

LONDON MATHEMATICAL SOCIETY MONOGRAPHS

NEW SERIES

Previous volumes of the LMS Monographs were published by Academic Press, to whom all enquiries should be addressed. Volumes in the New Series will be published by Oxford University Press throughout the world.

NEW SERIES

1. *Diophantine inequalities* R. C. Baker
2. *The Schur multiplier* Gregory Karoillovsky
3. *Existentially closed groups* Graham Higman and Elizabeth Scott
4. *The asymptotic solution of linear differential systems* M. S. P. Eastham
5. *The restricted Burnside problem* Michael Vaughan-Lee
6. *Pluripotential theory* Maciej Kumek
7. *Free Lie algebras* Christophe Reutenauer
8. *The restricted Burnside problem (2nd edition)* Michael Vaughan-Lee
9. *The geometry of topological stability* Andrew du Plessis and Terry Wall
10. *Spectral decompositions and analytic sheaves* J. Eschmeier and M. Putinar
11. *An atlas of Brauer characters* C. Jansen, K. Lux, R. Parker, and R. Wilson
12. *Fundamentals of semigroup theory* John M. Howie
13. *Area, lattice points, and exponential sums* M. N. Huxley
14. *Super-real fields* H. Garth Dales and W. Hugh Woodin
15. *Integrability, self-duality and twistor theory* L. J. Mason and N. M. J. Woodhouse
16. *Categories of symmetries and infinite-dimensional groups* Yu. A. Neretin
17. *Interpolation, identification, and sampling* Jonathan R. Partington
18. *Metric number theory* Glyn Harman
19. *Profinite groups* John S. Wilson
20. *An introduction to local spectral theory* Kjeld B. Laursen and Michael M. Neumann
21. *Characters of finite Coxeter groups and Iwahori-Hecke algebras* M. Geck and G. Pfeiffer
22. *Classical harmonic analysis and locally compact groups* Hans Reiter and Jan D. Stegeman
23. *Operator spaces* E. G. Effros and Z.-J. Ruan
24. *Banach algebras and automatic continuity* H. G. Dales
25. *The mysteries of the real prime* M. J. Shai Haran
26. *Analytic theory of polynomials* Q. I. Rahman and G. Schmeisser
27. *The structure of groups of prime power order* C. R. Leedham-Green and S. McKay
28. *Maximal orders* I. Reiner (reissue)
29. *Harmonic morphisms between Riemannian manifolds* P. Baird and J. C. Wood

Maximal Orders

I. Reiner

University of Illinois

CLARENDON PRESS • OXFORD

2003

Preface

The theory of maximal orders originates in the work of Dedekind, who studied the factorization properties of ideals of R , where R is a ring of algebraic integers in an algebraic number field K . As shown by Dedekind, the factorization theory is especially simple in the extreme case where R is the ring of *all* algebraic integers in K . This ring is in fact the unique maximal \mathbb{Z} -order in K .

In this book we shall consider the generalization of Dedekind's ideal theory to the case of maximal R -orders in separable K -algebras. The entire theory reduces almost immediately to the case of a maximal R -order Λ in a central simple K -algebra A . It turns out that there are *two* ideal theories, one concerned with two-sided ideals, the other with one-sided ideals. The two-sided theory is easier, since the group of two-sided fractional Λ -ideals in A is the free abelian group generated by the prime ideals of Λ . The difficulty in the one-sided theory is that a left Λ -ideal in A is also a right Λ' -ideal, where Λ' is some other maximal order in A . It is therefore necessary to consider the set of normal ideals in A , namely all one-sided ideals relative to the various possible maximal orders in A . These normal ideals need not form a group, and instead constitute the Brandt groupoid of A .

The deeper aspects of the theory of maximal orders depend on properties of central simple algebras over local and global fields. Many of these deeper results, such as splitting theorems, the theory of the different and discriminant, reduced norms, and so on, become almost trivial in the commutative case.

The theory of maximal orders is of interest in its own right, and is essentially the study of "noncommutative arithmetic". The beauty of the subject stems from the fascinating interplay between the arithmetical properties of orders, and the algebraic properties of the algebras containing them. Apart from aesthetic considerations, however, this theory provides an excellent introduction to the general theory of orders (maximal or not). Questions involving integral representations of groups, and those concerned with matrices with integer entries, often reduce to the study of non-maximal orders. Many problems can be handled by embedding such orders in maximal orders, and then using known facts on maximal orders.

One aim of this book is to present, in as self-contained a fashion as practicable, most of the basic algebraic techniques needed for the study of orders,

maximal or not. The subject matter is arranged in the form of a textbook, on the level of a second-year graduate course. The exercises at the end of each section are an integral part of the book. In many cases, the results of the exercises will be needed later in the book, and occasionally are needed within the section itself. For this reason, detailed hints are given for many exercises.

The reader is expected to be familiar with basic facts from module theory and algebraic number theory, such as those given in the introductory chapters of Curtis-Reiner [1]. We have included, for the convenience of the reader, a lengthy chapter on algebraic preliminaries. This chapter provides brief surveys of topics needed later in the book, and may be skimmed quickly in a first reading. Proofs are often omitted in sections 1–5, especially when long or computational. In the rest of the book, from section 6 on, proofs are given in detail. The only exceptions are the Hasse Norm Theorem and the Grunwald-Wang Theorem; these are stated without proof, since otherwise several additional chapters would become necessary.

This book is intended as an introduction to maximal orders, and no attempt has been made to compile an encyclopedic treatise, or to provide the historical background of each result. Our approach draws heavily from that in Deuring [1], and benefits from the numerous simplifications in Swan-Evans [1]. We have not covered any of the analytic theory, which is readily available in the excellent book by Weil [1]. We have also omitted the theory of Asano orders, which would require a book of its own. In many ways, the theory of orders merges into the vast topic of algebras over commutative rings. Among the many references on this subject, we may mention the fine books by Bass [1], DeMeyer-Ingraham [1], Kaplansky [1], and Matsumura [1].

Sections are numbered consecutively throughout the book. A list of permanent notation precedes Chapter 1. Boldface “**Theorem**” indicates that the theorem is one of the major results proved in the book. We have distributed such honors lavishly—there are about 50 such results in the book!

This book divides naturally into three parts. The first part consists of the preliminary material in Chapter 1, which may be skimmed in a first reading, together with some generalities on orders in Chapter 2. The second part, Chapters 3–6, deals mainly with the ideal theory of maximal orders. In Chapter 3 we consider such orders in skewfields, in the complete local case. The Morita correspondence, explained in Chapter 4, is used in Chapter 5 to study maximal orders in central simple algebras in the local case. The local results are then applied in Chapter 6 to obtain the global theory. Many of the techniques developed in this book are useful for the theory of non-maximal orders. Thus, for example, Chapter 6 contains a proof of the Jordan-Zassenhaus Theorem and a discussion of genus for arbitrary orders. We may

also mention the proof of the Krull–Schmidt Theorem in section 6 for algebras over local rings.

The final third of the book covers the deeper theory of central simple algebras over global fields, and maximal orders in such algebras. Chapter 7 treats Brauer groups, crossed-product and cyclic algebras. The results of Chapter 7 are combined with the Hasse Norm Theorem and Grunwald–Wang Theorem in Chapter 8, to derive some of the major theorems on simple algebras over global fields. In particular, Eichler’s Theorem is proved in Chapter 8, and is used to calculate the ideal class group of a maximal order.

Chapter 8 also contains an introduction to Fröhlich’s theory of Picard groups of orders, and a discussion of locally free class groups of non-maximal orders. The last chapter deals with hereditary orders, which are in a sense not much harder to handle than maximal orders. Chapter 9 also includes some miscellaneous facts about group rings.

This book is based on class notes for courses given at the University of Illinois in 1969 and 1973. I would like to thank Janet Largent and Melody Armstrong for their excellent work in typing these class notes. My thanks also go to the members of the classes who helped with the proofreading, and corrected errors in the notes. I especially thank Robert L. Long, who read the entire manuscript with great care and attention; he deserves credit for catching innumerable mistakes in printing and in the mathematical content. His suggestions have helped clarify the presentations. Finally I am glad to thank my wife Irma, not only for her advice on the contents and style of the book, and her help in its preparation, but also for her constant encouragement and support.

It is also a pleasure to acknowledge with thanks the financial support I received from the National Science Foundation and the Science Research Council, during part of the time when the book was being written.

November, 1974

Irving Reiner

Acknowledgements

I would like to express my deep appreciation to Colin J. Bushnell, Charles W. Curtis, the late Albrecht Fröhlich, Gerald J. Janusz, Tsit-Yuen Lam, Judith M. McCulloh, Leon R. McCulloh, Jürgen Ritter, Joseph J. Rotman, Martin J. Taylor, and other colleagues, all of whom, in various ways, have provided support and encouragement for this reissuance of *Maximal Orders*. My appreciation goes also to the London Mathematical Society and to Oxford University Press. Alison Jones, Ruth Walker, and Anne Moorhead at the Press deserve special thanks for their gracious professionalism. I wish very much that Irv could have seen this reprinting; I know that he would have been very pleased to have *Maximal Orders* available once again and to observe the special and valued place it occupies in the literature.

August, 2002

Irma Reiner

Contents

Foreword	v
Preface	vii
Acknowledgements	x
Permanent notation	xiii
1 Algebraic preliminaries	
1 Integral closure	1
2 Homological algebra	8
3 Localization	30
4 Dedekind domains	44
5 Completions and valuations	67
6 Radicals of rings	77
7 Semisimple rings and simple algebras	90
2 Orders	
8 Definitions and examples	108
9 Reduced norms and traces	112
10 Existence of maximal orders; discriminants	125
11 Localization of orders	131
3 Maximal orders in skewfields (local case)	
12 Uniqueness of maximal orders	135
13 Ramification index; inertial degree	138
14 Finite residue class field case	143
4 Morita equivalence	
15 Progenerators	154
16 Morita correspondence	161
5 Maximal orders over discrete valuation rings	
17 Maximal orders (complete local case)	170
18 Maximal orders (local case)	174

19	Ideals	181
20	Different, discriminant	184
6	Maximal orders over Dedekind domains	
21	Basic results	187
22	Ideal theory	190
23	Alternate approach to global ideal theory	204
24	Norms of ideals	210
25	Different, discriminant	217
26	Ideal classes; Jordan–Zassenhaus theorem	224
27	Genus	232
7	Crossed-product algebras	
28	Brauer groups	237
29	Crossed-product algebras	241
30	Cyclic algebras	259
31	Cyclic algebras over local fields	263
8	Simple algebras over global fields	
32	Splitting of simple algebras	272
33	Reduced norms	282
34	Eichler’s Theorem	292
35	Ideal class groups	306
36	K_0 of maximal orders	314
37	Picard groups	319
38	Non-maximal orders	340
9	Hereditary orders	
39	Local theory of hereditary orders	351
40	Global theory of hereditary orders	367
41	Group rings	379
	References	387
	Index	391

Permanent notation

$a b$	a divides b (for elements or ideals)
$a \nmid b$	a does not divide b
$\text{card } X$	cardinal number of the set X
$A < B$	A is a proper subset of B
$A - J$	complement of the subset J in the set A
$\text{char } k$	characteristic of the field (or ring) k
$u(A)$	group of units of the ring A
a.e.	almost everywhere, that is, except for a finite number of cases
$\Sigma^* \dagger$	external direct sum
\oplus	internal direct sum
$M \mid N$	module M is isomorphic to a direct summand of module N
$M^{(r)}$	external direct sum of r copies of M
${}_A A$	ring A viewed as left A -module
$\text{End}_A M$	endomorphism ring of A -module M
$M_n(A)$	ring of all $n \times n$ matrices over a ring A
$\text{diag}(a_1, \dots, a_n)$	diagonal matrix with main diagonal entries a_1, \dots, a_n
I, I_n	identity matrix (in proper context)
a_L, a_l (a_R, a_r)	left (right) multiplication by the element a
$\mathbf{Z} = \text{rational integers}$.	$\mathbf{Q} = \text{rational field}$
$\mathbf{R} = \text{real field}$.	$\mathbf{C} = \text{complex field}$
$\mathbf{R}^+ = \{x \in \mathbf{R} : x \geq 0\}$	
$\mathbf{H} = \text{quaternion skewfield over } \mathbf{R}$	
$K^* = K - \{0\}$, where K is a field	
$\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$	(Kronecker delta)

1. Algebraic Preliminaries

This chapter reviews some basic algebraic techniques. Proofs are often omitted, especially when they are readily available in standard references, or when they are too long or too detailed to warrant their inclusion in this preliminary chapter. Many readers may wish to glance briefly at the contents of this chapter, referring back to the relevant sections when they are needed later. Occasionally, results are stated somewhat more generally than necessary for later use.

Each ring considered below will be assumed to have a unity element, and each ring homomorphism preserves unity elements. Every module M over a ring A is assumed *unital*, that is, the unity element of A acts as identity operator on M . Let K be a commutative ring; a ring A is a K -*algebra* if there is a ring homomorphism of K into the center of A . Such a homomorphism permits us to view A , and all A -modules, as K -modules. If A, B are K -algebras, we call them isomorphic as K -*algebras* if there is a ring isomorphism $\varphi: A \cong B$ such that $\varphi(\alpha x) = \alpha\varphi(x)$, $\alpha \in K$, $x \in A$.

1. INTEGRAL CLOSURE

Throughout this section let K be a field, and A a finite dimensional K -algebra. Denote its dimension by $(A:K)$ or $\dim_K A$.

1a Minimum and characteristic polynomial; norm, trace

Let $K[X]$ denote the domain of polynomials over K in an indeterminate X . An element $f(X) \in K[X]$ is *monic* if its leading coefficient equals 1. Let V be a finite dimensional K -space, and φ a K -linear transformation on V . We may view V as a left $K[X]$ -module, by letting X act as φ on V . Since $(V:K)$ is finite, it is clear that V is a finitely generated module over the principal ideal domain $K[X]$. By the Structure Theorem for such modules (see Curtis-Reiner [1, § 16]), there is a $K[X]$ -isomorphism

$$(1.1) \quad V \cong \sum_{i=1}^t K[X]/(h_i(X)), \quad h_i(X) \in K[X].$$

Each $h_i(X)$ is nonzero in $K[X]$ since $(V:K)$ is finite. As is well known, the

characteristic polynomial of φ acting on V is given by

$$(1.2) \quad \text{char. pol.}_K \varphi = \prod_{i=1}^t h_i(X).$$

On the other hand, let $f(X) \in K[X]$; then $f(\varphi)$ acts on V just as $f(X)$ acts on the right hand expression in (1.1). Hence $f(\varphi) = 0$ if and only if $f(X)$ annihilates this right hand expression. There is thus a unique monic polynomial $f(X) \in K[X]$, of least degree, such that $f(\varphi) = 0$; call this polynomial the *minimum polynomial* of φ . It is given by

$$(1.3) \quad \min. \text{pol.}_K \varphi = \text{L.C.M.} \{h_i(X) : 1 \leq i \leq t\}.$$

From (1.2) and (1.3) we have at once

(1.4) **THEOREM.** *Let φ be a K -linear transformation on the finite dimensional K -space V , and let*

$$f(X) = \min. \text{pol.}_K \varphi, \quad g(X) = \text{char. pol.}_K \varphi.$$

Then $f(X)$ divides $g(X)$ in $K[X]$; furthermore, $f(X)$ and $g(X)$ have the same irreducible factors in $K[X]$, apart from multiplicities. Finally, if $h(X) \in K[X]$, then $h(\varphi) = 0$ if and only if $f(X)$ divides $h(X)$.

Now let A be a finite dimensional K -algebra. Each $\alpha \in A$ determines a K -linear transformation α_L on A , where α_L is the left multiplication $x \rightarrow \alpha x$, $x \in A$. Clearly

$$(1.5) \quad (r\alpha + s\beta)_L = r\alpha_L + s\beta_L, \quad (\alpha\beta)_L = \alpha_L \cdot \beta_L,$$

for all $r, s \in K$, $\alpha, \beta \in A$. Further, $\alpha_L = 0$ if and only if $\alpha = 0$, since A has a unity element. Therefore the map $\alpha \rightarrow \alpha_L$, $\alpha \in A$, is a K -algebra isomorphism of A into the ring $\text{Hom}_K(A, A)$ of K -linear transformations on A . Now define

$$(1.6) \quad \min. \text{pol.}_K \alpha = \min. \text{pol.}_K \alpha_L, \quad \text{char. pol.}_{A/K} \alpha = \text{char. pol.}_K \alpha_L.$$

For $h(X) \in K[X]$ we have $h(\alpha_L) = h(\alpha)_L$, and thus $h(\alpha) = 0$ if and only if $h(\alpha_L) = 0$. This shows that $\min. \text{pol.}_K \alpha$ is the unique monic polynomial $f(X) \in K[X]$, of least degree, such that $f(\alpha) = 0$. For later use, we record explicitly the following consequence of (1.4):

(1.7) **THEOREM.** *Let A be a finite dimensional K -algebra. For $\alpha \in A$, let*

$$f(X) = \min. \text{pol.}_K \alpha, \quad g(X) = \text{char. pol.}_{A/K} \alpha.$$

Then $f(X)$ is the unique monic polynomial in $K[X]$, of least degree, such that $f(\alpha) = 0$; it has the property that $f(X) | h(X)$ for each $h(X) \in K[X]$ such that

$h(\alpha) = 0$. Further, $f(X)|g(X)$, and the polynomials $f(X), g(X)$ have the same irreducible factors in $K[X]$, apart from multiplicities.

A remark about notation seems called for. If B is a K -algebra containing A , then each $\alpha \in A$ also lies in B . Viewing α as element of B does not affect the calculation of $\min. \text{pol.}_K \alpha$, and so we have suppressed the subscript A in this notation. On the other hand, $\text{char. pol.}_{A/K} \alpha$ certainly depends on the choice of A , since it must be computed by letting α act on a K -basis for A ; indeed, $\text{char. pol.}_{A/K} \alpha \neq \text{char. pol.}_{B/K} \alpha$ if $B \neq A$, since $\text{char. pol.}_{A/K} \alpha$ has degree $(A : K)$.

Suppose now that $A = \sum_{i=1}^m Ku_i$, and let $\alpha \in A$. We may write

$$\alpha \cdot u_j = \sum_{i=1}^m a_{ij} u_i, \quad a_{ij} \in K, \quad 1 \leq j \leq m.$$

Then

$$(1.8) \quad \begin{aligned} \text{char. pol.}_K \alpha &= \det(\delta_{ij}X - a_{ij}) \\ &= X^m - (T_{A/K} \alpha)X^{m-1} + \cdots + (-1)^m N_{A/K} \alpha. \end{aligned}$$

We call $T_{A/K}$ the *trace* map, and $N_{A/K}$ the *norm* map. Clearly

$$T_{A/K} \alpha = \text{trace of } \alpha_L, \quad N_{A/K} \alpha = \det \alpha_L,$$

so from (1.5) we deduce

$$(1.9) \quad \begin{cases} T(r\alpha + s\beta) = rT(\alpha) + sT(\beta) \\ N(\alpha\beta) = N(\alpha) \cdot N(\beta), \quad N(r\alpha) = r^m N(\alpha), \end{cases}$$

for $r, s \in K$, $\alpha, \beta \in A$. Here, $m = (A : K)$.

1b Integral elements

Now let R be an integral domain with quotient field K , and let A be a finite dimensional K -algebra. An element $\alpha \in A$ is *integral* over R if $f(\alpha) = 0$ for some monic polynomial $f(X) \in R[X]$.

(1.10) THEOREM. For an element $\alpha \in A$, the following three conditions are equivalent:

- (i) α is integral over R .
- (ii) $R[\alpha]$ is a finitely generated R -module.
- (iii) α is contained in some subring B of A , such that B is a finitely generated R -module.

Proof. If (i) holds, then there is a relation

$$\alpha^n = a_1 \alpha^{n-1} + \cdots + a_n, \quad a_i \in R.$$

It is then obvious that

$$R[\alpha] = R + R\alpha + \cdots + R\alpha^{n-1},$$

a finitely generated R -module. Thus (i) implies (ii). Clearly (ii) implies (iii), by choosing $B = R[\alpha]$.

To prove that (iii) implies (i), let us write

$$B = \sum_{i=1}^n R\beta_i, \quad \beta_i \in B.$$

Since B is a ring, and $\alpha \in B$, it follows that each $\alpha\beta_i \in B$. Therefore we have

$$\alpha\beta_i = \sum_{j=1}^n a_{ij}\beta_j, \quad a_{ij} \in R, \quad 1 \leq i \leq n.$$

We may rewrite these equations as

$$\sum_{j=1}^n (\alpha\delta_{ij} - a_{ij})\beta_j = 0, \quad 1 \leq i \leq n.$$

Let $d = \det(\alpha\delta_{ij} - a_{ij}) \in B$. By Cramer's Formula, it follows that $d \cdot \beta_j = 0$ for $1 \leq j \leq n$. Therefore $d \cdot B = 0$, and hence $d = 0$, since B is a ring with unity element. This shows that α is a zero of the monic polynomial $\det(X\delta_{ij} - a_{ij}) \in R[X]$, and thus α is integral over R . We have now shown that (iii) implies (i), and the theorem is proved.

(1.11) COROLLARY. Let $\alpha, \beta \in A$ be such that $\alpha\beta = \beta\alpha$. If both α and β are integral over R , then so are $\alpha \pm \beta$ and $\alpha\beta$.

Proof. Since α and β are integral over R , by (1.10) we may write

$$R[\alpha] = \sum_{i=1}^k Ru_i, \quad R[\beta] = \sum_{j=1}^m Rv_j.$$

Since $\alpha\beta = \beta\alpha$, every element of $R[\alpha]$ commutes with every element of $R[\beta]$, and therefore

$$R[\alpha, \beta] = \sum_{i,j} Ru_i v_j.$$

Thus $R[\alpha, \beta]$ is a finitely generated R -module, and is a subring of A . It follows from (1.10) that every element of $R[\alpha, \beta]$ is integral over R , and hence the corollary is established.

Remarks. (i) A slightly simpler proof can be given when R is a noetherian

domain (see section 2a). Keep the above notation, and let $x \in R[\alpha, \beta]$. Then $R[x]$ is an R -submodule of the finitely generated R -module $R[\alpha, \beta]$. Hence $R[x]$ is also finitely generated as R -module, and thus x is integral over R by (1.10).

(ii) If α and β are integral elements which do not commute, it may well occur that $\alpha + \beta$ is *not* integral. For example, let $R = \mathbf{Z}$, $K = \mathbf{Q}$, $A = M_2(\mathbf{Q})$ (the algebra of all 2×2 matrices with entries in \mathbf{Q}). Let

$$\alpha = \begin{pmatrix} 0 & \frac{1}{2} \\ 0 & 0 \end{pmatrix}, \quad \beta = \begin{pmatrix} 0 & 0 \\ \frac{1}{2} & 0 \end{pmatrix}.$$

Both α and β satisfy the equation $X^2 = 0$, and so are integral over \mathbf{Z} . However,

$$\min. \text{pol.}_\mathbf{Q}(\alpha + \beta) = X^2 - \frac{1}{4} \notin \mathbf{Z}[X].$$

Therefore $\alpha + \beta$ is not integral over \mathbf{Z} , by (1.14) below.

1c Integral closure

The *integral closure* of R in A is the set of all elements of A which are integral over R . If A is a *commutative* K -algebra, then by (1.11) the integral closure of R in A is a subring of A . If A is not commutative, the integral closure need not be a ring.

(1.12) **DEFINITION.** *The integral domain R is integrally closed if the integral closure of R in its quotient field K coincides with R . Thus, R is integrally closed if for $\alpha \in K$,*

$$f(\alpha) = 0, f(X) \in R[X], f(X) \text{ monic} \Rightarrow \alpha \in R.$$

(1.13) **GAUSS' LEMMA.** *Let R be an integrally closed domain with quotient field K . Let $f(X) \in R[X]$ be a monic polynomial, and suppose that*

$$f(X) = g(X) \cdot h(X),$$

where $g(X)$ and $h(X)$ are monic polynomials in $K[X]$. Then both $g(X)$ and $h(X)$ lie in $R[X]$.

Proof. Let K' be a finite extension of K which is a splitting field for $f(X)$, and write

$$f(X) = \prod (X - x_i), \quad x_i \in K'.$$

Let R' denote the integral closure of R in K' . Since $f(X) \in R[X]$ is monic, and $f(x_i) = 0$ for each i , it follows that each $x_i \in R'$.

In $K'[X]$ we have

$$g(X) \cdot h(X) = \prod (X - x_i),$$

whence both $g(X)$ and $h(X)$ are expressible as partial products $\Pi'(X - x_i)$. But R' is a ring by (1.11), so both $g(X)$ and $h(X)$ have coefficients in R' . The coefficients of $g(X)$ and $h(X)$ are thus in $R' \cap K$. However, $R' \cap K = R$, because R is integrally closed. Thus both $g(X)$ and $h(X)$ lie in $R[X]$, and the lemma is proved.

In order to determine whether an element $\alpha \in A$ is integral over R , we must in theory consider *all* monic polynomials $f(X) \in K[X]$ such that $f(\alpha) = 0$, and then we must see whether any such $f(X)$ lies in $R[X]$. In practice, however, this task is considerably simplified by use of the following result.

(1.14) THEOREM. *Let R be an integrally closed domain with quotient field K , and let A be a finite dimensional K -algebra. An element $\alpha \in A$ is integral over R if and only if*

$$\min. \text{pol}_K \alpha \in R[X].$$

Proof. If $\min. \text{pol}_K \alpha \in R[X]$, it is clear that α is integral over R . Conversely, let $g(X) = \min. \text{pol}_K \alpha$, and assume that α is integral over R . Then $f(\alpha) = 0$ for some monic polynomial $f(X) \in R[X]$. Therefore $f(X) = g(X) \cdot h(X)$ for some monic polynomial $h(X) \in K[X]$. It then follows from Gauss' Lemma that $g(X) \in R[X]$, as desired.

We shall conclude this section by listing some examples of integrally closed domains. Proofs are available in standard references such as Bourbaki [4, Ch. 5, §1] and Zariski-Samuel [1, Ch. V, §3].

(1.15) Examples of integrally closed domains.

- (a) Every principal ideal domain is integrally closed.
- (b) Every unique factorization domain is integrally closed.
- (c) Every Dedekind domain is integrally closed (see §4a).
- (d) Let R be a domain with quotient field K , and let K' be any extension field of K . Then the integral closure of R in K' is always integrally closed.
- (e) Let S be any multiplicative subset of R (see §3a). If R is integrally closed, so is the ring of quotients $S^{-1}R$.
- (f) Let $K[x_1, \dots, x_n]$ be the polynomial domain in n indeterminates over a field K (or more generally, over a unique factorization domain K). Then $K[x_1, \dots, x_n]$ is also a unique factorization domain, and thus is integrally closed by (b).

EXERCISES

1. Keep the notation and hypotheses of (1.14). Show that an element $\alpha \in A$ is integral over K if and only if $\text{char. pol.}_{A/K} \alpha \in R[X]$. [Hint: Use (1.7) and (1.14).]

2. Let A be a finite dimensional K -algebra, and let L be any extension field of K . Each element $a \in A$ gives rise to an element $1 \otimes a$ of the L -algebra $L \otimes_K A$. Prove that

$$\text{char. pol.}_{L \otimes_K A, L} 1 \otimes a = \text{char. pol.}_{A/K} a.$$

In other words, $\text{char. pol.}_{A/K} a$ is not affected by the change of ground field from K to L .

3. Let $E \supset K$ be fields, and let $(E:K) = n$. Each $\alpha \in E$ corresponds to a matrix $\tilde{\alpha} \in M_n(K)$, obtained by letting α act as left multiplication on a K -basis of E . Show by induction on r that for each matrix $(\alpha_{ij}) \in M_r$,

$$\det(\tilde{\alpha}_{ij}) = N_{E/K} \{\det(\alpha_{ij})\}.$$

4. Let L be a finite galois extension field of K , with galois group G . Show that for $a \in L$,

$$\text{char. pol.}_{L/K} a = \prod_{\sigma \in G} (X - a^\sigma)$$

and hence

$$T_{L/K} a = \sum_{\sigma \in G} a^\sigma, \quad N_{L/K} a = \prod_{\sigma \in G} a^\sigma.$$

[Hint: Let

$$f(X) = \min. \text{pol.}_{L/K} a = \prod_{i=1}^n (X - a_i), \quad a_i \in L.$$

Then $\prod_{\sigma \in G} (X - a^\sigma) \in K[X]$, hence is a power of $f(X)$. Then compare degrees of $\text{char. pol.}_{L/K} a$ and $\prod_{\sigma \in G} (X - a^\sigma)$.]

5. Keep the notation of Exercise 3, and let A be a finite dimensional E -algebra. Prove that for $a \in A$,

$$T_{A/K} a = T_{E/K}(T_{A/E} a), \quad N_{A/K} a = N_{E/K}(N_{A/E} a).$$

[Hint: Let

$$A = \sum E x_i, \quad ax_j = \sum \alpha_{ij} x_i, \quad \alpha_{ij} \in E.$$

Relative to a suitable K -basis of A , the K -linear transformation a_L on A corresponds to the matrix $(\tilde{\alpha}_{ij})$. Hence

$$\begin{aligned} T_{A/K} a &= \text{trace of } (\tilde{\alpha}_{ij}) = \sum_i \text{trace of } \tilde{\alpha}_{ii} \\ &= \sum_i T_{E/K} \alpha_{ii} = T_{E/K}(T_{A/E} a). \end{aligned}$$

A similar result holds for norms, by Exercise 3.]

2. HOMOLOGICAL ALGEBRA

This section contains a brief review of several topics from homological algebra. In most cases, proofs will be omitted. For details, we refer the reader to standard references such as Cartan–Eilenberg [1], Hilton–Stammbach [1], Jans [1], Northcott [1], Rotman [1]. We shall use the same terminology and notation as the last of these references.

2a Modules: homomorphisms, pullbacks, pushouts, tensor products, chain conditions

Throughout this section let Λ be a ring, not necessarily commutative, having a unity element 1. All Λ -modules are left Λ -modules, unless otherwise specified, and each Λ -module M is assumed *unital* (that is, $1 \cdot m = m$, $m \in M$). Given a pair of Λ -modules L and M , denote by $\text{Hom}_\Lambda(L, M)$ the additive group consisting of all Λ -homomorphisms from L into M . For each $\varphi \in \text{Hom}_\Lambda(L, M)$, let $\ker \varphi$ denote the *kernel* of φ , $\text{im } \varphi$ the *image* of φ , and $\text{cok } \varphi$ the *cokernel* of φ , that is,

$$\text{cok } \varphi = M/\varphi(L).$$

When there is no danger of confusion, we shall write Hom instead of Hom_Λ .

A sequence of Λ -modules and Λ -homomorphisms

$$(2.1) \quad X_1 \xrightarrow{f_1} X_2 \xrightarrow{f_2} X_3 \longrightarrow \dots \xrightarrow{f_{n-1}} X_n$$

is *exact* at X_i if $\ker f_i = \text{im } f_{i-1}$. The sequence is *exact* if it is exact at each place, that is,

$$\ker f_i = \text{im } f_{i-1}, \quad 2 \leq i \leq n-1.$$

An exact sequence of Λ -modules and Λ -homomorphisms will sometimes be called a Λ -*exact sequence*.

A *short exact sequence* is an exact sequence of the form

$$(2.2) \quad 0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0.$$

Exactness of (2.2) is equivalent to the following three conditions: f is monic, $\ker g = \text{im } f$, g is epic. In this case, g induces an isomorphism $M/f(L) \cong N$.

The short exact sequence (2.2) is *split* if $f(L)$ is a direct summand of M . This is equivalent to either of the following:

(i) There exists an $h \in \text{Hom}_\Lambda(M, L)$ such that $h \cdot f = 1_L$, where 1_L denotes the identity map on L .

(ii) There exists an $h' \in \text{Hom}_\Lambda(N, M)$ such that $g \cdot h' = 1_N$.

A diagram of Λ -modules and Λ -homomorphisms

$$\begin{array}{ccc} L & \xrightarrow{f} & M \\ & \searrow h & \downarrow g \\ & & N \end{array}$$

is *commutative* if $g \cdot f = h$. The same terminology applies to more complicated diagrams.

Given a Λ -homomorphism $f:L \rightarrow M$, and an arbitrary Λ -module X , there are two maps induced by f , namely

$$(2.3) \quad \begin{cases} f_*: \text{Hom}(X, L) \rightarrow \text{Hom}(X, M), \\ f^*: \text{Hom}(M, X) \rightarrow \text{Hom}(L, X). \end{cases}$$

These are defined by the commutative diagrams

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & L \\ & \searrow f_* \varphi & \downarrow f \\ & & M, \end{array} \quad \begin{array}{ccc} L & \xrightarrow{f} & M \\ \downarrow f & \nearrow f^* \psi & \downarrow \psi \\ M & \xrightarrow{\psi} & X. \end{array}$$

Note that $\text{Hom}_\Lambda(X, L)$, $\text{Hom}_\Lambda(X, M)$, etc., are additive groups (but not usually Λ -modules), and the maps f_* , f^* are additive homomorphisms.

The map f_* goes “in the same direction” as f , namely from L to M . Since f_* arises from a change in the second variable occurring in Hom , we say that Hom is *covariant* in the second variable.

Similarly, f^* goes “in the opposite direction” from f . Since f^* arises from a change in the first variable in Hom , we call Hom *contravariant* in the first variable.

If $f:L \rightarrow M$ and $g:M \rightarrow N$ are Λ -homomorphisms, then

$$(2.4) \quad (gf)_* = g_* \cdot f_*, \quad (gf)^* = f^* \cdot g^*.$$

(Contravariance reverses order of composition of mappings!)

The concepts of covariance and contravariance are extremely useful in working with modules. Thus, for example, let Δ be another ring, and let $M = {}_\Lambda M_\Delta$ be a (Λ, Δ) -bimodule, that is, M is a left Λ -module and right Δ -module, with the actions of Λ and Δ on M commuting:

$$(\lambda m)\delta$$

If $L = {}_\Lambda L$ is a left Λ -module, then $\text{Hom}_\Lambda(M, L)$ can be given the structure of a Δ -module, because of the bimodule structure on M . Since M is a *right* Δ -module, and M appears in a *contravariant* position, it is automatically true that $\text{Hom}_\Lambda(M, L)$ must be a *left* Δ -module. To be explicit, for each $f \in \text{Hom}_\Lambda(M, L)$ and each $\delta \in \Delta$, we define

$$(\delta f)m = f(m\delta).$$

This is the only “natural” definition, and it must use the fact that M is a right

Δ -module. The hypothesis that M be a (Λ, Δ) -bimodule is needed to verify that δf is again a Λ -homomorphism. Analogously, $\text{Hom}_{\Lambda}(L, M)$ can be made into a *right* Δ -module, by setting

$$(g\delta)x = g(x) \cdot \delta, \quad g \in \text{Hom}_{\Lambda}(L, M), \quad \delta \in \Delta, \quad x \in L.$$

We state without proof a theorem describing the effect of applying $\text{Hom}_{\Lambda}(X, \cdot)$ or $\text{Hom}_{\Lambda}(\cdot, Y)$ to Λ -exact sequences.

(2.5) THEOREM. (i) For each Λ -module X and each Λ -exact sequence

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N,$$

the sequence of additive groups

$$0 \longrightarrow \text{Hom}_{\Lambda}(X, L) \xrightarrow{f_*} \text{Hom}_{\Lambda}(X, M) \xrightarrow{g_*} \text{Hom}_{\Lambda}(X, N)$$

is exact.

(ii) For each Λ -module Y and each Λ -exact sequence

$$L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0,$$

the sequence of additive groups

$$0 \longrightarrow \text{Hom}_{\Lambda}(N, Y) \xrightarrow{g^*} \text{Hom}_{\Lambda}(M, Y) \xrightarrow{f^*} \text{Hom}_{\Lambda}(L, Y)$$

is exact.

It is sometimes convenient to use the concepts of pushouts and pullbacks of pairs of maps. Given a pair of Λ -homomorphisms $f_i : A \rightarrow M_i$, $i = 1, 2$, we define a Λ -module X , called the *pushout* of the pair (f_1, f_2) , by the formula

$$X = (M_1 + M_2)/\{(f_1 a, -f_2 a) : a \in A\}.$$

Thus X is obtained from the external direct sum $M_1 + M_2$ by identifying the image of A in M_1 with the image of A in M_2 . There is a commutative diagram (called a *pushout diagram* or *fibre sum*)

$$\begin{array}{ccc} A & \xrightarrow{f_1} & M_1 \\ f_2 \downarrow & & \downarrow g_1 \\ M_2 & \xrightarrow{g_2} & X \end{array}$$

where g_i is defined by composition: $M_i \rightarrow M_1 + M_2 \rightarrow X$, $i = 1, 2$. The pushout X is characterized up to isomorphism by a “universal mapping property”, as follows: given any commutative diagram of Λ -modules and Λ -homomorphisms

$$\begin{array}{ccc} A & \xrightarrow{f_1} & M_1 \\ f_2 \downarrow & & \downarrow g'_1 \\ M_2 & \xrightarrow{g'_2} & X' \end{array}$$

there is a unique Λ -homomorphism $\psi:X \rightarrow X'$ such that $\psi g_i = g'_i$, $i = 1, 2$.

Dually, given Λ -homomorphisms $f_i:M_i \rightarrow B$, $i = 1, 2$, we can form their *pullback* (or *fibre product*)

$$Y = \{(m_1, m_2) \in M_1 + M_2 : f_1 m_1 = f_2 m_2\}.$$

There is a commutative *pullback diagram*

$$\begin{array}{ccc} Y & \xrightarrow{g_1} & M_1 \\ g_2 \downarrow & & \downarrow f_1 \\ M_2 & \xrightarrow{f_2} & B, \end{array}$$

where $g_i(m_1, m_2) = m_i$, $i = 1, 2$. The pullback Y is also characterized by a universal mapping property: given any commutative diagram

$$\begin{array}{ccc} Y' & \xrightarrow{g'_1} & M_1 \\ g'_2 \downarrow & & \downarrow f_1 \\ M_2 & \xrightarrow{f_2} & B, \end{array}$$

there is a unique $\varphi:Y' \rightarrow Y$ such that $g'_i = g_i \varphi$, $i = 1, 2$.

Next, we recall some facts about tensor products (see Curtis-Reiner [1, §12], for example). Given a right Λ -module L and a left Λ -module M (notation: $L_{\Lambda}, {}_{\Lambda}M$), we may form their tensor product $L \otimes_{\Lambda} M$. This is an additive group, but not usually a Λ -module. The tensor product $L \otimes_{\Lambda} M$ is covariant in each variable: given Λ -homomorphisms $f:L_1 \rightarrow L_2$, $g:M_1 \rightarrow M_2$, there is an additive homomorphism

$$f \otimes g:L_1 \otimes_{\Lambda} M_1 \rightarrow L_2 \otimes_{\Lambda} M_2.$$

Consequently, if Δ is another ring with unity element, and if ${}_L L_{\Lambda}$ is a bimodule, then for each ${}_{\Lambda} M$ we can make $L \otimes_{\Lambda} M$ into a left Δ -module in a natural way. The action of an element $\delta \in \Delta$ on $L \otimes_{\Lambda} M$ is given by

$$\delta(\sum l_i \otimes m_i) = \sum \delta l_i \otimes m_i, \quad l_i \in L, \quad m_i \in M.$$

In particular, if Λ is commutative and L, M are viewed as two-sided Λ -modules, then $L \otimes_{\Lambda} M$ is also a Λ -module.

The effect of applying $X \otimes_{\Lambda} \cdot$ or $\cdot \otimes_{\Lambda} Y$ to exact sequences is described in the following result, stated without proof:

(2.6) THEOREM. (i) Given a right Λ -module X and an exact sequence of left Λ -modules $L \rightarrow M \rightarrow N \rightarrow 0$, there is an exact sequence of additive groups

$$X \otimes_{\Lambda} L \rightarrow X \otimes_{\Lambda} M \rightarrow X \otimes_{\Lambda} N \rightarrow 0.$$

(ii) Given ${}_{\Lambda}Y$ and an exact sequence of right Λ -modules $A \rightarrow B \rightarrow C \rightarrow 0$, there is an exact sequence of additive groups

$$A \otimes_{\Lambda} Y \rightarrow B \otimes_{\Lambda} Y \rightarrow C \otimes_{\Lambda} Y \rightarrow 0.$$

Next we list a number of natural isomorphisms involving Hom and \otimes . In most cases there is no difficulty in writing down explicitly the maps which yield these isomorphisms, and we shall leave this task to the reader. It will also be clear from the context whether the modules which occur are left Λ -modules or right Λ -modules, and we shall suppress such information in some of the statements below.

(2.7) THEOREM. (i) Given ${}_{\Lambda}M$, there is a left Λ -isomorphism

$$\text{Hom}_{\Lambda}(\Lambda, M) \cong M,$$

obtained by mapping each $f \in \text{Hom}_{\Lambda}(\Lambda, M)$ onto $f(1)$. The left Λ -structure of $\text{Hom}_{\Lambda}(\Lambda, M)$ arises from the Λ - Λ -bimodule structure of Λ .

(ii) For each index set I ,

$$\text{Hom}_{\Lambda}\left(\sum_{i \in I} M_i, N\right) \cong \prod_{i \in I} \text{Hom}_{\Lambda}(M_i, N),$$

$$\text{Hom}_{\Lambda}\left(M, \prod_{i \in I} N_i\right) \cong \prod_{i \in I} \text{Hom}_{\Lambda}(M, N_i).$$

Choosing I to be the finite set $\{1, \dots, k\}$, it follows as special cases of these formulas that Hom commutes with finite direct sums in either variable:

$$\text{Hom}_{\Lambda}\left(\sum_{i=1}^k M_i, N\right) \cong \sum_{i=1}^k \text{Hom}_{\Lambda}(M_i, N),$$

$$\text{Hom}_{\Lambda}\left(M, \sum_{i=1}^k N_i\right) \cong \sum_{i=1}^k \text{Hom}_{\Lambda}(M, N_i).$$

(2.8) THEOREM. (i) Given ${}_{\Lambda}M$, there is a left Λ -isomorphism

$$\Lambda \otimes_{\Lambda} M \cong M,$$

obtained by mapping $\sum \lambda_i \otimes m_i \in \Lambda \otimes_{\Lambda} M$ onto $\sum \lambda_i m_i \in M$. The left Λ -structure of $\Lambda \otimes_{\Lambda} M$ arises from the Λ - Λ -bimodule structure of Λ .

(ii) Tensor product commutes with direct sums:

$$\left(\sum_{i \in I} M_i \right) \otimes_{\Lambda} N \cong \sum_{i \in I} (M_i \otimes_{\Lambda} N),$$

$$M \otimes_{\Lambda} \left(\sum_{i \in I} N_i \right) \cong \sum_{i \in I} (M \otimes_{\Lambda} N_i),$$

for any index set I .

Finally we give some results on chain conditions. A Λ -module M is *noetherian* if the submodules of M satisfy the ascending chain condition (A.C.C.), that is, if every ascending chain of submodules terminates. The ring Λ is *left noetherian* if the left ideals of Λ satisfy the A.C.C. The following result is used repeatedly (see Curtis–Reiner [1, §11]):

(2.9) THEOREM. *For a ring Λ , the following are equivalent:*

- (i) Λ is left noetherian.
- (ii) Every finitely generated left Λ -module is noetherian.
- (iii) Every submodule of a finitely generated left Λ -module is finitely generated.
- (iv) Every nonempty collection of submodules of a finitely generated left Λ -module contains a maximal element.

(2.10) COROLLARY. *Let R be a commutative noetherian ring, and let Λ be an R -algebra which is finitely generated as R -module. Then Λ is left and right noetherian as a ring.*

Proof. Every left ideal of Λ is an R -submodule of the finitely generated R -module Λ . Since R is noetherian, it follows from (2.9 (ii)) that the R -submodules of Λ satisfy the A.C.C. Hence the left ideals of Λ satisfy the A.C.C., so Λ is left noetherian. Likewise Λ is right noetherian.

Next, a Λ -module M is *artinian* if its submodules satisfy the descending chain condition (D.C.C.), that is, if every descending chain of submodules terminates. The ring Λ is *left artinian* if its left ideals satisfy the D.C.C. We have (see Curtis–Reiner [1, §11])

(2.11) THEOREM. *The following statements are equivalent:*

- (i) Λ is left artinian.
- (ii) Every finitely generated left Λ -module is artinian.
- (iii) Every nonempty collection of submodules of a finitely generated Λ -module contains a minimal element.

Just as in the preceding discussion, we obtain

(2.12) COROLLARY. *Let R be a commutative artinian ring, and let Λ be an*

R-algebra which is finitely generated as R-module. Then Λ is left and right artinian as a ring.

2b Functors and categories

In order to simplify the remaining discussion of homological algebra, and also for later use in the chapter on Morita equivalence, it is convenient to introduce some of the concepts of category theory. For simplicity, we shall restrict our attention to categories of modules. (For a more detailed account of category theory, see MacLane [1].) If Λ is a ring with unity element, let \mathcal{M}_Λ denote the category of right Λ -modules. The objects of \mathcal{M}_Λ are right Λ -modules, and for each $L, M \in \mathcal{M}_\Lambda$, there is a set of *morphisms* (or *maps*) from L to M , namely $\text{Hom}_\Lambda(L, M)$.

Let \mathcal{A} be a category with objects A, A', \dots , and \mathcal{B} a category with objects B, B', \dots . A (covariant) *functor* $F: \mathcal{A} \rightarrow \mathcal{B}$ carries each $A \in \mathcal{A}$ onto an object $FA \in \mathcal{B}$, and carries each $\alpha \in \text{Hom}_\mathcal{A}(A, A')$ onto a map $F\alpha \in \text{Hom}_\mathcal{B}(FA, FA')$, in such a way as to preserve identity maps and compositions. We assume always that our functors are *additive*, that is, $F(\alpha_1 + \alpha_2) = F\alpha_1 + F\alpha_2$. A *contravariant* functor $F: \mathcal{A} \rightarrow \mathcal{B}$ carries $A \in \mathcal{A}$ onto $FA \in \mathcal{B}$, and carries each $\alpha \in \text{Hom}_\mathcal{A}(A, A')$ onto $F\alpha \in \text{Hom}_\mathcal{B}(FA', FA)$; such an F reverses composition of maps.

A covariant functor F is *right exact* if it carries each exact sequence $A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow 0$ in \mathcal{A} onto an exact sequence $FA_1 \rightarrow FA_2 \rightarrow FA_3 \rightarrow 0$ in \mathcal{B} . For example, if \mathcal{Ab} denotes the category of abelian groups, and X_Λ is some fixed right Λ -module, there is a functor $F: {}_\Lambda \mathcal{M} \rightarrow \mathcal{Ab}$, given by $M \rightarrow X \otimes_\Lambda M$, and $\alpha \mapsto 1 \otimes \alpha$. We often write $F = X \otimes_\Lambda \cdot$. Theorem 2.6 is just the assertion that F is a right exact functor.

On the other hand, let ${}_\Lambda X$ be a fixed left Λ -module, and define $F: {}_\Lambda \mathcal{M} \rightarrow \mathcal{Ab}$ by $M \rightarrow \text{Hom}_\Lambda(X, M)$, $M \in {}_\Lambda \mathcal{M}$. We must also describe the action of F on maps; if $\alpha \in \text{Hom}_\Lambda(M, M')$, we set $F\alpha = \alpha_*$ (see (2.3)). Then F is covariant, and (2.5) asserts that F is a left exact functor. We often write $F = \text{Hom}_\Lambda(\cdot, X)$. Theorem 2.6 is just the assertion that F is a left exact functor.

One can also define right- or left-exactness of contravariant functors. We shall not give the definition here, but remark only that the functor $F: {}_\Lambda \mathcal{M} \rightarrow \mathcal{Ab}$, given by $F = \text{Hom}_\Lambda(\cdot, X)$, is a contravariant functor which is left exact (by (2.5)).

A functor $F: \mathcal{A} \rightarrow \mathcal{B}$ is *exact* if F is both left and right exact. We state without proof:

(2.13) THEOREM. Let $F: \mathcal{A} \rightarrow \mathcal{B}$ be a covariant functor. The following conditions are equivalent:

- (i) F is an exact functor.
- (ii) F preserves exactness of short exact sequences, that is, if

$0 \rightarrow A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow 0$ is an \mathcal{A} -exact sequence, then $0 \rightarrow FA_1 \rightarrow FA_2 \rightarrow FA_3 \rightarrow 0$ is an exact sequence in \mathcal{B} .

(iii) F preserves exactness of sequences, that is, if $A' \rightarrow A \rightarrow A''$ is \mathcal{A} -exact, then $FA' \rightarrow FA \rightarrow FA''$ is \mathcal{B} -exact.

2c Projective and flat modules

A (left) Λ -module F is said to have a free Λ -basis $\{x_\alpha\}$, where α ranges over some index set, if there exist elements $x_\alpha \in F$ such that each $x \in F$ is expressible as a finite sum $x = \sum c_\alpha x_\alpha$ with uniquely determined coefficients $c_\alpha \in \Lambda$. Such modules F are called free Λ -modules. Equivalently, F is free if and only if F is isomorphic to a direct sum of copies of the left Λ -module ${}_A\Lambda$.

Every Λ -module M is a homomorphic image of some free module F . Indeed, choose any set of elements $m_\alpha \in M$ such that $M = \sum \Lambda m_\alpha$, and let F be free with basis $\{x_\alpha\}$; then define an epimorphism $\varphi: F \rightarrow M$ by letting $\varphi(x_\alpha) = m_\alpha$. Note that if M is finitely generated as Λ -module, then F may be chosen free with a finite basis.

A projective Λ -module is a direct summand of a free module. For example, if $\Lambda = J_1 \oplus J_2$, where each J_i is a left ideal of Λ , then J_1 and J_2 are projective left Λ -modules. Obviously, every free module is projective. Let $\{M_i\}$ be any family of Λ -modules. It is clear from the definition of projectivity that $\sum^* M_i$ is projective if and only if each M_i is projective. As we shall see, projective modules play a basic role in homological algebra, and in other areas of algebra as well. We state without proof (see references listed at the beginning of § 2):

2.14) THEOREM. *Let P be any Λ -module. The following statements are equivalent:*

- (i) P is projective.
- (ii) Every short exact sequence $0 \rightarrow X \rightarrow Y \rightarrow P \rightarrow 0$ must split.
- (iii) Given any diagram with exact bottom row

$$\begin{array}{ccc} & P & \\ & \swarrow h \quad \downarrow f & \\ X & \xrightarrow{g} & Y \rightarrow 0, \end{array}$$

there exists a Λ -homomorphism h such that $f = gh$.

- (iv) Given any epimorphism $g: X \rightarrow Y$, the induced map

$$g_*: \text{Hom}_\Lambda(P, X) \rightarrow \text{Hom}_\Lambda(P, Y)$$

is also an epimorphism.

(v) $\text{Hom}_\Lambda(P, \cdot)$ is an exact functor.

Remark. There is a concept of *injective* modules, dual to that of projective modules: a Λ -module L is *injective* if every short exact sequence $0 \rightarrow L \rightarrow X \rightarrow Y \rightarrow 0$ is necessarily split. The analogue of (2.14) holds true. We shall seldom need to use injective modules in this book.

