M satisfies the three conditions:

- (i) $q-1$ divides the rank of M ,
- (ii) if π is an irreducible element of D and if (π) ramifies in R , then no power of (π) occurs as an elementary divisor of M ,
- (iii) if π is an irreducible element of D and if (π) is unramified in R , and if $f(\pi)$ is the relative degree of any prime ideal of R lying over (π) , then for each $n = 1, 2, 3, \dots$, the number of times that $(\pi)^n$ occurs as an elementary divisor of M is a multiple of $f(\pi)$.

Proof. The theorem follows from (5.3), (5.4), and (5.5).

Remark. Theorem (5.6) furnishes necessary and sufficient conditions for a finitely generated abelian group to admit a fixed-point-free automorphism of prime order, since for any rational prime q , (Z, q) is a compatible pair.

5.4 Further observations

(a) That condition (ii) of the definition of compatible pair cannot be omitted without altering the definition is shown by the following example of a principal ideal domain D and prime number q for which Φ_q is irreducible but $D[\theta]$ is not integrally closed.

Let $D = Z[\sqrt{3}]$ and let $q = 3$. If $\Phi_3(X) = X^2 + X + 1$ were reducible over D , then it would have a linear factor $g(X) = X + \alpha$ for some $\alpha \in D$. Then $g(0)$ would divide $\Phi_3(0) = 1$ and $g(-1)$ would divide $\Phi_3(-1) = 1$, so both α and $-1 + \alpha$ would be units in D . The fundamental unit of D is $\epsilon = 2 + \sqrt{3}$. Suppose $\alpha = \pm \epsilon^a$, for some $a \in Z$, then $-1 - \alpha = -1 \pm \epsilon^a = \pm \epsilon^b$ for some $b \in Z$, so $\pm \epsilon^a \pm \epsilon^b = 1$ for some choice of signs. But this is impossible. Thus Φ_3 is irreducible over D .

$D[\theta] = D + D\theta$ is not integrally closed in its quotient field for $\omega = (2 + \theta)/\sqrt{3}$ is a D -integer which does not lie in D . (The irreducible polynomial of ω is $X^2 - \sqrt{3}X + 1$.)

(b) If (D, q) is a compatible pair and if M is a finitely generated D -module and α a fixed-point-free automorphism of M of order q , then we denote by $M^{(\alpha)}$ the R -module whose additive group is M and for which the action of θ on M is defined as in the proof of Theorem (5.4).

(5.7) Theorem. Let (D, q) be a compatible pair and let M be a finitely generated D -module. Let α, β be fixed-point-free automorphisms

of M of order q , and let $M^{(\alpha)}$, $M^{(\beta)}$ be the corresponding R -modules. Then α and β are conjugate to one another in the group of all automorphisms of M if and only if $M^{(\alpha)}$ and $M^{(\beta)}$ are isomorphic as R -modules.

Proof. Suppose $\beta = \gamma\alpha\gamma^{-1}$ for some automorphism γ of M . Then $\beta\gamma = \gamma\alpha$. Let $\tilde{\gamma}: M^{(\alpha)} \rightarrow M^{(\beta)}$ by $\tilde{\gamma}(x) = \gamma(x)$ for $x \in M^{(\alpha)}$. Then $\tilde{\gamma}$ is an R -isomorphism onto $M^{(\beta)}$. For $\tilde{\gamma}(\theta x) = \tilde{\gamma}(\alpha x) = \gamma\alpha x = \beta\gamma x = \beta\tilde{\gamma}(x) = \theta\tilde{\gamma}(x)$.

Conversely, if α, β , $M^{(\alpha)}$, $M^{(\beta)}$ are as above and if $\delta: M^{(\alpha)} \rightarrow M^{(\beta)}$ is an R -isomorphism onto $M^{(\beta)}$, then let $\hat{\delta}$ be the automorphism of the D -module M defined by $\hat{\delta}(x) = \delta(x)$ for $x \in M^{(\alpha)}$. Then $\hat{\delta}\alpha x = \hat{\delta}(\theta x) = \delta(\theta x) = \theta\delta(x) = \beta\hat{\delta}(x)$ for all $x \in M$, whence $\hat{\delta}\alpha = \beta\hat{\delta}$.

In consequence of (5.7), the number of conjugacy classes of fixed-point-free automorphisms of order q in the group of automorphisms of a finitely generated D -module M is equal to the number of non-isomorphic R -module structures which can be imposed on M . By separate examination of the free and primary components of M , that number can be easily determined.