A right Λ -module X is *flat* if $X \otimes_\Lambda \cdot$ preserves exactness, that is, if for every exact sequence of left Λ -modules

$$L \xrightarrow{f} M \xrightarrow{g} N,$$

the sequence of additive groups

$$X \otimes_\Lambda L \xrightarrow{1 \otimes f} X \otimes_\Lambda M \xrightarrow{1 \otimes g} X \otimes_\Lambda N$$

is also exact. We may rephrase this definition as follows: the module X_Λ determines a covariant functor $F : {}_{\Lambda}\mathcal{M} \rightarrow \mathcal{Ab}$ as in §2(b), by setting $F(M) = X \otimes_\Lambda M$, $M \in {}_{\Lambda}\mathcal{M}$. Then X is flat if and only if F is an exact functor. We have already remarked in (2.6) that F is always right exact, and the only question to be decided is whether F is also left exact. Hence we have

(2.15) **THEOREM.** A module X_Λ is flat if and only if $X \otimes_\Lambda \cdot$ preserves monomorphisms, that is, for each monomorphism $f : L \rightarrow M$ of left Λ -modules, the additive homomorphism

$$1 \otimes f : X \otimes_\Lambda L \rightarrow X \otimes_\Lambda M$$

is also monic.

(2.16) **COROLLARY.** Every projective module is flat.

Proof. The right Λ -module Λ_Λ is flat, because of the isomorphism given in (2.8(i)). Since tensor product commutes with direct sum (see (2.8)), it follows that every free right Λ -module is flat. Now let X_Λ be projective; then X is a direct summand of some free right Λ -module F , and we may write $F = X \oplus X'$ for some module X' . Let $f : L \rightarrow M$ be a monomorphism of left Λ -modules. Then there is a commutative diagram

$$\begin{array}{ccc} F \otimes_\Lambda L & \cong & X \otimes_\Lambda L + X' \otimes_\Lambda L \\ \downarrow l_F \otimes f & & \downarrow l_X \otimes f \\ F \otimes_\Lambda M & \cong & X \otimes_\Lambda M + X' \otimes_\Lambda L. \end{array}$$

Since F is flat, $l_F \otimes f$ is monic. Hence also $l_X \otimes f$ is monic, and therefore X is flat, as claimed.

(2.17) *Remark.* The technique of the preceding proof can be applied to many

similar situations. In order to prove certain types of theorems about projective modules, one first treats the case of a free module on one generator, then the case of an arbitrary free module, and finally the case of projective modules. Of course, one needs to know that the functors which occur commute with the operation of forming direct sums. In many arguments, it suffices to restrict attention to finite direct sums.

(2.18) *Remark.* We shall show in §3c that every ring of quotients R' of a commutative ring R is a flat R -module. From (2.15) it then follows that for each inclusion of R -modules $L \subset M$, there is an inclusion of R' -modules $R' \otimes_R L \subset R' \otimes_R M$. Further, there is an R' -isomorphism

$$R' \otimes_R (M/L) \cong (R' \otimes_R M)/(R' \otimes_R L),$$

a result to be used repeatedly.

Next we note

(2.19) **THEOREM.** *A right Λ -module X is flat if every finitely generated submodule of X is flat.*

Proof. See Rotman [1, Corollary 3.31]. The converse of this theorem is false.

Using this, we prove (see also Exercise 5.3):

(2.20) **THEOREM.** *Let R be a principal ideal domain. Then every torsionfree† R -module is flat.*

Proof. Submodules of torsionfree modules are also torsionfree. Hence by (2.19), it suffices to prove that every finitely generated torsionfree R -module X is flat. But by the Structure Theorem for modules over principal ideal domains (see Curtis–Reiner [1, §16]), each such X is R -free. Hence X is R -flat, by (2.16), and the theorem is proved.

As a matter of fact, the converse of (2.20) also holds: if X is a flat R -module, then X must be torsionfree (see Rotman [1, Exercise 3.11]).

A flat right Λ -module X is *faithfully flat* if for each left Λ -module L , the equality $X \otimes_{\Lambda} L = 0$ implies that $L = 0$. To test for faithful flatness, we may use the result:

(2.21) **THEOREM.** *Let X_{Λ} be flat. The following statements are equivalent:*

(i) *X is faithfully flat.*

(ii) *A sequence of left Λ -modules is exact if and only if it becomes exact after applying $X \otimes_{\Lambda} \cdot$ to it.*

† An R -module X is *torsionfree* if for each nonzero $x \in X$ and each nonzero $r \in R$, also $rx \neq 0$.

- (iii) For each left Λ -homomorphism $f: L \rightarrow M$, the map $1 \otimes f: X \otimes_{\Lambda} L \rightarrow X \otimes_{\Lambda} M$ is the zero map if and only if $f = 0$.
- (iv) For each maximal left ideal \mathfrak{m} of Λ , we have $X \neq X\mathfrak{m}$.

Proof. See Bourbaki [2, §3, no. 1].

(2.22) COROLLARY†. Let R be a principal ideal domain, P a prime ideal of R , and R^* the P -adic completion of R . Then R^* is a flat R -module. If R is a discrete valuation ring, then R^* is faithfully flat as R -module.

Proof. (See §4e for the relevant definitions.) There is an embedding $R \rightarrow R^*$ which makes R^* into an R -module. Then R^* is R -torsionfree, since R^* is also an integral domain. Therefore R^* is R -flat, by (2.20).

Now suppose that R is a discrete valuation ring, with unique maximal ideal P . Then PR^* is the unique maximal ideal of R^* , so $R^* \neq PR^*$. It follows from (2.21(iv)) that R^* is faithfully flat, as claimed.

(2.23) COROLLARY. Let R^* be the completion of a discrete valuation ring R . For each left R -module M let $M^* = R^* \otimes_R M$, a left R^* -module. Then R^* is faithfully flat as R -module. This means

- (i) For every exact sequence of R -modules

$$0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0,$$

the sequence of R^* -modules

$$0 \rightarrow L^* \rightarrow M^* \rightarrow N^* \rightarrow 0$$

is also exact, and

- (ii) $L^* = 0$ if and only if $L = 0$.

As a matter of fact, the results of (2.23) hold in a more general situation: given any commutative noetherian ring R having a unique maximal ideal P , we may form the P -adic completion R^* of R . It is then true that R^* is a faithfully flat R -module (see Bourbaki [3]).

2d Extensions of modules

We shall first give an informal discussion of $\text{Ext}_{\Lambda}^1(N, L)$ in terms of equivalence classes of extensions of a left Λ -module N by a left Λ -module L . Then we shall define Ext_{Λ}^n in terms of projective resolutions, and shall list standard properties of Ext . In what follows, all modules are left Λ -modules, and we shall write Hom instead of Hom_{Λ} for convenience.

† See also Exercises 5.3, 5.4.

A Λ -exact sequence

$$(2.24) \quad 0 \rightarrow L \xrightarrow{f} X \xrightarrow{g} N \rightarrow 0$$

is called an *extension* of N by L ; sometimes we refer to the module X itself as such an extension. Another extension $0 \rightarrow L \rightarrow X' \rightarrow N \rightarrow 0$ is *equivalent* to that in (2.24) if there exists a Λ -isomorphism θ making the following diagram commutative:

$$\begin{array}{ccccccc} 0 & \rightarrow & L & \rightarrow & X & \rightarrow & N \rightarrow 0 \\ & & \downarrow 1_L & & \downarrow \theta & & \downarrow 1_N \\ 0 & \rightarrow & L & \rightarrow & X' & \rightarrow & N \rightarrow 0, \end{array}$$

where $1_L, 1_N$ are identity maps. This defines an equivalence relation among extensions of N by L . *Caution:* it may happen that $X \cong X'$ even though the extensions are inequivalent.

We shall introduce an additive group $\text{Ext}_\Lambda^1(N, L)$ whose elements are in one-to-one correspondence with the equivalence classes of extensions of N by L . To begin with, choose an epimorphism $\varphi: P \rightarrow N$, where P is Λ -projective (we could even choose P Λ -free, if desired), and let $K = \ker \varphi$. This gives a Λ -exact sequence

$$0 \rightarrow K \xrightarrow{\psi} P \xrightarrow{\varphi} N \rightarrow 0,$$

with ψ the inclusion map. Keeping the Λ -module L fixed, let σ range over the elements of $\text{Hom}(K, L)$. For each such σ , let X_σ denote the pushout of the pair of maps $\psi: K \rightarrow P$, $\sigma: K \rightarrow L$ (see §2a). It follows readily from Exercise 2.2 that there is a commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \rightarrow & K & \xrightarrow{\psi} & P & \xrightarrow{\varphi} & N \rightarrow 0 \\ & & \downarrow \sigma & & \downarrow & & \downarrow 1_N \\ 0 & \rightarrow & L & \rightarrow & X_\sigma & \rightarrow & N \rightarrow 0. \end{array}$$

Thus each $\sigma \in \text{Hom}(K, L)$ yields an extension X_σ of N by L .

The map ψ induces a map $\psi^*: \text{Hom}(P, L) \rightarrow \text{Hom}(K, L)$. For each $\tau \in \text{im } \psi^*$, it is easily verified that the extension $X_{\sigma+\tau}$ is equivalent to X_σ . Hence, each element of the factor group $\text{Hom}(K, L)/\text{im } \psi^*$ determines an equivalence class of extensions of N by L . Conversely, we show that every class can be obtained in this manner. Given any extension (2.24), it follows from the fact that P is projective that there exists a homomorphism ρ making the diagram below commutative:

$$\begin{array}{ccccccc} 0 & \rightarrow & K & \xrightarrow{\psi} & P & \xrightarrow{\varphi} & N \rightarrow 0 \\ & & \downarrow \rho & & & & \downarrow 1_N \\ 0 & \rightarrow & L & \xrightarrow{f} & X & \xrightarrow{g} & N \rightarrow 0. \end{array}$$

Clearly ρ induces a map $\sigma: K \rightarrow L$, and it can be verified that the extension X is equivalent to X_σ . One also checks that the class of X uniquely determines σ modulo the image of ψ^* . Hence there is a bijection between the set of equivalence classes of extensions of N by L , and the additive group given by

$$(2.25) \quad \text{Ext}_\Lambda^1(N, L) = \text{Hom}(K, L)/\psi^*\{\text{Hom}(P, L)\}.$$

The split extension corresponds to 0 in this group. (One can define an additive structure on the set of equivalence classes of extensions, by using “Baer sums”, as in Rotman [1]. In that case, the above bijection is in fact an additive homomorphism, and the expression (2.25) defines Ext up to isomorphism, regardless of the choice of P and φ . We shall not go into further details of this matter, however, but pass at once to the definition of Ext^n by means of projective resolutions.)

Given a left Λ -module N , chose an epimorphism $\varphi_0: F_0 \rightarrow N$, with F_0 free. Then choose an epimorphism $\varphi_1: F_1 \rightarrow \ker \varphi_0$, with F_1 free, and so on. This yields a *free resolution* of N , that is, a Λ -exact sequence

$$\cdots \rightarrow F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} N \rightarrow 0$$

in which each F_i is Λ -free. It is often more convenient to use a more general concept: a *projective resolution* of N is an exact sequence

$$(2.26) \quad \cdots \rightarrow P_2 \xrightarrow{\varphi_2} P_1 \xrightarrow{\varphi_1} P_0 \xrightarrow{\varphi_0} N \rightarrow 0$$

in which each P_i is Λ -projective. (If it happens that $\ker \varphi_m$ is projective for some m , then the process of forming such a resolution can be terminated, giving a finite resolution

$$0 \rightarrow \ker \varphi_m \rightarrow P_m \rightarrow P_{m-1} \rightarrow \cdots \rightarrow P_0 \rightarrow N \rightarrow 0.$$

In this case, we say that N has *finite homological dimension*.)

Given a projective resolution (2.26), the subsequence

$$\mathbf{P}: \cdots \rightarrow P_2 \xrightarrow{\varphi_2} P_1 \xrightarrow{\varphi_1} P_0 \rightarrow 0$$

is called a *deleted projective resolution* of N ; it is an exact sequence except possibly at P_0 . Now let L be a Λ -module, and form the sequence of additive groups

$$\text{Hom}(\mathbf{P}, L): 0 \rightarrow \text{Hom}(P_0, L) \xrightarrow{\varphi_0^*} \text{Hom}(P_1, L) \xrightarrow{\varphi_1^*} \text{Hom}(P_2, L) \rightarrow \cdots,$$

where (as usual) Hom is an abbreviation for Hom_Λ . By (2.4) we have

$$(\varphi_{i+1})^* \cdot (\varphi_i)^* = (\varphi_i \cdot \varphi_{i+1})^* = 0, \quad i \geq 1,$$

and therefore $\text{im } \varphi_i^* \subset \ker \varphi_{i+1}^*$. Now define

$$(2.27) \quad \text{Ext}_\Lambda^n(N, L) = \ker \varphi_{n+1}^*/\text{im } \varphi_n^*, \quad n \geq 1.$$

This yields a sequence of additive groups $\text{Ext}_\Lambda^1(N, L), \text{Ext}_\Lambda^2(N, L), \dots$, the first of which coincides with that given in (2.25).

(2.28) *Remarks.* (i) Up to isomorphism, the group $\text{Ext}_{\Lambda}^n(N, L)$ depends only upon the modules N and L , and not upon the choice of the projective resolution (2.26). (See references.)

(ii) We could have defined $\text{Ext}_{\Lambda}^0(N, L)$ to be $\ker \varphi_1^*$. However, the exactness of the sequence

$$P_1 \xrightarrow{\varphi_1} P_0 \xrightarrow{\varphi_0} N \rightarrow 0$$

implies the exactness of the sequence

$$0 \rightarrow \text{Hom}(N, L) \xrightarrow{\varphi_0^*} \text{Hom}(P_0, L) \xrightarrow{\varphi_1^*} \text{Hom}(P_1, L),$$

by (2.5(ii)). Therefore

$$\ker \varphi_1^* \cong \text{im } \varphi_0^* \cong \text{Hom}(N, L).$$

It is therefore customary to identify $\text{Ext}^0(N, L)$ with $\text{Hom}(N, L)$.

(iii) The groups $\text{Ext}^n(N, L)$ may also be computed by keeping N fixed, and using an injective resolution of L (see references).

(iv) The groups $\text{Ext}^n(N, L)$, $n \geq 1$, have many of the same properties as $\text{Hom}(N, L)$. For instance, Ext^n is additive in each variable:

$$\text{Ext}^n(N_1 + N_2, L) \cong \text{Ext}^n(N_1, L) + \text{Ext}^n(N_2, L),$$

$$\text{Ext}^n(N, L_1 + L_2) \cong \text{Ext}^n(N, L_1) + \text{Ext}^n(N, L_2).$$

Further, Ext^n is contravariant in the first variable, and covariant in the second variable. Thus, each $f \in \text{Hom}(N, N')$ induces additive homomorphisms

$$f_n^*: \text{Ext}^n(N', L) \rightarrow \text{Ext}^n(N, L), \quad n \geq 1.$$

Likewise, each $g \in \text{Hom}(L, L')$ induces additive homomorphisms

$$(g_{*})_n: \text{Ext}^n(N, L) \rightarrow \text{Ext}^n(N, L'), \quad n \geq 1.$$

(v) If N is a projective module, then $0 \rightarrow N \rightarrow N \rightarrow 0$ gives a projective resolution of N . It follows at once from Definition (2.27) that $\text{Ext}^n(N, L) = 0$ for all L and all $n \geq 1$. Conversely, it may be shown that if $\text{Ext}^1(N, L) = 0$ for all L , then N is projective.

One of the most important properties of the groups Ext^n is as follows (see references):

(2.29) **THEOREM.** (Long exact sequence for Ext). *Let*

$$0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$$

be a short exact sequence of Λ -modules, and let L be any Λ -module. Then there is a long exact sequence of extension groups

$$\begin{aligned}
 0 \rightarrow \text{Hom}(C, L) &\xrightarrow{g^*} \text{Hom}(B, L) \xleftarrow{f^*} \text{Hom}(A, L) \\
 &\xrightarrow{\partial_0} \text{Ext}^1(C, L) \xrightarrow{g^*} \text{Ext}^1(B, L) \xleftarrow{f^*} \text{Ext}^1(A, L) \\
 &\xrightarrow{\partial_1} \text{Ext}^2(C, L) \xrightarrow{g^*} \text{Ext}^2(B, L) \xleftarrow{f^*} \text{Ext}^2(A, L) \xrightarrow{\partial_2} \dots
 \end{aligned}$$

(2.30) *Remarks.* (i) We have written Hom , Ext instead of Hom_Λ , Ext_Λ , for convenience. The subscripts on the various maps g^* , f^* have also been omitted; in accordance with the notation of (2.28(iv)), we should have denoted by g_n^* the map $\text{Ext}^n(C, L) \rightarrow \text{Ext}^n(B, L)$ induced by g .

(ii) It is instructive to compare Theorem 2.29 with (2.5(ii)); we now see that (2.5(ii)) gives the start of the long exact sequence of groups occurring in (2.29). Furthermore, we can describe the homomorphism ∂_0 explicitly, provided we view $\text{Ext}^1(C, L)$ as the set of equivalence classes of extensions of C by L . To be precise, given any $h \in \text{Hom}(A, L)$, we define $\partial_0(h)$ to be the equivalence class of the extension occurring in the bottom row of the commutative diagram

$$\begin{array}{ccccccc}
 0 & \rightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C \rightarrow 0 \\
 & & h \downarrow & & \downarrow & & \downarrow \iota_C \\
 0 & \rightarrow & L & \dashrightarrow & X & \dashrightarrow & C \rightarrow 0.
 \end{array}$$

Here, X represents the pushout of the pair of maps (f, h) , and the dotted arrows denote maps defined as in the discussion preceding (2.25).

(iii) It is somewhat more difficult to describe the additive homomorphisms $\partial_1, \partial_2, \dots$ explicitly. One procedure is to define them recursively, using the dimension-shifting techniques given in (iv) below. Another method uses the fact (2.28(iii)) that we can compute all of the groups $\text{Ext}^n(\cdot, L)$ by starting with an injective resolution of L ; in this context, the long exact sequence of (2.29) arises naturally from an exact triangle associated with an exact sequence of graded complexes.

(iv) Formula 2.25 now appears in a more natural setting. From the short exact sequence

$$0 \rightarrow K \xrightarrow{\psi} P \xrightarrow{\varphi} N \rightarrow 0, \quad P \text{ projective},$$

we obtain a long exact sequence of additive groups

$$\text{Hom}(P, L) \xrightarrow{\psi^*} \text{Hom}(K, L) \rightarrow \text{Ext}^1(N, L) \rightarrow \text{Ext}^1(P, L) \rightarrow \dots$$

But $\text{Ext}^1(P, L) = 0$ by (2.28v), and so we obtain an isomorphism between the expressions given in (2.25).

Furthermore, since $\text{Ext}^n(P, L) = 0, n \geq 1$, we obtain an isomorphism

$$\text{Ext}^{n+1}(N, L) \cong \text{Ext}^n(K, L), \quad n \geq 1,$$

for each module L . By means of this formula, the calculation of Ext^{n+1} may

be reduced to that of Ext^n . This procedure is called *dimension shifting*. A more general version is as follows: Given a Λ -exact sequence

$$(2.31) \quad 0 \rightarrow K_n \rightarrow P_n \rightarrow P_{n-1} \rightarrow \cdots \rightarrow P_0 \rightarrow N \rightarrow 0,$$

where P_i is projective, $0 \leq i \leq n$, then for each Λ -module L and for each $m \geq 1$, there is an isomorphism of additive groups

$$(2.32) \quad \text{Ext}^{m+n+1}(N, L) \cong \text{Ext}^m(K_n, L).$$

(v) Let N be a Λ -module, and let

$$0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$$

be a Λ -exact sequence. An analogue of Theorem 2.29 states that there is a long exact sequence of extension groups

$$\begin{aligned} 0 \rightarrow \text{Hom}(N, A) &\xrightarrow{f_*} \text{Hom}(N, B) \xrightarrow{g_*} \text{Hom}(N, C) \xrightarrow{\partial} \text{Ext}^1(N, A) \\ &\xrightarrow{f_*} \text{Ext}^1(N, B) \xrightarrow{g_*} \text{Ext}^1(N, C) \xrightarrow{\partial} \text{Ext}^2(N, A) \rightarrow \cdots. \end{aligned}$$

We shall not attempt to describe the maps ∂ occurring here.

Another basic property of extension groups is as follows (see references):

(2.33) **THEOREM** (Ladder theorem). *Given a commutative diagram of Λ -modules and Λ -homomorphisms with exact rows:*

$$\begin{array}{ccccccc} 0 & \rightarrow & A & \rightarrow & B & \rightarrow & C & \rightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \rightarrow & A' & \rightarrow & B' & \rightarrow & C' & \rightarrow 0, \end{array}$$

and given any Λ -module L , there is a commutative diagram of additive groups and homomorphisms with exact rows:

$$\begin{array}{ccccccccc} 0 \rightarrow \text{Hom}(C, L) & \rightarrow & \text{Hom}(B, L) & \rightarrow & \text{Hom}(A, L) & \rightarrow & \text{Ext}^1(C, L) & \rightarrow & \text{Ext}^1(B, L) \rightarrow \cdots \\ & \uparrow & \\ 0 \rightarrow \text{Hom}(C', L) & \rightarrow & \text{Hom}(B', L) & \rightarrow & \text{Hom}(A', L) & \rightarrow & \text{Ext}^1(C', L) & \rightarrow & \text{Ext}^1(B', L) \rightarrow \cdots. \end{array}$$

We conclude with some results on finite generation of extension groups. Let R be a commutative ring, and let Λ be an R -algebra. Then Λ itself, and all Λ -modules, can be viewed as R -modules. If L, M, \dots denote Λ -modules, then the additive groups $\text{Hom}_\Lambda(L, M)$, $L \otimes_\Lambda M$, $\text{Ext}_\Lambda^n(L, M)$ ($n \geq 1$) are also R -modules, and all of the various maps so far mentioned in this section are R -homomorphisms.

In particular, suppose that R is a noetherian commutative ring, and that Λ is finitely generated as R -module. For any Λ -module N which is finitely generated over R , all of the Λ -modules occurring in a projective resolution of N may be chosen finitely generated over R . This readily implies

(2.34) THEOREM. Let Λ be an R -algebra, finitely generated as module over the commutative noetherian ring R . Let L, M, \dots denote Λ -modules which are finitely generated over R (or equivalently, over Λ). Then the R -modules

$$\mathrm{Hom}_{\Lambda}(L, M), \quad L \otimes_{\Lambda} M, \quad \mathrm{Ext}_{\Lambda}^n(L, M), \quad n \geq 1,$$

are also finitely generated over R .

2e Change of rings in Hom and Ext

Throughout this section let R be a commutative ring with unity element. Suppose for the moment that R' is a ring of quotients of R with respect to some multiplicative subset of R (see §3a). For each R -module M , we may form the R' -module

$$M' = R' \otimes_R M.$$

It is often necessary to know how Hom and Ext behave under passage from R to R' . The aim of this section is to establish formulas such as

$$R' \otimes_R \mathrm{Hom}_R(M, N) \cong \mathrm{Hom}_{R'}(M', N')$$

and likewise for Ext, assuming that the R -modules M and N satisfy some mild hypotheses. A significant role is played by the fact that R' is R -flat (see §2c). We shall prove formulas of the above type in somewhat more general circumstances, which will in fact be met later on.

Let $\Lambda^{(r)}$ denote the left Λ -module which is the external direct sum of r copies of Λ . If M is any finitely generated left Λ -module, there is an epimorphism $\varphi_0: \Lambda^{(r)} \rightarrow M$ for some r . If Λ is left noetherian, then by (2.9) $\ker \varphi_0$ is also finitely generated, and so there is an epimorphism $\varphi_1: \Lambda^{(s)} \rightarrow \ker \varphi_0$ for some s . Thus we obtain a Λ -exact sequence

$$(2.35) \quad \Lambda^{(s)} \rightarrow \Lambda^{(r)} \rightarrow M \rightarrow 0.$$

Even if Λ is not necessarily noetherian, it may happen that the module M occurs in some sequence of this type, with r, s finite. In such case, we say that M is a *finitely presented* Λ -module. We emphasize that when Λ is left noetherian, every finitely generated left Λ -module is necessarily finitely presented.

Now let Λ and Γ be R -algebras and let M, N, \dots be left Λ -modules. Set

$$\Lambda' = \Gamma \otimes_R \Lambda, \quad M' = \Gamma \otimes_R M, \dots,$$

so M' is a left module over the R -algebra Λ' . There exists an R -homomorphism

$$(2.36) \quad \alpha: \Gamma \otimes_R \mathrm{Hom}_\Lambda(M, N) \rightarrow \mathrm{Hom}_{\Lambda'}(M', N'),$$

given by

$$\alpha(\gamma \otimes f) = \gamma_r \otimes f, \quad \gamma \in \Gamma, \quad f \in \mathrm{Hom}_\Lambda(M, N),$$

where γ_r denotes the right multiplication by γ acting on Γ . By virtue of the bimodule structures ${}_\Gamma\Gamma_R$ and ${}_{\Lambda'}(M')_\Gamma$, both sides of (2.36) have the structure of left Γ -modules. It is easily checked that α is a left Γ -homomorphism. Analogously, the bimodule structures $\Gamma_{\Gamma,R}$ and ${}_{\Lambda'}(N')_\Gamma$ make the expressions in (2.36) into right Γ -modules, and α is also a right Γ -homomorphism.

(2.37) **THEOREM.** *Let Λ and Γ be R -algebras, M and N left Λ -modules. Suppose that Γ is R -flat, and that M is finitely generated as Λ -module. Then the map α in (2.36) is a two-sided Γ -monomorphism.*

Proof. There is a Λ -exact sequence

$$0 \rightarrow K \rightarrow \Lambda^{(r)} \rightarrow M \rightarrow 0$$

for some r . It follows from (2.5) that the sequence of R -modules

$$0 \rightarrow \text{Hom}_\Lambda(M, N) \rightarrow \text{Hom}_\Lambda(\Lambda^{(r)}, N)$$

is also exact. Since Γ is R -flat, exactness is preserved when the functor $\Gamma \otimes_R \cdot$ is applied to the above two sequences. We obtain two new exact sequences:

$$0 \rightarrow K' \rightarrow \Lambda'^{(r)} \rightarrow M' \rightarrow 0,$$

and

$$0 \rightarrow \Gamma \otimes_R \text{Hom}_\Lambda(M, N) \rightarrow \Gamma \otimes_R \text{Hom}_\Lambda(\Lambda^{(r)}, N).$$

By virtue of (2.5), the first of these sequences gives rise to an exact sequence

$$0 \rightarrow \text{Hom}_{\Lambda'}(M', N') \rightarrow \text{Hom}_{\Lambda'}(\Lambda'^{(r)}, N').$$

Therefore we obtain a commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \rightarrow & \Gamma \otimes_R \text{Hom}_\Lambda(M, N) & \rightarrow & \Gamma \otimes_R \text{Hom}_\Lambda(\Lambda^{(r)}, N) & & \\ & & \downarrow \alpha & & \downarrow \alpha_1 & & \\ 0 & \rightarrow & \text{Hom}_{\Lambda'}(M', N') & \longrightarrow & \text{Hom}_{\Lambda'}(\Lambda'^{(r)}, N'), & & \end{array}$$

in which the vertical maps α, α_1 are precisely those given by (2.36). But α_1 is an isomorphism, since (2.7) gives

$$\Gamma \otimes_R \text{Hom}_\Lambda(\Lambda^{(r)}, N) \cong \Gamma \otimes_R N^{(r)} \cong (N')^{(r)} \cong \text{Hom}_{\Lambda'}(\Lambda'^{(r)}, N').$$

It follows at once that α is monic, and the theorem is proved.

A variant of the preceding result is as follows:

(2.38) **Theorem.** *Let Λ and Γ be R -algebras, M and N left Λ -modules. Suppose that Γ is R -flat, and that M is a finitely presented Λ -module. Then the map α in (2.36) is a two-sided Γ -isomorphism.*

Proof. There is a Λ -exact sequence

$$\Lambda^{(s)} \rightarrow \Lambda^{(r)} \rightarrow M \rightarrow 0$$

for some r and s . By (2.5), the sequence

$$0 \rightarrow \text{Hom}_{\Lambda}(M, N) \rightarrow \text{Hom}_{\Lambda}(\Lambda^{(r)}, N) \rightarrow \text{Hom}_{\Lambda}(\Lambda^{(s)}, N)$$

is R -exact. As in the proof of (2.37), we obtain a commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \rightarrow & \Gamma \otimes_R \text{Hom}_{\Lambda}(M, N) & \rightarrow & \Gamma \otimes_R \text{Hom}_{\Lambda}(\Lambda^{(r)}, N) & \rightarrow & \Gamma \otimes_R \text{Hom}_{\Lambda}(\Lambda^{(s)}, N) \\ & & \downarrow \alpha & & \downarrow \alpha_1 & & \downarrow \alpha_2 \\ 0 & \rightarrow & \text{Hom}_{\Lambda'}(M', N') & \longrightarrow & \text{Hom}_{\Lambda'}(\Lambda'^{(r)}, N') & \longrightarrow & \text{Hom}_{\Lambda'}(\Lambda'^{(s)}, N'). \end{array}$$

As in (2.37), both maps α_1 and α_2 are isomorphisms. This implies at once that α is an isomorphism, and the theorem is proved.

(2.39) **Theorem** (Change of rings). *Let R be a commutative ring, and let Γ and Λ be R -algebras such that Λ is left noetherian and Γ is R -flat. Let M be a finitely generated left Λ -module, and let N be arbitrary. Then the two-sided Γ -isomorphism given by (2.36) is the first of a family of two-sided Γ -isomorphisms*

$$\Gamma \otimes_R \text{Ext}_{\Lambda}^n(M, N) \cong \text{Ext}_{\Lambda'}^n(M', N'), \quad n \geq 0,$$

where

$$\Lambda' = \Gamma \otimes_R \Lambda, \quad M' = \Gamma \otimes_R M, \quad N' = \Gamma \otimes_R N.$$

Proof. The hypotheses on M and Λ imply that M is finitely presented, so the map α in (2.36) is an isomorphism by (2.38). Now let

$$\longrightarrow P_2 \xrightarrow{\varphi_2} P_1 \xrightarrow{\varphi_1} P_0 \longrightarrow M \longrightarrow 0$$

be a free Λ -resolution of M , chosen so that each P_i is Λ -free on a finite number of generators. (Such a resolution exists since Λ is left noetherian.) Then forming the sequence

$$(2.40) \quad 0 \longrightarrow \text{Hom}_{\Lambda}(P_0, N) \xrightarrow{\varphi_1^*} \text{Hom}_{\Lambda}(P_1, N) \xrightarrow{\varphi_2^*} \cdots,$$

we have (by (2.27))

$$\text{Ext}_{\Lambda}^n(M, N) \cong \ker \varphi_{n+1}^* / \text{im } \varphi_n^*, \quad n \geq 1.$$

Since Γ is R -flat, we have

$$(2.41) \quad \Gamma \otimes_R \text{Ext}_{\Lambda}^n(M, N) \cong \ker 1 \otimes \varphi_{n+1}^* / \text{im } 1 \otimes \varphi_n^*,$$

where for $n \geq 1$,

$$1 \otimes \varphi_n^*: \Gamma \otimes_R \text{Hom}_\Lambda(P_{n-1}, N) \rightarrow \Gamma \otimes_R \text{Hom}_\Lambda(P_n, N).$$

By (2.38), the vertical arrows in the following commutative diagram are two-sided Γ -isomorphisms:

$$(2.42) \quad \begin{array}{ccc} \Gamma \otimes_R \text{Hom}_\Lambda(P_{n-1}, N) & \xrightarrow{1 \otimes \varphi_n^*} & \Gamma \otimes_R \text{Hom}_\Lambda(P_n, N) \\ \downarrow & & \downarrow \\ \text{Hom}_{\Lambda'}(P'_{n-1}, N') & \xrightarrow{\psi_n^*} & \text{Hom}_{\Lambda'}(P'_n, N'). \end{array}$$

The map ψ_n^* occurring above is obtained as follows: applying the exact functor $\Gamma \otimes_{R'}$ to the original free resolution of M , we obtain a free Λ' -resolution of M' , namely,

$$\longrightarrow P'_2 \xrightarrow{\psi_2} P'_1 \xrightarrow{\psi_1} P'_0 \longrightarrow M' \longrightarrow 0.$$

This in turn yields a sequence

$$0 \longrightarrow \text{Hom}_{\Lambda'}(P'_0, N') \xrightarrow{\psi_1^*} \text{Hom}_{\Lambda'}(P'_1, N') \xrightarrow{\psi_2^*} \cdots,$$

in which the maps ψ_n^* occur. By definition,

$$\text{Ext}_{\Lambda'}^n(M', N') = \ker \psi_{n+1}^*/\text{im } \psi_n^*.$$

Comparing this formula with that given in (2.41), and using the fact that the vertical arrows in the commutative diagram (2.42) are isomorphisms, we conclude at once that

$$\Gamma \otimes_R \text{Ext}_{\Lambda'}^n(M, N) \cong \text{Ext}_{\Lambda'}^n(M', N'), \quad n \geq 1.$$

This is a two-sided Γ -isomorphism, since all of the maps occurring in the proof are two-sided Γ -maps. The result also holds when $n = 0$, if we set $\text{Ext}^0 = \text{Hom}$. This completes the proof.

(2.43) COROLLARY. *Let R be a commutative ring, and let R' be the ring of quotients† of R with respect to some multiplicative subset of R . Let Λ be any left noetherian R -algebra. Then for each finitely generated left Λ -module M , and any Λ -module N , there is an R' -isomorphism*

$$R' \otimes_R \text{Ext}_{\Lambda'}^n(M, N) \cong \text{Ext}_{\Lambda'}^n(M', N'), \quad n \geq 0,$$

where $\Lambda' = R' \otimes_R \Lambda$, $M' = R' \otimes_R M$, and so on. This isomorphism extends that given by (2.36) for the case $n = 0$.

2f Hereditary rings

A ring Λ with unity element is *left hereditary* if every left ideal of Λ is a projective Λ -module. As we shall see eventually, maximal orders are heredi-

† See §3a.

tary rings, and some of the important facts about maximal orders are actually special cases of assertions about hereditary rings.

(2.44) THEOREM. *If Λ is a left hereditary ring, then every submodule of a free left Λ -module M is isomorphic to an external direct sum of left ideals of Λ , and is therefore projective.*

Proof.[†] Let $\{m_1, \dots, m_k\}$ be a free Λ -basis of M , and let N be any submodule of M . We shall use induction on k to show that N is isomorphic to an external direct sum of left ideals of Λ . The result is obvious for $k = 1$, so now let $k > 1$, and assume that the theorem holds for submodules of M' , where $M' = \Lambda m_2 + \dots + \Lambda m_k$.

Each $n \in N$ is expressible in the form

$$n = r_1 m_1 + \dots + r_k m_k, \quad r_i \in \Lambda,$$

with uniquely determined coefficients $\{r_i\}$. Let J be the set of all first coefficients r_1 which occur as n ranges over all elements of N . Then J is a left ideal of Λ , and there is an epimorphism $\varphi: N \rightarrow J$ given by $\varphi(n) = r_1$, $n \in N$. Clearly $\ker \varphi = N \cap M'$, so there is a Λ -exact sequence

$$0 \longrightarrow N \cap M' \longrightarrow N \xrightarrow{\varphi} J \longrightarrow 0.$$

Since Λ is left hereditary, the left ideal J is Λ -projective, and so the above sequence splits by (2.14). Therefore

$$N \cong J \oplus N \cap M'.$$

But $N \cap M'$ is a submodule of M' , and thus $N \cap M'$ is isomorphic to an external direct sum of left ideals of Λ , by the induction hypothesis. Hence N is also isomorphic to such a sum. Finally, each summand is projective, whence so is N .

(2.45) Remarks. (i) If the ring Λ has the property that submodules of free left modules are projective, then in particular all left ideals of Λ are projective. By (2.44), we may conclude that Λ is left hereditary if and only if submodules of free modules are projective.

(ii) The importance of (2.44) is that it gives us a structure theorem for submodules of free Λ -modules when Λ is hereditary. This structure theorem generalizes the one valid for modules over a principal ideal domain, since clearly every such domain is hereditary. The above proof shows further that

[†]We give the proof only for the case where M is finitely generated: it is this special case which arises most frequently in practice. For the general case, see Cartan–Eilenberg [1].

a submodule of a free module on k generators is isomorphic to an external direct sum of at most k left ideals of Λ .

(iii) There are examples of rings which are left hereditary but not right hereditary. However, if Λ is left and right noetherian, then Λ is left hereditary if and only if Λ is right hereditary (see Rotman [1, Corollary 9.20]; the result is due to M. Auslander).

(iv) The proof of (2.44), for the case where M is not finitely generated, proceeds in much the same manner as the above proof. The main difference is that k must be allowed to be transfinite, and the proof uses transfinite induction.

EXERCISES

1. Let

$$\begin{array}{ccc} Y & \xrightarrow{g_1} & M_1 \\ g_2 \downarrow & & \downarrow f_1 \\ M_2 & \xrightarrow{f_2} & \overline{M} \end{array}$$

be a pullback diagram of Λ -modules. Prove

- (i) g_2 induces an isomorphism $\ker g_1 \cong \ker f_2$.
- (ii) If f_2 is epic, then so is g_1 .

2. Let

$$\begin{array}{ccc} L & \xrightarrow{f_1} & N_1 \\ f_2 \downarrow & & \downarrow g_1 \\ N_2 & \xrightarrow{g_2} & X \end{array}$$

be a pushout diagram of Λ -modules. Prove

- (i) g_1 induces an isomorphism $\operatorname{cok} f_1 \cong \operatorname{cok} g_2$.
- (ii) If f_1 is monic, then so is g_2 .

3. Let Γ and Δ be rings, and suppose we have modules M_Γ , L_Δ , and a bimodule ${}_\Delta N_\Gamma$. Show that there is a well-defined additive homomorphism

$$\alpha: L \otimes_\Delta \operatorname{Hom}_\Gamma(M, N) \rightarrow \operatorname{Hom}_\Gamma(M, L \otimes_\Delta N),$$

defined by $l \otimes f \mapsto (l, f)$, where

$$(l, f)m = l \otimes fm, \quad l \in L, \quad f \in \operatorname{Hom}_\Gamma(M, N), \quad m \in M.$$

Prove that α is an isomorphism whenever L is Δ -flat and M is a finitely presented Γ -module. [Hint: Imitate the proof of (2.38), using \otimes_Δ in place of \otimes_R .]

4. Let Δ be a ring, and let L_Δ be flat, and M_Δ finitely presented. Use Exercise 3 to prove that

$$L \otimes_\Delta \operatorname{Hom}_\Delta(M, \Delta) \cong \operatorname{Hom}_\Delta(M, L).$$

5. Let Δ be a ring, L_Δ any module, and let M_Δ be a finitely generated projective module. Prove that

$$L \otimes_\Delta \text{Hom}_\Delta(M, \Delta) \cong \text{Hom}_\Delta(M, L).$$

[Hint: Use (2.17).]

6. Let $\varphi: R \rightarrow S$ be a homomorphism of commutative rings, and let J be an ideal in R . Prove that

$$S \otimes_R (R/J) \cong S/S \cdot \varphi(J)$$

as S -modules.

7. Prove Schanuel's Lemma: Given two exact sequences of left Λ -modules

$$0 \rightarrow M \rightarrow P \xrightarrow{\varphi} X \rightarrow 0, \quad 0 \rightarrow M' \rightarrow P' \xrightarrow{\psi} X \rightarrow 0,$$

in which P and P' are projective, there is a Λ -isomorphism

$$M' \dotplus P \cong M \dotplus P'.$$

[Hint: Let A be the pullback of the pair of maps φ, ψ . Then there exist Λ -exact sequences

$$0 \rightarrow K \rightarrow A \rightarrow P \rightarrow 0, \quad 0 \rightarrow K' \rightarrow A \rightarrow P' \rightarrow 0,$$

with $K \cong \ker \psi \cong M'$, $K' \cong \ker \varphi \cong M$. Since P and P' are projective, $A \cong P \dotplus K \cong P' \dotplus K'$.]

8. Prove the Snake Lemma: Given a commutative diagram of modules, with exact rows:

$$\begin{array}{ccccccc} A & \xrightarrow{\varphi} & B & \rightarrow & C & \rightarrow & 0 \\ \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow & & \\ 0 \rightarrow A' \rightarrow B' & \xrightarrow{\psi} & C' & & & & \end{array}$$

there is an exact sequence

$$\ker \alpha \xrightarrow{\varphi_*} \ker \beta \rightarrow \ker \gamma \xrightarrow{\delta} \text{cok } \alpha \rightarrow \text{cok } \beta \xrightarrow{\psi_*} \text{cok } \gamma.$$

If φ is monic, so is φ_* . If ψ is epic, so is ψ_* . The lemma remains true for a diagram of groups and group homomorphisms, if each of the groups A', B' and C' is commutative. [Hint: Define $\delta(c) = a' + \text{im } \alpha$, where

$$a' \rightarrow b', \quad b' = \beta(b), \quad b \rightarrow c.]$$

3. LOCALIZATION

3a Rings of quotients

Throughout this section, R denotes a commutative ring. A *multiplicative subset* of R is a subset S closed under multiplication, and such that $0 \notin S$, $1 \in S$. We introduce an equivalence relation on the Cartesian product

$R \times S$ by setting $(a, s) \sim (a', s')$ if and only if $t(sa' - s'a) = 0$ for some $t \in S$. Let a/s (or $s^{-1}a$) denote the equivalence class of the pair (a, s) . Now define

$$\frac{a}{s} \pm \frac{b}{t} = \frac{ta \pm sb}{st}, \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st},$$

verifying that these operations are indeed well-defined. The set of symbols $\{a/s\}$ then forms a commutative ring, denoted by $S^{-1}R$, with unity element $1/1$ and zero element $0/1$. For $s \in S$, we have

$$(s/1) \cdot (1/s) = 1/1,$$

so $s/1$ is a unit in $S^{-1}R$, with inverse $1/s$. Denoting $1/s$ by s^{-1} , we obtain

$$a/s = (1/s)(a/1) = s^{-1}(a/1).$$

We shall call $S^{-1}R$ a *ring of quotients* of R .

An element $a \in R$ is an *S -torsion* element if $ta = 0$ for some $t \in S$. The above discussion shows at once that (a, s) lies in the zero class of $S^{-1}R$ if and only if a is an S -torsion element of R . There is a ring homomorphism

$$i: R \rightarrow S^{-1}R,$$

given by $i(x) = x/1$, $x \in R$. Then $\ker i$ is precisely the set of S -torsion elements of R . The map i permits us to view $S^{-1}R$ as R -module.

If R is an integral domain, the map i may be regarded as an embedding of R into $S^{-1}R$; in particular, if $S = R - \{0\}$, then $S^{-1}R$ is precisely the quotient field of R . For an arbitrary ring R , the map i is monic if and only if R is S -torsionfree (that is, R contains no nonzero S -torsion elements, or equivalently, S contains no divisors of zero).

(3.1) THEOREM. *Let S be a multiplicative subset of R . Then any ring homomorphism $\varphi: R \rightarrow R'$ which maps each element of S onto a unit of R' , extends uniquely to a ring homomorphism $\psi: S^{-1}R \rightarrow R'$ such that $\psi \circ i = \varphi$.*

Proof. Define

$$\psi(a/s) = \varphi(a)/\varphi(s), \quad a \in A, \quad s \in S.$$

It is easily checked that ψ is the desired homomorphism. If also $\psi' \circ i = \varphi$, then

$$\psi'(a/s) = \psi'(a/1) \cdot \psi'(1/s) = \varphi(a)/\varphi(s) = \psi(a/s),$$

so $\psi = \psi'$.

(3.2) COROLLARY. *Let $\varphi: R \rightarrow R'$ be a ring homomorphism mapping a multiplicative subset S of R into a multiplicative subset S' of R' . Then there is a*

unique ring homomorphism $\psi: S^{-1}R \rightarrow S'^{-1}R'$ which extends φ , that is, $\psi(a/1) = \varphi(a)/1$, $a \in R$.

3b Modules of quotients

Let S be a multiplicative subset of the commutative ring R , and M any R -module. We view $S^{-1}R$ as R -module by means of the canonical map $i: R \rightarrow S^{-1}R$, and we form the $S^{-1}R$ -module

$$S^{-1}M = S^{-1}R \otimes_R M.$$

We shall call $S^{-1}M$ a *module of quotients*. Each $x \in S^{-1}M$ is then expressible as a finite sum

$$x = \sum a_i s_i^{-1} \otimes m_i, \quad a_i \in R, \quad s_i \in S, \quad m_i \in M.$$

Set $s = \prod s_i \in S$; then

$$x = \sum s^{-1} \cdot a_i s s_i^{-1} \otimes m_i = s^{-1} \otimes \sum a_i s s_i^{-1} m_i = s^{-1} \otimes m,$$

say. Denote $s^{-1} \otimes m$ by m/s ; we have thus shown that every element of $S^{-1}M$ is of the form m/s for some $m \in M$, $s \in S$. It is easily checked that

$$m/s \pm m'/s' = (s'm \pm sm')/ss'.$$

We shall call an element m of an R -module M an *S -torsion element* if $sm = 0$ for some $s \in S$. The collection of all S -torsion elements of M is called the *S -torsion submodule* of M , and is an R -submodule of M .

(3.3) THEOREM. Let M' be the S -torsion submodule of M . Then $m/s = 0$ in $S^{-1}M$ if and only if $m \in M'$.

Proof. If $m \in M'$, then $tm = 0$ for some $t \in S$, whence

$$m/s = s^{-1} \otimes m = (st)^{-1} \otimes tm = 0.$$

Conversely, suppose that $s^{-1} \otimes m_0 = 0$ in $S^{-1}M$. Then $1 \otimes m_0 = s(s^{-1} \otimes m_0) = 0$, and therefore $1 \otimes m_0$ is expressible as a finite sum of elements of $S^{-1}M$ of the following three types:

$$(u + u') \otimes m - u \otimes m - u' \otimes m, \quad u \otimes (m + m') - u \otimes m - u \otimes m',$$

$$ua \otimes m - u \otimes am,$$

with $u, u' \in S^{-1}R$, $m, m' \in M$, $a \in R$. Choose $t \in S$ to be a common denominator for all of the u 's which occur in these terms, so that $tu \in R$ for each such u (or more precisely, $tu \in i(R)$). Let

$$R_1 = t^{-1} \cdot i(R) = \{a/t : a \in R\},$$

an R -submodule of $S^{-1}R$.

We shall now define a homomorphism

$$f: R_1 \otimes_R M \rightarrow M/M'$$

by setting

$$f(x \otimes m) = txm + M', \quad x \in R_1, \quad m \in M.$$

This map f is well-defined, since if $x = a/t = b/t$ in R_1 , then $a - b$ is an S -torsion element of R , and hence $(a - b)m \in M'$. Consider now the element $1 \otimes m_0$. From the manner in which R_1 was chosen, it is clear that $1 \otimes m_0 = 0$ in $R_1 \otimes_R M$. Therefore $f(1 \otimes m_0) = 0$ in M/M' , that is, $tm_0 \in M'$. This implies that m_0 also lies in M' , which completes the proof of the theorem.

(3.4) COROLLARY. *The module of quotients $S^{-1}M$ coincides with the module whose elements are equivalence classes of ordered pairs (m, s) , with $(m, s) \sim (m', s')$ if and only if $s'm - sm'$ is an S -torsion element of M . The class of (m, s) may be identified with the element $m/s = s^{-1} \otimes m$ in $S^{-1}M$.*

The $S^{-1}R$ -module $S^{-1}M$ may be viewed as an R -module by use of the homomorphism $i: R \rightarrow S^{-1}R$; in other words, an element $a \in R$ acts on $S^{-1}M$ as left multiplication by the element $a/1$ of $S^{-1}R$. We shall say that the element $a \in R$ acts invertibly on an R -module X if the mapping $x \mapsto ax$, $x \in X$, gives a one-to-one map of X onto itself. It is then clear that every element of S acts invertibly on the module of quotients $S^{-1}M$.

On the other hand, given any R -module X on which every element of S acts invertibly, we can make X into an $S^{-1}R$ -module by defining

$$(3.5) \quad (a/s) \cdot x = s^{-1} \cdot ax, \quad a \in R, \quad s \in S, \quad x \in X.$$

This is the unique way in which X can be made into an $S^{-1}R$ -module so as to preserve the action of R on X .

(3.6) THEOREM. *Let X be an R -module on which every element of S acts invertibly, and make X into an $S^{-1}R$ -module by means of (3.5). Then there is an $S^{-1}R$ -isomorphism*

$$S^{-1}R \otimes_R X \cong X.$$

Further, for each R -module Y , every R -homomorphism $f: Y \rightarrow X$ extends canonically to an $S^{-1}R$ -homomorphism $f': S^{-1}Y \rightarrow X$, given by the formula

$$f'(u \otimes y) = u \cdot f(y), \quad u \in S^{-1}R, \quad y \in Y.$$

Proof. By (3.4), every element of $S^{-1}R \otimes_R X$ is expressible as $s^{-1} \otimes x$, with $s \in S$, $x \in X$. Denote this element by x/s . By (3.4) we have $x/s = x'/s'$ if and

only if $s'x - sx'$ is an S -torsion element of X . But S acts invertibly on X , so X is S -torsion free. Thus $x/s = x'/s'$ if and only if $s'x = sx'$.

Now define a mapping $\theta: S^{-1}R \otimes_R X \rightarrow X$ by setting $\theta(x/s) = s^{-1}x$, $x \in X$, $s \in S$. The preceding remarks imply that θ is well-defined; for if $x/s = x'/s'$, then $s^{-1}x = s'^{-1}x'$. Clearly θ is epic, and is an $S^{-1}R$ -homomorphism. Finally, θ is monic, since if $\theta(x/s) = 0$, then $s^{-1}x = 0$ and hence also $x = 0$. This proves the first part of the theorem. We omit the straightforward proof of the second part.

3c Flatness

Recall that an R -module is *flat* if tensoring with it preserves exactness (see §2c). We shall now prove that every ring of quotients $S^{-1}R$ is a flat R -module.

Given any R -homomorphism $f:L \rightarrow M$ of R -modules, there is an $S^{-1}R$ -homomorphism $f_*: S^{-1}L \rightarrow S^{-1}M$, defined by setting $f_* = 1 \otimes f$, where

$$1 \otimes f: S^{-1}R \otimes_R L \rightarrow S^{-1}R \otimes_R M.$$

Thus

$$(3.7) \quad f_*(l/s) = f(l)/s, \quad l \in L, \quad s \in S.$$

Using this we prove

(3.8) THEOREM. Let $L \xrightarrow{f} M \xrightarrow{g} N$ be an R -exact sequence, and let f_* , g_* be defined as in (3.7). Then

$$S^{-1}L \xrightarrow{f_*} S^{-1}M \xrightarrow{g_*} S^{-1}N$$

is an exact sequence of $S^{-1}R$ -modules.

Proof. Since $gf = 0$, we have $g_*f_* = (gf)_* = 0$. Now let $x \in \ker g_*$, and write $x = m/s$, $m \in M$, $s \in S$. Then

$$0 = g_*(m/s) = s^{-1}g(m),$$

so $1 \otimes g(m) = 0$ in $S^{-1}N$. Hence there exists an element $t \in S$ such that $t \cdot g(m) = 0$, that is, $g(tm) = 0$. But $\ker g = \text{im } f$, and so we may write $tm = f(l)$ for some $l \in L$. Then

$$x = m/s = tm/ts = f_*(l/ts) \in \text{im } f_*.$$

This shows that $\ker g_* = \text{im } f_*$. Finally, it is clear that f_* and g_* are $S^{-1}R$ -homomorphisms, which completes the proof.

For later use, we state a special case of (3.8):

(3.9) COROLLARY. An inclusion $L \subset M$ of R -modules induces an inclusion $S^{-1}L \subset S^{-1}M$ of $S^{-1}R$ -modules, and there is an $S^{-1}R$ -isomorphism

$$S^{-1}(M/L) \cong S^{-1}M/S^{-1}L.$$

Recall that an R -module M is *noetherian* if its submodules satisfy the ascending chain condition. A ring Λ is (*left*) *noetherian* if Λ is noetherian as left Λ -module. Analogously, M is *artinian* if its submodules satisfy the descending chain condition.

We wish to prove that the properties of being noetherian or artinian are preserved under formation of rings or modules of quotients. This is best accomplished by using the concept of “saturation”. Let $L \subset M$ be R -modules; call L an *S -saturated*[†] submodule of M if M/L is S -torsionfree, that is, M/L has no nonzero S -torsion elements. Equivalently, L is S -saturated in M if for $m \in M, s \in S$, the inclusion $sm \in L$ implies that $m \in L$.

(3.10) THEOREM. Let $i: M \rightarrow S^{-1}M$ be defined by $i(m) = 1 \otimes m, m \in M$. There is a one-to-one inclusion-preserving correspondence between the set of S -saturated submodules X of the R -module M , and the set of $S^{-1}R$ -submodules X' of $S^{-1}M$, given by

$$X' = S^{-1}X, \quad X = i^{-1}(X').$$

Proof. Straightforward exercise for the reader.

As an immediate consequence of (3.10), we obtain

(3.11) THEOREM. If M is a noetherian R -module, then $S^{-1}M$ is a noetherian $S^{-1}R$ -module. In particular, if R is a noetherian ring, so is $S^{-1}R$. The analogous results hold true with “noetherian” replaced by “artinian”.

3d Localization at prime ideals

Let R be a commutative ring, and let J, J' denote ideals of R . We write $J < J'$ to indicate that J is properly contained in J' . Let us set

$$R - J = \{x: x \in R, x \notin J\}.$$

(3.12) Definitions. (i) J is a *proper* ideal if $J < R$.

(ii) J is a *maximal* ideal if $J < R$, and if there is no ideal J' such that $J < J' < R$.

(iii) J is a *prime* ideal if $J < R$, and R/J has no zero divisors.

Clearly, a proper ideal J is prime if and only if its complement $R - J$ is a multiplicative set. Starting with a prime ideal P of R , we may form the multiplicative set $S = R - P$, and then define a ring of quotients $S^{-1}R$.

[†] See Bourbaki, Algèbre Commutative, page 69 for this terminology.

This ring, hereafter denoted by R_P , is called the *localization* of R at P . Since every element of $R - P$ is invertible in R_P , it is easily verified that R_P has a unique maximal ideal, namely $P \cdot R_P$. We should remark that the ring homomorphism $i: R \rightarrow R_P$, defined in §3a, enables us to view R_P (and all R_P -modules) as R -modules. Thus $P \cdot R_P$ is the same as $i(P) \cdot R_P$.

If R happens to be an integral domain, then the mapping $i: R \rightarrow R_P$ is an embedding. In particular, when $P = \{0\}$ then R_P is precisely the quotient field of the domain R .

Returning to the general case, let M be any R -module. We define $M_P = R_P \otimes_R M$, an R_P -module called the *localization* of M at P .

(3.13) THEOREM. *Localization at maximal ideals does not affect residue class modules. Specifically, let P be a maximal ideal of R , and let M be an R -module. Then for each $r > 0$, we may view $M/P^r \cdot M$ as an R_P -module, and there is an R_P -isomorphism*

$$M/P^r \cdot M \cong M_P/P^r \cdot M_P.$$

Proof. Let $S = R - P$, and put $\bar{M} = M/P^r \cdot M$. We show first that \bar{M} can be made into an R_P -module. For each $s \in S$ we have $Rs + P = R$, since P is maximal. Hence there exist elements $\alpha \in R$, $\pi \in P$, such that $\alpha s + \pi = 1$. Taking r th powers, we obtain

$$\beta s + \pi^r = 1$$

for some $\beta \in R$. Therefore s is a unit in the ring R/P^r , and hence acts invertibly on the (R/P^r) -module \bar{M} . From (3.6) we deduce that \bar{M} can be viewed as R_P -module, and that there is an R_P -isomorphism

$$\bar{M} \cong R_P \otimes_R \bar{M} = (\bar{M})_P.$$

But by (3.9) we have

$$(\bar{M})_P = (M/P^r \cdot M)_P \cong M_P/P^r \cdot M_P.$$

Hence there is an R_P -isomorphism $\bar{M} \cong M_P/P^r \cdot M_P$, and the theorem is proved.

The preceding theorem is used most frequently for the special case where $r = 1$, and yields the (R/P) -isomorphism

$$(3.14) \quad M/P \cdot M \cong M_P/P \cdot M_P$$

for each maximal ideal P of R , and each R -module M .

We often refer to problems concerning R -modules and R -homomorphisms as *global* problems, whereas those involving R_P -modules are called *local* problems. A fundamental technique in algebraic number theory, and in its generalizations considered in this book, is the method of solving global

questions by first settling the local case, and then applying this local information to the global case. The next few theorems provide some connections between local and global information.

For each R -module M , and each prime ideal P of R , there is an R -homomorphism

$$i_P: M \rightarrow M_P,$$

given by $i_P(m) = 1 \otimes m \in R_P \otimes_R M, m \in M$. Consequently there is an R -homomorphism $M \rightarrow \prod_P M_P$, where P ranges over all maximal ideals of R .

(3.15) THEOREM. *The map $M \rightarrow \prod_P M_P$ is monic. In particular, $M = 0$ if and only if $M_P = 0$ for each maximal ideal P of R .*

Proof. Denote the above map by f , and suppose that $m \in \ker f$. Set

$$J = \{a \in R : a \cdot m = 0\},$$

an ideal in R . If $J < R$, then $\dagger J$ is contained in some maximal ideal P of R . But $i_P(m) = 0$, so by (3.3) there exists an $s \in R - P$ such that $s \cdot m = 0$. Hence $s \in J$, $s \notin P$, which contradicts the fact that $J \subset P$. This shows that $J = R$, and thus $m = 0$ as claimed. The second assertion in the theorem is then obvious.

(3.16) COROLLARY. *Let $f \in \text{Hom}_R(L, M)$ induce $f_P: L_P \rightarrow M_P$. Then*

(i) *There are R_P -isomorphisms*

$$(\ker f)_P \cong \ker f_P, (\text{im } f)_P \cong \text{im } f_P, (\text{cok } f)_P \cong \text{cok } f_P,$$

for each maximal ideal P of R .

(ii) *f is monic if and only if each f_P is monic.*

(iii) *f is epic if and only if each f_P is epic.*

(iv) *A sequence of R -modules*

$$0 \rightarrow L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$$

is exact if and only if the sequence

$$0 \rightarrow L_P \xrightarrow{f_P} M_P \xrightarrow{g_P} N_P \rightarrow 0$$

is exact for each P .

Proof. Given any $f \in \text{Hom}_R(L, M)$, there is an R -exact sequence

† This statement is a consequence of Zorn's Lemma (see Curtis-Reiner [1]); it does not require the hypothesis that R be noetherian.

$$0 \rightarrow \ker f \rightarrow L \xrightarrow{f} M.$$

Since R_P is R -flat, it follows that the sequence

$$0 \rightarrow (\ker f)_P \rightarrow L_P \xrightarrow{f_P} M_P$$

is R_P -exact. This gives an R_P -isomorphism $(\ker f)_P \cong \ker f_P$. Similar arguments yield the other assertions in (i).

If f is monic, then $\ker f = 0$, whence $\ker f_P = 0$ for each P , by (i). Conversely, if each f_P is monic, then by (i) and (3.15), also f is monic. This proves (ii), and the remaining assertions in the theorem follow in a similar manner.

(3.17) COROLLARY. *Let R be an integral domain with quotient field K , and regard R and all of its localizations R_P as embedded in K . Then*

$$R = \bigcap_P R_P,$$

where P ranges over all maximal ideals of R .

Proof. Obviously, R is contained in the intersection. Conversely, let $x \in K$ be such that $x \in R_P$ for all P . Writing $x = a/b$, $a, b \in R$, it follows that $a \in bR_P$ for all P . Let $f: R \rightarrow R$ be defined by $f(r) = rb$, $r \in R$. Then the image of a in $\text{cok } f_P$ is zero for all P . But by (3.15) and (3.16), the map

$$\text{cok } f \rightarrow \prod_P \text{cok } f_P$$

is monic. Hence a has zero image in $\text{cok } f$, that is, $a \in bR$. This shows that $x \in R$, so R contains $\bigcap R_P$, and the proof is complete.

The reader should be cautioned that (3.17) does not hold for arbitrary commutative rings R , nor does it generalize to the case of R -modules unless additional hypotheses are imposed.

Let us next record the following special cases of (2.38) and the “Change of rings” Theorem 2.43.

(3.18) THEOREM. *Let Λ be an R -algebra, where R is a commutative ring, and let M be any finitely presented left Λ -module. Then for every Λ -module N , and for each prime ideal P of R , there is an R_P -isomorphism*

$$R_P \otimes_R \text{Hom}_\Lambda(M, N) \cong \text{Hom}_{\Lambda_P}(M_P, N_P).$$

(3.19) THEOREM. *Let Λ be a left noetherian R -algebra, where R is a commutative ring, and let P be any prime ideal of R . Then there is an R_P -isomorphism*

$$R_P \otimes_R \text{Ext}_\Lambda^n(M, N) \cong \text{Ext}_{\Lambda_P}^n(M_P, N_P), \quad n \geq 0,$$

for each pair of left Λ -modules M, N such that M is finitely generated over Λ .

We may emphasize that when R is noetherian, and Λ is finitely generated as R -module, then Λ is left and right noetherian, and every finitely generated Λ -module is automatically finitely presented.

Now let Λ be any R -algebra; we shall show that the question, as to whether a given Λ -exact sequence is Λ -split, is a “local” question, that is, the answer is determined by the answers for the corresponding Λ_P -sequences, where P ranges over the maximal ideals of R .

(3.20) THEOREM. *Let Λ be an algebra over the commutative ring R , and let*

$$(3.21) \quad 0 \rightarrow L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$$

be a Λ -exact sequence, where N is a finitely presented Λ -module. Then the sequence is Λ -split if and only if for each maximal ideal P of R , the Λ_P -exact sequence

$$(3.22) \quad 0 \rightarrow L_P \xrightarrow{f_P} M_P \xrightarrow{g_P} N_P \rightarrow 0$$

is Λ_P -split.

Proof. The epimorphism g induces a map

$$g_* : \text{Hom}_\Lambda(N, M) \rightarrow \text{Hom}_\Lambda(N, N).$$

We claim that the sequence (3.21) is split if and only if g_* is epic. Indeed, if $h: N \rightarrow M$ is such that $gh = 1_N$, the identity map on N , then for each $\varphi \in \text{Hom}_\Lambda(N, N)$ we have $h\varphi \in \text{Hom}_\Lambda(N, M)$, and

$$g_*(h\varphi) = gh \cdot \varphi = \varphi.$$

Thus if (3.21) splits, then g_* is epic. Conversely, if g_* is epic, there exists an $h \in \text{Hom}_\Lambda(N, M)$ such that $g_* h = 1_N$, that is, $gh = 1_N$. This completes the proof of the claim.

Now let us define

$$(g_P)_* : \text{Hom}_{\Lambda_P}(N_P, M_P) \rightarrow \text{Hom}_{\Lambda_P}(N_P, N_P),$$

where g induces $g_P: M_P \rightarrow N_P$. By virtue of (3.18), we may identify $(g_P)_*$ with $(g_*)_P$. We have seen above that (3.21) is Λ -split if and only if g_* is epic, while analogously (3.22) is Λ_P -split if and only if $(g_*)_P$ is epic. The theorem then follows immediately from (3.16).

(3.23) COROLLARY. *Let Λ be an R -algebra, N a finitely presented left Λ -module. Then N is Λ -projective if and only if N_P is Λ_P -projective for each P .*

Proof. Choose a free Λ -module F mapping onto N , so there is a Λ -exact

sequence $0 \rightarrow L \rightarrow F \rightarrow N \rightarrow 0$. If N is projective, then $N|F$, whence $N_P|F_P$ and N_P is Λ_P -projective. Conversely, if each N_P is projective, then each localization of the above sequence is split. Hence the original sequence splits, by (3.22), and so N is projective.

Recall that Λ is a *left hereditary* ring if every left ideal of Λ is projective. We have at once

(3.24) COROLLARY. *Let Λ be a left noetherian R -algebra, where R is a commutative ring. Then Λ is left hereditary if and only if the ring Λ_P is left hereditary for every maximal ideal P of R .*

Proof. Suppose that Λ_P is left hereditary for each P , and let L be any left ideal of Λ . Then L is finitely presented as Λ -module, since Λ is left noetherian. Further, L_P is a left ideal of Λ_P , and hence L_P is projective. Therefore L is projective, by (3.23).

Conversely, let Λ be left hereditary, and let P be any maximal ideal of R . By (3.10), every left ideal of Λ_P is of the form L_P , for some left ideal L of Λ . Since L is projective as Λ -module, it follows as in (3.23) that L_P is Λ_P -projective, as desired. This complete the proof of the corollary.

In order to generalize (3.24), we introduce the concept of homological dimension, which is sometimes referred to as “projective dimension”. The *homological dimension* $\text{hd}_\Lambda M$ of a left Λ -module M is the least positive integer n for which there exists a Λ -exact sequence

$$(3.25) \quad 0 \rightarrow X_n \rightarrow X_{n-1} \rightarrow \cdots \rightarrow X_0 \rightarrow M \rightarrow 0, \quad X_i \text{ projective.}$$

We set $\text{hd}_\Lambda M = \infty$ if no such n exists. Once (3.25) is given, it follows directly from definition (2.27) that $\text{Ext}_\Lambda^r(M, \cdot) = 0$, $r \geq n+1$. (The notation $\text{Ext}_\Lambda^r(M, \cdot) = 0$ means that $\text{Ext}_\Lambda^r(M, L) = 0$ for each Λ -module L .)

Now consider a Λ -exact sequence

$$(3.26) \quad 0 \rightarrow K_n \rightarrow X_{n-1} \rightarrow \cdots \rightarrow X_0 \rightarrow M \rightarrow 0, \quad X_i \text{ projective.}$$

By (2.32) there is an isomorphism

$$\text{Ext}_\Lambda^{n+k}(M, \cdot) \cong \text{Ext}_\Lambda^k(K_n, \cdot).$$

But by (2.28 v), K_n is projective if and only if $\text{Ext}_\Lambda^1(K_n, \cdot) = 0$. This gives

(3.27) THEOREM. *Let M be a left Λ -module. The following statements are equivalent:*

- (i) $\text{hd}_\Lambda M \leq n$.
- (ii) $\text{Ext}_\Lambda^r(M, \cdot) = 0$ for $r \geq n+1$.

(iii) For every exact sequence (3.26) in which X_0, \dots, X_{n-1} are projective, also K_n is projective.

We note that $\text{hd}_\Lambda M = 0$ if and only if M is projective. The following result is thus a generalization of (3.23):

(3.28) THEOREM. Let Λ be a left noetherian R -algebra, where R is a commutative ring, and let M be any finitely generated left Λ -module. Then

$$\text{hd}_\Lambda M = \sup_P \{\text{hd}_{\Lambda_P} M_P\},$$

where P ranges over all maximal ideals of R .

Proof. Denote the sup by s , and let $n = \text{hd}_\Lambda M$. We show first that $n \geq s$. The result is clear if $n = \infty$, so assume n finite. Then there is an exact sequence (3.25) with each X_i projective. Localizing at P , we obtain a projective resolution of M_P , and therefore $\text{hd}_{\Lambda_P} M_P \leq n$. This holds for each P , whence $s \leq n$, as claimed.

Conversely, we prove that $n \leq s$, and we may assume that s is finite. From (3.19) we obtain

$$R_P \otimes_R \text{Ext}_\Lambda^{s+1}(M, N) = 0$$

for all P and for all Λ -modules N . It now follows from (3.15) that $\text{Ext}_\Lambda^{s+1}(M, \cdot) = 0$, and so $\text{hd}_\Lambda M \leq s$. This completes the proof of the theorem.

The *left global dimension* of Λ is defined as

$$\dim \Lambda = \sup \{ \text{hd}_\Lambda M : M = \text{left } \Lambda\text{-module} \}.$$

(We should really use the notation $1.\text{gl. dim. } \Lambda$, but will employ the simpler notation $\dim \Lambda$ when there is no danger of confusion.) Clearly, $\dim \Lambda = 0$ if and only if every left Λ -module is projective, that is, if and only if Λ is a semisimple artinian ring (see §7a).

We claim that $\dim \Lambda \leq 1$ if and only if Λ is left hereditary. Suppose that $\dim \Lambda \leq 1$, and let J be any left ideal of Λ . There is a Λ -exact sequence

$$0 \rightarrow J \rightarrow \Lambda \rightarrow \Lambda/J \rightarrow 0,$$

in which Λ is projective. Since $\text{hd}_\Lambda \Lambda/J \leq \dim \Lambda \leq 1$, it follows from (3.27) that J is projective, as desired. Conversely, let Λ be left hereditary, and let M be any left Λ -module. There is a Λ -exact sequence

$$0 \rightarrow K \rightarrow F \rightarrow M \rightarrow 0,$$

in which F is Λ -free. Since Λ is hereditary, the submodule K of the free module F must be projective, by (2.44). Therefore $\text{hd}_\Lambda M \leq 1$ for each M , whence also $\dim \Lambda \leq 1$.

We are now ready to give a generalization of (3.24).

(3.29) THEOREM. *Let Λ be a left noetherian R -algebra, where R is a commutative ring. Then*

$$\dim \Lambda = \sup_P \{\dim \Lambda_P\},$$

where P ranges over all maximal ideals of R .

Proof. We shall use a formula due to M. Auslander (see Rotman [1, Th. 9.14]):

$$\dim \Lambda = \sup \{hd_{\Lambda} \Lambda/J : J = \text{left ideal of } \Lambda\}.$$

But Λ/J is a finitely generated Λ -module, so by (3.28)

$$hd_{\Lambda} \Lambda/J = \sup_P \{hd_{\Lambda_P} \Lambda_P/J_P\}.$$

Further, by (3.10), as J ranges over all left ideals of Λ , J_P ranges over all left ideals of Λ_P . Therefore we have

$$\dim \Lambda = \sup_{J, P} \{hd_{\Lambda_P} \Lambda_P/J_P\} = \sup_P \{\dim \Lambda_P\},$$

as claimed.

To conclude this section, let us show that homological and global dimensions are unchanged by passage to P -adic completions. The preceding theorems reduce the calculations of $hd_{\Lambda} M$ and $\dim \Lambda$ to the case where the ground ring is R_P , a local ring. If we make the additional hypothesis that R is noetherian, then each R_P is also noetherian. The P -adic completion \hat{R}_P of the ring R_P is then a faithfully flat R_P -module (see remark following (2.23), or Exercise 5.3). Using this fact, we prove

(3.30) THEOREM. *Let \hat{R}_P be the P -adic completion of the local noetherian ring R_P , and let Λ_P be a left noetherian R_P -algebra. Set*

$$\hat{\Lambda}_P = \hat{R}_P \otimes_{R_P} \Lambda_P, \quad \hat{M}_P = \hat{R}_P \otimes_{R_P} M_P,$$

where M_P is any finitely generated left Λ_P -module. Then

$$hd_{\Lambda_P} M_P = hd_{\hat{\Lambda}_P} \hat{M}_P$$

for each M_P . Furthermore

$$\dim \Lambda_P = \dim \hat{\Lambda}_P.$$

Proof. As in the proof of (3.28), we find at once that $hd \hat{M}_P \leq hd M_P$. On the other hand, if $s = hd \hat{M}_P$, then for each Λ_P -module N_P we have

$$\hat{R}_P \otimes_{R_P} \text{Ext}_{\Lambda_P}^{s+1}(M_P, N_P) = 0.$$

Since \hat{R}_P is faithfully flat as R_P -module, it follows that $\text{Ext}^{s+1}(M_P, \cdot) = 0$, and therefore $\text{hd } M_P \leq s$. The remaining assertion in (3.30) follows from the formula of Auslander used in the proof of (3.29).

EXERCISES

1. Let R be a domain with quotient field K , and let M be a direct summand of a free R -module F of rank n . Show that M and all of its localizations M_P , where P ranges over the maximal ideals of R , may be embedded in the n -dimensional vector space $K \otimes_R F$ over K . Then use (3.17) to prove the formula

$$M = \bigcap M_P,$$

the intersection being taken over all maximal ideals P of R .

2. Let R be a domain with quotient field K , and let X, Y be submodules of an R -module M . Show that if $X_P = Y_P$ in M_P for each P , then $X = Y$. [Hint: For each P , $\{(X + Y)/Y\}_P = 0$.]

3. Let R be a commutative ring, and let S, T be multiplicative subsets of R such that $S \subset T$. Prove that $T^{-1}R$ is isomorphic to the ring of quotients of $S^{-1}R$ relative to the multiplicative set which is the image of T in $S^{-1}R$.

4. Let P_1, \dots, P_n be a set of prime ideals of the commutative ring R , no one of which contains another, and let

$$S = R - (P_1 \cup \dots \cup P_n).$$

(i) Show that S is a multiplicative subset of R , and that the distinct maximal ideals of $S^{-1}R$ are $P_i \cdot S^{-1}R$, $1 \leq i \leq n$.

(ii) Show that R_{P_i} is canonically isomorphic to the localization of $S^{-1}R$ at the maximal ideal $P_i \cdot S^{-1}R$.

(iii) Show that

$$S^{-1}R = \bigcap_{i=1}^n R_{P_i}$$

if R is an integral domain, the intersection being formed within the quotient field of R .

(Reference: Bourbaki [2, Ch. II, § 3, no. 5].)

5. Let S be a multiplicative subset of the commutative ring R , and let $R' = S^{-1}R$. Let Λ be an R -algebra, and set $\Lambda' = R' \otimes_R \Lambda$, an R' -algebra. Show that every finitely generated left Λ' -module X contains a finitely generated left Λ -module M such that

$$\Lambda' \otimes_{\Lambda} M \cong \Lambda' M = X.$$

[Hint: The ring homomorphism $\Lambda \rightarrow \Lambda'$ makes X into a left Λ -module. Let

$$X = \sum_{i=1}^n \Lambda' x_i, \text{ and set } M = \sum_{i=1}^n \Lambda x_i, \text{ so } \Lambda' M = X.$$

The inclusion $M \subset X$ yields an inclusion $\Lambda' \otimes_{\Lambda} M \subset \Lambda' \otimes_{\Lambda} X \cong X$, since R' is R -flat. Hence the map $\Lambda' \otimes_{\Lambda} M \rightarrow \Lambda' M$ is monic, and thus is an isomorphism. For another approach, see Exercise 26.5.]

4. DEDEKIND DOMAINS

Throughout this section R denotes an integral domain with quotient field K . To avoid trivialities, we assume always that $R \neq K$. We shall define Dedekind domains and shall state, without proof or detailed references, some of their most important properties. Proofs and complete expositions are readily available in texts such as Curtis-Reiner [1], Janusz [1], O'Meara [1], Ribenboim [1], Samuel [1], Weiss [1], Zariski-Samuel [1].

From the standpoint of ideal theory, Dedekind domains are the simplest type of domain beyond principal ideal domains, and share many of their arithmetical properties. Dedekind domains arise naturally, as follows: let R be a principal ideal domain with quotient field K , let L be a finite extension of K , and let S be the integral closure of R in L . Then S is a Dedekind domain with quotient field L . As a matter of fact (see (4.4)), this same conclusion holds under the weaker hypothesis that R itself is a Dedekind domain.

We may also remark that Dedekind domains are a special kind of maximal order. One of the main topics of this book is the study of arithmetical properties of maximal orders analogous to those of Dedekind domains. Many of the results stated in this section are special cases of the theorems to be developed in Chapter VI.

Let us fix some notation, to be used throughout this section. The *annihilator* of an R -module M is defined by

$$\text{ann}_R M = \{a \in R : a \cdot M = 0\}.$$

Likewise we set

$$\text{ann}_R m = \{a \in R : a \cdot m = 0\},$$

for $m \in M$. Call $m \in M$ an *R -torsion* element if $\text{ann}_R m \neq 0$. The set of all R -torsion elements of M is the *R -torsion submodule* of M , and is the kernel of the R -homomorphism $M \rightarrow K \otimes_R M$ given by $m \mapsto 1 \otimes m$, $m \in M$ (see §3b).

The *R -rank* of M is defined as

$$\text{rank}_R M = \dim_K (K \otimes_R M).$$

We call M *R -torsionfree* if M contains no torsion element except 0. In this case, we may identify M with its image $1 \otimes M$ in $K \otimes_R M$; we may then write $K \otimes_R M$ in the simpler form $K \cdot M$, where $K \cdot M$ denotes the set of all finite sums $\{\sum a_i m_i : a_i \in K, m_i \in M\}$. In the same way, for each ring of quotients R' of R , the R -torsionfree R -module M is embedded in the R' -module $R' \otimes_R M$; after making the obvious identification, we may denote $R' \otimes_R M$ by $R' \cdot M$.

An *R -lattice* is a finitely generated R -torsionfree R -module. Each R -lattice M is an R -submodule of a finite dimensional vector space V over K , namely $V = K \cdot M$. We call M a *full R -lattice* in V , the adjective indicating that M contains a K -basis of V . Let M and N be a pair of full R -lattices in a

K -space V . Since N contains a K -basis for V , it is clear that for each $x \in M$ there is a nonzero $r \in R$ such that $r \cdot x \in N$. But M is finitely generated as R -module. Therefore we can choose $r \in R$, $r \neq 0$, such that $r \cdot M \subset N$.

Let M be an R -lattice, and let N be a sublattice of M . We shall call N an R -pure sublattice of M if M/N is R -torsionfree. Equivalently, N is R -pure in M if for each nonzero $\alpha \in R$,

$$N \cap \alpha M = \alpha N.$$

Let S be the multiplicative set $R - \{0\}$. Then M/N is R -torsionfree if and only if N is an S -saturated† R -submodule of M . As a special case of (3.10), we thus obtain

(4.0) **THEOREM.** *Let M be an R -lattice. There is a one-to-one inclusion-preserving correspondence $N \leftrightarrow W$ between the set of R -pure sublattices N of M , and the set of K -subspaces W of KM , given by*

$$W = KN, \quad N = W \cap M.$$

4a Ideal theory, modules, order ideals

Let R be an integral domain with quotient field K . We call R a *Dedekind domain* if it satisfies any one of the following three equivalent conditions:

(4.1) R is a hereditary ring, that is, every ideal of R is a projective R -module (see §2f).

(4.2) R is a noetherian integrally closed domain such that every nonzero prime ideal of R is a maximal ideal.

(4.3) Every proper nonzero ideal of R is uniquely expressible as a product of nonzero prime ideals of R , apart from order of occurrence of the factors.

We recall that R is *noetherian* if its ideals satisfy the A.C.C. (see (2.9)). The ring R is *integrally closed* if each element of K integral over R necessarily lies in R . A *prime ideal* of R is an ideal J properly contained in R (notation: $J < R$) such that R/J has no zero divisors (see (3.12)). For the proof that these three conditions are equivalent, and also for the proofs of theorems stated below, the reader may consult the references listed at the beginning of §4. We shall seldom specify the exact location in these references where the proofs may be found.

(4.4) **THEOREM.** *Let R be a Dedekind domain with quotient field K , and let L be any field extension of K of finite degree. Then the integral closure of R in L is a Dedekind domain S with quotient field L .*

† This concept has been defined immediately preceding (3.10).

Remarks. (i) Recall from §1 that S consists of all elements of L which are zeros of monic polynomials in $R[X]$. By (1.11) we know that S is a ring. The assertion that S is a Dedekind domain contains the additional information that S is integrally closed. We may also point out that each $x \in L$ is expressible as a quotient $x = y/r$ with $y \in S$, $r \in R$; namely, we need only choose r to be a multiple of the denominators of the coefficients which occur in $\min.\text{pol}_K x$.

(ii) The integral closure of R in K is R itself, since R is integrally closed.

(iii) Clearly S is a torsionfree R -module, since R is a subring of the integral domain S .

(iv) Let K be an *algebraic number field*, that is, a finite extension of the rational field \mathbf{Q} . By (4.4), the integral closure of \mathbf{Z} in K is a Dedekind domain, hereafter denoted by $\text{alg. int. } \{K\}$. Its elements are called *algebraic integers*.

(v) In many texts, Theorem 4.4 is proved only when L is separable over K . For the general version, see Zariski–Samuel [1, Chapter V, §8, Theorem 19].

Let L be a finite field extension of K , and let $T_{L/K}$ be the trace map from L to K , defined as in §1a. From T we can construct a bilinear *trace form* $\tau: L \times L \rightarrow K$ by setting

$$(4.5) \quad \tau(x, y) = T_{L/K}(xy), \quad x, y \in L.$$

Then τ is a symmetric K -bilinear form. The form τ is called *nondegenerate* if for nonzero $x \in L$, the map $\tau(x, \cdot): L \rightarrow K$ is not the zero map. We may represent τ by a symmetric matrix τ as follows: let $L = \sum_{i=1}^n Kx_i$, where $n = (L:K)$, and put

$$\tau = (\tau(x_i, x_j))_{1 \leq i, j \leq n} = (T_{L/K}(x_i x_j))_{1 \leq i, j \leq n}.$$

Then τ is nondegenerate if and only if the matrix τ is nonsingular. A standard result in field theory is as follows:

(4.6) **THEOREM.** *Let L be a finite field extension of K . The following statements are equivalent:*

- (i) L is separable over K .
- (ii) The bilinear trace form from $L \times L$ to K is nondegenerate.
- (iii) There exists an $x \in L$ such that $T_{L/K}(x) = 1$.
- (iv) $T_{L/K}: L \rightarrow K$ is an epimorphism.

(We remind the reader that if $\text{char } K = 0$, or more generally if $\text{char } K$ does not divide the degree $(L:K)$, then L is necessarily separable over K . The same is true whenever K is a finite field.)

We give an addendum to (4.4) for the case of separable extensions.

(4.7) **THEOREM.** *Let R be a Dedekind domain with quotient field K , and let S be*

the integral closure of R in a finite separable field extension L of K . Then S is a finitely generated torsionfree R -module of R -rank $(L:K)$.

We turn now to the ideal theory of a Dedekind domain R . A *fractional R -ideal* is a full R -lattice in K , that is, a finitely generated R -submodule J contained in K , such that $K \cdot J = K$. Since R is noetherian, every nonzero ideal of R is necessarily a fractional ideal, and will be called an *integral ideal*.

Given fractional R -ideals J and J' , we may define

$$\begin{aligned} J + J' &= \{x + y : x \in J, y \in J'\}, \\ J \cdot J' &= \left\{ \sum_{\text{finite}} x_i y_i : x_i \in J, y_i \in J' \right\}, \\ J^{-1} &= \{x \in K : xJ \subset R\}. \end{aligned}$$

Then $J + J'$, $J \cap J'$, $J \cdot J'$ and J^{-1} are fractional R -ideals as well. Relative to the multiplication $J \cdot J'$ defined above, the set of fractional R -ideals forms a multiplicative group with identity element R , and with J^{-1} the inverse of J .

Property (4.3) of Dedekind domains extends readily to the factorization of fractional ideals, as follows:

(4.8) **THEOREM.** *The set of fractional R -ideals in K is a free abelian group, with free generators the nonzero prime ideals of R . In other words, every fractional ideal is uniquely expressible in the form*

$$J = P_1^{e_1} \dots P_t^{e_t}, \quad e_i \in \mathbf{Z},$$

where the $\{P_i\}$ are distinct nonzero prime ideals of R , and where no e_i is 0. (We agree to write R itself as an “empty product”, with $t = 0$).

Consider next the factorization $J = \prod P_i^{a_i}$, $J' = \prod P_i^{b_i}$, of a pair of fractional ideals. If $a_i \leq b_i$ for each i , we say that J divides J' (notation: $J | J'$), and in this case it is clear that $J \supset J'$. Conversely, if $J \supset J'$ then $J^{-1}J' \subset R$, whence by (4.8) $a_i \leq b_i$ for each i .

Given any pair of fractional ideals J , J' , we call $J + J'$ their *greatest common divisor*, and $J \cap J'$ their *least common multiple*. If the factorizations of J and J' are as above, it follows at once from the preceding paragraph that

$$(4.9) \quad J + J' = \prod P_i^{\min(a_i, b_i)}, \quad J \cap J' = \prod P_i^{\max(a_i, b_i)}.$$

Two ideals J, J' of R are *relatively prime* if $J + J' = R$. By (4.9), if J and J' are nonzero, they are relatively prime if and only if they have no prime ideal factor in common. A set of nonzero integral ideals $\{J_1, \dots, J_n\}$ is *pairwise relatively prime* if $J_i + J_k = R$ for $1 \leq i < k \leq n$.

(4.10) **THEOREM. (Chinese Remainder Theorem).** *Let $\{J_1, \dots, J_n\}$ be a set of pairwise relatively prime integral ideals of R . Then there is a ring isomorphism*

$$R/J_1 \cdots J_n \cong (R/J_1) \dot{+} \cdots \dot{+} (R/J_n).$$

An easy consequence of (4.10) is the extremely important

(4.11) THEOREM. (Strong Approximation Theorem). *Let P_1, \dots, P_n be distinct nonzero prime ideals of the Dedekind domain R , and let the elements $a_1, \dots, a_n \in K$ be given, as well as positive integers r_1, \dots, r_n . Then there exists an element $b \in K$ such that*

$$\begin{cases} b - a_i \in (P_i)^{r_i} \cdot R_{P_i}, & 1 \leq i \leq n, \\ b \in R_P \quad \text{for all } P \neq P_1, \dots, P_n, \end{cases}$$

where P denotes a variable nonzero prime ideal of R .

We shall also record

(4.12) THEOREM. *Let J be an integral ideal of the Dedekind domain R , and A any fractional R -ideal. Then there is an R -isomorphism*

$$R/J \cong A/JA.$$

We may partition the set of fractional ideals of R into *ideal classes*, putting J and J' into the same class whenever $J \cong J'$ as R -modules. Note that $J \cong J'$ if and only if $J' = Jx$ for some $x \in K$. The ideal classes form a multiplicative group, the *ideal class group* of R , hereafter denoted by $\text{Cl } R$. Multiplication of ideal classes is given by $[J][J'] = [J \cdot J']$, where $[J]$ is the class containing J . A basic result tells us that $\text{Cl } R$ is a finite group whenever $R = \text{alg. int. } \{K\}$, K an algebraic number field. (This is a special case of the Jordan–Zassenhaus Theorem 26.4).

Next we recall some properties of R -lattices. Let M be an R -lattice of R -rank n , and set $V = K \cdot M$, an n -dimensional vector space over K . We may write $V = \sum_{i=1}^n Kv_i$, and set $N = \sum Rv_i$, a free full R -lattice in V . Since M and N are full lattices in the same space V , there exists a nonzero $r \in R$ such that $r \cdot M \subset N$. But $M \cong r \cdot M$, and thus we conclude that M may be embedded in a free R -lattice on n generators. This argument holds for any domain R . If however R is a Dedekind domain, then by (4.1) R is hereditary. Hence M is R -projective by (2.44), and there is an R -isomorphism

$$M \cong J_1 \dot{+} \cdots \dot{+} J_n,$$

where the $\{J_i\}$ are fractional R -ideals. There must be n summands because $\text{rank}_R M = n$. To complete the discussion of the structure of lattices over a Dedekind domain, it is necessary to know under what conditions two such external direct sums of fractional ideals are isomorphic. The complete answer is given by a theorem of Steinitz:

(4.13) THEOREM. Let R be a Dedekind domain. Each R -lattice M is R -projective, and is isomorphic to an external direct sum

$$M \cong J_1 + \cdots + J_n,$$

where the $\{J_i\}$ are fractional R -ideals, and $n = \text{rank}_R M$. Further, two such sums $\sum_{i=1}^n J_i$ and $\sum_{i=1}^m J'_i$ are R -isomorphic if and only if $m = n$, and the products $J_1 \cdots J_n, J'_1 \cdots J'_m$ are in the same ideal class.

There is a generalization of the invariant factor theorem for modules over principal ideal rings, as follows:

(4.14) THEOREM (Invariant Factor Theorem). Let R be a Dedekind domain, and let M, N be R -lattices such that $N \subset K \cdot M$. Then there exist elements $\{m_i\}$ in M , and fractional R -ideals $\{J_i\}$ and $\{E_i\}$, such that

$$M = J_1 m_1 \oplus \cdots \oplus J_r m_r, \quad N = E_1 J_1 m_1 \oplus \cdots \oplus E_s J_s m_s,$$

where $r = \text{rank}_R M$, $s = \text{rank}_R N$, and where $E_1 \supset E_2 \supset \cdots \supset E_s$. If $N \subset M$, then $R \supset E_1$.

The ideals E_1, \dots, E_s occurring above are called the *invariant factors* of the pair M, N ; they are uniquely determined by the inclusion map $N \subset K \cdot M$. If $N \subset M$ and $K \cdot N = K \cdot M$, then M/N is an R -torsion module, and there is an R -isomorphism

$$(4.15) \quad M/N \cong \sum_{i=1}^r (J_i/E_i J_i) \cong \sum_{i=1}^r (R/E_i),$$

the latter isomorphism being a consequence of (4.12). Then (see below) the order ideal of M/N is given by

$$(4.16) \quad \text{ord } M/N = E_1 \cdots E_r.$$

Let us define the *order ideal* $\text{ord } X$ of a finitely generated R -module X as follows:

- (i) If $X = 0$, $\text{ord } X = R$.
- (ii) If X is not an R -torsion module, $\text{ord } X = 0$.
- (iii) If X is a nonzero R -torsion module, then X has an R -composition series (see Exercise 4.1), whose composition factors are $\{R/P_i\}$, with P_i ranging over some set of maximal ideals of R . We set $\text{ord } X = \prod P_i$, where the number of factors equals the number of composition factors of X . The ideal P_i can be recovered from the composition factor R/P_i , namely

$$P_i = \text{ann}_R R/P_i.$$

Since the set of composition factors is uniquely determined by X , according to the Jordan–Hölder Theorem, it follows that $\text{ord } X$ is well-defined.

We observe that if X is an R -torsion module, then $\text{ord } X = R$ if and only if $X = 0$. Further, we prove

(4.17) THEOREM. (i) *For each exact sequence of finitely generated R -modules*

$$0 \rightarrow X' \rightarrow X \rightarrow X'' \rightarrow 0,$$

we have

$$\text{ord } X = (\text{ord } X')(\text{ord } X'').$$

(ii) *For each nonzero ideal J of R , $\text{ord } (R/J) = J$.*

Proof. (i) is clear from the fact that the composition factors of X are those of X' together with those of X'' . For (ii), we can use the factorization $J = \prod P_i^{e_i}$ in (4.8) to write an explicit composition series for R/J , from which it is evident that the composition factors of R/J are the $\{R/P_i\}$ with multiplicities $\{e_i\}$.

From (4.14) we obtain a structure theorem for finitely generated R -modules:

(4.18) THEOREM. *Every finitely generated R -module is isomorphic to a finite external direct sum of ideals of R and cyclic† modules R/J , with J an integral ideal of R .*

Proof. Given a finitely generated R -module X , we can find an R -exact sequence

$$0 \rightarrow N \rightarrow M \rightarrow X \rightarrow 0,$$

with M R -free on r generators, r finite. We then have (in the notation of (4.14))

$$X \cong M/N \cong \sum_{i=r+1}^s J_i + \sum_{i=1}^r (R/E_i),$$

as claimed. Note that the expression $\sum J_i$ does not occur if X is an R -torsion module

4b Localizations, valuations

Throughout let R be an integral domain with quotient field K , $R \neq K$. We shall describe some properties of the ring R , and of R -modules, with respect to localization at prime ideals of R . In cases where proofs are omitted, the reader may consult the references listed at the beginning of §4. For the first part of this subsection, we shall restrict our attention to Dedekind

† An R -module is *cyclic* if it can be generated by one element.

domains. In the second part, we shall consider the more general situation in which R is a noetherian integrally closed domain. This more general material may be skipped in a first reading, since it will occur only peripherally in later chapters.

Let us introduce some concepts from valuation theory (we shall consider only rank one valuations!). Let \mathbf{R} be the real field, \mathbf{R}^+ the set of nonnegative real numbers.

(4.19) *Definition.* A *valuation* of K is a mapping $\varphi:K \rightarrow \mathbf{R}^+$ such that for $a, b \in K$,

- (i) $\varphi(a) = 0$ if and only if $a = 0$.
- (ii) $\varphi(ab) = \varphi(a)\varphi(b)$.
- (iii) $\varphi(a + b) \leq \varphi(a) + \varphi(b)$.

If the valuation also satisfies the stronger condition

- (iv) $\varphi(a + b) \leq \max(\varphi(a), \varphi(b))$,

we call φ *non-archimedean*. It is easily verified that every non-archimedean valuation satisfies

- (v) $\varphi(a + b) = \max(\varphi(a), \varphi(b))$ whenever $\varphi(a) \neq \varphi(b)$.

The *trivial* valuation is defined by the formulas $\varphi(0) = 0$, $\varphi(a) = 1$ for $a \in K, a \neq 0$. We shall always exclude the trivial valuation in our discussion in §§4–5, so hereafter the term “valuation” always means “non-trivial valuation”.

The *value group* of a valuation φ is the multiplicative group $\{\varphi(a):a \in K, a \neq 0\}$. If this value group is an infinite cyclic group, φ is a *discrete* valuation, and is necessarily non-archimedean.

Two valuations φ, ψ are *equivalent* if for $a \in K$,

$$\varphi(a) \leq 1 \quad \text{if and only if} \quad \psi(a) \leq 1.$$

Each valuation φ on K gives rise to a topology on K , by taking as basis for the neighborhoods of a point $a \in K$ the sets

$$\{x \in K: \varphi(x - a) < \varepsilon\},$$

where ε ranges over all positive real numbers. Equivalent valuations give the same topology on K .

Given any non-archimedean valuation φ on K , let us put

$$R = \{a \in K: \varphi(a) \leq 1\}.$$

Then R is a ring, and is called the *valuation ring* of φ . The set

$$P = \{a \in K: \varphi(a) < 1\}$$

is the unique maximal ideal of R . If φ is a discrete valuation, then P is a

principal ideal, namely $P = R\pi$ where π is any element of P such that $\varphi(\pi) < 1$ and $\varphi(\pi)$ generates the value group of φ . In this case R is a *discrete valuation ring*, by which we shall mean a principal ideal domain having a unique maximal ideal P , and such that $P \neq 0$.

One way of obtaining archimedean valuations is as follows: the ordinary absolute value $| \cdot |$ on the complex field \mathbf{C} is an archimedean valuation, whose restriction to any subfield of \mathbf{C} is an archimedean valuation on that subfield. Now let K be a field which can be embedded in \mathbf{C} , and let $\mu: K \rightarrow \mathbf{C}$ be an embedding. Define $\varphi: K \rightarrow \mathbf{R}^+$ by setting

$$\varphi(a) = |\mu(a)|, \quad a \in K.$$

Then φ is an archimedean valuation on K .

In particular, every algebraic number field K can be embedded in \mathbf{C} . For we may write $K = \mathbf{Q}(a)$, and let $f(X) = \min. \text{pol.}_\varphi(a)$. Then there exist elements $\{\alpha_i\}$ in \mathbf{C} such that $f(X) = \prod(X - \alpha_i)$, and we may define embeddings $\mu_i: K \rightarrow \mathbf{C}$ by

$$\mu_i\{g(a)\} = g(\alpha_i), \quad \text{for each } g(X) \in \mathbf{Q}[X].$$

If $f(X)$ has r_1 real zeros $\alpha_1, \dots, \alpha_{r_1}$ and $2r_2$ nonreal zeros in \mathbf{C} , arranged in pairs of complex conjugates $\alpha_{r_1+1}, \bar{\alpha}_{r_1+1}, \dots, \alpha_{r_1+r_2}, \bar{\alpha}_{r_1+r_2}$, then there are exactly $r_1 + r_2$ inequivalent archimedean valuations of K . These are given by the above construction, using the $r_1 + r_2$ embeddings $K \rightarrow \mathbf{C}$ defined by letting $a \rightarrow \alpha_i$, $1 \leq i \leq r_1 + r_2$. (The embedding in which $a \rightarrow \bar{\alpha}_i$ is equivalent to that where $a \rightarrow \alpha_i$, for $r_1 + 1 \leq i \leq r_1 + r_2$.)

The non-archimedean valuations of algebraic number fields can be described in a similar way, by means of embeddings into P -adic fields, which are fields complete with respect to certain non-archimedean valuations. We shall say more about this point of view in §5. In the present subsection, we shall instead give the connection between prime ideals of Dedekind domains and non-archimedean valuations.

Assume now that R is a Dedekind domain, and let P be a nonzero prime ideal of R , or equivalently, a maximal ideal of R . For each nonzero $a \in K$, we may factor the principal ideal Ra into a product of powers of prime ideals, as in (4.8). Let $v_P(a)$ denote the exponent to which P occurs in this factorization. If P does not occur, set $v_P(a) = 0$. Also, we put $v_P(0) = +\infty$. Now fix some $\kappa \in \mathbf{R}^+$, $\kappa > 1$, and define

$$\varphi_P(a) = \kappa^{-v_P(a)}, \quad a \in K, \quad a \neq 0,$$

and $\varphi_P(0) = 0$. Then φ_P is a discrete non-archimedean valuation on K , whose value group is the cyclic group generated by κ . (If instead of κ we used another real number κ' , with $\kappa' > 1$, the valuation φ'_P thus obtained would be equivalent to the above-defined valuation φ_P .)

We refer to v_p as the *exponential valuation* associated with P . The properties of φ_P listed in (4.19) are consequences of the following properties of v_p :

(4.19a) For any elements $a, b \in K$, we have

- (i) $v_p(a) = \infty$ if and only if $a = 0$.
- (ii) $v_p(ab) = v_p(a) + v_p(b)$.
- (iii) $v_p(a + b) \geq \min(v_p(a), v_p(b))$, with equality whenever $v_p(a) \neq v_p(b)$.

As in §3d, we shall denote by R_P the *localization* of R at P , defined by

$$R_P = \{x/s : x \in R, s \in R - P\}.$$

This ring is in fact the valuation ring of the P -adic valuation φ_P on K , and its unique maximal ideal is precisely $P \cdot R_P$. Thus R_P is a discrete valuation ring, and is automatically a principal ideal domain. We may choose a *prime element* π of the ring R_P , that is, an element $\pi \in R_P$ such that $\pi R_P = P \cdot R_P$. Indeed, π may be chosen to lie in R . The fractional R_P -ideals of K are $\{\pi^n R_P : n \in \mathbf{Z}\}$. It follows from (3.13) that localization does not affect residue class fields, that is,

$$R/P \cong R_P/P \cdot R_P.$$

This isomorphism is not only an R -isomorphism as asserted in (3.13), but is in fact an isomorphism of fields. More generally, there are ring isomorphisms

$$R/P^n \cong R_P/P^n \cdot R_P, \quad n \geq 1.$$

Keeping the above notation, let J be any fractional R -ideal in K . Let $v_p(J)$ denote the exponent to which P occurs in the factorization of J into a product of powers of prime ideals.

(4.20) THEOREM. *Let P be a maximal ideal of the Dedekind domain R .*

(i) *For each fractional R -ideal J of K , the localization J_P is given by*

$$J_P = (P \cdot R_P)^{v_p(J)}$$

(ii) *For any finitely generated R -module X ,*

$$(\text{ord } X)_P = \text{ord}(X_P).$$

(iii) *For any finitely generated R -module M , we have $M_P = 0$ if and only if $P + \text{ann}_R M = R$.*

Proof. Statement (i) is well known (see references), and can easily be deduced from the formula

$$v_p(J) = \min\{v_p(a) : a \in J\}.$$

As a consequence of (i), we have $R_P = J_P$ for each integral ideal J of R relatively prime to P .

Statement (ii) follows from the preceding remarks. First of all, unless X is an R -torsion module, both $\text{ord } X$ and $\text{ord } X_P$ are 0. Next, if X is a nonzero R -torsion module, it has a composition series

$$X \supset X' \supset X'' \supset \cdots \supset X^{(k)} \supset 0,$$

whose composition factors are (say) $R/P_1, R/P_2, \dots, R/P_k$, with the $\{P_i\}$ maximal ideals of R . Then

$$X_P \supset (X')_P \supset \cdots \supset (X^{(k)})_P \supset 0$$

is a descending chain of R -modules, possibly with repetitions, and with factor modules $\{(R/P_i)_P\}$. But

$$(R/P_i)_P \cong R_P/(P_i)_P \cong \begin{cases} 0, & P_i \neq P, \\ R/P, & P_i = P. \end{cases}$$

Therefore

$$\text{ord } X_P = \prod_{P_i=P} (P_i)_P = (\prod_{P_i=P} P_i)_P = (\text{ord } X)_P,$$

as claimed. (See also Exercise 4.4).

Finally we prove (iii), remarking in advance that the proof will be valid for the more general case where R is any commutative ring, and P a maximal ideal of R . Let $S = R - P$, a multiplicative subject of R . By definition, $M_P = S^{-1}M$; thus $M_P = 0$ if and only if M is an S -torsion module. Since M is finitely generated as R -module, we see that M is an S -torsion module if and only if there exists an $s \in S$ such that $s \cdot M = 0$. But this occurs if and only if $\text{ann}_R M \not\subset P$, that is, if and only if $P + \text{ann}_R M = R$. This completes the proof.

So far we have considered only localizations at a single maximal ideal P of R . In order to study relationships between “local” and “global” questions, one often needs results of the following type, in which the entire set of localizations are considered simultaneously.

(4.21) THEOREM. *Let R be a Dedekind ring with quotient field K , and let M be any R -lattice. View M and its localizations $\{M_P\}$ as embedded in the vector space KM over K . Then*

$$M = \bigcap_P M_P,$$

the intersection being formed within KM , and where P ranges over all maximal ideals of R .

Proof. By (4.13), the R -lattice M is R -projective. The desired assertion is now a consequence of Exercise 3.1.

In the same vein, we prove

(4.22) **Theorem.** Let R be a Dedekind domain, M an R -lattice, and let $V = KM$. For each maximal ideal P of R , let there be given a full R_P -lattice $X(P)$ in V , such that $X(P) = M_P$ a.e.[†] Define

$$N = \bigcap_P X(P),$$

the intersection being formed within V . Then N is a full R -lattice in V , and

$$N_P = X(P) \quad \text{for all } P.$$

Proof. Let $V = \sum_{i=1}^r Kv_i$, and set $L = \sum_{i=1}^r Rv_i$. Then L is a full R -lattice in V , and so $L_P = M_P$ a.e.[†] (See Exercise 4.6). Therefore $L_P = X(P)$ a.e., and so we may choose nonzero $a, b \in R$ such that

$$a \cdot X(P) \subset L_P \subset b \cdot X(P)$$

for all P . Then

$$N = \bigcap X(P) \subset a^{-1} \bigcap L_P = a^{-1}L,$$

so N is an R -lattice in V . Likewise $L \subset bN$, so N is a full R -lattice in V .