BIBLIOGRAPHY

1. Auslander, M. and O. Goldman, Maximal Orders, Trans. Amer. Math. Soc., 97 (1960), 1-24.
2. Bass, H., Finitistic Dimension and a Homological Generalization of Semi-primary Rings, Trans. Amer. Math. Soc., 95 (1960), 466-488.
3. _____, Injective Dimension in Noetherian Rings, Trans. Amer. Math. Soc., 102 (1962), 18-29.
4. _____, On the Ubiquity of Gorenstein Rings, Math. Z., 82 (1963), 8-28.
5. _____, Torsion Free and Projective Modules, Trans. Amer. Math. Soc., 102 (1962), 319-327.
6. Bourbaki, N., Algèbre Commutative, Chapters 1 and 2, Fascicule XXVII, Éléments de Mathématique, Hermann, Paris, 1961.
7. Cartan, H. and S. Eilenberg, Homological Algebra, Princeton Univ. Press, Princeton, 1956.
8. Cohen, I.S., Commutative Rings with Restricted Minimum Condition, Duke Math. J., 17 (1950), 27-42.
9. Curtis, C.W. and I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Interscience, New York, 1962.
10. Dade, E.C., O. Taussky, and H. Zassenhaus, On the Theory of Orders, in particular on the Semigroup of Ideal Classes and Genera of an Order in an Algebraic Number Field, Math. Ann., 148 (1962), 31-64.

11. Dedekind, R., Über die Anzahl der Ideal-Klassen in den
verschiedenen Ordnungen eines endlichen Körpers, Festschrift
Technische Hochschule Braunschweig 1877; Reprinted in: Richard
Dedekind: Gasammelte mathematische Werke, Vol. I, Braunschweig,
1930, 105-158.
12. Deuring, M., Algebren, (reprinted from the Ergebnisse der Mathematik
series, Vol. 4, Springer, Berlin, 1935), Chelsea, New York, 1948.
13. Diederichsen, F.E., Über die Ausreduktion ganzzahliger Gruppen-
darstellungen bei arithmetischer Äquivalenz, Hamb. Abh., 13 (1940),
357-412.
14. Dieudonné, J., Remarks on Quase-Frobenius Rings, Illinois J. Math.,
2 (1958), 346-354.
15. Fitting, H., Die Determinantenideale eines Moduls, Jber. Deutsch.
Math.-Verein., 46 (1936), I. Abt., 195-228.
16. Grell, H., Verzweigungstheorie in allgemeinen Ordnungen algebraischer
Zahlkörper, Math. Z., 40 (1936), 629-657.
17. _____, Zur Theorie der Ordnungen in algebraischen Zahl- und
Funktionskörpern, Math. Ann., 97 (1926-27), 524-558.
18. Gröbner, W., Über irreduzible Ideale in kommutativen Ringen, Math.
Ann., 110 (1934), 197-222.
19. Higman, G., Groups and Rings Having Automorphisms without Non-trivial
Fixed Elements, J. London Math. Soc., 32 (1957), 321-334.
20. Jacobson, N., Lectures in Abstract Algebra, Vol. II, Van Nostrand,
Princeton, 1953.
21. Jans, J. P., Duality in Noetherian Rings, Proc. Amer. Math. Soc.,
12 (1961), 829-835.

22. Kaplansky, I., Modules over Dedekind Rings and Valuation Rings,
Trans. Amer. Math. Soc., 72 (1952), 327-340.
23. MacLane, S., Homology, Springer, Berlin, 1963.
24. Nagata, M., Local Rings, Interscience, New York, 1962.
25. Neumann, B.H., Groups with Automorphisms that Leave only the Neutral
Element Fixed, Arch. Math., 7 (1956), 1-5.
26. Northcott, D.G., An Introduction to Homological Algebra, Cambridge
University Press, Cambridge, 1960.
27. _____, Prime Ideals and Dedekind Orders, Proc. Lond. Math. Soc.,
(3) 10 (1960), 480-496.
28. Patterson, E.M., On Regular Automorphisms of Certain Classes of
Rings, Quart. J. Math.-Oxford Ser., 12 (1961), 127-133.
29. Reiner, I., Integral Representations of Cyclic Groups of Prime
Order, Proc. Amer. Math. Soc., 8 (1957), 142-146.
30. Roquette, P., Über den Singularitätsgrad von Teilringen in
Funktionskörpern, Math. Z., 77 (1961), 228-240.
31. Steinitz, E., Rechteckige Systeme und Moduln in algebraischen
Zahlkörpern I, Math. Ann., 71 (1911-1912), 328-354.
32. _____, Rechteckige Systeme und Moduln in algebraischen
Zahlkörpern II, Math. Ann., 72 (1912), 297-345.
33. Thompson, J., Finite Groups with Fixed-point-free Automorphisms
of Prime Order, Proc. Nat. Acad. Sci. U.S.A., 45 (1959), 578-581.
34. van der Waerden, B.L., Modern Algebra, Vol. II, (trans. by T. Benac
from the 2nd German Ed.), Ungar, New York, 1950.
35. Zariski, O. and P. Samuel, Commutative Algebra, Vol. I, Van Nostrand,
Princeton, 1958.

36. Zassenhaus, H., Neuer Beweis der Endlichkeit der Klassenzahl bei unimodularer Äquivalenz endlicher ganzzahliger Substitutionsgruppen, Hamb. Abh., 12 (1938), 276-288.
37. _____, The Representations of Lie Algebras of Prime Characteristic, Proc. Glasgow Math. Assn., 2 (1954), 1-36.
38. _____, The Theory of Groups, 2nd Ed., Chelsea, New York, 1958.