It remains for us to show that $N_P = X(P)$ for each P . Since $N \subset X(P)$, it follows that

$$N_P \subset R_P \cdot X(P) = X(P).$$

To prove the reverse inclusion, let us first write $N = Rn_1 + \cdots + Rn_s$, where of course $s \geq r$. Then each $x \in X(P)$ is expressible as a sum $x = \sum_{i=1}^s a_i n_i$, $a_i \in K$. By the Strong Approximation Theorem (4.11), we may find elements $b_1, \dots, b_s \in K$ such that

$$b_i - a_i \in R_P, \quad b_i \in R_{P'} \quad (P' \neq P), \quad 1 \leq i \leq s,$$

where P' ranges over all maximal ideals of R distinct from P . Let us put $y = \sum b_i n_i$. Then for $P' \neq P$, we have $y \in R_{P'} \cdot N \subset X(P')$; on the other hand, $y - x = \sum (b_i - a_i)n_i \in R_P \cdot N \subset N_P$, so also $y \in X(P)$. Therefore $y \in N$, and so

$$x = y - (y - x) \in N_P.$$

This shows that $X(P) \subset N_P$, and completes the proof.

Let M be an R -module, where R is any domain, and define the R -modules

$$(4.23) \quad M^* = \text{Hom}_R(M, R), \quad M^{**} = \text{Hom}_R(M^*, R).$$

The *evaluation map* $\varphi: M \rightarrow M^{**}$ is given by

$$\{\varphi(m)\}f = f(m), \quad f \in M^*.$$

Clearly $\varphi = 0$ if and only if $M^* = 0$. We call M *reflexive* if φ is an isomorphism.

[†] “a.e.” means “almost everywhere”, that is, for all but a finite number of P ’s.

(4.24) THEOREM. Let R be a Dedekind domain. Then every R -lattice is reflexive, that is, $M \cong M^{**}$.

Proof. By (4.13) each R -lattice M is isomorphic to an external direct sum of fractional R -ideals J of K . Since the functors involved in (4.23) commute with finite direct sums, it suffices to prove the theorem for the case where $M = J$. Now $J^* = \text{Hom}_R(J, R)$, and each $f \in J^*$ extends to a map $f' \in \text{Hom}_K(K, K)$. Each such f' is given by a right multiplication by an element $a \in K$, and so there is an identification

$$J^* = \{a \in K; J \cdot a \subset R\}.$$

Therefore $J^* = J^{-1}$, and so $J^{**} = (J^{-1})^{-1} = J$. Thus the result holds for $M = J$, and hence also for every R -lattice M . (See also Exercise 4.17.)

Combining the results of (4.24) and (4.21), we find that

$$M^{**} = \bigcap_P M_P$$

for any lattice M over a Dedekind domain R . An analogous result holds under somewhat more general circumstances, described below. Let R be any domain; a *minimal prime* of R is a nonzero prime ideal of R which is minimal among the set of all nonzero prime ideals of R .

Let M be an R -lattice, where R is a noetherian domain, and let $V = KM$. Then define dual spaces

$$V^* = \text{Hom}_K(V, K), \quad V^{**} = \text{Hom}_K(V^*, K).$$

The evaluation map gives a K -isomorphism $V \cong V^{**}$. Since R is noetherian, M^* and M^{**} are also R -lattices, and there are embeddings $M^* \subset V^*$, $M^{**} \subset V^{**}$. Explicitly we have

$$M^{**} = \{v \in V; f(v) \in R \text{ for all } f \in M^*\}.$$

(4.25) THEOREM. Let R be a noetherian integrally closed domain, M an R -lattice, and let P range over the minimal primes of R . Then

(i) For each P , R_P is a discrete valuation ring (that is, a principal ideal domain with unique maximal ideal $P \cdot R_P$).

(ii) $R = \bigcap_P R_P$.

(iii) For each nonzero $x \in R$, x is a unit in R_P a.e.

(iv) $M^{**} = \bigcap_P M_P$.

Remarks. The proof of (i) may be found in Serre [1, p. 19, Prop. 3]. As general reference, see Bourbaki [5], Fossum [4].

Conditions (i)–(iii) are the postulates for a *Krull ring*. Thus the theorem asserts that every noetherian integrally closed domain is a Krull ring. The

converse is false: Krull rings are always integrally closed, but need not be noetherian. For example $\mathbf{Z}[X_1, X_2, \dots]$ is a non-noetherian Krull ring. Every unique factorization domain is automatically a Krull ring. As examples of noetherian integrally closed domains, we list $\mathbf{Z}[X_1, \dots, X_n]$ and $K[X_1, \dots, X_n]$.

The following generalization of (4.22) is proved in the above-named references (see, for instance, Bourbaki [5, Ch. 7, §4, No. 3]):

(4.26) **THEOREM.** *Let R be a noetherian integrally closed domain, and let M and L be full R -lattices in the K -space V . Let P range over the minimal primes of R . Then $M_P = L_P$ a.e. Further, let there be given for each P a full R_P -lattice $X(P)$ in V , such that $X(P) = M_P$ a.e. Set*

$$N = \bigcap_P X(P).$$

Then N is a full reflexive R -lattice in V , and $N_P = X(P)$ for all P .

4c Ramification index; residue class degree

Throughout this section, R is a Dedekind domain with quotient field K , and L is a finite separable field extension of K . We shall denote by S the integral closure of R in L , so by (4.4) and (4.7), S is a Dedekind domain with quotient field L , finitely generated as R -module, of R -rank $(L:K)$. To avoid trivialities, we assume always that $R \neq K$ and $L \neq S$.

Given a maximal ideal P of R , the integral ideal $P \cdot S$ can be written as

$$(4.27) \quad P \cdot S = \prod_{i=1}^g P_i^{e_i},$$

where the $\{P_i\}$ are distinct maximal ideals of S , and the $\{e_i\}$ are positive integers. Call e_i the *ramification index* of P_i for the extension L/K , and write

$$(4.28) \quad e_i = e(P_i, L/K), \quad 1 \leq i \leq g.$$

We say that P_i is *unramified* in L/K if $e_i = 1$ and S/P_i is a separable extension of R/P . Likewise, we say that P is *unramified* in the extension L/K if each P_i is unramified in L/K .

Turning to residue class fields, we observe at once that for $1 \leq i \leq g$, the field S/P_i is an extension field of R/P . We set

$$(4.29) \quad f_i = f(P_i, L/K) = (S/P_i : R/P),$$

and call f_i the *residue class degree* of P_i relative to the extension L/K . The finiteness of the $\{f_i\}$ is a consequence of the following basic result:

(4.30) THEOREM. *Keeping the above notation, we have*

$$\sum_{i=1}^g e_i f_i = (L:K).$$

Proof. Let $n = (L:K)$, so $\text{rank}_R S = n$. Let $S_P = R_P \cdot S$; then S_P is a torsion-free R_P -module of R_P -rank n . But R_P is a principal ideal domain, and so $S_P \cong R_P^{(n)}$. Therefore

$$S/PS \cong S_P/P \cdot S_P \cong (R_P/P \cdot R_P)^{(n)} \cong (R/P)^{(n)}$$

by virtue of (3.14). This shows that the dimension of S/PS as vector space over the field R/P is precisely n .

We may also compute this dimension as follows: by (4.10) we have

$$S/PS = S/\prod P_i^{e_i} \cong \sum_{i=1}^g (S/P_i^{e_i}).$$

There is a descending chain of R/P -modules

$$S/P_i^{e_i} \supset P_i/P_i^{e_i} \supset \cdots \supset P_i^{e_i-1}/P_i^{e_i} \supset 0,$$

each of whose factor modules is isomorphic to S/P_i by (4.12). Hence

$$\dim_{R/P}(S/P_i^{e_i}) = e_i \cdot \dim_{R/P}(S/P_i) = e_i f_i,$$

for each i , $1 \leq i \leq g$. This gives

$$\dim_{R/P}(S/PS) = \sum_{i=1}^g e_i f_i,$$

and the theorem is proved.

(4.31) *Comments.* (i) It is easily verified that S_P is the integral closure of R_P in L , and that $\{P_i \cdot S_P : 1 \leq i \leq g\}$ are the distinct maximal ideals of S_P . Furthermore,

$$S_P = S_{P_1} \cap \cdots \cap S_{P_g},$$

where S_{P_i} is the localization of S at P_i , and where $S_P = R_P \cdot S$. Note that R_P is a discrete valuation ring, but S_P is not (unless $g = 1$). In connection with this remark, see Exercise 3.4.

(ii) If (4.27) holds, then we claim that $P_i \cap R = P$, $1 \leq i \leq g$. Indeed, $P_i \cap R$ is a prime ideal of R containing P , or else possibly $P_i \cap R = R$. The latter alternative cannot occur, since $1 \notin P_i$.

On the other hand, starting with any maximal ideal P_i of S , we may set $P = P_i \cap R$, a prime ideal of R . Surely $P \neq 0$, since for each nonzero $a \in P_i$, the constant term in $\min.\text{pol}_K(a)$ is a nonzero element in P . Thus $P_i \supset P$,

and so $P_i \supset P \cdot S$, whence P_i occurs in the factorization of $P \cdot S$ into maximal ideals of S .

(iii) We may define a *relative norm map* $N_{L/K}$ which associates to each fractional S -ideal J of L , a fractional R -ideal $N_{L/K}(J)$ of K . For each maximal ideal P_i of S , we set

$$(4.32) \quad N_{L/K}(P_i) = P^{f_i}, \text{ where } P = P_i \cap R, \quad f_i = f(P_i, L/K).$$

Since these $\{P_i\}$ form a free basis for the abelian group of fractional S -ideals in L , we may then define $N_{L/K}$ on this group by requiring it to be multiplicative:

$$N_{L/K}(JJ') = N_{L/K}(J) \cdot N_{L/K}(J').$$

We could also have defined the norm map $N_{L/K}$ as follows: for each non-zero ideal J of S , put

$$\tilde{N}_{L/K}(J) = \text{ord}_R(S/J),$$

where ord_R denotes R -order ideal (see §4a). If J' is another nonzero ideal of S , there is an R -exact sequence

$$0 \rightarrow J/JJ' \rightarrow S/JJ' \rightarrow S/J \rightarrow 0,$$

and by (4.12) the term J/JJ' is isomorphic to S/J' . From (4.17) we then conclude

$$\text{ord}_R(S/JJ') = \text{ord}_R(S/J) \cdot \text{ord}_R(S/J'), \quad \text{that is,} \quad \tilde{N}(JJ') = \tilde{N}(J) \cdot \tilde{N}(J').$$

If we now put

$$\tilde{N}_{L/K}(J_1 \cdot J_2^{-1}) = \tilde{N}_{L/K}(J_1) \cdot \tilde{N}_{L/K}(J_2)^{-1}$$

for J_1, J_2 nonzero ideals of S , it follows that $\tilde{N}_{L/K}$ is well defined on the group of fractional S -ideals in L . We now show that $\tilde{N}_{L/K}$ coincides with $N_{L/K}$. It suffices to verify that

$$(4.33) \quad \text{ord}_R(S/P_i) = P^{f_i},$$

using the notation of (4.32). But S/P_i is a field extension of R/P of degree f_i , so as R -modules we have $S/P_i \cong (R/P)^{(f_i)}$, and then (4.33) is obvious.

(iv) In the special case where $K = \mathbf{Q}$, $R = \mathbf{Z}$, one defines a *counting norm* $\mathcal{N}_{L/\mathbf{Q}}$, by setting

$$\mathcal{N}_{L/\mathbf{Q}}(P_i) = p^{f_i}, \quad f_i = f(P_i, L/\mathbf{Q}),$$

where p is the positive rational prime such that $p\mathbf{Z} = P_i \cap \mathbf{Z}$. Thus $\mathcal{N}_{L/\mathbf{Q}}(P_i)$ is the number of elements in the finite field S/P_i . As usual, $\mathcal{N}_{L/\mathbf{Q}}$ is defined on all fractional S -ideals in L , so as to be multiplicative. Then for each nonzero ideal J in S ,

$$\mathcal{N}_{L/\mathbb{Q}}(J) = \text{card}(S/J),$$

where $\text{card}(S/J)$ denotes the number of elements in the ring S/J .

(v) If L is a Galois extension of K , with Galois group G , then for each $\sigma \in G$ we have $S^\sigma = S$, where $S^\sigma = \{x^\sigma : x \in S\}$. It is well known (see references) that G acts transitively on the set of prime ideals $\{P_i\}$ occurring in (4.27), that is, there exist elements $\{\sigma_i\} \in G$ such that $P_i = (P_1)^{\sigma_i}$, $1 \leq i \leq g$. Furthermore, in this case we have

$$e_1 = \cdots = e_g, \quad f_1 = \cdots = f_g.$$

4d Different, discriminant

As in §4c, let L be a finite separable field extension of K , let R be a Dedekind domain with quotient field K , and let S be the integral closure of R in L . Let $\tau: L \times L \rightarrow K$ be the nondegenerate bilinear trace form defined in (4.5), that is,

$$\tau(x, y) = T_{L/K}(xy), \quad x, y \in L.$$

For any set $J \subset L$, put

$$\tau(x, J) = T_{L/K}(xJ) = \{\tau(x, y) : y \in J\}.$$

We prove at once that $T_{L/K}(S) \subset R$. Indeed, each $a \in S$ is integral over R , so $\text{char. pol.}_{L/K} a \in R[X]$ by Exercise 1.1. Therefore $T_{L/K} a \in R$, as desired.

Given any full R -lattice M in L , we can define a *complementary* lattice

$$\tilde{M} = \{x \in L : \tau(x, M) \subset R\}.$$

The map $M \rightarrow \tilde{M}$ is inclusion-reversing. Let us verify that \tilde{M} is a full R -lattice in L . First observe that M is contained in some full free R -lattice $N = \sum_{i=1}^n Rx_i$, where $n = (L:K)$. There exist elements $\{y_j\} \in L$ such that $\tau(x_i, y_j) = \delta_{ij}$, $1 \leq i, j \leq n$. Then

$$\tilde{M} \supset \tilde{N} = \sum_{j=1}^n Ry_j.$$

Similarly, \tilde{M} is contained in some full R -lattice in L . Therefore \tilde{M} is itself a full R -lattice in L , as claimed.

In particular, if J is a fractional S -ideal in L , then \tilde{J} is an S -submodule of L which is an R -lattice, and thus \tilde{J} is also a fractional S -ideal of L ; we call \tilde{J} the *complementary ideal* of J . For the case where J is S itself, we note that $\tilde{S} \supset S$, so that \tilde{S}^{-1} is an integral ideal of S . Let us define the *different* of S with respect to R as

$$\mathfrak{D}(S/R) = \tilde{S}^{-1},$$

and then $\tilde{S} = \mathfrak{D}(S/R)^{-1}$ may be referred to as the *inverse different*.

(4.34) THEOREM. Let J be a fractional S -ideal in L . Then

$$\tilde{J} = J^{-1} \cdot \mathfrak{D}(S/R)^{-1}, \quad \tilde{\tilde{J}} = J.$$

Proof. Let us abbreviate $T_{L/K}$ as T , and $\mathfrak{D}(S/R)$ as \mathfrak{D} . We have

$$T(J \cdot J^{-1}\mathfrak{D}^{-1}) = T(S \cdot \mathfrak{D}^{-1}) \subset R,$$

so $\tilde{J} \supset J^{-1}\mathfrak{D}^{-1}$. On the other hand,

$$R \supset T(J\tilde{J}) = T(J\tilde{J} \cdot S),$$

whence $J\tilde{J} \subset \mathfrak{D}^{-1}$, so $\tilde{J} \subset J^{-1}\mathfrak{D}^{-1}$. This proves that $\tilde{J} = J^{-1} \cdot \mathfrak{D}^{-1}$. The formula for $\tilde{\tilde{J}}$ is then obvious (see also Exercise 4.12).

The *discriminant* of S with respect to R is defined as

$$d(S/R) = N_{L/K}(\mathfrak{D}(S/R)),$$

the norm of the different $\mathfrak{D}(S/R)$. Thus $d(S/R)$ is a nonzero ideal of R , often called the *discriminant ideal* of S/R .

(4.35) THEOREM. (i) For each maximal ideal P of R ,

$$\{d(S/R)\}_P = d(S_P/R_P).$$

(ii) If

$$S = \sum_{i=1}^n Rx_i, \quad n = (L:K),$$

then

$$d(S/R) = R \cdot \det(T_{L/K}(x_i x_j))_{1 \leq i, j \leq n}.$$

Proof. For P a maximal ideal of R , and J any S -ideal in L , we put $J_P = R_P \cdot J$, an S_P -ideal of L . As remarked earlier, S_P is the integral closure of R_P in L , so in the passage from the pair R, S to the pair R_P, S_P , we have introduced a new pair of Dedekind domains, with quotient fields K, L , respectively. The advantage of this procedure is that the new domain R_P is a principal ideal domain, and thus S_P is R_P -free on n generators, where $n = (L:K)$.

Since the trace map $T_{L/K}$ is K -linear, it follows easily that

$$(4.36) \quad \mathfrak{D}(S_P/R_P) = \{\mathfrak{D}(S/R)\}_P.$$

Furthermore, for each S -ideal J in L , we have

$$N_{L/K}(J_P) = \{N_{L/K}(J)\}_P,$$

that is, forming norms commutes with localization. Applying $N_{L/K}$ to (4.36) yields assertion (i) of the theorem.

Now suppose that S happens to be R -free, say $S = \sum_{i=1}^n Rx_i$. There exist elements $\{y_j\} \in L$ with $T_{L/K}(x_i y_j) = \delta_{ij}$, $1 \leq i, j \leq n$. Then

$$\mathfrak{D}(S/R) = \tilde{S}^{-1}, \text{ where } \tilde{S} = \sum_{j=1}^n Ry_j.$$

We have

$$\begin{aligned} d(S/R) &= N_{L/K}(\mathfrak{D}(S/R)) = \text{ord}_R(S/\mathfrak{D}(S/R)) \\ &= \text{ord}_R(S/\tilde{S}^{-1}) = \text{ord}_R(\tilde{S}/S) \text{ (by (4.12)).} \end{aligned}$$

Write

$$x_i = \sum_{j=1}^n a_{ij} y_j, \quad a_{ij} \in R, \quad 1 \leq i \leq n.$$

Then (Exercise 4.2)

$$\text{ord}_R(\tilde{S}/S) = R \cdot \det(a_{ij}).$$

But $a_{ij} = T_{L/K}(x_i x_j)$, which completes the proof of (ii).

We may remark that this theorem enables us to compute the discriminant $d(S/R)$ by calculating each “local” component $d(S/R)_P$, and that by (ii), each local component can be obtained once an R_P -basis of S_P is known.

The different $\mathfrak{D}(S/R)$ and the discriminant $d(S/R)$ are of great importance because they give information about ramification of prime ideals in the extension L/K . Recall that a maximal ideal P_i of S is *unramified* in L/K if

$$e(P_i, L/K) = 1, \text{ and } S/P_i \text{ is a separable extension of } R/P.$$

Likewise, a maximal ideal P of R is *unramified* in L/K if $P \cdot S = \prod P_i$, a product of distinct unramified prime ideals of S .

(4.37) **THEOREM.** A maximal ideal P_i of S is unramified in the extension L/K if and only if $P_i \nmid \mathfrak{D}(S/R)$. A maximal ideal P of R is unramified in L/K if and only if $P \nmid d(S/R)$.

Proof. Let $\bar{R} = R/P$, $\bar{S} = S/PS$, $n = (L:K)$; then \bar{S} is an algebra over the field \bar{R} , of dimension n . For $f(X) \in R[X]$, let $\bar{f}(X)$ denote its image in $\bar{R}[X]$. We claim that for $a \in S$,

$$(4.38) \quad \overline{\text{char. pol.}}_{L/K} a = \text{char. pol.}_{\bar{S}/\bar{R}} \bar{a}.$$

To prove this, first replace R by R_P , and S by S_P . Such a change does not affect \bar{R} or \bar{S} . Then we may write

$$S_P = \sum_{i=1}^n R_P x_i, \quad \bar{S} = \sum_{i=1}^n \bar{R} \bar{x}_i.$$

For $a \in S$, we have

$$ax_j = \sum \alpha_{ij}x_i, \quad \bar{a}\bar{x}_j = \sum \bar{\alpha}_{ij}\bar{x}_i, \quad \alpha_{ij} \in R.$$

Then $\text{char. pol.}(a)$ is the characteristic polynomial of the matrix (α_{ij}) , while $\text{char. pol.}(\bar{a})$ is that of $(\bar{\alpha}_{ij})$, which establishes (4.38) at once.

Now let P_1 be a maximal ideal of S , and let $P \cdot S = P_1^e J$, where $e \geq 1$ and where J is an integral ideal of S relatively prime to P_1 . For each $a \in P_1 J$ we have $\bar{a}^e = 0$ in \bar{S} , and therefore $\text{char. pol.}_{\bar{S}/\bar{R}} \bar{a} = X^n$. Hence from (4.38) we conclude that $T_{L/K}(P_1 J) \subset P$. Writing \mathfrak{D} instead of $\mathfrak{D}(S/R)$ for convenience, we then obtain $P_1 J \subset P\mathfrak{D}^{-1}$, and consequently $\mathfrak{D} \subset P_1^{e-1}$. Thus $P_1^{e-1} \mid \mathfrak{D}$, and therefore $P_1 \mid \mathfrak{D}$ whenever $e > 1$.

To complete the proof, we now assume that $e = 1$, and we must show that $P_1 \mid \mathfrak{D}$ if and only if S/P_1 is inseparable over \bar{R} . Since $e = 1$, we have

$$\bar{S} = S/PS \cong S/P_1 + S/J,$$

and each $a \in J$ maps onto an ordered pair $(a', 0)$, where a' is the image of a in S/P_1 . Set $S/P_1 = S'$ for convenience of notation, and let $k = (S/J: \bar{R})$. Then for $a \in J$,

$$\text{char. pol.}_{\bar{S}/\bar{R}} \bar{a} = X^k \cdot \text{char. pol.}_{S'/\bar{R}} a'.$$

This implies at once that

$$T_{\bar{S}/\bar{R}} \bar{a} = T_{S'/\bar{R}} a', \quad a \in J.$$

If S'/\bar{R} is inseparable, then $T_{S'/\bar{R}}$ is the zero map, and thus by (4.38) we have $T_{L/K}(J) \subset P$. This yields $J \subset P\mathfrak{D}^{-1}$, whence $P_1 \mid \mathfrak{D}$. The reverse argument is equally simple: suppose that S'/\bar{R} is separable. Then there exists an $a \in J$ such that $T_{S'/\bar{R}} a' \neq 0$, and therefore $T_{L/K}(J) \not\subset P$. Hence $J \not\subset P\mathfrak{D}^{-1}$, that is, $P_1 \nmid \mathfrak{D}$. This completes the proof of the first assertion of the theorem. The second assertion is an obvious consequence of the first.

4e Global fields

A *global field* K is either an *algebraic number field* (that is, a finite extension of the rational field \mathbf{Q}), or else a *function field* (that is, a finite extension of a field $k(X)$ of rational functions in an indeterminate X over a finite field k). A *prime* of K is an equivalence class of valuations of K . We exclude once and for all the “trivial” valuation φ , defined by $\varphi(0) = 0$, $\varphi(a) = 1$ for $a \in K$, $a \neq 0$. If K is an algebraic number field, there are the archimedean or *infinite primes*, arising from embeddings of K in the complex field \mathbf{C} , and the non-archimedean or *finite primes* of K , arising from discrete P -adic valuations of K , with P ranging over the distinct maximal ideals in the ring alg.int. $\{K\}$ of all algebraic integers in K .

If K is a function field, there are no archimedean primes, and the non-archimedean or *finite primes* arise from discrete valuation rings in K . In this case, as well as in the number field case, the residue class field associated with a finite prime P is a finite field; let $\mathcal{N}(P)$ denote the number of elements in this residue class field (see (4.31 (iv)).

For each finite prime P of a global field K , we *normalize* the P -adic valuation φ_P by setting

$$\varphi_P(a) = \mathcal{N}(P)^{-v_P(a)}, \quad a \in K, \quad a \neq 0,$$

$\varphi_P(0) = 0$ (see §4b). If P is a *real prime* of K , that is, an infinite prime arising from an embedding $\mu: K \rightarrow \mathbf{R}$, let

$$\varphi_P(a) = |\mu(a)|, \quad a \in K.$$

If P is a *complex prime* of K , that is, an infinite prime arising from an embedding $\mu: K \rightarrow \mathbf{C}$ such that $\mu(K) \not\subset \mathbf{R}$, let

$$\varphi_P(a) = |\mu(a)|^2, \quad a \in K.$$

Thus we have a *normalized valuation* φ_P for each prime P of K .

(4.39) THEOREM (Product Formula). *Let K be a global field. Then for each nonzero $a \in K$, $\varphi_P(a) = 1$ a.e., and*

$$\prod_P \varphi_P(a) = 1,$$

where P ranges over all primes of K .

For global fields, there is a stronger version of (4.11):

(4.40) THEOREM (Very Strong Approximation Theorem). *Let P_1, \dots, P_n be distinct primes of K (finite or infinite), and let P_0 be a fixed prime distinct from these. Given any elements $a_1, \dots, a_n \in K$ and any $\varepsilon > 0$, there exists an element $a \in K$ such that*

$$\varphi_{P_i}(a - a_i) < \varepsilon, \quad 1 \leq i \leq n,$$

$$\varphi_P(a) \leq 1, \quad P \neq P_0, P_1, \dots, P_n.$$

(4.41) COROLLARY. *Let $\{P_1, \dots, P_n\}$ be distinct primes of the algebraic number field K , and suppose that there exists an infinite prime P_0 of K distinct from P_1, \dots, P_n . Let $a_1, \dots, a_n \in K$ be such that $a_i \in R_{P_i}$ if P_i is a finite prime, where $R = \text{alg. int.}\{K\}$. Let $0 < \varepsilon < 1$. Then there exists an $a \in R$ such that*

$$\varphi_{P_i}(a - a_i) < \varepsilon, \quad 1 \leq i \leq n,$$

$$\varphi_P(a) < 1, \quad P \text{ infinite}, \quad P \neq P_0, P_1, \dots, P_n.$$

EXERCISES

Throughout, R is an integral domain with quotient field K . Unless otherwise stated, R is assumed to be a Dedekind domain.

1. Let J be a nonzero ideal of R . Using (4.9), find all ideals of R which contain J . Prove that R/J is an artinian and noetherian ring. Deduce from this that every finitely generated R -torsion R -module possesses an R -composition series.
2. Let R be a principal ideal domain, and let $N \subset M$ be R -lattices with $KN = KM$. Suppose that

$$M = \sum_{i=1}^r Rm_i, \quad N = \sum_{j=1}^r Rn_j, \quad n_j = \sum \alpha_{ij} m_i, \quad \alpha_{ij} \in R.$$

Show that

$$\text{ord}_R M/N = R \cdot \det(\alpha_{ij}).$$

[Hint: After change of R -bases of M and N , we may assume that the matrix (α_{ij}) is diagonal. Such basis changes have the effect of multiplying $\det(\alpha_{ij})$ by a unit factor from R , and thus do not change $R \cdot \det(\alpha_{ij})$. Finally, if (α_{ij}) is diagonal, it follows from (4.17) that $\text{ord}_R M/N$ is the principal ideal generated by the product of the diagonal entries.]

3. Let X be a finitely generated R -torsion module. Show that $\text{ord}_R X$ and $\text{ann}_R X$ have the same prime ideal factors, apart from multiplicities. Explain the connection between this result and Theorem 1.7.
4. Let $R \subset S$ be an inclusion of Dedekind domains, and let X be any finitely generated R -module. Prove that

$$S \otimes_R \text{ord}_R X = \text{ord}_S (S \otimes_R X).$$

[Hint: By (4.18) it suffices to handle the cases $X = J$ and $X = R/J$, with J a nonzero ideal of R . The result is obvious for $X = J$, while for $X = R/J$ it follows from Exercise 2.6.]

5. Let $f \in \text{Hom}_R(M, M)$, where M is an R -lattice. Prove that

$$\text{ord}_R M/f(M) = R \cdot \det f,$$

where $\det f$ is computed by extending f to a K -linear transformation on KM . [Hint: Use (4.20(ii)) to reduce the problem to the case where R is a principal ideal domain, and then use Exercise 2.]

6. Let M, N be full R -lattices in a K -space V . Prove that $M_P = N_P$ a.e. [Hint: There exist nonzero $\alpha, \beta \in R$ such that $\alpha M \subset N \subset \beta M$.]
7. Let R be any domain, M a finitely generated R -module, and let $\varphi: M \rightarrow M^{**}$ be the evaluation map (see (4.23)). Show that if M is R -torsionfree, then φ is monic. Show that $M^* = 0$ if and only if M is an R -torsion module.

8. Let R be a noetherian integrally closed domain, and let M, N be full R -lattices in a K -space V . Suppose that $M_P \subset N_P$ for each minimal prime P of R , and let N be reflexive. Prove that $M \subset N$.

9. Keeping the hypotheses and notation of §4c, prove that

$$N_{L/K}(Sa) = R \cdot N_{L/K}(a), \quad a \in L.$$

[Hint: Use (4.31(iii)) and Exercise 5.]

10. Prove that the symbols $e(P_i, L/K)$ and $f(P_i, L/K)$ defined in §4c are multiplicative for towers of separable extensions.

11. Prove that the different $\mathfrak{D}(S/R)$ defined in §4d is multiplicative for towers of separable extensions. [Hint: Let $L_2 \supset L_1 \supset K$ be such a tower, and let S_i be the integral closure of R in L_i , $i = 1, 2$. Set

$$T_i = T_{L_i/K}, \quad \mathfrak{D}_i = \mathfrak{D}(S_i/R), \quad T' = T_{L_2/L_1}, \quad \mathfrak{D}' = \mathfrak{D}(S_2/S_1).$$

To prove that $\mathfrak{D}_2 = \mathfrak{D}_1 \mathfrak{D}'$, show the equivalence of the following statements, for $x \in L_2$ (use Exercise 1.5):

$$x \in \mathfrak{D}_2^{-1}; \quad T_2(xS_2) \subset R; \quad T_1(S_1 \cdot T'(xS_2)) \subset R;$$

$$T'(xS_2) \subset \mathfrak{D}_1^{-1}; \quad x\mathfrak{D}_1 \subset \mathfrak{D}'^{-1}.$$

12. Let $\tau: V \times V \rightarrow K$ be a nondegenerate symmetric K -bilinear form on a finite dimensional K -space V , and let M be a full R -lattice in V . Define

$$\tilde{M} = \{x \in V : \tau(x, M) \subset R\}.$$

Show that \tilde{M} is a full R -lattice in V , and that $\tilde{\tilde{M}} = M$. [Hint: If $N = \sum Rx_i$ is a full R -lattice in V , then $\tilde{N} = \sum Ry_j$, where $\tau(x_i, y_j) = \delta_{ij}$, and then $\tilde{\tilde{N}} = \sum Rx_i = N$. Hence if $N_1 \subset M \subset N_2$ with N_1, N_2 R -free, we have $\tilde{N}_1 \supset \tilde{M} \supset \tilde{N}_2$, whence \tilde{M} is a full R -lattice in V . To prove that $\tilde{\tilde{M}} = M$ in general, show that the process of forming \tilde{M} from M commutes with localization, and thus the problem can be reduced to the case of R_p -lattices.]

13. Keeping the notation of Exercise 12, let $n = \text{rank}_R M$. Define the *discriminant ideal* of M with respect to τ to be the R -ideal $d(M)$ in K generated by

$$\{\det(\tau(x_i, x_j))_{1 \leq i, j \leq n} : x_1, \dots, x_n \in M\}.$$

Prove that $d(M_P) = d(M)_P$ for each maximal ideal P of R . Show that if $M = \sum_{i=1}^n Rx_i$, then

$$d(M) = R \cdot \det(\tau(x_i, x_j))_{1 \leq i, j \leq n}.$$

If $N \subset M$, where N is another full R -lattice in V , prove that

$$(4.42) \quad d(N) = (\text{ord}_R M/N)^2 \cdot d(M),$$

and that $d(N) \subset d(M)$. Deduce from this that $d(M) = d(N)$ if and only if $M = N$. [Hint: To prove (4.42), first localize, and then write R in place of R_P . Use the notation of Exercise 2. Then

$$d(N) = R \cdot \det(\tau(n_i, n_j)) = R \cdot \{\det(\alpha_{ij})\}^2 \cdot \det(\tau(m_i, m_j)).$$

14. Let $L = K(\alpha)$ be a finite separable extension of K , and let

$$f(X) = \min. \text{ pol.}_K \alpha = \prod_{i=1}^n (X - \alpha_i),$$

where $\alpha_1 (= \alpha)$, $\alpha_2, \dots, \alpha_n$ are the algebraic conjugates of α over K . Define the *discriminant* of α as

$$\text{disc } \alpha = \det(T_{L/K}(\alpha^i \cdot \alpha^j))_{0 \leq i, j \leq n-1}.$$

Prove that

$$\begin{aligned} \text{disc } \alpha &= \det \begin{bmatrix} 1 & \alpha_1 \cdots \alpha_1^{n-1} \\ 1 & \alpha_2 \cdots \alpha_2^{n-1} \\ \vdots & \vdots \\ 1 & \alpha_n \cdots \alpha_n^{n-1} \end{bmatrix}^2 \\ &= \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = \pm N_{L/K}(f'(\alpha)), \end{aligned}$$

where $f'(X)$ is the formal derivative of $f(X)$.

15. Keeping the above notation, let $f(X) \in R[X]$, so α is integral over R . Let S be the integral closure of R in L . Show that

$$R \oplus R\alpha \oplus \cdots \oplus R\alpha^{n-1} \subset S,$$

and hence prove that the discriminant $d(S/R)$ divides $R \cdot \text{disc } \alpha$.

16. Let ω be a primitive m th root of 1 over K , where $\text{char } K \nmid m$. Show that the only prime ideals of R dividing $\text{disc } \omega$ are those which divide m . Hence if $P \nmid Rm$, then P is unramified in the extension $K(\omega)$ of K .

17. Give another proof of (4.24) by showing that every finitely generated free R -module is reflexive, and then proving that every finitely generated projective R -module is reflexive.

5. COMPLETIONS AND VALUATIONS

5a Completions

We shall review, without proof for the most part, some elementary facts about completions. The reader is referred to the standard references, listed at the start of §4, for details and proofs.

Let K be a field with a valuation φ , topologized as in §4b. Let \hat{K} denote the completion of K relative to this topology; then \hat{K} is a field whose elements are equivalence classes of Cauchy sequences of elements of K , two sequences being *equivalent* if their difference is a null sequence. The field K is embedded in \hat{K} , and the valuation φ extends to a valuation $\hat{\varphi}$ on \hat{K} . The field \hat{K} is *complete* relative to the topology induced by $\hat{\varphi}$, that is, every Cauchy sequence from \hat{K} has a limit in \hat{K} .

If φ is an archimedean valuation, then so is $\hat{\varphi}$, and \hat{K} is a complete field with respect to an archimedean valuation. The only possibilities for \hat{K} are

R (the real field) or **C** (the complex field), and in each case $\hat{\varphi}$ is equivalent to the usual absolute value.

If φ is non-archimedean, so also is $\hat{\varphi}$; the two valuations have the same value group, and the same residue class field (up to isomorphism). In particular, let R be a Dedekind domain with quotient field K , where $K \neq R$, and let P be a maximal ideal of R . The completion of K with respect to the P -adic valuation φ_P on K (see §4b) will be denoted by \hat{K}_P (or just \hat{K} , if there is no danger of confusion). Call \hat{K}_P a P -adic field, and its elements P -adic numbers. The discrete valuation φ_P extends to a discrete valuation $\hat{\varphi}_P$ on \hat{K}_P . We have already remarked that the valuation ring of φ_P is the localization R_P ; let \hat{R}_P be the valuation ring of $\hat{\varphi}_P$. Every element of \hat{R}_P can be represented by a Cauchy sequence from R_P (or from R , for that matter). If π is a prime element of R_P , then π is also a prime element of \hat{R}_P . Let \mathcal{S} temporarily denote a full set of residue class representatives in R of the residue class field $\bar{R} = R/P$, with $0 \in \mathcal{S}$. Each $x \in \hat{R}_P$ is uniquely expressible as

$$x = \alpha_0 + \alpha_1\pi + \alpha_2\pi^2 + \cdots, \quad \alpha_i \in \mathcal{S},$$

and each $y \in \hat{K}_P$ is uniquely of the form $y = \pi^k \cdot x$, $k \in \mathbf{Z}$, where uniqueness is guaranteed by the condition that $\alpha_0 \neq 0$. (If $y = 0$, take $k = -\infty$).

We note that K is dense in \hat{K}_P , that is, given any $\alpha \in \hat{K}_P$ and any $\varepsilon > 0$, there exists an element $a \in K$ such that

$$\hat{\varphi}_P(a - \alpha) < \varepsilon.$$

Likewise R is dense in \hat{R}_P , and so also is R_P .

(5.1) THEOREM. (i) \hat{R}_P is a faithfully flat R_P -module.

(ii) For each $k \geq 1$, there are R -isomorphisms

$$R/P^k \cong R_P/\pi^k R_P \cong \hat{R}_P/\pi^k \hat{R}_P,$$

where π is a prime element of R_P .

Proof. The first assertion is contained in (2.22) (see also Exercise 5.3). The first part of (ii) is proved in (3.13). Finally, the composition of maps $R_P \rightarrow \hat{R}_P \rightarrow \hat{R}_P/\pi^k \hat{R}_P$ yields a map $\lambda: R_P \rightarrow \hat{R}_P/\pi^k \hat{R}_P$, and λ is an epimorphism since R_P is dense in \hat{R}_P . Clearly $\ker \lambda = R_P \cap \pi^k \hat{R}_P = \pi^k R_P$, which completes the proof.

For any R -module M , let

$$M_P = R_P \otimes_R M, \quad \hat{M}_P = \hat{R}_P \otimes_R M \cong \hat{R}_P \otimes_{R_P} M_P.$$

Thus the passage from M to \hat{M}_P can be accomplished in two steps: localization (from M to M_P), and completion (from M_P to \hat{M}_P). In the second step, we

start with a discrete valuation ring R_p , and pass to its completion \hat{R}_p . We shall analyze this step in some detail below.

(5.2) **THEOREM.** *Let R be a discrete valuation ring with prime element π , quotient field K , and let \hat{R} , \hat{K} denote completions.*

(i) *For each finitely generated R -module M , the map $M \rightarrow \hat{R} \otimes_R M$ is an inclusion. Denote $\hat{R} \otimes_R M$ by $\hat{R}M$ hereafter.*

(ii) *Let V be a finite dimensional K -space, and set $\hat{V} = \hat{K} \otimes_K V$. The formulas*

$$T = \hat{R}M, \quad M = T \cap V,$$

give a one-to-one inclusion-preserving correspondence between the set of full R -lattices M in V , and the set of full \hat{R} -lattice T in \hat{V} .

Proof. For (i), we note that M is isomorphic to a direct sum of cyclic modules of the form $R/\pi^k R$, $k \geq 0$, so it suffices to prove the result for $M = R/\pi^k R$. But then $M \rightarrow \hat{R} \otimes_R M = \hat{R}/\pi^k \hat{R}$ is surely monic (obvious when $k = 0$, and true for $k > 0$ by (5.1)).

To prove (ii), use bases! Suppose first that M is a full R -lattice in V . We may write

$$M = \sum_{i=1}^n Rx_i, \quad V = \sum_{i=1}^n Kx_i, \quad \hat{M} = \sum_{i=1}^n \hat{R}x_i,$$

where $n = (V:K)$. Then

$$\hat{M} \cap V = \sum (\hat{R} \cap K)x_i = \sum Rx_i = M,$$

as desired.

Conversely, let T be a full \hat{R} -lattice in \hat{V} , and write

$$T = \sum_{i=1}^n \hat{R}x_i, \quad \hat{V} = \sum_{i=1}^n \hat{R}x_i, \quad V = \sum_{i=1}^n Ky_i$$

(note that $(V:K) = (\hat{V}:\hat{K})$). Then $y_i = \sum \sigma_{ij}x_j$, $\sigma_{ij} \in \hat{K}$, $1 \leq i \leq n$, and $S = (\sigma_{ij})$ is an invertible matrix over \hat{K} . Choose $T = (\tau_{ij})$ with entries in K close to those of S^{-1} (in the topology induced by the valuation); then TS is a unit in the matrix ring $M_n(\hat{R})$. Set

$$y'_i = \sum \tau_{ij}y_j = \sum \tau_{ij}\sigma_{jk}x_k.$$

Then we have

$$T = \sum \hat{R}x_i = \sum \hat{R}y'_i, \quad V = \sum Ky'_i,$$

and so

$$T \cap V = \sum (\hat{R} \cap K)y'_i = \sum Ry'_i.$$

Thus $T \cap V$ is a full R -lattice in V such that $\hat{R}(T \cap V) = T$. This completes the proof of the theorem.

We may now prove analogues of (4.21) and (4.22):

(5.3) Theorem. *Let R be a Dedekind domain with quotient field K , let M be an R -lattice, and let $V = KM$. Let P range over all maximal ideals of R .*

(i) *We have*

$$M = KM \cap \left\{ \bigcap_P \hat{M}_P \right\}.$$

(ii) *For each P , let there be given a full \hat{R}_P -lattice $Y(P)$ in $\hat{K}_P V$, such that $Y(P) = \hat{M}_P$ a.e. Define*

$$N = V \cap \left\{ \bigcap_P Y(P) \right\}.$$

Then N is a full R -lattice in V , and $\hat{N}_P = Y(P)$ for all P .

Proof. By (5.2), $M_P = KM \cap \hat{M}_P$ for each P . Assertion (i) now follows at once from (4.21). To prove (ii), set $X(P) = V \cap Y(P)$ for each P . By (5.2), $X(P)$ is a full R_P -lattice in V . Clearly $X(P) = V \cap \hat{M}_P = M_P$ a.e., and $N = \bigcap_P X(P)$. By (4.22) N is a full R -lattice in V , and $N_P = X(P)$ for all P .

Therefore $\hat{N}_P = \hat{R}_P \cdot X(P) = Y(P)$ for all P , by (5.2), and the theorem is proved.

We indicate the generalization of (5.3) to the case where R is a noetherian integrally closed domain. Recall that for each minimal prime P of such a domain R , the localization R_P is a discrete valuation ring, and so we may form its completion \hat{R}_P just as above.

(5.4) THEOREM. *Let M be a full R -lattice in a finite dimensional K -space V , where R is a noetherian integrally closed domain with quotient field K . Suppose that for each minimal prime P of R , we are given an \hat{R}_P -lattice $Y(P)$ in \hat{V}_P , such that $Y(P) = \hat{M}_P$ a.e. Set*

$$N = V \cap \left\{ \bigcap_P Y(P) \right\}.$$

Then N is a full R -lattice in V , N is reflexive, and $\hat{N}_P = Y(P)$ for all P .

Proof. The theorem follows readily from (4.26) and (5.2).

5b Extensions of complete fields

Throughout this section, let K be a field complete with respect to a valuation φ , either archimedean or not, and let \tilde{K} be an algebraic closure of K . Then (see references) we may extend φ to a valuation $\tilde{\varphi}$ on \tilde{K} , as follows:

each $a \in \tilde{K}$ lies in some field L with $K \subset L \subset \tilde{K}$, $(L:K)$ finite (for example, $L = K(a)$ will do). Set

$$(5.5) \quad \tilde{\varphi}(a) = \{\varphi(N_{L/K}a)\}^{1/(L:K)}.$$

Then we find that the value $\tilde{\varphi}(a)$ is independent of the choice of L , and that every finite extension of K contained in \tilde{K} is complete with respect to the valuation $\tilde{\varphi}$.

When φ is archimedean, there are only two possibilities:

- (i) $K = \mathbf{C} = \tilde{K}$, $\varphi = \tilde{\varphi}$
- (ii) $K = \mathbf{R}$, $\tilde{K} = \mathbf{C}$, $\tilde{\varphi}$ extends φ ,

where φ and $\tilde{\varphi}$ are the usual absolute values on \mathbf{R} or \mathbf{C} .

If φ is non-archimedean, so is $\tilde{\varphi}$. However, $\tilde{\varphi}$ need not be a discrete valuation, even if φ is discrete.

We shall consider discrete valuations in more detail below, and for this purpose let us adopt a more systematic notation. If φ is a discrete valuation on K , denote by o_K its valuation ring, and by p_K the maximal ideal of o_K . Let $\bar{o}_K = o_K/p_K$ be the residue class field, and let $p_K = \pi_K \cdot o_K$, so π_K is a prime element of o_K . Let v_K be the *exponential valuation* on K , defined by setting

$$aR = p_K^{v_K(a)}, \quad a \in K, \quad a \neq 0,$$

and $v_K(0) = +\infty$.

Any finite extension L of K can be embedded in \tilde{K} , and the restriction of $\tilde{\varphi}$ to L gives a discrete valuation ψ which extends φ . We define the *ramification index* $e = e(L/K)$ and *residue class degree* $f = f(L/K)$ by the formulas

$$v_L(\pi_K) = e, \quad (\bar{o}_L : \bar{o}_K) = f.$$

(5.6) THEOREM. *Let L be a finite extension of the complete field K , and keep the above notation. Then*

- (i) o_L is the integral closure of o_K in L .
- (ii) Both $e(L/K)$ and $f(L/K)$ are finite, and

$$e(L/K) \cdot f(L/K) = (L:K).$$

- (iii) For each $a \in L$,

$$v_L(a) = f(L/K)^{-1} \cdot v_K(N_{L/K}a).$$

- (iv) Let $a_1, \dots, a_f \in o_L$ be such that $\bar{o}_L = \sum \bar{o}_K \bar{a}_i$, and let $\pi_0, \pi_1, \dots, \pi_{e-1} \in o_L$ be such that $v_L(\pi_j) = j$, $0 \leq j \leq e-1$, where $e = e(L/K)$, $f = f(L/K)$. Then the $e \cdot f$ elements $\{a_i \pi_j\}$ form a free o_K -basis for o_L .

For future use, we state

(5.7) THEOREM. (Hensel's Lemma). *Let $f(X) \in o_K[X]$ and suppose that in $\bar{o}_K[X]$ there is a factorization*

$$\bar{f}(X) = u(X)v(X), \quad u(X) \text{ monic},$$

where $u(X)$ and $v(X)$ are relatively prime. Then there is a factorization in $\bar{o}_K[X]$:

$$f(X) = g(X)h(X), \quad g(X) \text{ monic},$$

such that $\bar{g} = u$, $\bar{h} = v$.

Recall that L is an *unramified* extension of K if $e(L/K) = 1$ and \bar{o}_L is a separable extension of \bar{o}_K . The study of unramified extensions reduces at once to the study of separable extensions of the residue class field \bar{o}_K by virtue of the following basic result (see references):

(5.8) THEOREM. (i) *There is a one-to-one inclusion-preserving correspondence between the set fields L such that*

$$K \subset L \subset \tilde{K}, \quad L = \text{finite unramified extension of } K,$$

and the set of fields k finite separable over \bar{o}_K . This correspondence assigns to each such field L the field k given by $k = \bar{o}_L$.

(ii) *If $L = K(a)$, where a is a zero of a monic $f(X) \in o_K[X]$ such that \bar{a} is a simple zero of $\bar{f}(X)$, then L is unramified over K , and*

$$o_L = o_K[a], \quad \bar{o}_L = \bar{o}_K(\bar{a}), \quad (L:K) = (\bar{o}_L:\bar{o}_K).$$

Conversely, every unramified extension L of K is of this form.

(iii) *Given $k = \bar{o}_K(\xi)$, let $f(X) \in o_K[X]$ be any monic polynomial such that $\bar{f}(X) = \min. \text{pol.}_{\bar{o}_K}\xi$. Then there exists a field $L = K(a) \subset \tilde{K}$ such that L is unramified over K , and $\bar{o}_L = k$, and further*

$$f(X) = \min. \text{pol.}_K a, \quad \bar{a} = \xi \text{ in } \bar{o}_L.$$

(iv) *L/K is a galois extension if and only if \bar{o}_L/\bar{o}_K is a galois extension. If G is the galois group of L/K , then each $\sigma \in G$ induces an element $\bar{\sigma}$ in the galois group \bar{G} of \bar{o}_L/\bar{o}_K . The map $\sigma \rightarrow \bar{\sigma}$ gives an isomorphism $G \cong \bar{G}$.*

(5.9) COROLLARY. *Let $(E:K) < \infty$. There is a unique field W which is maximal with respect to the properties*

$$K \subset W \subset E, \quad W \text{ is unramified over } K.$$

This field W is the *inertia field* of the extension E/K ; it is characterized by the facts that W/K is unramified, and \bar{o}_W is the separable closure of \bar{o}_K in \bar{o}_L , that is,

$$\bar{o}_W = \{x \in \bar{o}_L : x \text{ is separable over } \bar{o}_K\}.$$

(5.10) THEOREM. *Suppose that the complete field K has finite residue class field \bar{o}_K , and let $q = \text{card } \bar{o}_K$. Then for each positive integer f , there is a*

unique unramified extension W of K such that $(W:K) = (\bar{o}_W:\bar{o}_K) = f$, namely, $W = K(\omega)$ for ω a primitive $(q^f - 1)$ -th root of 1 over K . Furthermore,

$$o_W = o_K[\omega], \quad \bar{o}_W = \bar{o}_K(\bar{\omega}).$$

Proof. There is a unique separable extension of \bar{o}_K of degree f , namely $\bar{o}_K(\xi)$, where ξ is a primitive $(q^f - 1)$ -th root of 1 over \bar{o}_K . Hence by (5.8) there is a unique unramified extension W of K such that $(W:K) = (\bar{o}_W:\bar{o}_K) = f$. We need only show that $K(\omega)$ is an unramified extension of K such that $(K(\omega):K) = f$. However, ω is a zero of the polynomial

$$f(X) = X^{q^f - 1} - 1 \in o_K[X].$$

Since $f(X)$ has no repeated zeros, it follows from (5.8ii) that $K(\omega)$ is unramified over K . Further

$$f(X) = \prod(X - \omega^i), \quad f(X) = \prod(X - \bar{\omega}^i),$$

where $1 \leq i \leq q^f - 1$ in each product. Hence $\bar{\omega}$ is a primitive $(q^f - 1)$ -th root of 1, so by (5.8 ii)

$$(K(\omega):K) = (\bar{o}_K[\bar{\omega}]:\bar{o}_K) = f.$$

This completes the proof of the theorem.

(5.11) COROLLARY. *Keep the notation of (5.10). Then W/K and \bar{o}_W/\bar{o}_K are galois extensions, with galois groups G, \bar{G} cyclic of order f . The group G has generator $\sigma: \omega \rightarrow \omega^q$, while \bar{G} is generated by $\bar{\sigma}: \bar{\omega} \rightarrow \bar{\omega}^q$. Call σ the Frobenius automorphism of the extension W/K .*

Proof. It is well-known that \bar{G} is cyclic of order f with generator $\bar{\sigma}$, since \bar{G} is the galois group of $\bar{o}_K(\bar{\omega})/\bar{o}_K$, and $\bar{o}_K(\bar{\omega})$ is the splitting field of $f(X)$ over \bar{o}_K . If $g(X) = \min. \text{pol.}_{\bar{o}_K}(\bar{\omega})$, then

$$g(X) = \prod_{i=0}^{f-1} (X - \bar{\omega}^{q^i}).$$

Therefore

$$\min. \text{pol.}_K \omega = \prod_{i=0}^{f-1} (X - \omega^{q^i}),$$

and hence $\sigma: \omega \rightarrow \omega^q$ is a generator of the group G .

The extreme opposites of unramified extensions are the completely ramified extensions. Recall that L is a *completely ramified* extension of K if $\bar{o}_L = \bar{o}_K$, that is, $f(L/K) = 1$. Such extensions can be classified, as follows: an *Eisenstein polynomial* is one of the form

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in o_K[X],$$

where each $a_i \in p_K$, and $a_n \notin p_K^2$. By Exercise 5.1, $f(X)$ is irreducible in $K[X]$.

(5.12) THEOREM. (i) Let L be a completely ramified extension of K of degree n . Then $\min. \text{pol.}_K \pi_L$ is an Eisenstein polynomial over o_K , and $L = K(\pi_L)$.

(ii) Let $f(X)$ be an n -th degree Eisenstein polynomial over o_K , and let $L = K(\alpha)$, where $\min. \text{pol.}_K \alpha = f(X)$. Then L is completely ramified over K , $(L:K) = n$, and α is a prime element of o_L . Furthermore, $o_L = o_K[\alpha]$.

The proof is straightforward (see references), and we omit it. We call L/K an *Eisenstein extension* if it is of the type described in (5.12).

Now let E be any finite extension of K , and suppose that the residue class field \bar{o}_K is perfect, that is, \bar{o}_K has no inseparable extensions. This certainly is the case when \bar{o}_K is a finite field. If W is the inertia field of the extension E/K , then we have

$$\begin{aligned} K &\subset W \subset E, \quad \bar{o}_W = \bar{o}_E, \quad e(W/K) = 1, \quad f(E/W) = 1, \\ f(W/K) &= f(E/K), \quad e(E/W) = e(E/K). \end{aligned}$$

Thus the step from K to E is divided into an unramified step from K to W , followed by a completely ramified step from W to E . We have seen that E is an Eisenstein extension of W , and if \bar{o}_K is finite, then W is a cyclotomic extension of E .

5c Extensions of valuations

Throughout this section, K denotes a field with a valuation φ , archimedean or not, and $\hat{\varphi}$ the extension of φ to the algebraic closure Ω of the completion \hat{K} , as in § 5b. Given a finite separable extension L over K , we wish to determine all extensions of the valuation φ from K to L . Each such extension determines an embedding of L in Ω which preserves the embedding of K in \hat{K} . Two embeddings μ, μ' of L in Ω are called *equivalent* if there exists a K -isomorphism $\sigma: \mu(L) \cong \mu'(L)$ such that $\sigma\mu = \mu'$. Let μ_1, \dots, μ_r be a full set of inequivalent isomorphisms of L into Ω which preserve the embedding of K in \hat{K} . Let $\hat{L}_i = \hat{K} \cdot \mu_i(L)$, the composite of \hat{K} and $\mu_i(L)$ in Ω (that is, the smallest subfield of Ω containing both), and set $n_i = (\hat{L}_i : \hat{K})$. Then (see references) there are precisely r inequivalent valuations ψ_1, \dots, ψ_r of L which extend φ , and these are given by the formula

$$(5.13) \quad \psi_i(a) = \hat{\varphi}(\mu_i(a)) = \{\hat{\varphi}(N_{\hat{L}_i/\hat{K}}(\mu_i a))\}^{1/n_i}, \quad 1 \leq i \leq r.$$

In order to obtain a full set of inequivalent embeddings of L in Ω , write $L = K(\theta)$, $f(X) = \min. \text{pol.}_K \theta$, so $f(X)$ is a separable polynomial. Factor

$f(X)$ into irreducible factors in $\hat{K}[X]$:

$$f(X) = \prod_{i=1}^r f_i(X), \quad f_i(X) \text{ irreducible, } f_i(X) \in \hat{K}[X].$$

The $\{f_i\}$ are necessarily distinct, and we may choose elements $\{\theta_i\} \in \Omega$ such that $f_i(\theta_i) = 0$. Any K -isomorphism $\mu: L \rightarrow \Omega$ must carry θ into a \hat{K} -conjugate of some θ_i , and since we are interested in embeddings only up to equivalence, we may indeed choose μ_i so that $\mu_i(\theta) = \theta_i$. In this way we obtain r inequivalent embeddings μ_1, \dots, μ_r of L in Ω , and for each i , $1 \leq i \leq r$, we have

$$\hat{L}_i = \hat{K}(\theta_i), \quad \min. \text{pol.}_{\hat{K}} \theta_i = f_i(X).$$

Now

$$L = K(\theta) \cong K[X]/(f(X)),$$

and thus

$$\hat{K} \otimes_K L \cong \hat{K}[X]/(f(X)) \cong \sum_{i=1}^r \hat{K}[X]/(f_i(X)) \cong \sum_{i=1}^r \hat{L}_i.$$

Hence for each $a \in L$, we have

$$(5.14) \quad \text{char. pol.}_{L/K} a = \prod_{i=1}^r \text{char. pol.}_{\hat{L}_i/\hat{K}} \mu_i(a),$$

since a acts on $\hat{K} \otimes_K L$ just as $\sum \mu_i(a)$ acts on $\sum \hat{L}_i$. In particular, we obtain from (5.14) the important formulas

$$T_{L/K} a = \sum_i T_{\hat{L}_i/\hat{K}} \mu_i(a), \quad N_{L/K} a = \prod_i N_{\hat{L}_i/\hat{K}} \mu_i(a).$$

Briefly, *global trace is the sum of local traces, and global norm the product of local norms.*

Suppose now that R is a Dedekind domain with quotient field K , and S the integral closure of R in L . For each maximal ideal P of R , let

$$P \cdot S = \prod_{i=1}^r P_i^{e_i}$$

be the factorization of $P \cdot S$ into a product of powers of distinct maximal ideals $\{P_i\}$ of S . Then there are precisely r inequivalent valuations ψ_1, \dots, ψ_r on L which extend the P -adic valuation φ_P on K , obtained by choosing ψ_i to be the P_i -adic valuation on L . The fields \hat{L}_i defined above are precisely the P_i -adic completions of L , and we have

$$n_i = (\hat{L}_i : \hat{K}_P) = e_i f_i, \quad e_i = e(P_i, L/K) = e(\hat{L}_i / \hat{K}_P),$$

$$f_i = f(P_i, L/K) = f(\hat{L}_i / \hat{K}_P), \quad 1 \leq i \leq r.$$

If K is a global field, so that the residue class fields $R/P, S/P_i$ are finite, we may *normalize* the P -adic valuation φ_P of K , and the P_i -adic valuation φ_{P_i} of L , by setting

$$\varphi_P(a) = \mathcal{N}(P)^{-v_P(a)}, \quad \varphi_{P_i}(b) = \mathcal{N}(P_i)^{-v_{P_i}(b)}, \quad a \in K, \quad b \in L,$$

where

$$\mathcal{N}(P) = \text{card } R/P, \quad \mathcal{N}(P_i) = \text{card } S/P_i = \mathcal{N}(P)^{f_i}.$$

In this case, $\varphi_{P_i} = \varphi_P^{n_i}$ on K , so $\varphi_{P_i}^{-1/n_i}$ is the valuation on \hat{L}_i which extends φ_P on \hat{K}_P . Thus

$$\varphi_{P_i}(y) = \varphi_P(N_{\hat{L}_i/\hat{K}_P} y), \quad y \in \hat{L}_i.$$

Hence for $a \in L$,

$$\varphi_P(N_{L/K} a) = \prod_{i=1}^r \varphi_P(N_{\hat{L}_i/\hat{K}} \mu_i a) = \prod_{i=1}^r \varphi_{P_i}(a), \quad a \in L.$$

(This also holds if P is archimedean, with the standard normalizations of φ_P, φ_{P_i} as in §4e).

EXERCISES

1. Let P be a maximal ideal of the Dedekind domain R , and let

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in R[X],$$

where each $a_i \in P$, and $a_n \notin P^2$. (Call f an *Eisenstein polynomial*). Show that $f(X)$ is irreducible in $K[X]$. [Hint: By Gauss' Lemma, it suffices to show that $f(X)$ is irreducible in $R[X]$. Let bars denote passage to $R/P = \bar{R}$. If $f = gh$ in $R[X]$, then $X^n = \bar{f} = \bar{g} \cdot \bar{h}$ in $\bar{R}[X]$, so $g(0), h(0) \in P$, whence $a_n \in P^2$.]

2. Let R be a complete discrete valuation ring, \bar{R} its residue class field, and suppose that \bar{R} is a finite field with q elements. Using Hensel's Lemma (5.7), show that the polynomial $X^{q-1} - 1$ splits into $q - 1$ distinct linear factors in $R[X]$.

3. Let \hat{R} be the P -adic completion of the discrete valuation ring R . Prove directly† that \hat{R} is faithfully flat as R -module. [Hint: We show that \hat{R} is R -flat, that is, for each inclusion $i: L \subset M$ of R -modules, the map $1 \otimes i: \hat{R} \otimes L \rightarrow \hat{R} \otimes M$ is also an inclusion, where \otimes is over R . If $(1 \otimes i)u = 0$, this equation in $\hat{R} \otimes M$ holds as a consequence of finitely many defining relations of the tensor product $\hat{R} \otimes M$. Hence it suffices to prove that $i': R' \otimes L \rightarrow R' \otimes M$ is monic, where R' is some finitely generated R -submodule of \hat{R} . But then R' is R -free, and so i' is clearly monic.]

To show that \hat{R} is faithfully flat, we show that $\hat{R} \otimes M \neq 0$ if $M \neq 0$. Choose any nonzero $m \in M$. Since \hat{R} is R -flat, $\hat{R} \otimes Rm$ is a submodule of $\hat{R} \otimes M$. But $Rm \cong R/J$, $J = \text{ann}_R m < R$, and then

$$\hat{R} \otimes (R/J) \cong \hat{R}/J\hat{R} \neq 0.$$

4. Let \hat{R}_P be the P -adic completion of a Dedekind domain R . Prove directly† that

† That is, without using (2.23).

\hat{R}_P is R -flat. [Hint: Flatness is transitive, since

$$\hat{R}_P \otimes_R \cdot = \hat{R}_P \otimes_{R_P} (R_P \otimes_R \cdot).$$

But R_P is R -flat, and \hat{R}_P is R_P -flat, by Exercise 3.]

5. Does (5.2 i) remain true without the hypothesis that M be finitely generated?

6. Keeping the notation of (5.2), show that if T is an \hat{R} -lattice of V with $\text{rank}_{\hat{R}} T < (V:K)$, then it may happen that $T \cap V = 0$.

7. Let R be a discrete valuation ring with maximal ideal $P = \pi R$, and let \hat{R} be its P -adic completion. For M a finitely generated R -module, we set $\hat{M} = \hat{R} \otimes_R M$. Prove

$$(i) M/\pi^k M \cong \hat{M}/\pi^k \hat{M}, k \geq 1.$$

$$(ii) M \cap \pi^k \hat{M} = \pi^k M, k \geq 0, \text{ where we view } M \text{ as a submodule of } \hat{M} \text{ as in (5.2).}$$

[Hint: We can express M as a direct sum of cyclic modules of the form R/P^n , $n \geq 0$, and it suffices to prove the results when $M = R/P^n$. For $M = R$, (i) follows from (5.1), while (ii) is clear. For $M = R/P^n$, $n \geq 1$, we have $\hat{M} \cong \hat{R}/P^n \hat{R}$, so $M \cong \hat{M}$ by (5.1). Identifying M with \hat{M} , it is then obvious that (i) and (ii) hold true.]

6. RADICALS OF RINGS

Throughout this section, A is a ring (with unity element), not necessarily commutative. All modules are unital. For an A -module M , define its *annihilator* as

$$\text{ann}_A M = \{a \in A : aM = 0\},$$

and omit the subscript A when there is no danger of confusion. We shall also write Hom instead of Hom_A . By an *epimorphism* $A \rightarrow B$ of the ring A onto the ring B , we shall mean always a ring homomorphism which is surjective. (This represents a change from the terminology used in category theory.) As general reference for the material in this section, we cite Jacobson [1, 2].

6a Jacobson radical

An A -module M is *irreducible* (or *simple*) if $M \neq 0$ and M contains no submodules except 0 and M . If M is simple, then for each nonzero $m \in M$ we have $M = Am$. The module epimorphism $A \rightarrow M$ defined by $a \rightarrow am$, $a \in A$, has kernel a left ideal L in A , and thus $M \cong A/L$. Since M is simple, L must be a maximal left ideal of A . Conversely, for each such L , the A -module A/L is simple.

The *Jacobson radical* of A , denoted by $\text{rad } A$, is defined as

$$(6.1) \quad \text{rad } A = \bigcap_M \text{ann } M = \bigcap_L \text{ann } A/L,$$

where M ranges over all simple left A -modules, and L over all maximal left ideals of A . Since each $\text{ann } M$ is a two-sided ideal of A , so is $\text{rad } A$.

The ring A is *semisimple* if $\text{rad } A = 0$. (Some authors call such rings “semisimple in the sense of Jacobson”.)

(6.2) **THEOREM.** $A/\text{rad } A$ is a semisimple ring.

Proof. Let $\bar{A} = A/\text{rad } A$; since $(\text{rad } A) M = 0$ for each simple left A -module M , we may view M as a simple \bar{A} -module. Now let $x \in A$ be such that $x + \text{rad } A \in \text{rad } \bar{A}$. Then $(x + \text{rad } A) M = 0$, whence $xM = 0$. Hence $x \in \text{rad } A$, which shows that $\text{rad } \bar{A} = 0$, and so \bar{A} is semisimple.

(6.3) **THEOREM.** $\text{rad } A$ is the intersection of all maximal left ideals of A .

Proof. For each maximal left ideal L of A we have $\text{ann}(A/L) \subset L$, since A has a unity element. Therefore

$$\text{rad } A = \bigcap_L \text{ann}(A/L) \subset \bigcap_L L$$

For the reverse inclusion, let M be any simple A -module. Then

$$\text{ann } M = \bigcap_{m \in M} \text{ann } m.$$

But if $m \in M$, $m \neq 0$, then $\text{ann } m$ is the kernel of the epimorphism $A \rightarrow Am = M$, and so $\text{ann } m$ is a maximal left ideal of A . Hence

$$\text{ann } M \supset \bigcap_L L,$$

where L ranges over all maximal left ideals of A . Therefore

$$\text{rad } A = \bigcap_M \text{ann } M \supset \bigcap_L L,$$

and the theorem is proved.

An element $u \in A$ is a *unit* if there exists an element $v \in A$ such that $uv = vu = 1$. We shall denote by $u(A)$ the group of units of A . In most of the cases arising in this book, each element of A having a one-sided inverse is necessarily a unit of A . To prove this, we begin with a result of independent interest:

(6.3a) **THEOREM.** Let M be a noetherian left A -module, and let $f \in \text{Hom}_A(M, M)$ be such that $f(M) = M$. Then f is an isomorphism.

Proof. We need only show that f is monic. For $n \geq 1$, set

$$K_n = \ker f^n = \{x \in M : f^n(x) = 0\}.$$

Then $0 \subset K_1 \subset K_2 \subset \dots$ is an ascending chain of submodules of M , and

hence $K_n = K_{n+1}$ for some n , since M is noetherian. Now let $x \in M$ be such that $f(x) = 0$. From the hypothesis that $f(M) = M$, it follows that $M = f^n(M)$, and so we may write $x = f^n(y)$ for some $y \in M$. Then $0 = f(x) = f^{n+1}(y)$, whence $y \in K_{n+1}$. But then $y \in K_n$, and thus $x = f^n(y) = 0$. This completes the proof that f is monic, and establishes the theorem.

As an immediate consequence of the above, we have

(6.4) THEOREM. *Let A be a left noetherian ring, and let $ab = 1$ in A . Then also $ba = 1$.*

Proof. Let $M = {}_A A$, a noetherian left A -module; by (6.3a), every A -epimorphism $f: M \rightarrow M$ must be an isomorphism. Since

$$A = Aab \subset Ab \subset A,$$

we have $A = Ab$. Let $f: M \rightarrow M$ be the epimorphism defined by setting $f(x) = xb$, $x \in M$. Then f is an isomorphism. However, $f(1 - ba) = (1 - ba)b = 0$, and therefore $1 - ba = 0$. This completes the proof.

Returning to the general case, we prove next

(6.5) THEOREM. *For any ring A ,*

$$\text{rad } A = \{x \in A : 1 - axb \in u(A) \text{ for all } a, b \in A\}.$$

Proof. (i) Let $x \in \text{rad } A$, and let $a, b \in A$; since $\text{rad } A$ is a two-sided ideal of A , we have $y = axb \in \text{rad } A$. We now show that $1 - y \in u(A)$ for each $y \in \text{rad } A$. If $A(1 - y) < A$, there is a maximal left ideal L of A such that $A(1 - y) \subset L$, and then $1 - y \in L$. Since $\text{rad } A \subset L$, this gives $1 \in L$, a contradiction. Therefore $A(1 - y) = A$ for all $y \in \text{rad } A$, and so $t(1 - y) = 1$ for some $t \in A$. Therefore $1 - t = -ty \in \text{rad } A$, whence (as above) $A(1 - (1 - t)) = A$, that is $At = A$. Hence there exists $u \in A$ such that $ut = 1$, and thus

$$u = ut(1 - y) = 1 - y.$$

This proves that t is a two-sided inverse of $1 - y$, so $1 - y \in u(A)$, as desired.

(ii) Let $x \in A$ be such that $1 - axb \in u(A)$ for all $a, b \in A$. To show that $x \in \text{rad } A$, we need prove that $xM = 0$ for every simple left A -module M . Let $m \in M$, $m \neq 0$; if $xm \neq 0$, then $M = A \cdot xm$, so $m = axm$ for some $a \in A$, and thus $(1 - ax)m = 0$. But $1 - ax \in u(A)$, and hence $m = 0$, a contradiction. This proves that $xm = 0$ for each nonzero $m \in M$, and therefore $xM = 0$, completing the proof of the theorem.

(6.6) COROLLARY. *If we compute a radical of A by using right A -modules rather than left A -modules, we obtain the same $\text{rad } A$.*

Proof. The preceding theorem gives a left-right symmetric characterization of the radical.

A left ideal N of A is *nilpotent* if there exists a positive integer k such that

$$\underbrace{N \cdot N \cdots N}_k = 0,$$

or equivalently, $x_1 \cdots x_k = 0$ for all $\{x_i\} \in N$. An element $x \in A$ is *nilpotent* if $x^k = 0$ for some k . An element $e \in A$ is *idempotent* if $e \neq 0$ and $e^2 = e$. Obviously, a nilpotent ideal cannot contain any idempotent elements.

(6.7) THEOREM. *Let N be a nilpotent left ideal of A , and let $x \in A$ be a non-nilpotent element such that $x^2 - x \in N$. Then the left ideal Ax contains an idempotent y such that $y - x \in N$.*

Proof. Let $N^k = 0$, and set $n_1 = x^2 - x \in N$. If $n_1 = 0$, choose $y = x$, and we are done. If $n_1 \neq 0$, let

$$x_1 = x + n_1 - 2xn_1 \in Ax.$$

Then x, x_1 and n_1 commute with each other, and hence if x_1 is nilpotent, so also is $x = x_1 - n_1 + 2xn_1$, a contradiction. Thus x_1 is a non-nilpotent element of Ax , and direct calculation gives

$$x_1^2 - x_1 = 4n_1^3 - 3n_1^2.$$

The element $n_2 = x_1^2 - x_1$ is nilpotent, contains n_1^2 as factor, and commutes with x_1 . Continuing in this manner, we may construct a sequence $\{x_i\}$ of non-nilpotent elements of Ax , such that $n_1^{2^i}$ occurs as a factor in $x_i^2 - x_i$. If we choose i so that $2^i \geq k$, then we have $x_i^2 - x_i = 0$. Further, $x_i \neq 0$ since x_i is non-nilpotent. Thus we may take $y = x_i$, the desired idempotent in Ax such that $y - x \in N$.

(6.8) COROLLARY. *Let L be a non-nilpotent left ideal in a left artinian ring A . Then L contains an idempotent element.*

Proof. Let L_1 be a minimal member of the (non-empty) set of non-nilpotent left ideals contained in L ; then $L_1^2 \subset L_1$, whence $L_1^2 = L_1$. Now let I be minimal in the set of left ideals contained in L_1 such that $L_1 \cdot I \neq 0$, and choose $a \in I$ so that $L_1 \cdot a \neq 0$. Then $L_1 \cdot L_1 a \neq 0$ and $L_1 a \subset I$, whence $L_1 a = I$. Hence $a = xa$ for some $x \in L_1$, and thus $a = x^k a$ for all $k \geq 0$. Therefore I contains the non-nilpotent element x .

If we now set

$$N = \{b \in L_1 : ba = 0\},$$

then $x^2 - x \in N$. Further, $L_1 a = I \neq 0$ so $N < L_1$. Then N is nilpotent, by the way in which L_1 was chosen. Thus Ax contains an idempotent element by (6.7), whence so does L , since $L \supset L_1 \supset Ax$.

(6.9) THEOREM. *If A is left artinian, then $\text{rad } A$ is the largest nilpotent left ideal of A .*

Proof. If L is a nilpotent left ideal, and $x \in L$, then for all $a, b \in A$ also axb is nilpotent; namely,

$$(axb)^k = ax \cdot (bax)^{k-1} \cdot b \in L^k \cdot b = 0.$$

But then $1 - axb \in u(A)$, since

$$1 + axb + (axb)^2 + \dots$$

is a two-sided inverse of $1 - axb$. This proves that $L \subset \text{rad } A$, by (6.5).

On the other hand, $\text{rad } A$ must itself be nilpotent; for, if not, then by (6.8) $\text{rad } A$ contains an idempotent e . Hence $1 - e \in u(A)$ by (6.5), which is impossible since $(1 - e)e = 0$ but $e \neq 0$.

We may remark that if A is left artinian, then $\text{rad } A$ is also the largest nilpotent right ideal. For if J is any nilpotent right ideal of A , then AJ is a nilpotent two-sided ideal, whence $J \subset AJ \subset \text{rad } A$.

Now we prove some easy properties of radicals.

(6.10) THEOREM. *If $f : A \rightarrow B$ is an epimorphism of rings, then $f(\text{rad } A) \subset \text{rad } B$. Hence f induces an epimorphism $A/\text{rad } A \rightarrow B/\text{rad } B$.*

Proof. Let $x \in \text{rad } A$, $y = f(x)$, and let $b_1, b_2 \in B$. Then there exist $a_1, a_2 \in A$ such that $b_i = f(a_i)$, $i = 1, 2$. But $1 - a_1 x a_2 \in u(A)$, whence $1 - b_1 y b_2 \in u(B)$. Hence $y \in \text{rad } B$, by (6.5).

(6.11) THEOREM (Nakayama's Lemma). *Let M be a finitely generated left A -module such that $(\text{rad } A)M = M$. Then $M = 0$.*

Proof. If $M \neq 0$, let m_1, \dots, m_k be a minimal set of generators of the left A -module M . Since $m_1 \in M = (\text{rad } A)M$, we may write

$$m_1 = r_1 m_1 + \dots + r_k m_k, \quad r_i \in \text{rad } A.$$

But then $1 - r_1 \in u(A)$, so we can solve for m_1 in terms of m_2, \dots, m_k , thereby reducing the number of generators of M .

(6.12) COROLLARY. *Let M be a finitely generated left A -module, and N a submodule such that*

$$N + (\text{rad } A)M = M.$$

Then $N = M$.

Proof. The hypothesis implies that M/N is finitely generated, and $(\text{rad } A)(M/N) = M/N$. The result then follows from (6.11).

(6.13) COROLLARY. *Every maximal two-sided ideal J of A contains $\text{rad } A$.*

Proof. If $J \not\supset \text{rad } A$, then $J + \text{rad } A$ is a two-sided ideal of A properly containing J . Hence $J + \text{rad } A = A$, whence $J = A$ by applying (6.12) with $N = J$, $M = A$.

6b Local rings

The ring A is *local* (or *completely primary*) if A has a unique maximal left ideal.

(6.14) THEOREM. *The following are equivalent:*

- (i) A is local.
- (ii) The set S of non-units of A is a left ideal of A .
- (iii) $A/\text{rad } A$ is a skewfield (that is, a ring whose nonzero elements form a multiplicative group).

Proof. Suppose first that A is local, with J its unique maximal left ideal, so of course $J \subset S$. Since $\text{rad } A$ is the intersection of all maximal left ideals of A , we have $\text{rad } A = J$, and so J is a two-sided ideal. We claim that $S = J$. For let $x \in S$; if $Ax \neq A$, then Ax lies in a maximal left ideal of A , whence $Ax \subset J$, so $x \in J$. On the other hand, if $Ax = A$ then for some $y \in A$, $yx = 1$. Clearly $y \notin J$, otherwise, $1 = yx \in \text{rad } A$. Hence $Ay = A$, so there exists an element $z \in A$ with $zy = 1$, and hence $z = x$. Thus $x \in u(A)$, a contradiction. This proves that $S = J$, and shows also that each element of $A - J$ is a unit in A , whence $A/\text{rad } A$ is a skewfield.

Next, suppose that S is a left ideal of A . Since every proper one-sided ideal of A lies in S , it is clear that S is the unique maximal left ideal (and also right ideal), so A is local.

Finally, suppose that $A/\text{rad } A$ is a skewfield. Clearly $\text{rad } A \subset S$, and we need only prove the reverse inclusion. If $x \in A - \text{rad } A$, there exists $y \in A$ such that $yx = 1 + n$, for some $n \in \text{rad } A$. Hence $yx \in u(A)$, and x has a left inverse in A . Analogously, x has a right inverse, whence $x \in u(A)$. Thus $A - \text{rad } A \subset u(A)$, so $\text{rad } A \subset S$, as desired. This completes the proof.

(6.15) THEOREM. *Let R be a commutative local ring, with maximal ideal*

$P = \text{rad } R$, and residue class field $\bar{R} = R/P$. Let A be an R -algebra, finitely generated as R -module, and let $\varphi: A \rightarrow \bar{A} = A/PA$ be the natural epimorphism of A onto the finite dimensional \bar{R} -algebra \bar{A} . Then we have

$$PA \subset \varphi^{-1}(\text{rad } \bar{A}) = \text{rad } A,$$

and $(\text{rad } A)^t \subset PA$ for some t . Further, φ induces a ring isomorphism

$$A/\text{rad } A \cong \bar{A}/\text{rad } \bar{A}.$$

Proof. We show first that $\text{rad } A \supset PA$. Let M be any simple left A -module; then $M = Am$ for each nonzero $m \in M$, whence M is finitely generated as R -module. Now PM is an A -submodule of M , hence is 0 or M . But $PM \neq M$, otherwise by Nakayama's Lemma we find that $M = 0$. Thus $PM = 0$, and so PA annihilates every such M . Therefore $PA \subset \text{rad } A$.

By (6.10), φ induces an epimorphism

$$A/\text{rad } A \rightarrow \bar{A}/\text{rad } \bar{A}.$$

On the other hand, there is an epimorphism $\psi: \bar{A} \rightarrow A/\text{rad } A$, since $PA \subset \text{rad } A$. By (6.2) we have $\psi(\text{rad } \bar{A}) \subset \text{rad}(A/\text{rad } A) = 0$, and thus ψ induces an epimorphism $\bar{A}/\text{rad } \bar{A} \rightarrow A/\text{rad } A$. Both of these quotients are finite dimensional \bar{R} -algebras, and thus are isomorphic. This shows that $\text{rad } A = \varphi^{-1}(\text{rad } \bar{A})$, as well.

Next, $\text{rad } \bar{A}$ is a nilpotent ideal of the left (and right) artinian ring \bar{A} , by (6.9), and hence $(\text{rad } \bar{A})^t = 0$ for some n . Thus $\varphi(\text{rad } A)^t = 0$, whence $(\text{rad } A)^t \subset PA$, as claimed.

We shall need some standard results on completions of a commutative local ring R , and of modules over such a ring. Suppose first that $X = \sum_{i=1}^k Rx_i$ is a free R -module, and let P denote the maximal ideal of R . We define a P -adic topology on X , by taking as basis for the neighborhoods of a point $x \in X$ the sets $\{x + P^m X : m = 0, 1, 2, \dots\}$. Given a sequence $\{y_n\}$ from X , we may write

$$y_n = r_n^{(1)}x_1 + \cdots + r_n^{(k)}x_k, \quad r_n^{(i)} \in R.$$

Then $\{y_n\}$ is a Cauchy sequence in X if and only if, for each i , $\{r_n^{(i)}\}$ is a Cauchy sequence in R . Further, $\{y_n\}$ converges if and only if each $\{r_n^{(i)}\}$ converges, and we have

$$\lim_{n \rightarrow \infty} \sum r_n^{(i)}x_i = \sum (\lim_{n \rightarrow \infty} r_n^{(i)})x_i.$$

Thus if R is complete in the P -adic topology, then so is X . When R is not complete, we may form its P -adic completion \hat{R} . Then $\hat{R} \otimes_R X$ is a free

\hat{R} -module, and can be topologized as above. If \hat{X} denotes the P -adic completion of X , the above discussion shows that there is an \hat{R} -isomorphism

$$\hat{X} \cong \hat{R} \otimes_R X,$$

and that this is a topological isomorphism.

The following generalization of the above holds true, and we refer the reader to Bourbaki [2, Ch. 3] or Matsumura [1] for proofs:

(6.16) THEOREM. *Let R be a commutative noetherian local ring, with maximal ideal P , and let \hat{R} be the P -adic completion of R . Let X be a finitely generated R -module, and let \hat{X} be the completion of X relative to the P -adic topology on X , defined by taking $\{x + P^n X\}$ as basis for the neighborhoods of $x \in X$. Let $\hat{R} \otimes_R X$ be topologized by taking $\{\xi + P^n(\hat{R} \otimes X)\}$ as basis for the neighborhoods of $\xi \in \hat{R} \otimes X$. Then there is a topological \hat{R} -isomorphism*

$$\hat{X} \cong \hat{R} \otimes_R X,$$

and \hat{X} is a complete Hausdorff space relative to its P -adic topology.

(6.17) COROLLARY. *Let R be a complete commutative noetherian local ring, and let A be an R -algebra which is finitely generated as R -module. Then A is a complete Hausdorff space relative to the P -adic topology on A .*

For the most part, we shall be dealing with the case where R is a complete discrete valuation ring, and A is an R -order. In this case, A is of course R -free, and we need not use (6.16) and (6.17) in their full generality.

6c Lifting idempotents

We shall discuss here the relationship between idempotents in a ring A , and idempotents in a factor ring $\bar{A} = A/N$, where N is a two-sided ideal of A contained in $\text{rad } A$. To begin with, suppose that there is a direct sum decomposition

$$A = L_1 \oplus \cdots \oplus L_k,$$

where each L_i is an indecomposable left ideal of A . We may write

$$1 = e_1 + \cdots + e_k, \quad e_i \in L_i.$$

For each $x \in L_i$, we obtain $x = \sum x e_i$, whence $x e_i = x$ and $x e_j = 0$ for $j \neq i$. This gives

$$e_i^2 = e_i, \quad e_i e_j = 0 \quad (j \neq i), \quad L_i = A e_i.$$

Thus each e_i is idempotent, and we call $\{e_1, \dots, e_k\}$ a full set of *orthogonal*

idempotents in A . Further, each e_i is *primitive*, that is, e_i cannot be expressed as a sum $e' + e''$ of orthogonal idempotents; for if $e_i = e' + e''$, then $L_i = Ae' \oplus Ae''$ gives a decomposition of L_i .

We have thus shown that there is a one-to-one correspondence between decompositions of A into direct sums of indecomposable left ideals, and decompositions of 1_A into a sum of primitive orthogonal idempotents.

Now let $\bar{A} = A/N$, where N is a two-sided ideal of A such that $N \subset \text{rad } A$, and let $a \in A$ have image $\bar{a} \in \bar{A}$. If $e \in A$ is idempotent, then \bar{e} is an idempotent in \bar{A} ; indeed, $e^2 = e$ implies that $\bar{e}^2 = \bar{e}$, while if $\bar{e} = 0$ then $e \in \text{rad } A$, an impossibility (see proof of (6.9)). Thus each decomposition $1 = \sum e_i$ into orthogonal idempotents in A gives a corresponding such decomposition $\bar{1} = \sum \bar{e}_i$ in \bar{A} . In general, however, it may happen that e_i is primitive but \bar{e}_i is not. Our aim here is to show that under suitable hypotheses, \bar{e}_i is primitive whenever e_i is primitive, and indeed, that every decomposition $\bar{1} = \sum \bar{e}_i$ into a sum of primitive orthogonal idempotents “lifts” to a decomposition $1 = \sum e_i$ into primitive orthogonal idempotents, such that $\bar{e}_i = e_i$ for each i .

Given any two-sided ideal N of A , we may give A the N -adic topology by taking as basis for the open neighbourhoods of an element $a \in A$ the sets $\{a + N^r : r = 0, 1, \dots\}$. We call A *complete* in the N -adic topology if each Cauchy sequence (relative to this topology) converges to an element of A . If $N \subset \text{rad } A$, there are two obvious cases where A is necessarily complete in the N -adic topology:

(i) if A is a left artinian ring, then N is a nilpotent ideal by (6.9), and hence any Cauchy sequence from A , relative to the N -adic topology, is constant from some point on;

(ii) if A is an R -algebra, finitely generated as R -module, where R is a complete noetherian local ring with maximal ideal P , then by (6.15) we have

$$N^t \subset (\text{rad } A)^t \subset PA$$

for some t . Hence any Cauchy sequence (from A) relative to the N -adic topology is also a Cauchy sequence in the P -adic topology and thus converges by (6.17).

For the remainder of this section, we assume that A is complete in the N -adic topology.

(6.18) THEOREM. *Each idempotent $\varepsilon \in \bar{A}$ can be lifted to an idempotent $e \in A$, that is, $\bar{e} = \varepsilon$. If e_1, e_2 are idempotents of A , then $Ae_1 \cong Ae_2$ as left A -modules if and only if $\bar{A}\bar{e}_1 \cong \bar{A}\bar{e}_2$ as left \bar{A} -modules.*

Proof. We examine the proof of (6.7). Given an idempotent $\varepsilon \in \bar{A}$, choose any $x_1 \in A$ with $\bar{x}_1 = \varepsilon$. Then $n_1 = x_1^2 - x_1 \in N$. Once x_i and n_i are chosen, let

$$x_{i+1} = x_i + n_i - 2x_i n_i, \quad n_{i+1} = x_{i+1}^2 - x_{i+1}.$$

Then $n_i \in N^{2^i}$, and so $\{x_i\}$ is a Cauchy sequence in the N -adic topology of A . Let $e = \lim_{i \rightarrow \infty} x_i \in A$. Then

$$e^2 - e = \lim n_i = 0,$$

and furthermore $\bar{e} = \bar{x}_1 = \varepsilon$, so $e \neq 0$, and e is the desired idempotent in A .

Now let $e_1, e_2 \in A$ be idempotent. Any isomorphism $Ae_1 \cong Ae_2$ carries Ne_1 onto Ne_2 , and induces an isomorphism $\bar{A}\bar{e}_1 \cong \bar{A}\bar{e}_2$. Conversely, let $f: \bar{A}\bar{e}_1 \cong \bar{A}\bar{e}_2$, and let $\bar{g} = f^{-1}$. Then in the diagram

$$\begin{array}{ccccc} & & f & & \\ & Ae_1 & \dashleftarrow & Ae_2 & \\ \downarrow & g & \dashrightarrow & \downarrow & \\ \bar{A}\bar{e}_1 & \xrightarrow{f} & \bar{A}\bar{e}_2 & \xleftarrow{\bar{g}} & \end{array}$$

the vertical arrows are epic. Since $A = Ae_i \oplus A(1 - e_i)$, each Ae_i is A -projective. Hence we can find A -homomorphisms f, g lifting \bar{f}, \bar{g} , respectively. We claim that f is an isomorphism, and need only show that $\theta = g \cdot f$ is an automorphism of Ae_1 (for then, by symmetry, $f \cdot g$ is an automorphism of Ae_2). Clearly θ lifts $\bar{g} \cdot \bar{f}$, and hence $(\theta - 1)Ae_1 \subset Ne_1$. Let $\xi = 1 - \theta$; then $\xi^k \cdot Ae_1 \subset N^k e_1$; thus $1 + \xi + \xi^2 + \dots$ is a well defined endomorphism of Ae_1 , and is a two-sided inverse of $1 - \xi$. Since $1 - \xi = \theta$, this shows that θ is an A -automorphism of Ae_1 , as claimed. This completes the proof.†

(6.19) THEOREM. Let $\bar{1} = \varepsilon_1 + \dots + \varepsilon_n$ be a decomposition of $\bar{1}$ into orthogonal idempotents in \bar{A} . Then there exist orthogonal idempotents $e_1, \dots, e_n \in A$ such that

$$1 = e_1 + \dots + e_n, \quad \bar{e}_i = \varepsilon_i.$$

Proof. We proceed by induction on n , the result being trivial when $n = 1$. Assume that $n > 1$ and that the result holds at $n - 1$. Set $\delta = \varepsilon_{n-1} + \varepsilon_n$, so now $\bar{1} = \varepsilon_1 + \dots + \varepsilon_{n-2} + \delta$ is an orthogonal decomposition. By the induction hypothesis there exists an orthogonal decomposition

$$1 = e_1 + \dots + e_{n-2} + e, \quad \bar{e}_1 = \varepsilon_1, \dots, \bar{e}_{n-2} = \varepsilon_{n-2}, \quad \bar{e} = \delta,$$

Choose $a \in A$ such that $\bar{a} = \varepsilon_{n-1}$, and set $b = eae$. Then $\bar{b} = \delta \cdot \varepsilon_{n-1} \cdot \delta = \varepsilon_{n-1}$, and $e_i b = b e_i = 0$, $1 \leq i \leq n - 2$. In the proof of (6.18), we take $x_1 = b$. Then the sequence $\{x_i\}$ converges to an idempotent $e_{n-1} \in A$ such that $\bar{e}_{n-1} = \varepsilon_{n-1}$, and $e_i e_{n-1} = e_{n-1} e_i = 0$, $1 \leq i \leq n - 2$. Finally, set

† For more general theorems of this type, see Azumaya [1, Th. 24].

$e_n = e - e_{n-1}$; then $1 = e_1 + \cdots + e_n$ is the desired orthogonal decomposition in A such that $\bar{e}_i = e_i$ for $1 \leq i \leq n$.

(6.20) COROLLARY. *An idempotent $e \in A$ is primitive if and only if its image $\bar{e} \in \bar{A}$ is primitive.*

Proof. If e is imprimitive, there is an orthogonal decomposition $e = e_1 + e_2$ into idempotents $e_1, e_2 \in A$. Then $\bar{e} = \bar{e}_1 + \bar{e}_2$ is an orthogonal decomposition of \bar{e} . Conversely, let $\bar{e} = \bar{e}_1 + \bar{e}_2$ be an orthogonal decomposition into idempotents of \bar{A} . The proof of (6.19) shows that there exist orthogonal idempotents $e_1, e_2 \in A$ such that $\bar{e}_1 = e_1$, $\bar{e}_2 = e_2$, and $e = e_1 + e_2$. This completes the proof.

(6.21) THEOREM. *Let A be a left artinian ring, and let $\bar{A} = A/\text{rad } A$. Let $1 = e_1 + \cdots + e_n$ be a decomposition of $1 \in A$ into orthogonal primitive idempotents in A . Then*

$$A = Ae_1 \oplus \cdots \oplus Ae_n$$

is a decomposition of A into indecomposable left ideals of A , and

$$\bar{A} = \bar{A}\bar{e}_1 \oplus \cdots \oplus \bar{A}\bar{e}_n$$

is a decomposition of \bar{A} into minimal left ideals. Further, $Ae_i \cong Ae_j$ if and only if $\bar{A}\bar{e}_i \cong \bar{A}\bar{e}_j$.

Proof. Since A is left artinian, it can be expressed as a finite direct sum $\sum_1^n L_i$ of indecomposable left ideals of A . Writing $1 = \sum e_i$, $e_i \in L_i$, we obtain a decomposition of 1 into orthogonal primitive idempotents. Then $\bar{1} = \sum \bar{e}_i$ is such a decomposition in \bar{A} , and so each $\bar{A}\bar{e}_i$ is an indecomposable left ideal of \bar{A} . But \bar{A} is a semisimple artinian ring, so (see (7.1)) every indecomposable left ideal of \bar{A} is a minimal left ideal. The last statement in the theorem has already been established in (6.18), so the proof is completed.

(6.22) COROLLARY. *Let A be an R -algebra, finitely generated as R -module, where R is a complete noetherian commutative local ring. Then the assertions in the preceding theorem remain valid for this case.*

Proof. In the proof of (6.21), we used the hypothesis there that A be left artinian, in order to guarantee that

- (i) A is expressible as a finite direct sum of indecomposable left ideals, and
- (ii) $A/\text{rad } A$ is a semisimple artinian ring.

However, both of these remain valid under the hypotheses of the present

corollary. The first is true, since in the present case A is a left noetherian ring. The second holds true, by virtue of (6.15). Thus the proof of (6.21) applies equally well in this case, and the corollary is established.

EXERCISES

1. Let J be a two-sided ideal of a ring A , such that A/J is semisimple. Prove that $J \supset \text{rad } A$. [Hint: By (6.10), $(J + \text{rad } A)/J \subset \text{rad}(A/J) = 0$.]
2. Let $x \in A$ map onto $\bar{x} \in A/\text{rad } A$. Show that $x \in u(A)$ if and only if $\bar{x} \in u(A/\text{rad } A)$.
3. Keep the notation and hypotheses of (6.15), and let J be any two-sided ideal of A such that $J^m \subset PA$. Show that $J \subset \text{rad } A$. [Hint: $\varphi(J)$ is a nilpotent ideal in the artinian ring \bar{A} , whence $\varphi(J) \subset \text{rad } \bar{A}$, so $J \subset \varphi^{-1}(\text{rad } \bar{A}) = \text{rad } A$.]

In Exercises 4–8 below, let R be a complete noetherian commutative local ring, and let A be an R -algebra which is finitely generated as R -module. We include here the special case where R is a field, and $\{0\}$ is its maximal ideal.

4. Prove that A is a local ring if and only if 1 is the only idempotent in A . [Hint: Let A be local, and let $e \in A$ be idempotent, $e \neq 1$. Since $e(1 - e) = 0$, both e and $1 - e$ are non-units, whence so is their sum; this is a contradiction. Conversely, if A is not local, then $A/\text{rad } A$ is not a skewfield. If $P = \text{rad } R$, then by (6.15) we know that $A/\text{rad } A$ is a finite dimensional semisimple (R/P) -algebra. Hence by §7, $A/\text{rad } A$ contains an idempotent other than 1. Therefore A contains an idempotent different from 1, by (6.18).]

5. An *indecomposable* left A -module is a nonzero left A -module which is not expressible as a direct sum of non-trivial submodules. Let M be a nonzero finitely generated left A -module, and set $E = \text{Hom}_A(M, M)$. Show that E is an R -algebra which is finitely generated as R -module. Using Exercise 6.4, deduce that M is indecomposable as A -module if and only if E is a local ring. [Hint: Given a non-trivial decomposition $M = M_1 \oplus M_2$ into A -submodules, let $\pi_1: M \rightarrow M_1$ be the corresponding projection of M onto M_1 . Then $\pi_1 \in E$ is an idempotent, and $\pi_1 \neq 1$. Conversely, if $e \in E$ is an idempotent different from 1, then $M = eM \oplus (1 - e)M$ gives a decomposition of M .]

6. Prove the **Krull–Schmidt Theorem**: Every finitely generated left A -module M is expressible as a finite direct sum of indecomposable modules, and these direct summands are uniquely determined by M , up to A -isomorphism and order of occurrence. [Hint: Since M is finitely generated over the commutative noetherian ring R , M is itself a noetherian module. The process of decomposing M into direct summands must therefore terminate.]

Now let

$$M = M_1 \oplus \cdots \oplus M_t = N_1 \oplus \cdots \oplus N_u,$$

where the $\{M_i\}$ and $\{N_j\}$ are indecomposable. Let $\mu_i: M \rightarrow M_i$, $\nu_j: M \rightarrow N_j$, be the projections associated with these decompositions. Restrict the operators in the equation $\mu_1 = \sum \mu_i \nu_j$ to M_1 , getting the relation $1 = \sum \mu_1 \nu_j$ in the local ring $\text{Hom}_A(M_1, M_1)$. Hence some $\mu_1 \nu_j$ must be a unit in this ring, that is, must be an automorphism of M_1 . If (say) $\mu_1 \nu_1$ is an automorphism φ of M_1 , then in the diagram

$$M_1 \xrightarrow{\quad v_1 \quad} N_1, \\ \xleftarrow{\varphi^{-1}\mu_1}$$

v_1 is monic and $\varphi^{-1}\mu_1 \cdot v_1$ is the identity on M_1 . Hence there is a splitting $N_1 \cong M_1 \oplus \ker \varphi^{-1}\mu_1$, and therefore $N_1 \cong M_1$. Thus both v_1 and μ_1 are isomorphisms.

Next verify that the sum

$$M' = N_1 \oplus M_2 \oplus \cdots \oplus M_t$$

is direct. Then show that $M' = M$, since for each $x \in N_1$,

$$\mu_1 x = x - \mu_2 x - \cdots - \mu_t x \in M',$$

and thus $M_1 = \mu_1(N_1) \subset M'$. Prove next that the map

$$\rho = v_1\mu_1 + \mu_2 + \cdots + \mu_t$$

defines an A -isomorphism of M onto M' , carrying M_1 onto N_1 . Therefore ρ induces an A -isomorphism

$$M_2 \oplus \cdots \oplus M_t \cong M/N_1 \cong N_2 \oplus \cdots \oplus N_u.$$

An induction argument completes the proof.]

7. Let L, M, N be finitely generated left A -modules such that

$$L \dot{+} M \cong L \dot{+} N.$$

Prove that $M \cong N$. [Hint: Express L, M, N as direct sums of indecomposable modules, and then use the Krull–Schmidt Theorem proved above.]

8. Let $\{M_1, \dots, M_t\}$ be finitely generated indecomposable left A -modules, and let L be a left A -module which is isomorphic to a direct summand of $M_1 \dot{+} \dots \dot{+} M_t$. Show that

$$L \cong M_{i_1} \dot{+} \dots \dot{+} M_{i_r},$$

where $\{i_1, \dots, i_r\}$ is some subset of $\{1, \dots, t\}$. [Hint: The hypothesis implies that $\sum_{i=1}^t M_i \cong L \dot{+} L'$, where both L and L' are finitely generated left A -modules. Now express L and L' as direct sums of indecomposable modules, and then use the Krull–Schmidt Theorem.]

9. Let A be an R -algebra as in (6.22), and let P be the unique maximal ideal of R . Assume that P does not annihilate any nonzero R -submodule of A . Let $J = \text{rad } A$, and set $\bar{A} = A/J$. Show that every simple left \bar{A} -module occurs as a direct summand of the left \bar{A} -module J/J^2 . [Hint: Assume the result false. By § 7, there is a central idempotent ϵ in the semisimple artinian ring \bar{A} such that $\epsilon \cdot (J/J^2) = 0$. By (6.18) there exists an idempotent $e \in A$ mapping onto ϵ . Then $eJ \subset J^2$, whence multiplying by e we obtain $eJ = eJ^2 = eJ \cdot J$. Therefore $eJ = 0$ by Nakayama's Lemma. But $J \supset PA$ by (6.15), and so $P \cdot eA = 0$. This gives $eA = 0$, so $e = 0$ and $\epsilon = 0$, a contradiction.]

7. SEMISIMPLE RINGS AND SIMPLE ALGEBRAS

7a Wedderburn's Theorem

Recall that a ring A is *semisimple* if $\text{rad } A = 0$. Of particular interest, because they occur so frequently in practice, are the left artinian semisimple rings. The algebraic structure of such rings can be described explicitly, as we shall see below. We shall omit proofs of some of the relatively well known theorems stated below, referring the reader to Curtis-Reiner [1] or Bourbaki [1] for details.

A *minimal left ideal* of A is any minimal member of the set of nonzero left ideals of A . Equivalently, a minimal left ideal is a simple submodule of $_A A$.

(7.1) THEOREM. *Let A be a left artinian ring. The following are equivalent:*

- (i) *A is semisimple.*
- (ii) *A is a finite direct sum of minimal left ideals.*
- (iii) *Every exact sequence of left A -modules is split.*
- (iv) *Every left ideal of A is a direct summand of A .*
- (v) *A contains no nonzero nilpotent ideals.*
- (vi) *Every left A -module is a direct sum of simple A -modules.*

Given a left artinian semisimple ring A , we may write $A = L_1 \oplus \cdots \oplus L_r$, $L_i =$ minimal left ideal in A . Set

$$1 = e_1 + \cdots + e_r, \quad e_i \in L_i.$$

From the equation $e_i = \sum_j e_i e_j$ we deduce at once that

$$e_i^2 = e_i, \quad e_i e_j = 0 \quad \text{for } i \neq j, \quad L_i = Ae_i.$$

Call $\{e_i\}$ a full system of *primitive idempotents* of A . Let B_1 denote the sum of those $\{L_j\}$ which are isomorphic to L_1 , B_2 the sum of those $\{L_j\}$ isomorphic to a remaining summand (if any), and so on. Then we have

$$A = B_1 \oplus \cdots \oplus B_t$$

for some $t \leq r$. It is easily shown (see references) that each B_i is a subring of A , and that $B_i \cdot B_j = 0$ for $i \neq j$, so A is the ring direct sum† of the $\{B_i\}$. Each B_i is a *simple* ring, that is, a ring whose only two-sided ideals are 0 and B_i ;

† The *ring direct sum* $\sum_{i=1}^t B_i$ of the rings $\{B_i\}$ is defined to be the Cartesian product $B_1 \times \cdots \times B_t$, with componentwise addition and multiplication. This ring is in fact the *direct product* (in the sense of category theory), and is often denoted by $\prod_{i=1}^t B_i$. We shall use the older terminology “ring direct sum” throughout this book.

of course, B_i is left artinian (since A is). Call these $\{B_i\}$ the *simple components* of A ; they are uniquely determined inside A , although the $\{L_i\}$ are not. Further, every simple A -module is isomorphic to a minimal left ideal of A , hence to some minimal left ideal of some B_i .

Conversely, if B_1, \dots, B_t are simple left artinian rings, then their ring direct sum $\sum B_i$ is a semisimple left artinian ring whose simple components are the $\{B_i\}$.

Now let D be a *skewfield* (or *division ring*), that is, a ring whose nonzero elements form a multiplicative group. Denote by $M_n(D)$ the ring of all $n \times n$ matrices with entries in D . We call $M_n(D)$ a *full matrix algebra* over D .

Let D° (or D^{opp}) denote the *opposite ring* of D ; the elements of D° are the symbols $\{x^\circ : x \in D\}$, with

$$(x^\circ \pm y^\circ) = (x \pm y)^\circ, \quad x^\circ \cdot y^\circ = (yx)^\circ, \quad x, y \in D.$$

Then D° is also a skewfield.

(7.2) THEOREM. (i) If $V = \sum_1^n Dv_i$ is a left vector space over the skewfield D , then $\text{Hom}_D(V, V) \cong M_n(D^\circ)$.

(ii) If $V = \sum_1^n v_i D$ is a right vector space over the skewfield D , then $\text{Hom}_D(V, V) \cong M_n(D)$.

Proof. In case (i), for $a \in \text{Hom}_D(V, V)$, let

$$av_j = \sum_{i=1}^n \alpha_{ij} v_i, \quad \alpha_{ij} \in D.$$

Then the desired isomorphism is given by $a \rightarrow (\alpha_{ij}^\circ)$.

In case (ii), let

$$av_j = \sum_{i=1}^n v_i \alpha_{ij}, \quad \alpha_{ij} \in D,$$

and let $a \rightarrow (\alpha_{ij})$.

(7.3) THEOREM. For each n , the matrix ring $A = M_n(D)$ is a simple ring, both left and right artinian. Every minimal left ideal of A is A -isomorphic to the left A -module L of n -component column vectors with entries in D . Further, $M_n(D) \cong L^{(n)}$ as left A -modules and $D^\circ \cong \text{Hom}_A(L, L)$. If we view L as right D -space, then $A \cong \text{Hom}_D(L, L)$.

(7.4) THEOREM (Wedderburn Structure Theorem). Every left artinian simple ring A is isomorphic to an algebra of $n \times n$ matrices over a skewfield. The

ring A determines n uniquely, and determines the skewfield up to isomorphism. If L is any minimal left ideal of A , then $D = \text{Hom}_A(L, L)$ is a skewfield, and

$$A = \text{Hom}_D(L, L) \cong M_n(D^\circ),$$

where n is the dimension of the left D -space L .

(7.5) COROLLARY. Every left artinian simple ring is also right artinian and is left and right noetherian. The same holds for left artinian semisimple rings.

By virtue of (7.5), we may speak unambiguously of artinian simple or semisimple rings, without having to distinguish between “left” and “right”. A quick proof of (7.4) is sketched in Exercise 7.4. See also Exercises 16.9 and 16.10.

7b Splitting fields

Let K, L, E denote fields, and D, D' skewfields. The center of an algebra A will be denoted by A^c . A *central simple K-algebra* is a simple K -algebra A for which $A^c = K$ and $(A : K)$ is finite. Call D a *skewfield over K* if $D^c \supseteq K$ and $(D : K)$ is finite. By Wedderburn's Theorem, every central simple K -algebra A is of the form $M_n(D)$ for some skewfield D over K . Further,

$$A^c = \{\alpha I_n : \alpha \in D^c\} \cong D^c,$$

so D has center K , and $(A : K) = n^2(D : K)$.

(7.6) THEOREM. Let A be a central simple K -algebra, B an artinian simple K -algebra, not necessarily finite dimensional over K . Then $B \otimes_K A$ is an artinian simple algebra with center B^c .

Proof. We shall first compute $(B \otimes A)^c$, where we write \otimes instead of \otimes_K for brevity. Let $B = \sum K e_i$, so $B \otimes A = \sum e_i \otimes A$. If $u = \sum e_i \otimes a_i \in (B \otimes A)^c$, then u commutes with $1 \otimes a$ for all $a \in A$, whence $\sum e_i \otimes (aa_i - a_i a) = 0$. Therefore $aa_i = a_i a$ for all $a \in A$, whence each $a_i \in A^c = K$, and so $u = b_0 \otimes 1$ for some $b_0 \in B$. But now u commutes with $b \otimes 1$ for all $b \in B$, whence $b_0 \in B^c$. Identifying B with $B \otimes 1$ in $B \otimes A$, we have thus shown that $(B \otimes A)^c \subseteq B^c$. The reverse inclusion is obvious, and therefore $(B \otimes A)^c = B^c$.

Since B is artinian and $(A : K)$ is finite, it is clear that $B \otimes A$ is also artinian. It remains to show that $B \otimes A$ is simple. We may write $B = M_r(D)$, $A = M_s(D')$, where $(D')^c = K$. Now for any skewfields D, D' whose centers contain K , we have

$$\begin{aligned} (7.7) \quad M_r(D) \otimes_K M_s(D') &\cong M_r(K) \otimes M_s(K) \otimes D \otimes D' \\ &\cong M_{rs}(K) \otimes (D \otimes D') \cong M_{rs}(D \otimes_K D'). \end{aligned}$$

Hence to prove that $B \otimes A$ is simple, it suffices to prove that $D \otimes D'$ is simple.

Let $D = \sum Kd_i$, so $D \otimes D' = \sum d_i \otimes D'$. Let $X \neq 0$ be a two-sided ideal of $D \otimes D'$, and choose a shortest $x = \sum_1^m d_i \otimes \delta_i$ in X , $\delta_i \in D'$. Then $x(1 \otimes \delta_1^{-1}) \in X$, so after changing notation, we have

$$x = d_1 \otimes 1 + \sum_2^m d_i \otimes \delta_i \in X.$$

Now let $\delta \in D'$, $\delta \neq 0$; then $y = (1 \otimes \delta) \cdot x \cdot (1 \otimes \delta^{-1}) \in X$, and

$$y = d_1 \otimes 1 + \sum_2^m d_i \otimes \delta \delta_i \delta^{-1}.$$

Since $x - y \in X$ and $x - y$ is shorter than x , this gives $y = x$. Therefore each δ_i commutes with each nonzero $\delta \in D'$, whence each $\delta_i \in K$. Thus $x \in D$, and so x is a unit in $D \otimes D'$, whence $X = D \otimes D'$. This completes the proof.

(7.8) COROLLARY. *Let A be a central simple K -algebra, $L \supset K$. Then $L \otimes_K A$ is a central simple L -algebra.*

Let A be any ring, M a left A -module. Each $a \in A$ determines a left multiplication $a_L : m \rightarrow am$, $m \in M$. The map $a \rightarrow a_L$ is a ring homomorphism of A onto a subring A_L of $\text{Hom}_A(M, M)$. Call M a *faithful* A -module if $A \rightarrow A_L$ is monic, that is, if $a \cdot M = 0$ implies that $a = 0$.

We shall say that the pair (A, M) has the *double centralizer property* if $A_L = \text{Hom}_D(M, M)$, where $D = \text{Hom}_A(M, M)$. It is trivially verified that $(A, {}_A A)$ has the double centralizer property, since in this case $D = A_R$, the set of right multiplications by elements of A .

(7.9) THEOREM. (i) *For each A -module N , the pair $(A, {}_A N + N)$ has the double centralizer property.*

(ii) *Let M be an A -module, k a positive integer. If $(A, M^{(k)})$ has the double centralizer property, then so does (A, M) .*

Proof. (i) Let $D = \text{Hom}_A(M, M)$, where $M = {}_A A + N$. Each $d \in D$ is represented by a 2×2 matrix (d_{ij}) of A -homomorphisms, where

$$d_{11}: A \rightarrow A, \quad d_{12}: A \rightarrow N, \quad d_{21}: N \rightarrow A, \quad d_{22}: N \rightarrow N.$$

Now let $\varphi \in \text{Hom}_D(M, M)$, and write $\varphi = (\varphi_{ij})$, a 2×2 matrix of additive homomorphisms. Since φ commutes with the element $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ of D , it follows

that $\varphi_{12} = 0$, $\varphi_{21} = 0$. Next, fix $n_0 \in N$, and define $d_{n_0} \in D$ by $d_{n_0}(a, n) = (0, an_0)$. Then

$$\varphi d_{n_0}(a, n) = \varphi(0, an_0) = (0, \varphi_{22}(an_0)),$$

while

$$d_{n_0}\varphi(a, n) = d_{n_0}(\varphi_{11}a, \varphi_{22}n) = (0, (\varphi_{11}a)n_0).$$

Thus $(\varphi_{11}a)n_0 = \varphi_{22}(an_0)$ for all $(a, n_0) \in M$, whence (taking $a = 1$)

$(\varphi_{11}(1))n_0 = \varphi_{22}(n_0)$. But φ commutes with $\begin{pmatrix} a_R & 0 \\ 0 & 0 \end{pmatrix} \in D$ for each $a \in A$,

whence φ_{11} commutes with each a_R , and so $\varphi_{11} = (a_0)_L$ for some $a_0 \in A$. Thence $\varphi_{22}(n_0) = a_0n_0$, and so φ is $(a_0)_L$ on M . This completes the proof of (i).

To prove (ii), let $D = \text{Hom}_A(M, M)$, and let $V = M^{(k)}$ be the set of $1 \times k$ row vectors with entries in M . If we think of D as a domain of *right* operators on M , then M may be viewed as a bimodule ${}_A M_D$. In that case, $E = \text{Hom}_A(V, V) \cong M_k(D)$, and we may view V as a bimodule ${}_A V_E$. Now let $f \in \text{Hom}_D(M, M)$; we must prove that $f = a_L$ for some $a \in A$. Define $f^*: V \rightarrow V$ by

$$f^*(m_1, \dots, m_k) = (fm_1, \dots, fm_k), \quad m_i \in M.$$

It is easily checked that $f^* \in \text{Hom}_E(V, V)$. But (A, V) has the double centralizer property, whence $f^* = a_L$ for some $a \in A$. Then also $f = a_L$ (on M), as desired.

(7.10) COROLLARY. *Let M be any faithful finitely generated left module over a semisimple artinian ring A . Then (A, M) has the double centralizer property.*

Proof. Let B_1, \dots, B_t be the simple components of A , and let M_i be a simple left B_i -module. Then by (7.1) we may write $M = \sum_1^t M_i^{(r_i)}$. Since $B_j \cdot M_i = 0$ for $j \neq i$, and since M is a faithful A -module, it follows that each $r_i > 0$. Further, we know that $B_i \cong M_i^{(s_i)}$ as left B_i -modules, for some s_i . It follows that if $k = \max \{s_i\}$, then ${}_A A$ is a direct summand of the module $M^{(k)}$. Hence by (7.9(i)) the pair $(A, M^{(k)})$ has the double centralizer property, whence so does (A, M) by (7.9(ii)).

We are now ready to apply this corollary to the study of simple subalgebras of a central simple algebra A , and eventually to the study of maximal subfields of A . We begin with a fundamental result:

(7.11) THEOREM. *Let $K \subset B \subset A$, where B is a simple subring of the central simple K -algebra A . Let*

$$B' = \{x \in A : xb = bx \text{ for all } b \in B\},$$

the centralizer of B in A . Then B' is a simple artinian ring, and B is its centralizer in A .

Proof. Let V be a simple left A -module, and let $D = \text{Hom}_A(V, V)$, viewed as left operator domain on V . Then $A = \text{Hom}_D(V, V)$, and D is a skewfield with center K . For $a \in A$, $d \in D$, let a_L and d_L denote left multiplications on V . Then $b_L \cdot d_L = d_L \cdot b_L$ for all $b \in B$, $d \in D$, and therefore we may make V into a left $D \otimes_K B$ -module by setting

$$(d \otimes b)v = d_L b_L v, \quad v \in V.$$

By (7.6), $D \otimes_K B$ is a simple artinian algebra of finite K -dimension. Both D_L and B_L are K -subalgebras of $\text{Hom}_K(V, V)$, and the elements of D_L commute with those of B_L . Hence the map $D \otimes_K B \rightarrow D_L \cdot B_L$ is a K -algebra isomorphism (the kernel must be a two-sided ideal of $D \otimes_K B$), and so letting S denote $D_L \cdot B_L$, it follows that S is a simple algebra. Further, V is a finitely generated faithful S -module, so the pair (S, V) has the double centralizer property, by (7.10).

Let $\varphi \in \text{Hom}_S(V, V)$; then $\varphi \in \text{Hom}_{D_L}(V, V) = A_L$, so $\varphi = a_L$ for some $a \in A$ which centralizes B_L . Since both A and B act faithfully on V , this shows that $a \in B'$, and therefore

$$(B')_L = \text{Hom}_S(V, V).$$

Since $B' \cong (B')_L$, it follows from Exercise 7.2a that B' is a simple artinian ring. Further, since (S, V) has the double centralizer property, we have

$$(7.12) \quad S = D_L \cdot B_L = \text{Hom}_{(B')_L}(V, V).$$

Now let $x \in A$ centralize B' ; then x_L centralizes $(B')_L$, so $x_L \in S$ by (7.12). On the other hand, since $x_L \in A_L$, it follows that x_L centralizes D_L in S . We now make use of the isomorphism $S \cong D \otimes_K B$. The proof of (7.6) shows that the elements in $D \otimes_K B$ which centralize $D \otimes 1$ are contained in $D^c \otimes B$, that is, in B itself (since $D^c = K$). Therefore $x_L \in B_L$, whence $x \in B$, as desired.

For later use, we give two important consequences of (7.12):

(7.13) COROLLARY. Keeping the notation of (7.11), let V be a simple left A -module, and set $D = \text{Hom}_A(V, V)$. Then

$$D \otimes_K B \cong \text{Hom}_B(V, V), \quad (B:K)(B':K) = (A:K).$$

Proof. The first assertion is a restatement of (7.12). To prove the second, let W be a simple left B' -module. Since V is a left B' -module, we have $V \cong W^{(k)}$

where $k = \dim V/\dim W$, and $\underline{\dim}$ denotes \dim_K . Let $d_0 = \dim D_0$, where $D_0 = \text{Hom}_{B'}(W, W)$ is the skewfield part of B' . Let us write

$$\begin{aligned}\dim D &= d, & \dim V &= dn, & \dim A &= dn^2, \\ \dim D_0 &= d_0, & \dim W &= d_0 m, & \dim B' &= d_0 m^2,\end{aligned}$$

for some m, n . Then

$$k = \dim V/\dim W = dn/d_0 m,$$

while from the first part of the corollary,

$$d \cdot \dim B = \dim \text{Hom}_{B'}(W^{(k)}, W^{(k)}) = \dim M_k(D_0) = k^2 d_0.$$

Consequently

$$\begin{aligned}(\dim B)(\dim B') &= (k^2 d_0/d) \cdot d_0 m^2 = k^2 d_0^2 m^2/d \\ &= d^2 n^2/d = \dim A,\end{aligned}$$

which completes the proof.

(7.14) COROLLARY. *In the notation of (7.11), we have*

$$A \otimes_K B^\circ \cong M_r(B'), \quad \text{where } r = (B:K).$$

Further, $B \otimes_K B' \cong A$ if B has center K .

Proof. Keeping the terminology of the proof of (7.13), we have $A \cong M_n(D^\circ)$, so

$$A \otimes B^\circ \cong M_n(D^\circ \otimes B^\circ) \cong M_n((D \otimes B)^\circ).$$

On the other hand $D \otimes B \cong M_k(D_0)$, whence $A \otimes B^\circ \cong M_{kn}(D_0^{\text{opp}})$. Since $B' \cong M_m(D_0^{\text{opp}})$, we need only show that $\dim B = kn/m$. But this is clear, since

$$\dim B = k^2 d_0/d = k \cdot (kd_0/d) = k \cdot (n/m).$$

For the second part of the corollary, we observe that B is a central simple K -algebra, and thus $B \otimes B'$ is simple. Therefore the algebra homomorphism

$$B \otimes_K B' \rightarrow B \cdot B' \subset A$$

must be monic. Comparison of dimensions then shows that $B \otimes B' \cong A$, and the corollary is established.

Now let $A = M_n(D)$ be a central simple K -algebra, where D is a skewfield with center K . We say that an extension field E of K splits A , or is a *splitting field* for A , if

$$E \otimes_K A \cong M_r(E) \quad \text{for some } r.$$

Since

$$E \otimes_K M_n(D) \cong M_n(E \otimes_K D),$$

it follows from the uniqueness part of Wedderburn's Theorem that E splits A if and only if E splits D . We may further remark that if E splits A , then so also does every field $\Omega \supset E$, since

$$\Omega \otimes_K A \cong \Omega \otimes_E (E \otimes_K A) \cong \Omega \otimes_E M_r(E) \cong M_r(\Omega).$$

We are going to show that splitting fields always exist. Indeed, if \tilde{K} is any algebraic closure of K , then necessarily \tilde{K} splits A . To see this, observe that $\tilde{K} \otimes_K A$ is a central simple \tilde{K} -algebra, hence is of the form $M_r(D')$ for some skewfield D' over \tilde{K} . But then $D' = \tilde{K}$, since each element of D' is algebraic over \tilde{K} , and hence lies in \tilde{K} (see Exercise 31.6).

The important problem for us is to show the existence of splitting fields which are finite separable extensions of K . This fact is contained in the following basic result:

(7.15) **Theorem.** *Let D be a skewfield with center K , and let $(D:K)$ be finite.*

(i) *Every maximal subfield E of D contains K , and is a splitting field for D . Further, if $m = (E:K)$, then*

$$(D:K) = m^2, \quad E \otimes_K D \cong M_m(E).$$

(ii) *There exists a maximal subfield L of D which is separable over K .*

Proof. (i) Since $(D:K)$ is finite, D contains maximal subfields. Let E be a maximal subfield of D . Clearly $E \supset K$, otherwise $E(K)$ is a larger subfield of D . Now choose $A = D$, $V = {}_p D$, $B = E$ in (7.11). Obviously $B' \supset E$, and equality must hold, since for each $x \in B'$, $E(x)$ is a subfield of D containing E . Thus $B' = B = E$, and (7.13) becomes

$$D \otimes_K E \cong \text{Hom}_E(V, V) \cong M_r(E), \quad (E:K)^2 = (D:K),$$

where $r = (V:E)$. But

$$r^2 = (D \otimes_K E : E) = (D:K) = (E:K)^2,$$

so $r = (E:K)$, and (i) is proved.

(ii) We use induction on $(D:K)$, and let $(D:K) = n > 1$, the result being trivial when $n = 1$. It clearly suffices to handle the case where $\text{char } K = p \neq 0$.

Let us show first that D contains a separable extension E of K , with $E \neq K$. For each $x \in D - K$ we have $K < K(x)$; call x *purely inseparable* over K if $\min. \text{pol}_K x$ is of the form $X^{p^e} - a$ for some $a \in K$. If x is not purely inseparable, then

$$\min. \text{pol.}_K x = f(X^{p^e})$$

for some separable polynomial $f(X) \in K[X]$. In this case, we need only choose $E = K(x^{p^e})$. So now suppose that each $x \in D - K$ is purely inseparable over K . Then for each $x \in D$, $\min. \text{pol.}_K x$ is of the form $X^{p^e} - a$, $a \in K$, $e \geq 0$. We note that $p|n$, since n is a multiple of $(K(x):K)$ for each $x \in D - K$. Choose F to be any maximal subfield of D , so by (i) there is an isomorphism of F -algebras

$$\mu: F \otimes_K D \cong M_r(F) \quad \text{for some } r.$$

Then $[\mu(1 \otimes x)]^{p^e} = \mu(1 \otimes x^{p^e}) = a \cdot I_n$, whence all of the characteristic roots of $\mu(1 \otimes x)$ are equal, and thus (since $p|n$) $\text{Tr } \mu(1 \otimes x) = 0$. This holds for each $x \in D$. But the matrices $\{\mu(1 \otimes x): x \in D\}$ form an F -basis for $M_r(F)$. Hence every matrix in $M_r(F)$ has zero trace, which is impossible. This completes the proof that there exists a field E such that $K < E \subset D$, E separable over K .

Continuing with the proof, we let

$$D' = \{a \in D: ax = xa \text{ for all } a \in E\},$$

the *centralizer* of E in D . Then D' is a sub-skewfield of D , and we claim that E is the center of D' . By (7.11), E is the centralizer of D' in D . Any $x \in (D')^c$ centralizes D' , hence lies in E . This proves that $(D')^c \subset E$, and the reverse inclusion is obvious, because D' centralizes E .

We have thus obtained a central simple E -algebra D' , and $(D':E) < (D:K)$. By the induction hypothesis, there is a maximal subfield L of D' such that L is separable over E . Since E is separable over K , it follows (by transitivity of separability) that L is separable over K . Finally, we show that L is a maximal subfield of D . If not, then there exists an $x \in D - L$ centralizing L . Then x centralizes E , so $x \in D'$, and then $L < L(x) \subset D'$, so $L(x)$ is a subfield of D' properly containing L . This is impossible, and therefore L must be a maximal subfield of D , as desired. This completes the proof of the theorem.

To conclude this subsection, we present a basic result concerning the behavior of K -algebras under separable extensions of the ground field:

(7.16) **THEOREM.** *Let L be a finite separable field extension of K , and let A be a finite dimensional semisimple E -algebra, where E is any field containing K (possibly $(E:K)$ is infinite). Then $L \otimes_K A$ is also a finite dimensional semisimple E -algebra.*

Proof. It is clear that $L \otimes_K A$ is an E -algebra of dimension $(L:K)(A:E)$. It

suffices to prove the result when A is a central simple E -algebra. We may write $L \cong K[X]/(f(X))$, where $f(X)$ is an irreducible separable polynomial in $K[X]$. Let $f(X) = \prod f_i(X)$ be the factorization of $f(X)$ into irreducible polynomials in $E[X]$. Since $f(X)$ is separable, the $\{f_i(X)\}$ are distinct, and therefore

$$L \otimes_K E \cong E[X]/(f(X)) \cong \sum E[X]/(f_i(X)).$$

Setting $F_i = E[X]/(f_i(X))$, we see that each F_i is a field containing E . Therefore

$$L \otimes_K A \cong (L \otimes_K E) \otimes_E A \cong \sum F_i \otimes_E A.$$

But now each $F_i \otimes_E A$ is a central simple F_i -algebra by (7.8), whence $L \otimes_K A$ is a semisimple E -algebra, as claimed.

(7.17) COROLLARY. *Let A be a finite dimensional E -algebra, where $E \supset K$, and let L be a finite separable extension of K . Then*

$$\text{rad}(L \otimes_K A) = L \otimes_K \text{rad } A.$$

Proof. Let $N = \text{rad } A$. Then $L \otimes N$ is a nilpotent ideal of $L \otimes A$, hence lies in $\text{rad}(L \otimes A)$. On the other hand,

$$L \otimes (A/N) \cong (L \otimes A)/(L \otimes N),$$

and $L \otimes (A/N)$ is semisimple by (7.16). Hence $L \otimes N \supset \text{rad}(L \otimes A)$, by Exercise 6.4. Thus $L \otimes N = \text{rad}(L \otimes A)$, as claimed.

7c Separable algebras

Throughout this section, let K, E, L denote fields, D and D' skewfields, and A, B finite dimensional K -algebras. If L is a finite extension of K , the assumption that L be separable over K has many important consequences (see (4.7), (7.16) and (7.17), for example). There is a more general concept of separability for K -algebras, and in this section we shall present this definition and some of its consequences. Indeed, one can even define separability of R -algebras, where R is a commutative ring (see for instance DeMeyer-Ingramham [1] or Exercise 7.9).

The most direct definition of separability is as follows: a *separable K -algebra* is a finite dimensional semisimple K -algebra A , such that the center of each simple component of A is a separable field extension of K . Note that separability is not an intrinsic property of A , but depends on the choice of ground field. If $(K:E)$ is finite and A is K -separable, then A will be E -separable precisely when K is separable over E .

(7.18) THEOREM. Let A be a finite dimensional K -algebra. The following statements are equivalent:

- (i) A is a separable K -algebra.
- (ii) There exists a finite separable field extension E of K such that $E \otimes_K A$ is a direct sum of full matrix algebras over E .
- (iii) For every field $F \supset K$, $F \otimes_K A$ is semisimple.

Proof. Let A be a separable K -algebra with simple components B_1, \dots, B_t , and let K_i be the center of B_i , so K_i is separable over K , $1 \leq i \leq t$. For each i , by (7.15) we may choose a separable finite extension field E_i of K_i which splits B_i , say

$$E_i \otimes_{K_i} B_i \cong M_{r_i}(E_i).$$

Let us set $K_i \cong K[X]/(f_i(X))$, where $f_i(X)$ is a separable polynomial over K , and let E'_i be the splitting field of $f_i(X)$ over K . Then E'_i is a finite separable extension of K for each i . By Exercise 7.6, we can find a finite separable extension E of K which contains the fields $E_1, \dots, E_t, E'_1, \dots, E'_t$ (or, more precisely, E contains K -isomorphic copies of the $\{E_i\}$ and $\{E'_i\}$). Therefore

$$E \otimes_K K_i \cong E[X]/(f_i(X)) \cong \sum^* E,$$

where the number of summands on the right equals the degree of $f_i(X)$. We then have $E \otimes_K A = \sum^* E \otimes_K B_i$, and

$$\begin{aligned} E \otimes_K B_i &\cong (E \otimes_K K_i) \otimes_{K_i} B_i \cong \sum^* E \otimes_{K_i} B_i \\ &\cong \sum^* E \otimes_{E_i} (E_i \otimes_{K_i} B_i) \cong \sum^* E \otimes_{E_i} M_{r_i}(E_i) \cong \sum^* M_{r_i}(E). \end{aligned}$$

This shows that (i) implies (ii).

To prove that (ii) implies (iii), suppose that

$$E \otimes_K A \cong \sum^* M_{r_i}(E),$$

and let $F \supset K$. By Exercise 7.6, we may find a field L containing both E and F , and then

$$L \otimes_K A \cong L \otimes_E (E \otimes_K A) \cong \sum^* M_{r_i}(L).$$

On the other hand,

$$L \otimes_K A \cong L \otimes_F (F \otimes_K A).$$

If $F \otimes_K A$ were not semisimple, it would contain a nonzero nilpotent ideal N , and then $L \otimes_F N$ would be a nonzero nilpotent ideal in the semisimple ring $L \otimes_K A$. This is impossible, and so $F \otimes_K A$ is semisimple, as claimed.

Finally, we show that (iii) implies (i), by proving that if (i) is false, then so is (iii). If (i) is false, then either

(a) $\text{rad } A \neq 0$, or

(b) A is semisimple, but some K_i is inseparable over K , (using the notation of the first part of the proof).

In case (a), (iii) is false (just pick $F = K$!). In case (b), K_i contains an element y such that

$$\min. \text{pol}_K y = (X^p)^n + \alpha_1(X^p)^{n-1} + \cdots + \alpha_n \in K[X],$$

where $\text{char } K = p \neq 0$. Choose F to be the field $K(\alpha_1^{1/p}, \dots, \alpha_n^{1/p})$, and let

$$z = 1 \otimes y^n + \alpha_1^{1/p} \otimes y^{n-1} + \cdots + \alpha_n^{1/p} \otimes 1 \in F \otimes_K K_i.$$

Then $z \neq 0$, since $\{1, y, \dots, y^n\}$ are K -linearly independent elements of K_i . Further,

$$z^p = 1 \otimes y^{pn} + \alpha_1 \otimes y^{p(n-1)} + \cdots + \alpha_n \otimes 1 = 0.$$

Thus $F \otimes_K K_i$ contains a nonzero nilpotent element z . Since

$$F \otimes_K B_i \cong (F \otimes_K K_i) \otimes_{K_i} B_i,$$

it follows that $z \otimes 1$ is a nonzero nilpotent element in the center of $F \otimes_K B_i$, and thus generates a nonzero nilpotent ideal in $F \otimes_K B_i$. Therefore neither $F \otimes_K B_i$ nor $F \otimes_K A$ can be semisimple. This completes the proof of the theorem.

(7.19) COROLLARY. If A and B are separable K -algebras, so is $A \otimes_K B$.

Proof. Choose fields F, F' containing K such that

$$F \otimes_K A \cong M_r(F), \quad F' \otimes_K B \cong M_s(F'),$$

and then choose a field E containing both F and F' (Exercise 7.6). Then

$$E \otimes_K A \cong M_r(E), \quad E \otimes_K B \cong M_s(E),$$

and so by (7.7)

$$E \otimes_K (A \otimes_K B) \cong (E \otimes_K A) \otimes_E (E \otimes_K B) \cong M_{rs}(E).$$

Thus $A \otimes_K B$ is separable over K , as claimed.

Let A° denote the *opposite ring* of A , that is, $A^\circ = \{x^\circ : x \in A\}$, with

$$x^\circ + y^\circ = (x + y)^\circ, \quad x^\circ \cdot y^\circ = (yx)^\circ, \quad x, y \in A.$$

Then A and A° have the same center. We set

$$A^e = A \otimes_K A^\circ,$$

a finite dimensional K -algebra called the *enveloping algebra* of A . We may

view A as a left A^e -module, by means of the formula

$$(x \otimes y^o)a = xay, \quad x, a \in A, \quad y^o \in A^o.$$

(Indeed, every two-sided A - A -bimodule can be viewed as a left A^e -module.) There is a left A^e -epimorphism

$$\mu: A^e \rightarrow A,$$

defined by setting $\mu(x \otimes y^o) = xy$. Clearly A is a projective left A^e -module if and only if there exists a map $v \in \text{Hom}_{A^o}(A, A^e)$ such that $\mu \cdot v = 1$. It is obvious that such a map v exists if and only if for each K -basis $\{x_1, \dots, x_n\}$ of A , there exist elements $\{y_i\}$ of A such that

- (i) $\sum x_i y_i = 1$, and
- (ii) For each $a \in A$, if $ax_i = \sum \alpha_{ij} x_j$, $1 \leq i \leq n$, with the $\{\alpha_{ij}\} \in K$, then $y_i a = \sum \alpha_{ji} y_j$, $1 \leq i \leq n$.

Indeed, once v is given, we set $v(1) = \sum_{i=1}^n x_i \otimes y_i^o$; condition (i) asserts that $\mu \cdot v = 1$, while (ii) asserts that v is an A^e -homomorphism. Conversely, given a K -basis $\{x_i\}$ of A , and given elements $\{y_i\} \in A$ satisfying (i) and (ii), we need only set $v(a) = a \cdot \sum x_i \otimes y_i^o$, $a \in A$.

(7.20) **THEOREM.** *Let A be a finite dimensional K -algebra. Then A is a separable K -algebra if and only if A is A^e -projective.*

Proof. If A is K -separable, so is A^o , and thus A^e is K -separable by (7.19). In particular, then, A^e is semisimple, and so *every* A^e -module is projective. Conversely, suppose that A is A^e -projective. We shall prove that A is K -separable by showing that $B = F \otimes_K A$ is semisimple for each field $F \supset K$. We have

$$\begin{aligned} B^e &= B \otimes_F B^o = (F \otimes_K A) \otimes_F (F \otimes A^o) \\ &\cong F \otimes_K (A \otimes_K A^o) = F \otimes_K A^e. \end{aligned}$$

Let $\mu' = 1 \otimes \mu: F \otimes_K A^e \rightarrow F \otimes_K A$, and likewise let $v' = 1 \otimes v$. Then v' is a B^e -homomorphism such that $\mu' \cdot v' = 1$; let us set

$$v'(1) = \sum x_i \otimes y_i^o, \quad x_i, y_i \in B,$$

so $\sum x_i y_i = 1$.

In order to prove that B is semisimple, we show that if $N \subset M$ are left B -modules, then N is a direct summand of M . We may view $\text{Hom}_K(M, M)$ as a B - B -bimodule, hence as a left B^e -module, with

$$(x \otimes y^o)f = xfy, \quad x, y \in B, \quad f \in \text{Hom}_K(M, M).$$

Let $\pi: M \rightarrow N$ be a K -projection of M onto N , so $\pi^2 = \pi$. We set

$$\pi' = v'(1) \cdot \pi = \sum x_i \pi y_i.$$

Since $\pi = 1$ on N , for each $n \in N$ we have

$$\pi'(n) = \sum x_i \pi(y_i n) = \sum x_i y_i n = n,$$

whence $(\pi')^2 = \pi'$. Finally, for $b \in B$ we have

$$\begin{aligned} b\pi' &= (b \otimes 1) \cdot v'(1)\pi = v'((b \otimes 1) \cdot 1)\pi \\ &= v'((1 \otimes b^\circ) \cdot 1)\pi = (1 \otimes b^\circ)\pi' = \pi'b. \end{aligned}$$

Thus π' is a B -homomorphism, whence N is a B -direct summand of M as claimed, and the theorem is proved.

7d Skolem–Noether Theorem

Throughout this subsection, A denotes a central simple K -algebra. Each invertible element $a \in A$ determines an inner automorphism of A , given by $x \mapsto axa^{-1}$, $x \in A$, and this automorphism fixes each element of K . The Skolem–Noether Theorem, to be proved below, asserts the converse: every algebra automorphism of A fixing each element of K must be an inner automorphism. We shall prove a slightly more general version of this result, namely:

(7.21) **Theorem.** (Skolem–Noether). *Let $K \subset B \subset A$, where B is a simple subring of the central simple K -algebra A . Then every K -isomorphism φ of B onto a subalgebra \tilde{B} of A extends to an inner automorphism of A , that is, there exists an invertible $a \in A$ such that*

$$\varphi(b) = aba^{-1}, \quad b \in B.$$

Proof. Let \otimes stand for \otimes_K throughout this proof, and let us use the notation introduced in the first paragraph of the proof of (7.11). We have seen there that a simple left A -module V is a left $D \otimes B$ -module, under the action

$$(d \otimes b)v = d \cdot b \cdot v, \quad v \in V.$$

In the same way, we may view V as left $D \otimes \tilde{B}$ module.

We now make use of the structure of V as left $D \otimes \tilde{B}$ -module, together with the K -algebra isomorphism

$$1 \otimes \varphi: D \otimes B \cong D \otimes \tilde{B},$$

to define an action (denoted by $*$) of $D \otimes B$ on V . We then obtain a left $D \otimes B$ -module \tilde{V} , having the same elements as V , but with the action of

$D \otimes B$ on \tilde{V} given by

$$(d \otimes b) * v = d \cdot \varphi(b) \cdot v, \quad v \in V.$$

Then V and \tilde{V} are a pair of left modules over the simple artinian ring $D \otimes B$, and have the same K -dimension. It follows at once that there is a left $D \otimes B$ -isomorphism $\theta: V \cong \tilde{V}$. In other words, there is an isomorphism $\theta \in \text{Hom}_K(V, V)$ such that

$$(7.22) \quad \theta(d \cdot b \cdot v) = (d \otimes b) * \theta(v) = d \cdot \varphi(b) \cdot \theta(v), \quad v \in V.$$

Taking $b = 1$, it follows that $\theta \in \text{Hom}_D(V, V) = A$, so θ is given by a left multiplication by an element $a \in A$. Since θ is an isomorphism, a is invertible. Formula (7.22) becomes

$$a \cdot (d \cdot b \cdot v) = d \cdot \varphi(b) \cdot av, \quad v \in V.$$

If we put $d = 1$, and remember that A acts faithfully on V , we may conclude that

$$a \cdot b = \varphi(b) \cdot a, \quad b \in B,$$

which proves the theorem.

(7.23) COROLLARY. (i) Every K -automorphism of A is inner.

(ii) Any two K -isomorphic subfields L and L' of A are conjugate, that is, $L' = aLa^{-1}$ for some invertible $a \in A$.

(7.24) Theorem. (Wedderburn). Every finite skewfield is a field.

Proof. Let D be a finite skewfield with center K , and let $D^* = D - \{0\}$, $K^* = K - \{0\}$. If L is a maximal subfield of D , then $(D:K) = n^2$, $(L:K) = n$. Any other maximal subfield L' is a finite field, and $(L':K) = n$, so $\text{card } L = \text{card } L'$. Thus L' is K -isomorphic to L , whence by (7.23) L' is conjugate to L . Since every $x \in D$ lies in a subfield $K(x)$ of D , and hence in some maximal subfield, we conclude that

$$(7.25) \quad D^* = \bigcup aL^*a^{-1},$$

where a ranges over some set of invertible elements of D . But for $x \in L^*$,

$$(ax)L^*(ax)^{-1} = aL^*a^{-1},$$

so in (7.25) it suffices to let a range over the left coset representatives of L^* in D^* . Hence there are $(D^*:L^*)$ sets $\{aL^*a^{-1}\}$ occurring in (7.25), each of cardinality $\text{card } L^*$; these sets are *not* disjoint, since each contains 1. Thus D^* cannot be their union, unless there is only one such set, that is, $D^* = L^*$. Thus $D = L = K$, as desired.

EXERCISES

1. Prove Schur's Lemma: if M is a simple left A -module, then $\text{Hom}_A(M, M)$ is a skewfield. [Hint: For each nonzero $f \in \text{Hom}_A(M, M)$, both $\ker f$ and $\text{im } f$ are submodules of M , and so $\ker f = 0, \text{im } f = M$.]

2. Let $V^{(k)}$ be the direct sum of k copies of the left A -module V , and let $E = \text{Hom}_A(V, V)$. Prove that

$$\text{Hom}_A(V^{(k)}, V^{(k)}) \cong M_k(E).$$

2a. Let M be a finitely generated left A -module, where A is a simple artinian ring. Show that $\text{Hom}_A(M, M)$ is also a simple artinian ring. [Hint: Write $M \cong V^{(k)}$, where V is a simple left A -module. Then use the preceding exercises and (7.3).]

2b. Prove that the result in Exercise 2a remains valid when "simple" is replaced by "semisimple".

3. Let A be a ring direct sum $\sum_{i=1}^t B_i$, where each B_i is a ring having no two-sided ideals except 0 and B_i . Show that every two-sided ideal J of A is a subsum $\sum B_{i_v}$. [Hint: $J \cdot B_i = 0$ or B_i for each i , and $J = \sum JB_i$.]

4. Let L be a minimal left ideal of the simple left artinian ring A , and let $D = \text{Hom}_A(L, L)$. Show that $A = \text{Hom}_D(L, L)$. Using Exercises 1 and 2, prove that D is a skewfield, and that $A \cong M_n(D^\circ)$, where n is the dimension of L as left D -space. [Hint: This is the harder part of the Wedderburn Structure Theorem (7.4). The following quick proof is due to Milnor [1]. Since $L \cdot A$ is a two-sided ideal of A , we have $L \cdot A = A$. Let

$$1 = \sum_{i=1}^m l_i a_i, \quad l_i \in L, \quad a_i \in A,$$

with m minimal. There is a left A -epimorphism $L^{(m)} \rightarrow A$, given by $(x_1, \dots, x_m) \mapsto \sum_1^m x_i a_i$. The map is monic, since if $\sum x_i a_i = 0$ with (say) $x_1 \neq 0$, then $Ax_1 = L$ implies that

$$La_1 = Ax_1 a_1 \subset La_2 + \cdots + La_m,$$

contradicting the minimality of m . Thus $A \cong L^{(m)}$ as left A -modules, whence

$$A^\circ \cong \text{Hom}_A(A, A) \cong \text{Hom}_A(L^{(m)}, L^{(m)}) \cong M_m(D),$$

so $A \cong M_m(D^\circ)$. Note that $m = n$.]

5. Let A be a semisimple finite dimensional K -algebra, and let E be a separable algebraic extension field of K , that is, for each field L with $K \subset L \subset E$, $(L:K)$ finite, the extension L/K is separable. Prove that $E \otimes_K A$ is semisimple. [Hint: Let $N = \text{rad}(E \otimes_K A)$. For each L , $N \cap (L \otimes_K A)$ is a nilpotent ideal of $L \otimes_K A$, hence is zero. But each $x \in N$ lies in some $L \otimes_K A$.]

6. Let L_1, \dots, L_n be a set of field extensions of K . Show that there exists a field Ω containing K , for which there exist K -isomorphisms $\mu_i: L_i \rightarrow \Omega$, $1 \leq i \leq n$. Further, if each $(L_i:K)$ is finite, the field Ω may be chosen so that $(\Omega:K)$ is finite. If in addition

each L_i is separable over K , then Ω may be chosen finite separable over K . [Hint: Let $A = L_1 \otimes_K \cdots \otimes_K L_n$, a commutative K -algebra. By Zorn's Lemma, A has a maximal ideal M . Set $\Omega = A/M$, a field containing K , and define μ_i by composition of maps: $L_i \rightarrow A \rightarrow \Omega$. If each $(L_i : K)$ is finite, so is $(\Omega : K)$. If each L_i is finite separable over K , then by (7.19) A is a direct sum of fields Ω_i , each of which is a finite separable extension of K , and we may pick Ω to be any Ω_j .]

7. Let A be a separable K -algebra, B any semisimple finite dimensional K -algebra. Prove that $A \otimes_K B$ is semisimple. [Hint: We may assume that both A and B are simple, and set $L = A^\circ$, $E = B^\circ$. As in the proof of (7.16), we have $L \otimes_K E \cong \sum F_i$, since L is separable over K , where each F_i is a field containing K -isomorphic copies of L and E . Hence

$$A \otimes_K B \cong A \otimes_L (L \otimes_K E) \otimes_E B \cong \sum (A \otimes_L F_i) \otimes_E B.$$

But $A \otimes_L F_i$ is a central simple F_i -algebra, and B is a central simple E -algebra, so each summand $(A \otimes_L F_i) \otimes_E B$ is simple by (7.6).]

8. Let $G = \{g_1, \dots, g_n\}$ be a finite group of order n , and let K be a field. Show that the group algebra KG is a separable K -algebra if and only if $\text{char } K \nmid n$. [Hint: If $\text{char } K | n$, then $\sum g_i$ is a nilpotent element in the center of KG , so KG is not semisimple. If $\text{char } K \nmid n$, set $A = KG$, and define $v: A \rightarrow A \otimes_K A^\circ = A^\circ$ by

$$v(1) = n^{-1} \sum_i g_i \otimes g_i^{-1},$$

$v(a) = a \cdot v(1)$, $a \in A$. Show that v is an A° -homomorphism such that $uv = 1$, where $u: A^\circ \rightarrow A$ is as in § 7c.]

9. Let Λ be an R -algebra, where R is a commutative ring. Call Λ *R-separable* if Λ is Λ° -projective, where $\Lambda^\circ = \Lambda \otimes_R \Lambda^\circ$. Show that if Λ is R -separable, then every R -projective Λ -module is Λ -projective. [Hint: Imitate the proof of (7.20)].

10. Let R be a commutative ring, G a group of order n . Show that RG is R -separable if n is a unit in R .

11. Let e, e' be idempotents in the simple artinian ring A , such that $Ae \cong Ae'$ as left A -modules. Show that there exists a unit $u \in A$ such that $e' = ueu^{-1}$. [Hint: Let $A = \text{Hom}_D(V, V)$, where V is a right vector space over the skewfield D . Since $V = eV \oplus (1 - e)V$ is a D -decomposition of V , then relative to a suitable D -basis of V , e is represented by a diagonal matrix $\text{diag}(1, \dots, 1, 0, \dots, 0)$. The same holds for e' , with the same number of 1's, since $Ae \cong Ae'$. If $u \in A$ gives a suitable change of D -bases of V , then $e' = ueu^{-1}$.]

12. If e is a primitive idempotent of the simple artinian ring A , show that Ae is a minimal left ideal of A , and $A(1 - e)$ a maximal left ideal. Further, let Ax be a maximal left ideal of A . Show that xA is a maximal right ideal. Prove that if Ax and Ay are any pair of maximal left ideals in A , then $u \cdot Ax \cdot u^{-1} = Ay$ for some unit $u \in A$. [Hint: Let Ax be maximal, and write $A = Ae \oplus Ax$ with e a primitive idempotent. Set $1 = e + ax$, $a \in A$. Then $A = eA \oplus axA$, so axA is a maximal left ideal. But axA is a homomorphic image of xA , and $xA \neq A$, whence xA is also a maximal right ideal. Further, if e and e' are primitive idempotents of A , then $e' = ueu^{-1}$ for some unit

$u \in A$, by Exercise 11. But every maximal left ideal of A is of the form $A(1 - e)$ for some primitive idempotent e .]

13. Let A be a separable K -algebra, L any extension field of K . Show that $L \otimes_K A$ is a separable L -algebra. [Hint: For any field $F \supset L$, we have

$$F \otimes_L (L \otimes_K A) \cong F \otimes_K A,$$

and the latter is semisimple by (7.18).]

14. Let the separable K -algebra A have simple components $\{A_i\}$, and let K_i be the center of A_i . Let F be a field containing K , where possibly $(F:K)$ is infinite. Prove that there is an F -algebra isomorphism

$$F \otimes_K A \cong \sum_i \sum_j F_{ij} \otimes_{K_i} A_i,$$

where each F_{ij} is a field containing K -isomorphic copies of K_i and F , and where $(F_{ij}:F)$ is finite. Show that each summand $F_{ij} \otimes_{K_i} A_i$ is a central simple F_{ij} -algebra. [Hint: We have

$$F \otimes_K A \cong \sum_i (F \otimes_K K_i) \otimes_{K_i} A_i.$$

Since K_i/K is finite separable, the F -algebra $F \otimes_K K_i$ is semisimple by (7.16), hence is expressible as a direct sum of fields F_{ij} . Each F_{ij} contains K -isomorphic copies of $F \otimes 1$ and $1 \otimes K_i$.]

2. Orders

Throughout this chapter let R denote a noetherian integral domain with quotient field K , and let A be a finite dimensional K -algebra. Our aim here is to define orders, and to develop some of their basic properties. In later chapters we shall concentrate on maximal orders. Usually R will be a Dedekind domain, or at the very least, an integrally closed domain (see (1.12)), but occasionally theorems will be stated for the general situation in which R is only assumed to be noetherian.

8. DEFINITIONS AND EXAMPLES

For any finite dimensional K -space V , a *full R -lattice* in V is a finitely generated R -submodule M in V such that $K \cdot M = V$, where

$$K \cdot M = \{ \sum \alpha_i m_i \text{ (finite sum)} : \alpha_i \in K, m_i \in M \}.$$

An *R -order* in the K -algebra A is a subring Λ of A , having the same unity element as A , and such that Λ is a full R -lattice in A . Note that Λ is both left and right noetherian, since Λ is finitely generated over the noetherian domain R .

Let us give some examples of orders:

(i) If $A = M_n(K)$, the algebra of all $n \times n$ matrices over K , then $\Lambda = M_n(R)$ is an R -order in A .

(ii) Let R be a Dedekind domain, and let L be a finite separable extension of K . Denote by S the integral closure of R in L . Then S is an R -order in L (see (4.7)). In particular, taking $R = \mathbf{Z}$, we see that alg. int. $\{L\}$ is a \mathbf{Z} -order in L .

(iii) Let $a \in A$ be integral over R , that is, a is a zero of a monic polynomial over R . Then the ring $R[a]$ is an R -order in the K -algebra $K[a]$.

(iv) Let G be a finite group, and let $A = KG$ be its *group algebra* over K , that is, KG consists of all formal sums $\sum_{x \in G} \alpha_x \cdot x$, $\alpha_x \in K$, with

$$(\sum \alpha_x \cdot x) + (\sum \beta_x \cdot x) = \sum (\alpha_x + \beta_x) \cdot x,$$

$$(\sum \alpha_x \cdot x)(\sum \beta_y \cdot y) = \sum_{x, y} \alpha_x \beta_y \cdot (xy).$$

Then $RG = \{ \sum_{x \in G} \alpha_x x : \alpha_x \in R \}$ is an R -order in A .

From example (ii) it is evident that the study of orders includes as a special case the classical subject of algebraic number theory. On the other hand, in dealing with representations of a finite group G by means of matrices with entries in a domain R , one of the first steps is to pass from matrix theory to the study of RG -modules (see Curtis-Reiner [1]), so as to be able to take advantage of the ring structure of RG . Thus the study of orders also includes the theory of integral representations of finite groups.

Let us show at once that every K -algebra A contains R -orders. Let M be any full R -lattice in A ; such M 's exist, and indeed if $A = \sum' Kx_i$, then $\sum Rx_i$ is a full R -lattice in A . We define the *left order* of M as

$$(8.1) \quad O_l(M) = \{x \in A : xM \subset M\}.$$

Clearly $O_l(M)$ is a subring of A , and is an R -module. Let us verify that $O_l(M)$ is a full R -lattice in A . For each $y \in A$, yM is an R -lattice in A , and so by §4 there exists a nonzero $r \in R$ such that $r \cdot yM \subset M$. Thus $ry \in O_l(M)$, which proves that $K \cdot O_l(M) = A$. Next, there exists a nonzero $s \in R$ such that $s \cdot 1_R \in M$. Therefore $O_l(M) \cdot (s \cdot 1_R) \subset M$, whence $O_l(M) \subset s^{-1}M$. Since R is noetherian and $s^{-1}M$ is an R -lattice, the above implies that $O_l(M)$ is also an R -lattice. This completes the proof that $O_l(M)$ is an R -order in A . Likewise, the *right order*

$$(8.2) \quad O_r(M) = \{x \in A : Mx \subset M\}$$

is an R -order in A .

For a full R -lattice M in A , and an R -order Γ in A such that $\Gamma \cdot M \subset M$, let us compute $\text{Hom}_\Gamma(M, M)$. Each $\varphi \in \text{Hom}_\Gamma(M, M)$ extends uniquely to an element of $\text{Hom}_A(KM, KM)$, hence is given by a right multiplication by an element of $O_r(M)$. Thus we have an identification

$$(8.3) \quad O_r(M) = \text{Hom}_\Gamma(M, M),$$

where M is a left Γ -module. Note that $\text{Hom}_\Gamma(M, M)$ does not depend on the choice of the R -order Γ in A .

Now let R' be an integral domain containing R , with quotient field K' . Then $R' \otimes_R M$ is a full R' -lattice in the K' -algebra $K' \otimes_K A$. Since M is finitely generated over the noetherian ring Γ , we have by (2.39)

$$R' \otimes_R \text{Hom}_\Gamma(M, M) \cong \text{Hom}_{R' \otimes_R \Gamma}(R' \otimes_R M, R' \otimes_R M),$$

provided that R' is R -flat. It then follows from (8.3) that there is a ring isomorphism

$$(8.4) \quad R' \otimes_R O_r(M) \cong O_r(R' \otimes_R M).$$

This holds in particular if R' is any ring of quotients of R . Hence

$$(8.5) \quad O_{r'}(M_p) = \{O_r(M)\}_P$$

for each prime ideal P of R . Here, the subscript P indicates localization at P (see § 3d).

The following result is fundamental:

(8.6) **THEOREM.** *Every element of an R -order Λ is integral over R . Furthermore, if R is integrally closed, then for each $a \in \Lambda$ we have*

$$\min. \text{pol.}_K a \in R[X], \quad \text{char. pol.}_{A/K} a \in R[X].$$

Proof. For each $a \in \Lambda$, it follows from the inclusion $R[a] \subset \Lambda$ that $R[a]$ is a finitely generated R -module, so a is integral over R by (1.10). If we assume in addition that R is integrally closed, the remaining assertions are consequences of (1.14) and Exercise 1.1.

A maximal R -order in A is an R -order which is not properly contained in any other R -order in A . If the integral closure R^{cl} of R in A happens to be an R -order in A , then by (8.6) R^{cl} is automatically the unique maximal R -order in A . However, most of the time R^{cl} is not a ring; furthermore, even in the case where A is commutative, so that R^{cl} is a ring by (1.11), it may happen that R^{cl} is not an R -lattice. Thus, in example (ii) of maximal orders given above, if we drop the hypothesis of separability of L over K , then S need not be finitely generated as R -module (see Artin [1]); in this case, there are no maximal R -orders in L .

By way of reassurance, as well as for later use, we now prove

(8.7) **THEOREM.** *If Λ is a maximal R -order in A , then for each n , $M_n(\Lambda)$ is a maximal R -order in $M_n(A)$. If R is integrally closed, then $M_n(R)$ is a maximal R -order in $M_n(K)$.*

Proof. Let $B = M_n(A)$, $\Gamma = M_n(\Lambda)$, where Λ is a maximal R -order in A . Clearly Γ is an R -order in B . Let $\Gamma \subset \Gamma'$, where Γ' is an R -order in B , and let Λ' be the set of all those elements of A which occur as some entry of some matrix in Γ' . Obviously $\Lambda \subset \Lambda' \subset A$, and we shall show that Λ' is an R -order in A . Let $\lambda \in \Lambda'$ occur in the (r, s) -position of a matrix $X \in \Gamma'$. We can find permutation matrices $P_1, P_2 \in \Gamma$ such that λ occurs in the $(1, 1)$ -position of $P_1 X P_2 \in \Gamma'$. Let $E_\lambda = \text{diag}(\lambda, 0, \dots, 0) \in M_n(\Lambda)$. Then

$$E_\lambda = E_1 P_1 X P_2 E_1 \in \Gamma' \quad \text{for all } \lambda \in \Lambda'.$$

Since

$$E_\lambda + E_\mu = E_{\lambda+\mu}, \quad E_\lambda E_\mu = E_{\lambda\mu}, \quad rE_\lambda = E_{r\lambda}, \quad \lambda, \mu \in \Lambda', \quad r \in R,$$

it follows that Λ' is a ring containing R . Further, the map $\lambda \rightarrow E_\lambda$, $\lambda \in \Lambda'$, embeds Λ' in the R -lattice Γ' , and hence Λ' is also an R -lattice.

The above shows that Λ' is an R -order in A . Therefore $\Lambda' = \Lambda$, since Λ is maximal. Hence every entry of every matrix in Γ' lies in Λ , whence $\Gamma' \subset \Gamma$. This shows that $\Gamma = \Gamma'$, and proves that Γ is a maximal order. If R is integrally closed, then R is a maximal R -order in K , so the second assertion in the theorem is the special case of the first assertion, in which $A = K$, $\Lambda = R$.

We shall see in §§17–18 that under suitable hypotheses on R and A , the converse of (8.7) is true: *every* maximal R -order in $M_n(A)$ is of the form $M_n(\Lambda)$ for some maximal R -order Λ in A .

To conclude this section, let us consider the situation where an integral domain R is contained in a larger integral domain R' having the same quotient field as R . For convenience, we treat only the case where R is a Dedekind domain. We shall show that every R' -order Λ' comes from an R -order Λ by extension of the ground ring from R to R' , and that likewise every Λ' -lattice comes from some Λ -lattice.

(8.8) **THEOREM.** *Let R be a Dedekind ring with quotient field K , and let R' be an integral domain such that $R \subset R' \subset K$. Then*

- (i) *Every R' -lattice M' contains an R -lattice M such that $M' = R'M$.*
- (ii) *Every R' -order Λ' (in a finite dimensional K -algebra A) contains an R -order Λ in A , such that $\Lambda' = R'\Lambda$.*
- (iii) *Let $\Lambda' = R'\Lambda$, as in (ii). Then every left Λ' -lattice M' contains a left Λ -lattice M such that $M' = \Lambda'M = R'M$.*

Proof. It is clear that K is the quotient field of R' . The domain R' is also a Dedekind domain (see references listed in §4), though we shall not require this fact here. To prove (i), we note that any R' -lattice M' can be written as a sum

$$M' = \sum_{i=1}^s R'm_i, \quad m_i \in M'.$$

Set $M = \sum Rm_i$; then M is an R -lattice in M' such that $R'M = M'$, as desired.

As usual, we identify an R -lattice M with its image $1 \otimes M$ in $K \otimes_R M$, and denote the latter by KM . We may then compute the R' -module $R'M$ in KM . Let us show that

$$(8.9) \quad R' \otimes_R M \cong R'M \subset KM.$$

Indeed, the above R' -isomorphism holds when $M = R$, and hence by (2.17) it also holds true for every projective R -module. Since R is a Dedekind domain, by (4.13) every R -lattice is R -projective. This proves (8.9), and we may hereafter identify $R' \otimes_R M$ with $R'M$, by means of the map $\alpha \otimes m \mapsto \alpha m$, $\alpha \in R'$, $m \in M$.

In order to apply the “Change of Rings” Theorem (2.37), we shall need to know that R' is R -flat. If X is any finitely generated R -submodule of R' , then X is an R -lattice. Therefore X is R -projective, and hence X is R -flat by (2.16). This shows that every finitely generated R -submodule of R' is R -flat, whence also R' is R -flat by (2.19).

Now let Λ' be an R' -order in A . By (i), we may choose an R -lattice L in Λ' such that $\Lambda' = R'L$. We set

$$\Lambda = O_r(L) = \{x \in A : Lx \subset L\}, \quad \Gamma = O_\ell(L).$$

Then Λ and Γ are R -orders in A , and there is an identification $\Lambda = \text{Hom}_\Gamma(L, L)$, where L is viewed as left Γ -module. By (2.37) we obtain

$$R'\Lambda = R' \otimes_R \Lambda = \text{Hom}_{R'/\Gamma}(R'L, R'L) = \text{Hom}_{R'/\Gamma}(\Lambda', \Lambda') = O_r(\Lambda') = \Lambda'.$$

Therefore $R'\Lambda = \Lambda'$, and (ii) is proved.

Finally, any left Λ' -lattice M' may be written as

$$M' = \sum_{i=1}^s \Lambda' m_i, \quad m_i \in M.$$

Then $M = \sum \Lambda m_i$ is a left Λ -lattice in M' such that $M' = \Lambda' M$. Furthermore, $R'M = R'(\Lambda M) = \Lambda' M$. This completes the proof of the theorem.

EXERCISE

- Let R be a noetherian integrally closed domain with quotient field K , and let A be a finite dimensional K -algebra. Let Γ be a subring of A containing R , and suppose that Γ is a finitely generated R -module. Show that Γ is contained in an R -order in A . [Hint: if M is any full R -lattice in A , then so is $M \cdot \Gamma$, and $\Gamma \subset O_r(M \cdot \Gamma)$.]

9. REDUCED NORMS AND TRACES

9a Central simple algebras

Throughout this subsection, let A denote a central simple K -algebra, that is, a simple K -algebra with center K , such that $(A:K)$ is finite. We have seen in § 1a how to assign to each $a \in K$ a characteristic polynomial, norm and trace, as follows: let $a_L \in \text{Hom}_K(A, A)$ be left multiplication by a on A , and set

$$\begin{aligned} \text{char. pol.}_{A/K} a &= \text{char. pol. of } a_L \\ &= X^m - (T_{A/K} a) X^{m-1} + \cdots + (-1)^m N_{A/K} a, \end{aligned}$$

where $m = (A:K)$. Here $T = T_{A/K}$ is the *trace* map, and $N = N_{A/K}$ the *norm* map. For any $X, Y \in M_m(K)$ we know that $\text{trace}(XY) = \text{trace}(YX)$. Therefore

$$(9.1) \quad \begin{cases} T(ab) = T(ba), T(a + b) = T(a) + T(b), T(ra) = rT(a), \\ N(ab) = N(a)N(b), N(ra) = r^m N(a), \end{cases}$$

for $a, b \in A, r \in K$.

The above definitions make no use of the assumption that A is a central simple algebra. For central simple algebras, it is possible to introduce more useful concepts, namely those of reduced characteristic polynomial, reduced norm and reduced trace. We proceed to show how this may be done.

Since A is a simple algebra with center K , there exists by § 7b an extension field E of K which splits A . This means that there is an isomorphism of E -algebras

$$(9.2) \quad h: E \otimes_K A \cong M_n(E), \quad \text{where } (A:K) = n^2.$$

If g is another such isomorphism, then $h \cdot g^{-1}$ is an E -automorphism of $M_n(E)$. Each such automorphism is inner, by (7.23), and so there exists an invertible $t \in M_n(E)$ such that

$$h(u) = t \cdot g(u) \cdot t^{-1}, \quad u \in E \otimes_K A.$$

Consequently the matrices $g(u)$ and $h(u)$ have the same characteristic polynomial. This shows that char. pol. $h(u)$ does not depend on the choice of the E -isomorphism h in (9.2).

For $a \in A$, define its *reduced characteristic polynomial* as

$$\text{red. char. pol.}_{A/K} a = \text{char. pol. } h(1 \otimes a).$$

We shall omit the subscript A/K when there is no danger of confusion.

(9.3) **THEOREM.** *For each $a \in A$, red. char. pol. $_{A/K} a$ lies in $K[X]$, and is independent of the choice of the splitting field E of A used to define red. char. pol.*

Proof. Let us show first that if $F \supset K$ is another splitting field for A , then red. char. pol. obtained using F is the same as that obtained by using E . By Exercise 7.6, there exists K -embeddings $E \rightarrow \Omega, F \rightarrow \Omega$, where Ω is some field containing K . It suffices to prove that red. char. pol. via E is the same as red. char. pol. via Ω . We have an Ω -algebra isomorphism

$$! \otimes h: \Omega \otimes_E (E \otimes_K A) \cong \Omega \otimes_E M_n(E).$$

After canonical identifications, we may rewrite the above Ω -isomorphism as (say)

$$h': \Omega \otimes_K A \cong M_n(\Omega),$$

so Ω is also a splitting field for A . Any element $u \in E \otimes_K A$ may also be viewed as element of $\Omega \otimes_K A$. When this is done, $h'(u)$ is precisely the matrix $h(u)$

viewed as element of $M_n(\Omega)$. Consequently

$$\text{char. pol. } h(u) = \text{char. pol. } h'(u), \quad u \in E \otimes_K A.$$

This holds in particular when $u = 1 \otimes a$, $a \in A$, and so red. char. pol. ${}_{A/K} a$ is the same when computed via E as via Ω . This completes the proof that red. char. pol. does not depend on the choice of splitting field.

In order to prove that red. char. pol. $a \in K[X]$ for $a \in A$, we observe that by (7.15) we may find a finite separable extension E of K which splits A . Since any extension field of E also splits A , we may in fact take E to be a finite Galois extension of K . Let G be the Galois group of E over K ; then each $\sigma \in G$ is a K -automorphism of E , and K is the subfield of E fixed by G . To clarify the following argument, we start with any K -isomorphism $f: E \cong E'$ of fields containing K , and later on we will choose $E' = E$, and $f = \sigma \in G$.

Consider the diagram

$$\begin{array}{ccc} E \otimes_K A & \xrightarrow{f \otimes 1} & E' \otimes_K A \\ h \downarrow & & \downarrow h' \\ M_n(E) & \xrightarrow{f^*} & M_n(E'). \end{array}$$

Here, h is the E -isomorphism in (9.2), and f^* takes a matrix in $M_n(E)$ onto a matrix in $M_n(E')$ by applying f to each of its entries. The map h' is then defined by requiring the diagram to be commutative. Then h' is an isomorphism of E' -algebras, since h is an E -isomorphism. Hence for $a \in A$,

$$f^*\{h(1 \otimes a)\} = \{h'(f \otimes 1)\}(1 \otimes a) = h'(1 \otimes a).$$

Therefore

$$\begin{aligned} \text{red. char. pol. } a \text{ (via } E') &= \text{char. pol. } h'(1 \otimes a) \\ &= \text{char. pol. } f^*\{h(1 \otimes a)\} \\ &= f\{\text{char. pol. } h(1 \otimes a)\} \\ &= f\{\text{red. char. pol. } a \text{ (via } E)\}, \end{aligned}$$

where f is applied to a polynomial in $E[X]$ by acting on each of its coefficients.

Now let $E' = E$, and let f range over all elements of G . Then the above shows that for $a \in A$, each coefficient in red. char. pol. a is fixed by f . Therefore each coefficient lies in K , and so red. char. pol. $a \in K[X]$, as claimed. This completes the proof.

(9.4) *Example.* Let $A = \mathbf{Q} \oplus \mathbf{Q}i \oplus \mathbf{Q}j \oplus \mathbf{Q}k$ be the skewfield of quaternions over \mathbf{Q} , where

$$i^2 = j^2 = -1, \quad k = ij = -ji.$$

Clearly A has center \mathbf{Q} , and $E = \mathbf{Q}(i)$ is a maximal subfield of A , hence is a splitting field for A . Each $a \in A$ is uniquely expressible as

$$a = \alpha + \beta j, \quad \alpha, \beta \in E.$$

There is an E -isomorphism

$$h: E \otimes_{\mathbf{Q}} A \cong M_2(E),$$

given by

$$1 \otimes \alpha \rightarrow \begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix}, \quad 1 \otimes \beta j \rightarrow \begin{pmatrix} 0 & \beta \\ -\bar{\beta} & 0 \end{pmatrix},$$

where bars denote complex conjugation. Therefore

$$\begin{aligned} \text{red. char. pol.}_{A/\mathbf{Q}} a &= \text{char. pol.} \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \\ &= \det \begin{pmatrix} X - \alpha & -\beta \\ \bar{\beta} & X - \bar{\alpha} \end{pmatrix} \\ &= X^2 - (\alpha + \bar{\alpha})X + (\alpha\bar{\alpha} + \beta\bar{\beta}) \in \mathbf{Q}[X]. \end{aligned}$$

Hence (see (9.6a) below

$$\text{tr}_{A/\mathbf{Q}} a = \alpha + \bar{\alpha}, \quad \text{nr}_{A/\mathbf{Q}} a = \alpha\bar{\alpha} + \beta\bar{\beta}.$$

Returning to the general case, we have

(9.5) THEOREM. If $(A:K) = n^2$, then

$$\text{char. pol.}_{A/K} a = \{\text{red. char. pol.}_{A/K} a\}^n, \quad a \in A.$$

Proof. Let $E \supset K$ split A , so $E \otimes_K A \cong M_n(E)$. By Exercise 1.2,

$$\text{char. pol.}_{A/K} a = \text{char. pol.}_{E \otimes A/E} 1 \otimes a, \quad a \in A,$$

where \otimes denotes \otimes_K . By (7.3) there is a left $E \otimes A$ -isomorphism $E \otimes A \cong V^{(n)}$, where V is a minimal left ideal of $E \otimes A$. Hence

$$\text{char. pol.}_{E \otimes A/E} 1 \otimes a = f(X)^n,$$

where $f(X)$ is the characteristic polynomial of the matrix $(1 \otimes a)_L$ which describes the action of $1 \otimes a$ on some E -basis of V . On the other hand, the E -isomorphism in (9.2) can be obtained by mapping each $y \in E \otimes A$ onto the matrix y_L giving the action of y on some E -basis of V , and thus

$$\text{char. pol. } h(y) = \text{char. pol. } y_L, \quad y \in E \otimes A.$$

Taking $y = 1 \otimes a$ with $a \in A$, we obtain

$$(9.6) \quad \begin{aligned} \text{red. char. pol.}_{A/K} a &= \text{char. pol. } h(1 \otimes a) \\ &= \text{char. pol. } (1 \otimes a)_L. \end{aligned}$$

Hence $\text{char. pol.}_{A/K} a = f(X)^n$, as desired.

Let us write

$$(9.6a) \quad \text{red. char. pol.}_{A/K} a = X^n - (\text{tr } a)X^{n-1} + \cdots + (-1)^n \text{nr}(a), \quad a \in A.$$

We call $\text{tr}(a)$ the *reduced trace* of a , and $\text{nr}(a)$ the *reduced norm* of a . It follows at once from (9.5) that

$$(9.7) \quad T_{A/K} a = n \cdot \text{tr}(a), \quad N_{A/K} a = (\text{nr}(a))^n.$$

Furthermore, using the notation of (9.6), the map $a \rightarrow (1 \otimes a)_L$, $a \in K$, gives a K -algebra isomorphism of A into $\text{Hom}_E(V, V)$. Since

$$\text{tr}(a) = \text{trace of } (1 \otimes a)_L, \quad \text{nr}(a) = \text{determinant of } (1 \otimes a)_L,$$

we conclude that

$$(9.8) \quad \begin{cases} \text{tr}(ab) = \text{tr}(ba), & \text{tr}(a+b) = \text{tr}(a) + \text{tr}(b), & \text{tr}(sa) = s \cdot \text{tr}(a), \\ \text{nr}(ab) = \text{nr}(a) \cdot \text{nr}(b), & \text{nr}(sa) = s^n \cdot \text{nr}(a), & \end{cases}$$

for $a, b \in A$, $s \in K$.

(9.9) THEOREM. *The reduced trace map gives rise to a symmetric nondegenerate K -bilinear form $\tau: A \times A \rightarrow K$, by setting*

$$\tau(a, b) = \text{tr}(ab), \quad a, b \in A.$$

Further, τ is associative, that is,

$$\tau(ab, c) = \tau(a, bc) \text{ for } a, b, c \in A.$$

Proof. It is clear that τ is symmetric and associative, and we need only prove that τ is nondegenerate. Let $E \supset K$ split A , so $E \otimes_K A \cong M_n(E)$. We may extend τ to an E -bilinear map

$$\tau': (E \otimes A) \times (E \otimes A) \rightarrow E,$$

and indeed from the definition of reduced trace, we have

$$\tau'(u, v) = \text{trace}(uv), \quad u, v \in E \otimes A \cong M_n(E),$$

where $\text{trace}(uv)$ is the ordinary trace of the matrix uv . Furthermore, τ is nondegenerate if and only if τ' is nondegenerate.

Let

$$B = \{u \in M_n(E) : \text{trace}(uv) = 0 \text{ for all } v \in M_n(E)\}.$$

Since τ' is symmetric, B is a two-sided ideal in the ring $M_n(E)$. But B does not contain the identity matrix I_n , and thus $B = 0$. Hence τ' is nondegenerate, whence so is τ . This completes the proof.

If $\text{char } K$ divides n , it follows from (9.7) that the ordinary trace map $T_{A/K}$ is the zero map. Hence in this case it is essential to use the reduced trace, rather than the ordinary trace, in Theorem 9.9 and its applications.

9b Semisimple algebras

In the preceding subsection we have defined the reduced characteristic polynomial, reduced norm and reduced trace, for elements of a central simple K -algebra A . The aim of this subsection is to generalize these concepts to the case where A is an arbitrary finite dimensional semisimple K -algebra.

We begin the discussion with some elementary results from linear algebra. Let $K \subset L$ be fields, with $(L:K) = n$. Each $\alpha \in L$ maps onto a matrix $\tilde{\alpha} \in M_n(K)$ describing the action of left multiplication by α on some K -basis of L . Given

$$f(X) = \sum \alpha_i X^i \in L[X],$$

define

$$\tilde{f}(X) = \sum \tilde{\alpha}_i X^i \in M_n(K[X]).$$

We now define a *norm* map $N_{L/K}: L[X] \rightarrow K[X]$ by setting

$$N_{L/K} f(X) = \det \tilde{f}(X), \quad f(X) \in L[X].$$

Let us establish some basic properties of this norm:

(9.10) THEOREM. *Let $K \subset L$ be fields, with $(L:K) = n$. Then*

- (i) $N_{L/K}$ is multiplicative.
- (ii) For $\alpha_1, \dots, \alpha_s \in L$, we have

$$(9.11) \quad \begin{aligned} N_{L/K}(X^s + \alpha_1 X^{s-1} + \cdots + \alpha_s) \\ = X^{ns} + (T_{L/K} \alpha_1) X^{ns-1} + \cdots + N_{L/K} \alpha_s. \end{aligned}$$

(iii) *Let V be an s -dimensional L -space, and let φ be an L -endomorphism of V . We may view φ as a K -endomorphism of V . Then*

$$(9.12) \quad \text{char. pol.}_{V/K} \varphi = N_{L/K}(\text{char. pol.}_{V/L} \varphi).$$

Proof. Write N in place of $N_{L/K}$, and let $f, g \in L[X]$. The map $\alpha \rightarrow \tilde{\alpha}$, $\alpha \in L$, is a ring homomorphism. Therefore $\tilde{fg} = \tilde{f}\tilde{g}$, and so

$$N(fg) = \det(\tilde{fg}) = (\det \tilde{f})(\det \tilde{g}) = (Nf)(Ng).$$

This establishes (i).

Next we have

$$\begin{aligned} N(X^s + \alpha_1 X^{s-1} + \cdots + \alpha_s) &= \det(\tilde{X} X^s + \tilde{\alpha}_1 X^{s-1} + \cdots + \tilde{\alpha}_s) \\ &= X^{ns} + (\text{tr } \tilde{\alpha}_1) X^{ns-1} + \cdots + \det \tilde{\alpha}_s, \end{aligned}$$

with the second equality following from an obvious calculation. This yields assertion (ii), since by §1 we have

$$\text{tr } \tilde{\alpha}_1 = T_{L/K} \alpha_1, \quad \det \tilde{\alpha}_s = N_{L/K} \alpha_s.$$

To prove (iii), we first write $V = \sum V_i$ where each V_i is an L -subspace of V such that $\varphi(V_i) \subset V_i$. Then

$$\text{char. pol.}_{V/K} \varphi = \prod_i \text{char. pol.}_{V_i/K} \varphi,$$

and likewise with K replaced by L . In view of assertion (i), it therefore suffices to establish (9.12) for each V_i . Changing notation, we may hereafter assume that V is an indecomposable $K[\varphi]$ -module. Thus we may write

$$V = L[X]/(f(X)) \text{ for some } f(X) \in L[X],$$

with φ acting on V as left multiplication by X . Then

$$\text{char. pol.}_{V/L} \varphi = f(X) = X^s + \alpha_1 X^{s-1} + \cdots + \alpha_s \text{ (say).}$$

Now let $L = \sum_{j=1}^n Ku_j$, and let us calculate the action of φ on the K -basis of V consisting of the elements $\{u_j X^i : 1 \leq j \leq n, 0 \leq i \leq s-1\}$. Relative to a suitable indexing of these basis elements, the action of φ is given by the matrix

$$\mu = \begin{bmatrix} 0 & 0 & \dots & 0 & -\tilde{\alpha}_s \\ I & 0 & \dots & 0 & -\tilde{\alpha}_{s-1} \\ 0 & I & \dots & 0 & -\tilde{\alpha}_{s-2} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & I & -\tilde{\alpha}_1 \end{bmatrix}.$$

This matrix μ is an $s \times s$ array of blocks, each of size $n \times n$. We have

$$\text{char. pol.}_{V/K} \varphi = \det(XI - \mu) = \begin{vmatrix} X\tilde{1} & \tilde{0} & \dots & \tilde{0} & \tilde{\alpha}_s \\ -\tilde{1} & X\tilde{1} & \dots & \tilde{0} & \tilde{\alpha}_{s-1} \\ \dots & \dots & \dots & \dots & \dots \\ \tilde{0} & \tilde{0} & \dots & X\tilde{1} & \tilde{\alpha}_2 \\ \tilde{0} & \tilde{0} & \dots & -\tilde{1} & X\tilde{1} + \tilde{\alpha}_1 \end{vmatrix}.$$

Now perform elementary row operations on this determinant, from the bottom up: add X times the s th row of blocks to the $(s - 1)$ th row, then X times the $(s - 1)$ th row of blocks to the $(s - 2)$ th row, and so on. This gives

$$\begin{aligned} \text{char. pol.}_{V/K} \varphi &= \left| \begin{array}{cccc} \tilde{0} & \tilde{0} & \dots & \tilde{0} & \tilde{f}(X) \\ -\tilde{1} & \tilde{0} & \dots & \tilde{0} & * \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \tilde{0} & \tilde{0} & \dots & \tilde{0} & * \\ \tilde{0} & \tilde{0} & \dots & -\tilde{1} & * \end{array} \right| \\ &= \det \tilde{f}(X) = N_{L/K} f(x). \end{aligned}$$

This completes the proof of (iii), and establishes the theorem.

Any semisimple K -algebra A may be written as a direct sum $\sum A_i$ of simple algebras A_i , whose centers are finite extensions of K . In order to define red. char. pol. $_{A/K} a$ for each $a \in A$, we shall first treat the case in which A is a simple K -algebra; the extension to the semisimple case will be straightforward.

(9.13) *Definition.* Let B denote a central simple L -algebra with $(B:L) = m^2$, and let K be a subfield of L with $(L:K) = n$. For each $b \in B$, we define its *reduced characteristic polynomial relative to K* by

$$\text{red. char. pol.}_{B/K} b = N_{L/K} (\text{red. char. pol.}_{B/L} b)$$

$$= X^{mn} - (\text{tr}_{B/K} b) X^{mn-1} + \dots + (-1)^{mn} \text{nr}_{B/K} b.$$

We call $\text{tr}_{B/K}$ the *relative reduced trace*, and $\text{nr}_{B/K}$ the *relative reduced norm*. When $L = K$, the preceding concepts reduce to those given in §9a.

Before proceeding to the case of semisimple K -algebras, let us establish some basic properties of relative reduced traces, norms, and characteristic polynomials.

(9.14) **THEOREM.** *Let B be a central simple L -algebra, K a subfield of L , and let $(B:L) = m^2$, $(L:K) = n$. For each $b \in B$, we have*

$$(9.15) \quad \text{tr}_{B/K} b = T_{L/K} (\text{tr}_{B/L} b), \quad \text{nr}_{B/K} b = N_{L/K} (\text{nr}_{B/L} b),$$

$$(9.16) \quad \text{char. pol.}_{B/K} b = \{\text{red. char. pol.}_{B/K} b\}^m,$$

$$(9.17) \quad T_{B/K} b = m \cdot \text{tr}_{B/K} b, \quad N_{B/K} b = \{\text{nr}_{B/K} b\}^m.$$

Proof. Given $b \in B$, let us set

$$h(X) = \text{red. char. pol.}_{B/L} b = X^m - \alpha_1 X^{m-1} + \dots + (-1)^m \alpha_m.$$

Then $\alpha_1 = \text{tr}_{B/L} b$, $\alpha_m = \text{nr}_{B/L} b$, according to the definitions in §9a. But therefore

$$\begin{aligned}\text{red. char. pol.}_{B/K} b &= N_{L/K} h(X) \\ &= X^{mn} - (T_{L/K} \alpha_1) X^{mn-1} + \cdots + (-1)^{mn} N_{L/K} \alpha_m,\end{aligned}$$

by (9.11). Comparing this expression with that given in (9.13), we conclude at once that

$$\text{tr}_{B/K} b = T_{L/K} \alpha_1, \quad \text{nr}_{B/K} b = N_{L/K} \alpha_m.$$

This yields the desired formulas (9.15).

Next, we may compute $\text{char. pol.}_{B/K} b$ by considering the left multiplication by the element b acting on a K -basis for B ; a corresponding statement holds with K replaced by L . Therefore

$$\begin{aligned}\text{char. pol.}_{B/K} b &= N_{L/K} (\text{char. pol.}_{B/L} b) \quad \text{by (9.12)} \\ &= N_{L/K} \{(\text{red. char. pol.}_{B/L} b)^m\} \quad \text{by (9.5)} \\ &= \{N_{L/K} (\text{red. char. pol.}_{B/L} b)\}^m \quad \text{by (9.10)} \\ &= \{\text{red. char. pol.}_{B/K} b\}^m.\end{aligned}$$

This proves (9.16); since (9.17) is an obvious consequence of (9.16), the theorem is established.

(9.18) COROLLARY. *The analogues of formulas (9.8) hold for $\text{tr}_{B/K}$ and $\text{nr}_{B/K}$.*

Proof. The assertion is clear from (9.8) and (9.15). We remark merely that

$$\text{nr}_{B/K} \alpha b = \alpha^{mn} \cdot \text{nr}_{B/K} b, \quad \alpha \in K, \quad b \in B.$$

We are now ready to generalize Theorem 9.9, as follows:

(9.19) THEOREM. *Let B be a simple K -algebra whose center L is separable over K . Then the map $\text{tr}_{B/K}$ gives rise to a symmetric associative nondegenerate bilinear form from $B \times B$ to K .*

Proof. The form is given by $\tau(a, b) = \text{tr}_{B/K}(ab)$, $a, b \in B$, and we need only check that τ is nondegenerate. If $\tau(a, b) = 0$ for all $b \in B$, then

$$T_{L/K}(\alpha \cdot \text{tr}_{B/L}(ab)) = T_{L/K}(\text{tr}_{B/L}(\alpha \cdot ab)) = 0 \text{ for all } \alpha \in L, \quad b \in B.$$

But $T_{L/K}$ gives a nondegenerate trace form, since L is separable over K , and

hence we have $\text{tr}_{B/L} ab = 0$ for all $b \in B$. Therefore $a = 0$ by (9.9), which completes the proof.

(We remark that the existence of a symmetric associative bilinear form on B to K tells us that B is a Frobenius algebra over K (see Curtis-Reiner [1, (61.3)]); we know this anyway, since every simple K -algebra is a Frobenius algebra. The significance of (9.19) lies in the fact that the form arises from the reduced trace map $\text{tr}_{B/K}$.)

Suppose now that A is any semisimple K -algebra, and write

$$A = A_1 \oplus \cdots \oplus A_t \text{ (simple components),}$$

$$K_i = \text{center of } A_i, \quad (A_i : K_i) = m_i^2, \quad 1 \leq i \leq t.$$

Each K_i is a finite extension field of K . Every element $a \in A$ is uniquely expressible as $a = a_1 + \cdots + a_t$, $a_i \in A_i$. We define

$$\begin{aligned} (9.20) \quad \text{red. char. pol.}_{A/K} a &= \prod_{i=1}^t \text{red. char. pol.}_{A_i/K} a_i \\ &= \prod_{i=1}^t N_{K_i/K} (\text{red. char. pol.}_{A_i/K_i} a_i). \end{aligned}$$

As usual, we define $\text{tr}_{A/K}$ and $\text{nr}_{A/K}$ by the equation

$$(9.21) \quad \text{red. char. pol.}_{A/K} a = X^r - (\text{tr}_{A/K} a)X^{r-1} + \cdots + (-1)^r \text{nr}_{A/K} a$$

for each $a \in A$, where $r = \sum m_i (K_i : K)$. For future use, we record the following obvious consequences of these definitions:

$$(9.22) \quad \text{tr}_{A/K} a = \sum_{i=1}^t \text{tr}_{A_i/K} a_i = \sum_{i=1}^t T_{K_i/K} (\text{tr}_{A_i/K_i} a_i),$$

$$(9.23) \quad \text{nr}_{A/K} a = \prod_{i=1}^t \text{nr}_{A_i/K} a_i = \prod_{i=1}^t N_{K_i/K} (\text{nr}_{A_i/K_i} a_i).$$

From (9.16), we also obtain

$$(9.24) \quad \text{char. pol.}_{A/K} a = \prod_{i=1}^t \text{char. pol.}_{A_i/K} a_i = \prod_{i=1}^t \{\text{red. char. pol.}_{A_i/K} a_i\}^{m_i},$$

$$(9.25) \quad T_{A/K} a = \sum_{i=1}^t m_i \text{tr}_{A_i/K} a_i, \quad N_{A/K} a = \prod_{i=1}^t \{\text{nr}_{A_i/K} a_i\}^{m_i}.$$

Of course, the analogues of formulas (9.8) remain true for $\text{tr}_{A/K}$ and $\text{nr}_{A/K}$.

From (9.19) we have at once

(9.26) **THEOREM.** *Let A be a separable K -algebra. Then the map $\text{tr}_{A/K}$ gives rise to a symmetric associative nondegenerate bilinear trace form from $A \times A$ to K .*

Finally, we show that reduced characteristic polynomials, norms and traces, are not affected by change of ground field. We prove

(9.27) THEOREM. *Let A be a separable K -algebra, and let F be any field containing K (not necessarily finite dimensional over K). View A as embedded in the separable F -algebra $F \otimes A$, where \otimes means \otimes_K . Then for all $a \in A$,*

$$(9.28) \quad \text{red. char. pol}_{F \otimes A/F} a = \text{red. char. pol}_{A/K} a,$$

$$(9.29) \quad \text{tr}_{F \otimes A/F} a = \text{tr}_{A/K} a, \quad \text{nr}_{F \otimes A/F} a = \text{nr}_{A/K} a.$$

Proof. By Exercise 7.13, $F \otimes A$ is a separable F -algebra. We have

$$(9.30) \quad \text{char. pol}_{F \otimes A/F} a = \text{char. pol}_{A/K} a$$

by Exercise 1.2, a fact which we shall use presently. It suffices to prove the theorem for the case where A is a central simple L -algebra, with L a finite separable extension of K . By Exercise 7.14, we may write

$$F \otimes A \cong \sum_{j=1}^d B_j, \quad B_j = F_j \otimes_L A,$$

where each F_j is a field containing L and F . Here, each B_j is a central simple F_j -algebra, and $(B_j : F_j) = (A : L) = m^2$, say. For $a \in A$, write $a = b_1 + \cdots + b_d$, $b_j \in B_j$. Then (9.24) yields

$$\begin{aligned} \text{char. pol}_{F \otimes A/F} a &= \prod_{j=1}^d \{\text{red. char. pol}_{B_j/F} b_j\}^m \\ &= \{\text{red. char. pol}_{F \otimes A/F} a\}^m. \end{aligned}$$

Since

$$\text{char. pol}_{A/K} a = \{\text{red. char. pol}_{A/K} a\}^m$$

by (9.16), we now deduce (9.28) as a direct consequence of (9.30). The formulas in (9.29) follow from (9.28), and the theorem is proved.

For each element a of a K -algebra A , we have computed $\text{char. pol}_{A/K} a$ by letting a act from the left on a K -basis of A . We shall conclude this section by showing that when A is a separable K -algebra, we could equally well have calculated the characteristic polynomial of a by letting a act from the right. For each $a \in A$, we defined

$$a_L : x \rightarrow ax, \quad x \in A, \quad a_R : x \rightarrow xa, \quad x \in A,$$

so a_L and a_R are a pair of K -linear transformations on A . In §1 we defined

$$\text{char. pol}_{A/K} a = \text{char. pol}_K a_L.$$

We now prove

(9.31) THEOREM. Let A be a separable K -algebra. Then

$$\text{char. pol.}_K a_L = \text{char. pol.}_K a_R$$

for each $a \in A$.

Proof. Let $A = \sum_{i=1}^n Kx_i$, and let $\{y_1, \dots, y_n\}$ be a dual basis of A relative

to the reduced trace form, so

$$A = \sum_{j=1}^n Ky_j, \quad \text{tr } x_i y_j = \delta_{ij}, \quad 1 \leq i, j \leq n,$$

where tr is an abbreviation for $\text{tr}_{A/K}$. We shall compute $\text{char. pol.}_K a_L$ by letting a_L act on the K -basis $\{x_i\}$, and we shall compute $\text{char. pol.}_K a_R$ by letting a_R act on the K -basis $\{y_j\}$. For $1 \leq j \leq n$, let

$$a_L(x_j) = ax_j = \sum_i \alpha_{ij} x_i, \quad a_R(y_j) = y_j a = \sum_i \beta_{ij} y_i,$$

where the $\alpha_{ij}, \beta_{ij} \in K$. Then

$$\text{char. pol.}_K a_L = \det(X\delta_{ij} - \alpha_{ij}), \quad \text{char. pol.}_K a_R = \det(X\delta_{ij} - \beta_{ij}).$$

However, for each i, j we have

$$\alpha_{ij} = \text{tr } y_i a x_j, \quad \beta_{ij} = \text{tr } y_j a x_i.$$

Thus the matrices (α_{ij}) and (β_{ij}) are transposes of one another, and hence have the same characteristic polynomial. This completes the proof of the theorem.

(9.32) COROLLARY. Let $A = \sum Kx_i$, and let

$$x_j a = \sum \gamma_{ij} x_i, \quad \gamma_{ij} \in K.$$

Then

$$N_{A/K} a = \det(\gamma_{ij}), \quad T_{A/K} a = \text{trace of } (\gamma_{ij}).$$

It should be pointed out that (9.31) and (9.32) need not be true for arbitrary finite dimensional K -algebras A . The following example is given in Bourbaki [1, §12, no. 3]: let $A = K \oplus Kx \oplus Ky$, where

$$x^2 = x, \quad xy = y, \quad yx = 0, \quad y^2 = 0.$$

Relative to the basis $\{1, x, y\}$, we have

$$x_L = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_R = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

and x_L, x_R have different characteristic polynomials. Furthermore, x_L and x_R have different traces, and if $\text{char } K \neq 2$, then $(1+x)_L$ and $(1+x)_R$ have different determinants.

EXERCISES

1. Let A be a central simple K -algebra, and let E be a subfield of A such that $(A:K) = (E:K)^2$. Show that for every $a \in E$,

$$\text{red. char. pol.}_{A/K} a = (\min. \text{pol.}_K a)^{(E:K(a))}.$$

[Hint: Let $f(X) = \min. \text{pol.}_K a$; then $f(X)$ has degree $(K(a):K)$. But $\text{red. char. pol.}_{A/K} a$ is a power of $f(X)$, and has degree $(E:K)$.]

2. Let A be a central simple K -algebra, where K is any perfect field (that is, K has no inseparable extensions). Using (9.5), prove directly that $\text{red. char. pol.}_{A/K} a \in K[X]$ for each $a \in A$. [Hint: Show that if E is an extension field of K , and $f(X) \in E[X]$ is such that $f(X)^n \in K[X]$, then also $f(X) \in K[X]$.]

3. Let A be a separable K -algebra, and choose a field $E \supset K$ such that

$$E \otimes_K A = \sum_{j=1}^d B_j, \quad \text{where } \varphi_j: B_j \cong M_{n_j}(E), \quad 1 \leq j \leq d.$$

Let $\pi_j: E \otimes_K A \rightarrow B_j$. Prove that for every $a \in A$,

$$(9.33) \quad \text{red. char. pol.}_{A/K} a = \prod_{j=1}^d \text{char. pol. } \varphi_j \pi_j(1 \otimes a).$$

[Hint: Let $f(X)$ denote the expression on the right hand side of (9.33). As in the proof of (9.3), the isomorphism φ_j is unique up to an inner automorphism of $M_{n_j}(E)$, and hence $f(X)$ does not depend on the choice of the maps $\{\varphi_j\}$. The proof of (9.3) carries over to this case, and shows that $f(X)$ does not depend on the choice of E , and that $f(X) \in K[X]$.]

To prove (9.33), it suffices to treat the case where A is a central simple L -algebra, with L/K separable. Choose $E \supset L$ so that

$$E \otimes_L A \cong M_m(E), \quad \text{where } (A:L) = m^2,$$

and so that

$$E \otimes_K L \cong \sum_{i=1}^n E_i, \quad \text{where } (L:K) = n,$$

and where each E_i equals E and contains an isomorphic copy of L . Then

$$E \otimes_K A \cong (E \otimes_K L) \otimes_L A \cong \sum_{i=1}^n E_i \otimes_L A = \sum_{i=1}^n M_m(E_i).$$

But then by (9.28)

$$\begin{aligned} \text{red. char. pol.}_{A/K} a &= \text{red. char. pol.}_{E \otimes_K A/E} 1 \otimes a \\ &= \prod_{i=1}^n \text{char. pol.}(\psi_i(1 \otimes a)) = f(X), \end{aligned}$$

where $\psi_i: E \otimes_K A \rightarrow M_m(E_i)$.]

4. Let L be a finite separable extension of K with $(L:K) = n$, and let ψ_1, \dots, ψ_n be the distinct embeddings of L into an algebraic closure of K . Prove that for each $f(X) \in L[X]$,

$$N_{L/K} f(X) = \prod_{i=1}^n \psi_i f(X),$$

where $\psi_i f(X)$ is obtained from $f(X)$ by applying ψ_i to each of its coefficients.

5. Let $A = M_r(D)$, where D is a skewfield with center K . Let $a \in A$ be given by $a = (\alpha_{ij}) \in M_r(D)$. Show that

$$\text{tr}_{A/K} a = \sum_{i=1}^r \text{tr}_{D/K}(\alpha_{ii}).$$

[Hint: Choose $E \supset K$ to be a splitting field for D , and let

$$\mu: D \rightarrow E \otimes_K D \cong M_s(E).$$

Then $\mu': A \rightarrow E \otimes_K A \cong M_{rs}(E)$ is given by

$$\mu'(a) = (\mu(\alpha_{ij}))_{1 \leq i,j \leq r},$$

and

$$\begin{aligned} \text{tr}_{A/K} a &= \text{trace of } \mu'(a) = \sum_{i=1}^r \text{trace of } \mu(\alpha_{ii}) \\ &= \sum_{i=1}^r \text{tr}_{D/K}(\alpha_{ii}). \end{aligned}$$

10. EXISTENCE OF MAXIMAL ORDERS; DISCRIMINANTS

Throughout this section, A is a separable K -algebra, where K is the quotient field of a noetherian integrally closed domain R . Let Λ be an R -order in A . In dealing with reduced characteristic polynomials and reduced norms and traces, we shall omit the subscripts A/K when there is no danger of confusion.

(10.1) THEOREM. *For each $a \in \Lambda$ we have*

$$\text{red. char. pol. } a \in R[X], \quad \text{tr } a \in R, \quad \text{nr } a \in R.$$

Proof. By (8.6), $\text{char. pol. } a \in R[X]$. The same holds for $\text{red. char. pol. } a$ by

(9.24) and Gauss' Lemma. The assertions about tr , nr are then clear from (9.21).

In brief, (10.1) asserts that integral elements have integral reduced norms and reduced traces. We shall use this fact repeatedly. Let us define the *discriminant* of Λ to be the ideal $d(\Lambda)$ of R generated by the set of elements

$$\{\det(\text{tr } x_i x_j)_{1 \leq i, j \leq m}\}, \quad x_i \in \Lambda,$$

where $m = (A : K)$. Each $x_i x_j \in \Lambda$, so the $m \times m$ matrix $(\text{tr } x_i x_j)$ has entries in R , and thus $d(\Lambda) \subset R$. Furthermore, if x_1, \dots, x_m are chosen so as to be linearly independent over K , then since the bilinear reduced trace form $A \times A \rightarrow K$ is nondegenerate, it follows at once that $\det(\text{tr } x_i x_j) \neq 0$. Thus $d(\Lambda)$ is a nonzero ideal of R .

(10.2) THEOREM. *Let Λ have a free R -basis u_1, \dots, u_m . Then the discriminant $d(\Lambda)$ is the principal ideal $R \cdot \det(\text{tr } u_i u_j)$.*

Proof. This principal ideal surely lies in $d(\Lambda)$. On the other hand, let $x_1, \dots, x_m \in \Lambda$. We may write $x_i = \sum r_{ik} u_k$, $r_{ik} \in R$, and then

$$\text{tr } x_i x_j = \sum_{k,l} r_{ik} r_{jl} \cdot \text{tr } u_k u_l, \quad 1 \leq i, j \leq m.$$

Therefore

$$\det(\text{tr } x_i x_j) = \det(r_{ik}) \cdot \det(\text{tr } u_k u_l) \cdot \det(r_{jl}),$$

where ' denotes transpose. But $\det(r_{ik}) \in R$, and thus we deduce that $d(\Lambda) \subset R \cdot \det(\text{tr } u_i u_j)$, which completes the proof.

If P is any prime ideal of R , and R_P is the localization of R at P , then $\Lambda_P = R_P \otimes_R \Lambda$ is an R_P -order in A . It follows at once from Exercise 4.13 that $d(\Lambda_P) = \{d(\Lambda)\}_P$. If R is a Dedekind domain, then each R_P is a principal ideal domain, and Λ_P has a free R_P -basis. Thus we may use (10.2) to compute $d(\Lambda_P)$, and then we have (by Exercise 3.1 or (4.21))

$$d(\Lambda) = \bigcap_P d(\Lambda_P).$$

Returning to the case where R is any noetherian integrally closed domain, we prove

(10.3) THEOREM. *Let Γ be a subring of A containing R , such that $K \cdot \Gamma = A$, and suppose that each $a \in \Gamma$ is integral over R . Then Γ is an R -order in A . Conversely, every R -order in A has these properties.*

Proof. We already know that every R -order has the indicated properties. Now let Γ be a subring satisfying the given conditions; we need only check that

Γ is an R -lattice. Let

$$A = \sum_{i=1}^m Ku_i, \quad u_i \in \Gamma, \quad \alpha = \det(\operatorname{tr} u_i u_j)_{1 \leq i, j \leq m} \in R.$$

Then $\alpha \neq 0$ since A is separable over K . We claim that

$$\Gamma \subset \alpha^{-1} \cdot \sum_{i=1}^m Ru_i.$$

Let $x \in \Gamma$, and write $x = \sum r_i u_i$, $r_i \in K$. Then

$$\operatorname{tr} xu_j = \sum_{i=1}^m r_i \cdot \operatorname{tr} u_i u_j, \quad 1 \leq j \leq m.$$

Since each $xu_j \in \Gamma$, we have $\operatorname{tr} xu_j \in R$. If we use Cramer's Rule to solve the above system of equations for the $\{r_i\}$, we thus obtain

$$r_i = (\text{element of } R)/\alpha, \quad 1 \leq i \leq m.$$

This proves that $\Gamma \subset \alpha^{-1} \cdot \sum Ru_i$, and hence that Γ is an R -lattice.

(10.4) **Corollary.** *Every R -order in A is contained in a maximal R -order in A . There exists at least one maximal R -order in A .*

Proof. Let Λ be an R -order in A , and let C be the collection of R -orders in A containing Λ . Then C is non-empty. If $\{\Lambda_\alpha\}$ is a chain of orders containing Λ , let

$$\Lambda' = \sum_\alpha \Lambda_\alpha = \bigcup_\alpha \Lambda_\alpha.$$

Then Λ' is a subring of A containing R , and $K \cdot \Lambda' = A$. Each $x \in \Lambda'$ lies in some Λ_α , hence is integral over R . It follows from (10.3) that Λ' is an R -order in A . We have now shown that any increasing chain of elements of C has an upper bound in C . By Zorn's Lemma, C has a maximal element Λ_0 , which is then obviously a maximal R -order in A .

It remains to prove that A contains at least one maximal R -order. The discussion preceding (8.1) shows that there exists a full R -lattice M in A . Setting $\Lambda = O_i(M)$, it follows from §8 that Λ is an R -order in A . Hence Λ is contained in some maximal R -order Λ_0 in A , by the first part of this proof, and the corollary is established.

We remark that the crucial step in the proof of (10.3) is the fact that $(\operatorname{tr} u_i u_j)$ is a nonsingular matrix, or equivalently that $\operatorname{tr}_{A/K}$ gives rise to a nondegenerate bilinear form $A \times A \rightarrow K$. If $\operatorname{char} K = 0$, it is clear from (9.25) that the ordinary trace $T_{A/K}$ already gives a nondegenerate form, and so the proof of (10.3) could have been given using ordinary traces instead of reduced

traces. Nevertheless, even when $\text{char } K = 0$, the reduced trace and reduced norm will play a basic role in our later discussions.

(Without the hypothesis that A be a separable K -algebra, it may happen that there are *no* maximal R -orders in A , as already pointed out in §8. The following example, due to Faddeev [1, §25] (see Roggenkamp and Huber-Dyson [1, pp. 201–202]) shows how to construct an infinite strictly increasing chain of orders, in case A is not semisimple.

Let Λ be any R -order in the K -algebra A , and assume that $\text{rad } A \neq 0$. Set

$$L_k = \Lambda \cap (\text{rad } A)^k, \quad k \geq 1.$$

Then each L_k is an R -pure Λ -submodule of Λ (see (4.0)), and is a full R -lattice in $(\text{rad } A)^k$. Since $\text{rad } A$ is nilpotent, there exists an integer $n \geq 1$ such that $(\text{rad } A)^n \neq 0$, $(\text{rad } A)^{n+1} = 0$. Let r be a non-unit in R , and set

$$\Lambda_k = \Lambda + r^{-k} L_1 + r^{-2k} L_2 + \cdots + r^{-nk} L_n, \quad k \geq 1.$$

Then each Λ_k is an R -order in A , and $\Lambda = \Lambda_0 \subset \Lambda_1 \subset \Lambda_2 \subset \dots$. We show that the chain is strictly increasing. For suppose that $\Lambda_k = \Lambda_{k+1}$ for some k . Multiplying by $r^{(k+1)}$, it follows that $L_n \subset r^k \Lambda$. Therefore

$$L_n \subset r^k \Lambda \cap (\text{rad } A)^n = r^k L_n,$$

the equality following from the fact that L_n is R -pure in Λ . This gives $L_n = r^k L_n$, a contradiction since L_n is an R -lattice and r is not a unit of R .

In particular, the above shows that Λ is always strictly contained in the larger R -order Λ_1 , and thus A has no maximal R -orders whatsoever.)

Let us now return to the case where A is a separable K -algebra. We shall now prove that a decomposition of A into simple components $A = A_1 \oplus \cdots \oplus A_t$ yields a corresponding decomposition of maximal orders and hereditary orders in A . We may write $1 = e_1 + \cdots + e_t$, $e_i \in A_i$; the $\{e_i\}$ are then central idempotents of A such that $e_i e_j = 0$, $i \neq j$, and $A_i = Ae_i$ for each i .

(10.5) THEOREM. *Let A be a separable K -algebra with simple components $\{A_i\}$, and let R_i be the integral closure of R in the center K_i of A_i . Then*

(i) *For each maximal R -order Λ in A , we have $\Lambda = \sum \Lambda e_i$, where the $\{e_i\}$ are the central idempotents of A such that $A_i = Ae_i$. Further, each Λe_i is a maximal R -order in A_i .*

(ii) *If Λ_i is a maximal R -order in A_i , $1 \leq i \leq t$, then $\sum \Lambda_i$ is a maximal R -order in A .*

(iii) *An R -order Λ_i in A_i is a maximal R -order if and only if Λ_i is a maximal R_i -order.*

(iv) *When R is a complete discrete valuation ring, all the preceding assertions remain true under the weaker hypothesis that A is a semisimple K -algebra, not necessarily K -separable.*

Proof. Suppose that A is a separable K -algebra until further notice, and let Λ be a maximal R -order in A . Then

$$\Lambda = \Lambda(e_1 + \cdots + e_t) \subset \Lambda e_1 \oplus \cdots \oplus \Lambda e_t,$$

and each Λe_i is an R -order in A_i . If $\Lambda e_i \subset \Gamma_i \subset A_i$, where Γ_i is a maximal R -order, then $\sum \Gamma_i$ is an R -order in A containing Λ . Therefore $\Lambda = \sum \Gamma_i$, and so $\Lambda e_i = \Gamma_i$ for each i .

Conversely, let $\Lambda_i \subset A_i$ be a maximal R -order, $1 \leq i \leq t$, and let $\Lambda = \sum \Lambda_i$. If $\Lambda \subset \Gamma \subset A$ with Γ maximal, then $\Lambda_i \subset \Gamma e_i$, whence $\Lambda_i = \Gamma e_i$ for each i . Therefore $\Gamma = \sum \Gamma e_i = \Lambda$, proving that Λ is a maximal order.

We claim next that R_i is an R -lattice, and is also a noetherian integrally closed domain. Indeed, R_i is an R -lattice by (10.3), since K_i is a separable K -algebra. Thus R_i is noetherian. Further, if $a \in K_i$ is integral over R_i , then $R_i[a]$ is a finitely generated R_i -module, hence is also finitely generated over R . But then it follows by (1.10) that every element of $R_i[a]$ is integral over R . Thus a is integral over R , and so $a \in R_i$. This completes the proof that R_i is integrally closed.

Now let Λ_i be a maximal R -order in A_i . Since the elements of R_i commute with those of Λ_i , and both R_i and Λ_i are R -lattices, also $R_i \cdot \Lambda_i$ is an R -lattice. Thus $R_i \cdot \Lambda_i$ is an R -order in A_i , whence $\Lambda_i = R_i \cdot \Lambda_i$, which shows that Λ_i is necessarily an R_i -order in A_i . But any R_i -order in A_i is also an R -order in A_i , since R_i is finitely generated over R . Hence Λ_i must be a maximal R_i -order in A_i . Conversely, the same remarks show that every maximal R_i -order in A_i is also a maximal R -order in A_i . This completes the proof of (i)–(iii).

To prove (iv), let us now assume that R is a complete discrete valuation ring, and that A is a semisimple K -algebra. The hypothesis of separability was used to establish that each R_i is an R -lattice, and is a noetherian integrally closed domain. But these facts hold even without this hypothesis, by §5, since we are assuming that R is complete. Indeed, each R_i is also a complete discrete valuation ring, and is finitely generated over R by Theorem 5.6. The preceding proofs of (i)–(iii) thus hold equally well in the present case, and the proof of the theorem is complete.

The preceding theorem shows that the study of maximal orders always reduces to the case of simple algebras, and even to the central simple case if the ground ring is a Dedekind domain. As we shall see eventually, when R is a Dedekind domain, every maximal R -order is hereditary. We shall not use this result in the discussion below, however.

Let Λ be any R -order in A ; by a left Λ -lattice we mean a left Λ -module M which is an R -lattice. In analogy with the results in §4a, we prove

(10.6) THEOREM. *Let Λ be an R -order in a semisimple K -algebra A . Then*

every left Λ -lattice M is Λ -isomorphic to a submodule of a free module $\Lambda^{(k)}$ for some k .

Proof. We may embed M in $KM (= K \otimes_R M)$, and KM is a finitely generated left A -module. Hence there is an A -exact sequence

$$A^{(k)} \rightarrow KM \rightarrow 0$$

for some k , and this sequence splits since A is semisimple. Thus there is an A -isomorphism φ of KM into $A^{(k)}$; this isomorphism carries M into a Λ -lattice $\varphi(M)$ in $A^{(k)}$. Since $\Lambda^{(k)}$ is a full R -lattice in $A^{(k)}$, there exists a nonzero $r \in R$ such that $r \cdot \varphi(M) \subset \Lambda^{(k)}$. The map defined by $m \mapsto r \cdot \varphi(m)$, $m \in M$, then gives the desired embedding of M into $\Lambda^{(k)}$.

The ring Λ is *left hereditary* if every left ideal of Λ is projective, or equivalently (see §2f) if submodules of free Λ -modules are projective. The above result gives at once

(10.7) COROLLARY. *The R -order Λ is left hereditary if and only if every left Λ -lattice is projective.*

(10.8) THEOREM. *If Λ is a left hereditary R -order in the semisimple K -algebra A , with central idempotents $\{e_i\}$ as in (10.5), then $\Lambda = \sum \Lambda e_i$, and each Λe_i is a left hereditary R -order in A_i . Conversely, the direct sum of left hereditary orders is left hereditary.*

Proof. Let Λ be a left hereditary order. There is an exact sequence of left Λ -modules

$$0 \rightarrow \Lambda' \rightarrow \Lambda \rightarrow \Lambda e_i \rightarrow 0,$$

and $\Lambda' = \Lambda \cap A(1 - e_i)$ is an R -order in the algebra $A' = A \oplus \cdots \oplus A_t$. It is easily seen that Λ' is also left hereditary. Now Λe_i is a left Λ -lattice, hence is Λ -projective by (10.7), and so the above sequence splits, that is, Λ' is a direct summand of Λ :

$$\Lambda = \Lambda' \oplus J, \quad J = \text{left ideal of } \Lambda.$$

Multiplying by e_i , we find that $J = \Lambda e_i$. An induction argument then proves that $\Lambda = \sum \Lambda e_i$.

Suppose conversely that Λ_i is a left hereditary R -order in A_i , $1 \leq i \leq t$, and let $\Lambda = \sum \Lambda_i$. Each left Λ -lattice M then decomposes as $M = \sum e_i M$, and $e_i M$ is a left Λ_i -lattice. Thus each $e_i M$ is Λ_i -projective, and so M is Λ -projective.

It should be pointed out that an R -order Λ is left and right noetherian, so

by the discussion in §2f, the ring Λ is left hereditary if and only if Λ is right hereditary. We may remark that hereditary orders enjoy yet another property of maximal orders; in (40.7) we shall prove the following result of Harada [2]:

(10.9) THEOREM. *Every hereditary R -order Λ_i in A_i is also an R_i -order, where R_i is the integral closure of R in the center of A_i , as in (10.5).*

EXERCISES

Throughout, R is a Dedekind domain with quotient field K , and A is a separable K -algebra.

1. Let $\text{tr}: A \rightarrow K$ be the reduced trace map. If $a \in A$ is integral over R , show that $\text{tr}(a^m) \in R$ for each positive integer m . Is the converse true?
2. Find $d(\Lambda)$ for $\Lambda = \mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}j \oplus \mathbf{Z}k$ (see (9.4)). Set $\Lambda_0 = \Lambda + \mathbf{Z}a$, where $a = (1 + i + j + k)/2$, and find $d(\Lambda_0)$. Prove that Λ_0 is a maximal \mathbf{Z} -order in A , where $A = \mathbf{Q}\Lambda$.
3. Let $\Lambda \subset \Lambda'$ be a pair of R -orders in A . Show that $d(\Lambda')|d(\Lambda)$, and that $d(\Lambda') = d(\Lambda)$ if and only if $\Lambda' = \Lambda$. [Hint: First localize so as to reduce the problem to the case where R is a principal ideal domain.]
4. Let Λ be any R -order in A . Deduce from Exercise 3 that Λ is contained in a maximal R -order in A .

5. Let Γ be a subring of A containing R , such that Γ is finitely generated as R -module. Prove that Γ lies in a maximal R -order in A . [Hint: Use Exercise 8.1.]

6. Let Λ be an R -order in a separable K -algebra A , and let S be a domain containing R , with quotient field L . Then $S \otimes_R \Lambda$ is an S -order in $L \otimes_K A$. Prove the discriminant formula:

$$d(S \otimes_R \Lambda) = S \otimes_R d(\Lambda) = S \cdot d(\Lambda),$$

where the last equality is an identification.

7. Let Λ be an R -order in A , and let L be a left Λ -lattice in A , M a right Λ -lattice in A , such that $K \cdot L = K \cdot M = A$. Prove that for each $a \in \Lambda$,

$$\text{ord}_R L/aL = R \cdot N_{A/K} a = \text{ord}_R M/Ma.$$

[Hint: By (4.20) or Exercise 4.4, it suffices to prove the result when R is a discrete valuation ring. In this case, L and M have free R -bases, which are also K -bases for A . If $L = \sum Rx_i$ and we write $ax_j = \sum \alpha_{ij}x_i$, $\alpha_{ij} \in R$, then $\text{ord}_R L/aL = R \cdot \det(\alpha_{ij})$ by Exercise 4.2. But $\det(\alpha_{ij}) = N_{A/K} a$ by §1. For the corresponding statement about M , use (9.32).]

11. LOCALIZATION OF ORDERS

Here we investigate the relation between an R -order Λ in A and its

localizations Λ_P and completions $\hat{\Lambda}_P$, where P ranges over the prime ideals of R . We keep the hypotheses of section 10.

(11.1) THEOREM. *Let S be a multiplicatively closed subset of R . For each maximal R -order Λ in A , $S^{-1}\Lambda$ is a maximal $S^{-1}R$ -order in A .*

Proof. By (1.15e) and (3.11), we know that $S^{-1}R$ is noetherian and integrally closed, since R has these properties by hypothesis. Let $i: \Lambda \rightarrow S^{-1}\Lambda$ be the homomorphism $x \mapsto 1 \otimes x$, $x \in \Lambda$, defined as in (3.10).

Now $S^{-1}\Lambda$ is an $S^{-1}R$ -order in A ; let Γ be any larger order in A , and choose a nonzero $\alpha \in R$ such that $\alpha \cdot \Gamma \subset S^{-1}\Lambda$. Then $\Delta = i^{-1}(\alpha\Gamma)$ is an S -saturated submodule of Λ such that $\alpha\Gamma = S^{-1}\Delta$. Since i is a two-sided Λ -homomorphism, Δ is a two-sided Λ -module. Then the right order $O_r(\Delta)$ coincides with Λ , since $O_r(\Delta) \supset \Lambda$ and Λ is maximal. Hence by (8.4) we have

$$S^{-1}\Lambda = O_r(S^{-1}\Delta) = O_r(\alpha\Gamma) = \Gamma,$$

which completes the proof.

(11.2) COROLLARY. *An R -order Λ in A is maximal if and only if for each maximal ideal P of R , Λ_P is a maximal R_P -order in A .*

Proof. If Λ is maximal, so is each Λ_P by (11.1). Conversely, assume that each Λ_P is maximal, and let $\Lambda \subset \Gamma$, where Γ is any R -order in A . Then $\Lambda_P \subset \Gamma_P$, so that $\Lambda_P = \Gamma_P$ for all P . But then $(\Gamma/\Lambda)_P = 0$ for all P , whence $\Gamma = \Lambda$ by (3.15).

The following material, up to (11.5), can be skipped by the reader interested only in the case where R is a Dedekind domain. The above result shows that the question of whether an R -order Λ is maximal is a “local” one, and can be decided by knowing whether the localizations Λ_P are maximal orders, where P ranges over the maximal ideals of R . Now if $P' \subset P$ are a pair of prime ideals of R , we have an inclusion $\Lambda_P \subset \Lambda_{P'}$, and indeed

$$\Lambda_{P'} \cong (R_P)_{P'} \cdot R_P \otimes_{R_P} \Lambda_P,$$

that is, $\Lambda_{P'}$ is a localization of Λ_P at the prime ideal $P' \cdot R_P$ of R_P . Hence if Λ_P is a maximal R_P -order, then by (11.1), $\Lambda_{P'}$ is necessarily a maximal $R_{P'}$ -order. Thus the hypothesis that Λ_P be a maximal order for each maximal ideal P of R is a rather strong one, since it implies that $\Lambda_{P'}$ is a maximal $R_{P'}$ -order for every prime ideal P' of R . The weakest hypothesis would be the assumption that $\Lambda_{P'}$ is a maximal order for every minimal prime P' of R . (Recall that a *minimal prime* of R is any minimal member in the set of nonzero prime ideals of R .)

The following result shows that in order to decide whether Λ is maximal, it suffices to consider the ring structure of the localizations of Λ at the minimal primes of R , together with the structure of Λ as an R -module. We recall (see page 55) that Λ is a *reflexive* R -module if $\Lambda = \Lambda^{**}$, where

$$\Lambda^* = \text{Hom}_R(\Lambda, R), \quad \Lambda^{**} = \text{Hom}_R(\Lambda^*, R).$$

We saw in (4.25) that for any noetherian integrally closed domain R , we have

$$(11.3) \quad \Lambda^{**} = \bigcap_P \Lambda_P,$$

where P ranges over the minimal left ideals of R . Using this, we prove

(11.4) THEOREM. (Auslander–Goldman [1]). *An R -order Λ is maximal if and only if Λ is a reflexive R -module such that for each minimal prime P of R , Λ_P is a maximal R_P -order.*

Proof. Obviously $\Lambda \subset \Lambda^{**}$ since $\Lambda \subset \Lambda_P$ for each P . By (4.26), Λ^{**} is a full R -lattice in A . Furthermore, Λ^{**} is a ring by (11.3), since it is an intersection of rings. Thus Λ^{**} is an R -order in A containing Λ . If Λ is a maximal R -order, then we have $\Lambda^{**} = \Lambda$, and hence Λ is reflexive. The fact that each Λ_P is maximal has already been shown in (11.1).

Conversely, let Λ be reflexive, and let each Λ_P be maximal. Then

$$\Lambda = \Lambda^{**} = \bigcap_P \Lambda_P, \quad P \text{ minimal.}$$

If $\Lambda \subset \Gamma$, with Γ an R -order in A , then $\Lambda_P \subset \Gamma_P$ for each P , whence $\Lambda_P = \Gamma_P$ for each P . Thence

$$\Gamma \subset \bigcap_P \Gamma_P = \bigcap_P \Lambda_P = \Lambda,$$

so Λ is maximal. This completes the proof.

In applying (11.2) or (11.4), we are faced with the problem of deciding whether the R_P -order Λ_P in A is maximal. The underlying ring R_P is an integrally closed local noetherian domain, with unique maximal ideal $P \cdot R_P$. For such a domain, we now show that we may pass to the completion, and then consider the problem in the complete case.

(11.5) THEOREM. *Let R be an integrally closed local noetherian domain, \hat{R} its completion, and \hat{K} the quotient field of \hat{R} . Let Λ be an R -order in A , and set*

$$\hat{\Lambda} = \hat{R} \otimes_R \Lambda, \quad \hat{A} = \hat{K} \otimes_K A,$$

so $\hat{\Lambda}$ is an \hat{R} -order in \hat{A} . Then Λ is a maximal R -order in A if and only if $\hat{\Lambda}$ is a maximal \hat{R} -order in \hat{A} .

Proof. Suppose Λ maximal, and let $\hat{\Lambda} \subset \Delta$, where Δ is an \hat{R} -order in \hat{A} . Then $\Gamma = A \cap \Delta$ is an R -order in A and $\hat{\Gamma} = \Delta$, by (5.4). Since $\Lambda \subset \Gamma$, we deduce that $\Lambda = \Gamma$, and thus $\hat{\Lambda} = \Delta$. This proves that $\hat{\Lambda}$ is maximal.

Conversely, let $\hat{\Lambda}$ be maximal, and let $\Lambda \subset \Gamma$ for some R -order Γ in A . Then $\hat{\Lambda} \subset \hat{\Gamma}$, so $\hat{\Lambda} = \hat{\Gamma}$, and thus by (5.4) $\Lambda = A \cap \hat{\Lambda} = A \cap \hat{\Gamma} = \Gamma$. This completes the proof.

(11.6) COROLLARY. *Let R be a Dedekind domain, and Λ an R -order in A . Then Λ is a maximal order if and only if for each prime ideal P of R , the P -adic completion $\hat{\Lambda}_P$ is a maximal \hat{R}_P -order in \hat{A}_P .*

Proof. This follows from (11.2) and (11.5).

EXERCISE

1. Let R' be a ring of quotients of the domain R , and let M be an R -lattice, X a full R' -lattice in KM . Show that $M \cap X$ is an R -lattice in M of the same R -rank as M .

3. Maximal Orders in Skewfields (Local Case)

Throughout this chapter, let R be a *complete discrete valuation ring*, that is, R is a principal ideal domain with a unique maximal ideal $P = \pi R \neq 0$, and R is complete relative to the P -adic valuation. Let K be the quotient field of R , and $\bar{R} = R/P$ its residue class field. We call K a *local field*. Let D be a skewfield whose center contains K , such that $(D:K)$ is finite. The aim of this chapter is to study the structure of maximal R -orders in D . As we shall see, the results in this case are surprisingly explicit, and generalize several of the theorems listed in § 5. The presentation below is based on a beautifully written article by Hasse [1].

12. UNIQUENESS OF MAXIMAL ORDERS

We are going to show that D contains a *unique* maximal R -order Δ . The argument will depend strongly on the use of Hensel's Lemma (5.7). Let v be the exponential P -adic valuation defined on K (see § 5b, where v was denoted by v_K). Then it is easily seen that for $a, b \in K$ we have

$$(12.1) \quad \left\{ \begin{array}{l} \text{(i)} \ v(a) = \infty \text{ if and only if } a = 0 \\ \text{(ii)} \ v(ab) = v(a) + v(b) = v(ba) \\ \text{(iii)} \ v(a+b) \geq \min(v(a), v(b)) \\ \text{(iv)} \ \text{The value group of } v \text{ is infinite cyclic,} \end{array} \right.$$

where the *value group* of v is defined to be $\{v(a): a \neq 0\}$.

(12.2) THEOREM. Let $f(X) = \alpha_0 X^n + \alpha_1 X^{n-1} + \cdots + \alpha_n \in K[X]$ be irreducible. Then

$$v(\alpha_i) \geq \min(v(\alpha_0), v(\alpha_n)), \quad 0 \leq i \leq n.$$

Proof. Let $t = \min \{v(\alpha_i): 0 \leq i \leq n\}$. If the theorem is false, then $t < \min(v(\alpha_0), v(\alpha_n))$. Let r be the largest subscript for which $v(\alpha_r) = t$. Then $r \neq 0, r \neq n$, and

$$\alpha_r^{-1} \cdot f(X) = \beta_0 X^n + \cdots + \beta_r X^{n-r} + \cdots + \beta_n, \quad \beta_i \in R,$$

where $\beta_r = 1$ and $\beta_{r+1}, \dots, \beta_n \in P$. However, in $\bar{R}[X]$ the right hand expression is a product $X^{n-r}(1 + \bar{\beta}_{r-1} X + \cdots + \bar{\beta}_0 X^r)$ of two relatively prime

polynomials, with the first factor monic. It follows by Hensel's Lemma that $\alpha_r^{-1} \cdot f(X)$ is reducible, whence so is $f(X)$, a contradiction. This completes the proof.

Now let $N_{D/K}$ and $T_{D/K}$ be the norm and trace maps, defined by

$$\text{char. pol.}_{D/K} a = X^m - (T_{D/K} a)X^{m-1} + \cdots + (-1)^m N_{D/K} a, \quad a \in A,$$

where for the rest of this section we put $(D:K) = m$. We now set

$$(12.3) \quad w(a) = m^{-1} \cdot v(N_{D/K} a), \quad a \in D.$$

(12.4) THEOREM. *For $a \in D$, let $f(X) = \min. \text{pol.}_K a$. Then*

$$w(a) = (K(a):K)^{-1} \cdot v(f(0)) = (K(a):K)^{-1} \cdot v(N_{K(a)/K} a).$$

Proof. Since D is a skewfield, $f(X)$ is irreducible, and therefore $\text{char. pol.}_{D/K} a = f(X)^{m/n}$, where $n = \text{degree of } f(X) = (K(a):K)$. Therefore

$$N_{D/K} a = (-1)^m \cdot \{f(0)\}^{m/n},$$

whence

$$w(a) = m^{-1} \cdot v(\{f(0)\}^{m/n}) = n^{-1} \cdot v(f(0)),$$

which completes the proof.

Using (12.2) and (12.4), we may prove the fundamental

(12.5) THEOREM. *An element $a \in D$ is integral over R if and only if $N_{D/K} a \in R$, or equivalently, if and only if $w(a) \geq 0$.*

Proof. It is obvious that $w(a) \geq 0$ if and only if $Na \in R$, where we write N for $N_{D/K}$. If a is integral over R , then $\text{char. pol.}_{D/K} a \in R[X]$ by Exercise 1.1, whence $Na \in R$. Conversely, let $Na \in R$, and set

$$f(X) = X^n + \alpha_1 X^{n-1} + \cdots + \alpha_n = \min. \text{pol.}_K a.$$

Then $f(0) = \alpha_n$, and since $\pm Na$ is a power of $f(0)$, it follows that $\alpha_n \in R$. But $f(X)$ is irreducible in $K[X]$, so by (12.2) we deduce that

$$v(\alpha_i) \geq \min(v(1), v(\alpha_n)) = 0, \quad 0 \leq i \leq n.$$

Hence $f(X) \in R[X]$, so a is integral over R . This completes the proof.

(12.6) THEOREM. *The map w is a discrete valuation on D which extends v , that is, w satisfies conditions (12.1), and $w(\alpha) = v(\alpha)$, $\alpha \in K$.*

Proof. Consider the conditions (12.1) on w ; (i) clearly holds, since $a = 0$ if and only if $Na = 0$. Condition (ii) is satisfied since N is multiplicative, and

v satisfies (ii). For $\alpha \in K$, we have $w(\alpha) = v(\alpha)$ by (12.4). Next, the value group of w , $\{w(a):a \in D, a \neq 0\}$, is a nonzero additive subgroup of $m^{-1}\mathbf{Z}$, and is therefore isomorphic to \mathbf{Z} .

It remains for us to show that w satisfies (iii), and for this it suffices to consider the case where $a = 1$ and $w(b) \geq 0$, with $b \in D$. But then b is integral over R by (12.5), so by (1.11) also $1 + b$ is integral over R . Hence

$$w(1 + b) \geq 0 = \min(w(1), w(b)),$$

as desired. This completes the proof.

Let us set

$$(12.7) \quad \Delta = \{a \in D : w(a) \geq 0\} = \{a \in D : N_{D/K} a \in R\}.$$

Then Δ is a ring containing R , by (12.6). We call Δ the *valuation ring* of w . We shall show in (13.3) that Δ is finitely generated as R -module. Taking this for granted, we have

(12.8) **Theorem.** Δ is the unique maximal R -order in D , and is the integral closure of R in D .

Proof. Clearly $K \cdot \Delta = D$, and so Δ is an R -order in D . But by (8.6), every element of an R -order in D is integral over R , hence lies in Δ by (12.5). Therefore Δ is the unique maximal R -order in D , and the result is proved.

We are now going to prove that w is the *unique* extension of v to D satisfying (12.1), and begin with

(12.9) **LEMMA†.** Let $f(X) = X^n + \alpha_1 X^{n-1} + \cdots + \alpha_n \in K[X]$ be irreducible. Then

$$v(\alpha_k) \geq \frac{k}{n} \cdot v(\alpha_n), \quad 1 \leq k \leq n.$$

Proof. Let E be a splitting field for $f(X)$ over K , and write $f(X) = (X - \beta_1) \cdots (X - \beta_n)$, $\beta_i \in E$. Let v' be the extension of v to E defined as in (12.3), namely,

$$v'(\beta) = (E:K)^{-1} \cdot v(N_{E/K} \beta), \quad \beta \in E.$$

But $\min_{K} \beta_j = f(X)$, so by (12.4) we have

$$v'(\beta_j) = (K(\beta_j):K)^{-1} \cdot v(f(0)) = n^{-1} \cdot v(\alpha_n)$$

for each j . However, $\pm \alpha_k$ is the k th elementary symmetric polynomial in

† For a generalization of this lemma, see the discussion of Newton's polygon in Weiss [1, section 3.1].

β_1, \dots, β_n , so by (12.1) ii) and iii) we obtain

$$v(\alpha_k) = v'(\alpha_k) \geq \frac{k}{n} \cdot v(a_n)$$

for each k , as desired.

(12.10) THEOREM. *The valuation w is the unique extension of v to D having properties (12.1).*

Proof. Let $u: D \rightarrow \mathbf{R} \cup \{\infty\}$ be another such extension of v . If $u \neq w$, there exists a nonzero $a \in D$ such that $u(a) \neq w(a)$. Replacing a by a^{-1} if need be, we may assume that $u(a) > w(a)$. Let

$$f(X) = \min_{a \in D} \text{pol}_K a = X^n + \alpha_1 X^{n-1} + \cdots + \alpha_n \in K[X].$$

Then $w(a) = v(\alpha_n)/n$ by (12.4), while $v(\alpha_j) \geq (j/n) v(\alpha_n)$ by (12.9), since $f(X)$ is irreducible. Therefore

$$u(\alpha_j \cdot a^{n-j}) = v(\alpha_j) + (n-j) u(a) > \frac{j}{n} \cdot v(\alpha_n) + \frac{n-j}{n} \cdot v(\alpha_n) = v(\alpha_n),$$

for $0 \leq j \leq n-1$, where $\alpha_0 = 1$. But now

$$\alpha_n = -\alpha_{n-1} \cdot a - \alpha_{n-2} \cdot a^2 - \cdots - a^n,$$

whence

$$v(\alpha_n) = u(\alpha_n) \geq \min \{u(\alpha_j \cdot a^{n-j}) : 0 \leq j \leq n-1\} > v(\alpha_n).$$

This gives a contradiction, so the theorem is proved.

The preceding discussion is of course valid for the special case where D is an extension field of the complete P -adic field K . It shows that the P -adic valuation on K can be extended to a discrete valuation on D , by means of formula (12.3), and that this extension is unique (up to equivalence).

13. RAMIFICATION INDEX, INERTIAL DEGREE

Keeping the notation of §12, let D be a skewfield of finite dimension over a complete P -adic field K contained in the center of D , and let Δ be the unique maximal R -order in D . We shall define the *ramification index* $e = e(D/K)$ and *inertial degree* $f = f(D/K)$, and shall show that the analogue of Theorem 5.6 holds true in this case. In fact, the discussion below does not make use of any of the earlier results from §5, and so provides a proof of Theorem 5.6, by choosing D to be a field.

Let v be the exponential valuation on K , and let w be the extension of v to the skewfield D . We have seen that the value group of v is \mathbf{Z} , while the value

group of w is a subgroup of $m^{-1}\mathbf{Z}$, where $m = (D:K)$. Hence the value group of w equals $e^{-1}\mathbf{Z}$, for some positive integer e dividing m . We write $e = e(D/K)$, and call e the *ramification index* of D over K . Thus, the least positive number in the set $\{w(a): a \in \Delta\}$ is precisely $1/e$.

We shall now *normalize* the valuation w , by replacing w by the equivalent valuation v_D , where $v_D = e \cdot w$. Then v_D has value group \mathbf{Z} , and for $a \in D$,

$$(13.1) \quad \begin{cases} v_D(a) = (e/m) \cdot v(N_{D/K}a) \\ = e \cdot (K(a):K)^{-1} v(f(0)), \text{ where } f(X) = \min. \text{ pol.}_K a. \end{cases}$$

Let $\pi \in R$ be a prime element, so $v(\pi) = 1$. We may choose $\pi_D \in \Delta$ so that $v_D(\pi_D) = 1$; call π_D a *prime element* of Δ . We have at once

$$v_D(\pi) = e.$$

The group of units of Δ is given by

$$u(\Delta) = \{a \in \Delta : v_D(a) = 0\} = \{a \in \Delta : N_{D/K} a \in u(R)\}.$$

Each nonzero $a \in D$ is uniquely expressible as

$$a = \pi_D^n \cdot a' = a'' \cdot \pi_D^n, \quad n = v_D(a), \quad \text{where } a', a'' \in u(\Delta).$$

Note that a' and a'' need not be equal.

(13.2) THEOREM. *Let π_D be a prime element of Δ , and set $\mathfrak{p} = \pi_D \Delta$. Then every nonzero one-sided ideal of Δ is a two-sided ideal, and is a power of \mathfrak{p} . The residue class ring Δ/\mathfrak{p} is a skewfield over the field \bar{R} , and $\mathfrak{p} \cap R = P$.*

Proof. For L any nonzero left ideal in Δ , let

$$l = \min \{v_D(a) : a \in L\},$$

and choose an element $x \in L$ such that $v_D(x) = l$. Then for each $y \in L$ we have $yx^{-1} \in \Delta$, so $y \in \Delta x \subset L$. This proves that $L = \Delta x$. Furthermore, $\Delta x = x\Delta$ since

$$v_D(x^{-1}ax) = v_D(a), \quad a \in D.$$

Thus L is a two-sided ideal of Δ , and clearly

$$L = \pi_D^l \Delta = \Delta \pi_D^l = \mathfrak{p}^l, \quad \text{since } x \cdot \pi_D^{-l} \in \Delta.$$

The above shows that \mathfrak{p} is a maximal left ideal of Δ . The ring $\bar{\Delta} = \Delta/\mathfrak{p}$ therefore has no left ideals except 0 and $\bar{\Delta}$, and thus $\bar{\Delta}$ is a skewfield. Finally, $\mathfrak{p} \cap R$ is a prime ideal of R , and is nonzero since \mathfrak{p} is a full R -lattice in D . Thus $\mathfrak{p} \cap R = P$, whence $P \cdot \bar{\Delta} = 0$, so $\bar{\Delta}$ is a skewfield over \bar{R} .

We now define the *inertial degree* of D over K as

$$f = f(D/K) = (\bar{\Delta} : \bar{R}).$$

Note that $\bar{\Delta} = \Delta/\mathfrak{p}$ is a vector space over \bar{R} , since $P \subset \mathfrak{p}$. The fact that f is finite follows from the theorem below, which generalizes Theorem 5.6, and indeed provides an independent proof thereof.

(13.3) THEOREM. *Let D be a skewfield of finite dimension m over a complete P -adic field K contained in the center of D . Let $e = e(D/K)$ be the ramification index of D over K , and $f = f(D/K)$ the inertial degree of D over K . Both e and f are finite, and*

$$e \cdot f = (D : K) = m.$$

Let $a_1, \dots, a_f \in \Delta$ be such that $\bar{\Delta} = \sum \bar{R}\bar{a}_i$, and let $b_0, \dots, b_{e-1} \in \Delta$ be such that $v_D(b_j) = j$, $0 \leq j \leq e-1$. Then the $e \cdot f$ products $\{a_i b_j\}$ form a free R -basis for Δ .

Proof. First, let $\{a_i : 1 \leq i \leq s\}$ be elements in Δ whose images $\{\bar{a}_i\}$ in $\bar{\Delta}$ are linearly independent over \bar{R} , and let $\{b_j : 1 \leq j \leq t\}$ be elements of K such that the integers $\{v_D(b_j)\}$ are incongruent mod e . We claim that the $s \cdot t$ products $\{a_i b_j\}$ are linearly independent over K . If not, there is a relation

$$(13.4) \quad (\sum \alpha_{1i} a_i) b_1 + \cdots + (\sum \alpha_{ti} a_i) b_t = 0, \quad \alpha_{ji} \in K,$$

where we may assume that for each b_j , at least one of the coefficients $\alpha_{j1}, \dots, \alpha_{js}$ is nonzero. Write

$$n_j = \min \{v(\alpha_{ji}) : 1 \leq i \leq s\}, \quad \alpha_{ji} = \pi^{n_j} \cdot \beta_{ji}.$$

Then each $\beta_{ji} \in R$, and for each j there is an index k for which $\beta_{jk} \notin P$. We may rewrite (13.4) as

$$(\sum \beta_{1i} a_i) \pi^{n_1} b_1 + \cdots + (\sum \beta_{ti} a_i) \pi^{n_t} b_t = 0.$$

Since $v_D(\pi) = e$, replacing each b_j by $\pi^{n_j} b_j$ does not affect the hypotheses or the conclusion. After making this replacement, and renumbering the a 's and b 's if need be, we obtain a relation

$$(\sum \gamma_{1i} a_i) b_1 + \cdots + (\sum \gamma_{ti} a_i) b_t = 0,$$

where each $\gamma_{ji} \in R$, and

$$v_D(b_1) < \cdots < v_D(b_t),$$

and $\gamma_{11} \notin P$. Therefore

$$\sum_j (\sum_i \gamma_{ji} a_i) b_j / b_1 = 0, \quad \text{and} \quad b_j / b_1 \in \mathfrak{p} \quad \text{for } 2 \leq j \leq t.$$

Passing to the residue class ring $\bar{\Delta}$, we obtain the relation $\sum \bar{y}_{1i} \bar{a}_i = 0$, with $\bar{y}_{11} \neq 0$, which contradicts the linear independence of the $\{\bar{a}_i\}$ over \bar{R} . We have therefore established that the $s \cdot t$ products $\{a_i b_j\}$ are elements of D linearly independent over K , so $st \leq m$. This proves that f is finite, and shows also that $ef \leq m$.

Now let $a_1, \dots, a_f, b_0, \dots, b_{e-1} \in \Delta$ be elements satisfying the hypotheses of the theorem. The $e \cdot f$ elements $\{a_i b_j\}$ are linearly independent over K , by the first part of the proof, and we need only show that $\Delta = \sum_{i,j} Ra_i b_j$. Let $x \in \Delta$, $x \neq 0$, and let $v_D(x) = ke + j$, where $0 \leq j \leq e - 1$. Then

$$x = (\pi^k b_j)u, \quad u \in u(\Delta).$$

Since the $\{\bar{a}_i\}$ form an \bar{R} -basis for $\bar{\Delta}$, we may find elements $\{r_i\}$ in R such that $u = r_1 a_1 + \dots + r_f a_f + z$, with $z \in \mathfrak{p}$. Hence we have

$$x = \left(\sum_i r_i \pi^k a_i \right) b_j + x_1, \quad \text{where} \quad v_D(x_1) > v_D(x).$$

If $x_1 \neq 0$, we may repeat this procedure with x_1 , and continue if need be with x_2, x_3, \dots . Note that k is the greatest integer in $v_D(x)/e$. Hence after $n \cdot e$ steps, we obtain an equality

$$(13.5) \quad x = \sum_{j=0}^{e-1} \sum_{i=1}^f (r_{ij}^{(1)} \pi^k + r_{ij}^{(2)} \pi^{k+1} + \dots + r_{ij}^{(n)} \pi^{k+n-1}) a_i b_j + y_n,$$

where $v_D(y_n) \geq v_D(x) + ne$.

For fixed i, j , the sequence

$$r_{ij}^{(1)} \pi^k, \quad r_{ij}^{(1)} \pi^k + r_{ij}^{(2)} \pi^{k+1}, \dots$$

is a Cauchy sequence from R , relative to the P -adic valuation of R . Since R is assumed complete, this sequence has a limit $s_{ij} \in R$. If we set $x' = \sum_{i,j} s_{ij} a_i b_j \in \Delta$, then for each n we have from (13.5)

$$v_D(x - x') \geq \min(v_D(y_n), k + n - 1).$$

Thus $v_D(x - x') = \infty$, so $x = x'$. Therefore $x \in \sum Ra_i b_j$, and the theorem is proved.

We have now established that Δ is finitely generated as R -module, and indeed that Δ is a free R -module on m generators. This shows that Theorem 12.8 is valid, that is, Δ is the unique maximal R -order in D .

(13.6) COROLLARY. *The skewfield D is complete relative to the valuation v_D .*

Proof. Keeping the notation of (13.3), we have $D = \sum_{i,j} K a_i b_j$. Let $\{x_1, x_2, \dots\}$ be a Cauchy sequence from D , whence $v_D(x_n - x_{n-1}) \rightarrow \infty$ as $n \rightarrow \infty$. Write

$$x_n = \sum_{i,j} r_{ij}^{(n)} a_i b_j, \quad r_{ij}^{(n)} \in K, \quad n \geq 1.$$

Set

$$v_D(x_n - x_{n-1}) = e \cdot k_n + l_n, \quad 0 \leq l_n \leq e-1,$$

so also $\lim_{n \rightarrow \infty} k_n = \infty$. We have then

$$x_n - x_{n-1} = \pi^{k_n} \cdot y_n, \quad y_n \in \Delta.$$

Write y_n as an R -linear combination of the $\{a_i b_j\}$; then by (13.3), it follows from the above equation that

$$r_{ij}^{(n)} - r_{ij}^{(n-1)} \in \pi^{k_n} R.$$

Hence $\{r_{ij}^{(1)}, r_{ij}^{(2)}, \dots\}$ is a Cauchy sequence from K , with limit ρ_{ij} , say. Then obviously

$$\lim_{n \rightarrow \infty} x_n = \sum_{i,j} \rho_{ij} a_i b_j.$$

(13.7) THEOREM. *Let K be the center of the skewfield D , and set $(D:K) = n^2$, $e = e(D/K)$, $f = f(D/K)$. Then*

$$ef = n^2, \quad e|n, \quad n|f.$$

Proof. Let w be the extension of v to D defined in (12.3). By definition of e , we have $w(\pi_D) = 1/e$. Then $K(\pi_D)$ is a subfield of D , and has ramification index e . Hence by (5.6) or (13.3), we have $e|(K(\pi_D):K)$. But $K(\pi_D)$ lies in some maximal subfield E of D , whence $(K(\pi_D):K)|(E:K)$. Since $(E:K) = n$ by (7.15), the result follows.

EXERCISES

1. Let \mathcal{S} be any full set of representatives in Δ of the residue classes in $\bar{\Delta}$, where we assume that $0 \in \mathcal{S}$. Prove that every nonzero $x \in D$ is uniquely expressible as

$$x = \pi_D^{v_D(x)} \cdot (s_0 + s_1 \pi_D + s_2 \pi_D^2 + \dots), \quad s_i \in \mathcal{S}, \quad s_0 \neq 0.$$

2. Prove that the order ideal $\text{ord}_{\bar{R}} \bar{\Delta}$ equals P^f , where $f = f(D/K)$.

[Hint: $\bar{\Delta} \cong \bar{R}^{(f)}$ as \bar{R} -modules.]

3. Prove that $v(N_{D/K} \pi_D) = f$, and that $v(\text{nr}_{D/K} \pi_D) = \sqrt{f/e}$.

[Hint: $e^{-1} = m^{-1} v(N_{D/K} \pi_D)$, $m = (D:K)$, so $v(N_{D/K} \pi_D) = f$. Next,

$$N_{D/K} \pi_D = (\text{nr } \pi_D)^{\sqrt{(D:K)}}, \text{ so } f = \sqrt{(D:K)} v(\text{nr } \pi_D) = \sqrt{ef} \cdot v(\text{nr } \pi_D).$$

4. A *fractional* Δ -ideal is a full left Δ -lattice in D . Show that the set of fractional Δ -ideals, with the obvious definition of multiplication, is an infinite cyclic group generated by the ideal \mathfrak{p} . Prove also that $\mathfrak{p} = \text{rad } \Delta$.

14. FINITE RESIDUE CLASS FIELD CASE

Throughout this section we assume that \bar{R} is a finite field with q elements. Let D be a skewfield with center K , and let $(D : K) = n^2$. We call n the *index* of D . Denote by v the valuation v_K on K , and by v_D that on D , as in (13.1). Let Δ be the unique maximal R -order in D . We shall see here that the structures of D and Δ can be described explicitly in this case, and depend only on the index n and some integer r such that $1 \leq r \leq n$, $(r, n) = 1$.

The discussion to follow depends heavily on the results listed in §5b, and we shall use the notation introduced there. Since \bar{R} is finite, we know from (5.10) and (5.11) that for each positive integer f , there is a unique unramified extension W of K with $(W : K) = f$, given by $W = K(\omega)$, where ω is a primitive $(q^f - 1)$ th root of 1. If \mathcal{o}_W denotes the valuation ring of W , and $\bar{\mathcal{o}}_W$ the residue class field of \mathcal{o}_W , then

$$\mathcal{o}_W = R[\omega], \quad \bar{\mathcal{o}}_W = \bar{R}[\bar{\omega}], \quad (W : K) = (\bar{\mathcal{o}}_W : \bar{R}) = f.$$

Further, W/K is a galois extension with cyclic galois group of order f , generated by the Frobenius automorphism σ defined by $\omega \rightarrow \omega^q$. Likewise, $\bar{\mathcal{o}}_W/\bar{R}$ is a galois extension, with galois group cyclic of order f , generated by the automorphism $\bar{\sigma}$ which maps $\bar{\omega}$ onto $\bar{\omega}^q$.

Before turning to the study of skewfields, we need one more preliminary result.

(14.1) THEOREM. *Let W be an unramified extension of K of degree f , and let v be the valuation on K . Given any element $\alpha \in K$, the equation*

$$N_{W/K} x = \alpha, \quad x \in W,$$

is solvable for x if and only if f divides $v(\alpha)$.

Proof. The prime element π of R is also a prime element for \mathcal{o}_W . Each nonzero $x \in W$ is thus expressible as $x = \pi^k x_0$, $x_0 \in u(\mathcal{o}_W)$. Then $v_W(x_0) = 0$, whence $Nx_0 \in u(R)$, where N denotes $N_{W/K}$. But

$$Nx = \pi^{nf} N(x_0),$$

and thus the condition that f divides $v(\alpha)$ is a necessary one.

To prove sufficiency, it is enough to deal with the case where $\alpha \in u(R)$. Since the galois groups of W/K and of $\bar{\mathcal{o}}_W/\bar{R}$ are isomorphic, it follows at

once from Exercise 1.4 that

$$\bar{N}(\bar{\alpha}) = \bar{N}(\bar{\alpha}), \quad \bar{T}(\bar{\alpha}) = \bar{T}(\bar{\alpha}), \quad \alpha \in o_W,$$

where \bar{N} , \bar{T} are the norm and trace maps from \bar{o}_W to \bar{R} , while N and T are those from W to K . We shall show that both \bar{N} and \bar{T} are epic. We know this for \bar{T} , since \bar{o}_W is separable over \bar{R} (see (4.6)). Next, the multiplicative group of \bar{o}_W is cyclic of order $q^f - 1$, with generator $\bar{\omega}$. Since $\text{Gal}(\bar{o}_W/\bar{R})$ is cyclic with generator $\bar{\sigma}: \bar{\omega} \rightarrow \bar{\omega}^q$, the distinct algebraic conjugates of $\bar{\omega}$ over \bar{R} are

$$\{\bar{\omega}^{q^i} : 0 \leq i \leq f-1\}.$$

Each nonzero element of \bar{o}_W is of the form $\bar{\omega}^t$, $1 \leq t \leq q^f - 1$, and (by Exercise 1.4) we have

$$\bar{N}(\bar{\omega}^t) = \bar{\omega}^{t(1+q+\dots+q^{f-1})} = \bar{\omega}^{t(q^f-1)/(q-1)}.$$

Thus $\bar{N}(\bar{\omega}^t) = 1$ if and only if $(q-1)|t$. Hence exactly $(q^f-1)/(q-1)$ elements of \bar{o}_W have norm 1, so there are $q-1$ distinct nonzero norms. This proves that \bar{N} is epic.

Continuing with the proof, let $\alpha \in u(R)$. Since \bar{N} is epic, we may choose $b_0 \in o_W$ such that $\alpha \equiv Nb_0 \pmod{\pi R}$. For $i \geq 1$, suppose that we have found an element

$$a_i = b_0 + \pi b_1 + \dots + \pi^{i-1} b_{i-1} \in o_W$$

such that

$$\alpha \equiv Na_i \pmod{\pi^i R}.$$

Of course $a_i \in u(o_W)$ since $Na_i \in u(R)$. We proceed to construct the next approximation, and set $a_{i+1} = a_i + b\pi^i$, with $b \in o_W$ to be determined so that

$$(14.2) \quad \alpha \equiv Na_{i+1} \pmod{\pi^{i+1} R}.$$

Since $i \geq 1$, by Exercise 1.4 we have

$$\begin{aligned} Na_{i+1} &= \prod_{s=0}^{f-1} (\sigma^s(a_i) + \sigma^s(b)\pi^i) \\ &\equiv Na_i + \pi^i \sum_{s=0}^{f-1} c_s \pmod{\pi^{i+1} R}, \end{aligned}$$

where for each s ,

$$c_s = a_i \cdot \sigma(a_i) \cdots \sigma^{s-1}(a_i) \cdot \sigma^{s+1}(a_i) \cdots \sigma^{f-1}(a_i) \cdot \sigma^s(b).$$

If we set $y = \sigma(a_i) \cdot \sigma^2(a_i) \cdots \sigma^{f-1}(a_i)$, then $c_s = \sigma^s(y) \cdot \sigma^s(b) = \sigma^s(yb)$, whence

$$\sum_{s=0}^{f-1} c_s = T_{W/K}(yb).$$

Condition (14.2) thus becomes

$$\alpha \equiv Na_i + \pi^i T_{W/K}(yb) \pmod{\pi^{i+1} R}.$$

But y is a unit in o_W , and \bar{T} is epic, so we can always choose $b \in o_W$ satisfying the above condition. We have therefore obtained our next approximation a_{i+1} . If we set $x = \lim_{i \rightarrow \infty} a_i$, then $x \in o_W$ and $\alpha = N_{W/K} x$, which completes the proof of the theorem.

Now we are ready to consider skewfields. The first important consequence of the hypothesis that \bar{R} be finite is as follows:

(14.3) **Theorem.** *If $(D:K) = n^2$, then*

$$e(D/K) = f(D/K) = n.$$

Proof. $\bar{\Delta}$ is a skewfield of finite dimension f over \bar{R} , hence is a finite skewfield. By Wedderburn's Theorem (7.24), $\bar{\Delta}$ must be a field. Hence $\bar{\Delta} = \bar{R}(\bar{a})$ for some $a \in \Delta$, so by (13.3) or (5.6) we have

$$(K(a):K) \geq (\bar{\Delta}:\bar{R}) = f.$$

But $K(a)$ is a subfield of D , whence $(K(a):K) \leq n$ by (7.15). Therefore $f \leq n$, so $f = n$ by (13.7). Finally, $ef = n^2$ implies that $e = n$, and the proof is complete.

As a consequence of the above theorem, we now know that

$$\pi\Delta = \mathfrak{p}^n, \quad \bar{\Delta} = \bar{R}(\xi),$$

where \mathfrak{p} is the unique maximal ideal of Δ , π is a prime element of R , and ξ is a primitive $(q^n - 1)$ th root of 1 over \bar{R} . We wish to prove, in analogy with the results of § 5b for the case of fields, that the skewfield D comes from an unramified extension, followed by a completely ramified extension. To begin with, choose any element $\omega \in \Delta$ such that $\bar{\omega} = \xi$, and set $W = K(\omega)$. Then W is a subfield of D , and by (5.8) W is an unramified extension of K such that $(W:K) = (\bar{\Delta}:\bar{R}) = n$, and hence W is a maximal subfield of D . Further, by (5.10) W is a cyclotomic extension of K containing all of the $(q^n - 1)$ th roots of 1. Hence we could have chosen ω to be a primitive $(q^n - 1)$ th root of 1 over K . We shall call W an *inertia field* of D .

We now know that every skewfield D of index n contains an inertia field $K(\omega)$ as maximal subfield, where ω is a primitive $(q^n - 1)$ th root of 1 over K . To what extent is the subfield W of D unique? It is unique up to K -isomorphism by (5.10), but there may be many mutually K -isomorphic subfields of D . Obviously $W = K(\omega^j)$ for any j relatively prime to $q^n - 1$, so replacing

ω by such a power ω^j does not affect W . However, (see Exercise 14.1) there are usually more than $q^n - 1$ distinct $(q^n - 1)$ th roots of 1 in D . Indeed, if $\alpha \in D$ is nonzero, then $\alpha\omega\alpha^{-1}$ is also a $(q^n - 1)$ th root of 1, and need not be a power of ω . We call the elements $\omega, \alpha\omega\alpha^{-1}$ *conjugate* in D , and likewise the fields W and $\alpha W \alpha^{-1}$ are *conjugate* subfields of D .

(14.4) THEOREM. *The inertia field of D is unique up to conjugacy.*

Proof. By (5.10), W is unique up to K -isomorphism. Hence W is unique up to conjugacy in D by (7.23). We remark that if K is an infinite field, then by Exercise 14.1, there are infinitely many primitive $(q^n - 1)$ th roots of 1 in D , and thus there are infinitely many distinct inertia fields in D .

Let π_D be a prime element of Δ . Since $\pi\Delta = \pi_D^n\Delta$, the field $K(\pi_D)$ is a completely ramified extension of K of degree n , and is a maximal subfield of D . By (13.3) we have

$$\Delta = \sum_{i,j=0}^{n-1} R\omega^i\pi_D^j = R[\omega, \pi_D], \quad D = K[\omega, \pi_D].$$

Thus D is obtained by adjoining the element π_D to any of its inertia fields $K(\omega)$, or equivalently, by adjoining ω to the field $K(\pi_D)$. Note that ω and π_D do *not* commute, unless $n = 1$.

The inertia field $K(\omega)$ is uniquely determined up to K -isomorphism by the index n , and our next task is to improve our choice of the prime element π_D .

(14.5) THEOREM. *Let $\omega \in D$ be a primitive $(q^n - 1)$ th root of 1, and let π be any prime element of R . Then there exists a prime element $\pi_D \in \Delta$ such that*

$$\pi_D^n = \pi, \quad \pi_D \omega \pi_D^{-1} = \omega^q,$$

where r is a positive integer such that $1 \leq r \leq n$, $(r, n) = 1$. The integer r is uniquely determined by D , and does not depend upon the choice of ω or π .

Proof. By Exercise 14.2, there exists a nonzero $\alpha \in D$ such that

$$\alpha\omega\alpha^{-1} = \omega^q.$$

Replacing α by $\pi^l\alpha$ if need be, we may assume that $\alpha \in \Delta$. Now let $v_D(\alpha) = k$, and put $h = n/(k, n)$. Then

$$\alpha^h = \varepsilon \cdot \pi^b, \quad \varepsilon \in u(\Delta), \quad b \in \mathbf{Z},$$

and h is the least positive integer for which such an expression for α^h is possible. Then

$$\omega^{q^h} = \alpha^h \cdot \omega \cdot \alpha^{-h} = \varepsilon \cdot \omega \cdot \varepsilon^{-1} \equiv \omega \pmod{\mathfrak{p}},$$

since $\bar{\Delta} = \Delta/\mathfrak{p}$ is a field. But $\bar{\omega}$ is a primitive $(q^n - 1)$ th root of 1 in $\bar{\Delta}$, whence $n = h$, and so $(k, n) = 1$. Now choose $r, t \in \mathbf{Z}$ with $kr - nt = 1$, $1 \leq r \leq n$, so surely $(r, n) = 1$. Setting

$$\pi_D = \pi^{-t}\alpha^r,$$

we have

$$v_D(\pi_D) = rv_D(\alpha) - tv_D(\pi) = rk - tn = 1,$$

so π_D is indeed a prime element of Δ . Furthermore,

$$\pi_D \cdot \omega \cdot \pi_D^{-1} = \alpha^r \cdot \omega \cdot \alpha^{-r} = \omega^{qr}.$$

Therefore π_D^n commutes with ω , and certainly also commutes with π_D . Thus π_D^n lies in the center of D , and is then obviously a prime element of R .

We do not know at this point that π_D^n equals a *preassigned* prime element π of R , and we show next that we can modify the above π_D so as to accomplish this. For any $\lambda \in u(o_W)$, $\lambda\pi_D$ is also a prime element of Δ , and

$$(\lambda\pi_D) \cdot \omega \cdot (\lambda\pi_D)^{-1} = \lambda \cdot \omega^{qr} \cdot \lambda^{-1} = \omega^{qr},$$

since λ lies in the inertia field $K(\omega)$. It remains to prove that λ may be chosen so that $(\lambda\pi_D)^n = \pi$. Now the Galois group $\text{Gal}(W/K)$ is cyclic of order n , generated by the automorphism $\sigma: \omega \rightarrow \omega^q$. Since $(r, n) = 1$, the automorphism $\rho: \omega \rightarrow \omega^{qr}$ also generates this Galois group. But $\rho(x) = \pi_D x \pi_D^{-1}$, $x \in W$. Therefore by Exercise 1.4,

$$\begin{aligned} N_{W/K}x &= x \cdot \pi_D x \pi_D^{-1} \cdot \pi_D^2 x \pi_D^{-2} \cdots \pi_D^{n-1} x \pi_D^{-(n-1)} \\ &= (x\pi_D)^n \cdot \pi_D^{-n}, \quad x \in W. \end{aligned}$$

This shows that for each $\lambda \in u(o_W)$,

$$(\lambda\pi_D)^n = (N_{W/K}\lambda) \cdot \pi_D^n.$$

Now any preassigned prime element π of R is expressible as $\pi = \beta \cdot \pi_D^n$ for some $\beta \in u(R)$. By (14.1) we may choose $\lambda \in u(o_W)$ such that $N_{W/K}\lambda = \beta$. Therefore $(\lambda\pi_D)^n = \pi$, as desired.

Finally, we prove the uniqueness of r . To begin with, if ω' is another primitive $(q^n - 1)$ th root of 1 in D , then there exists a nonzero $\beta \in D$ such that $\omega' = \beta\omega^t\beta^{-1}$ for some t . Let $\pi'_D = \beta\pi_D\beta^{-1}$, another prime element of Δ . Then we have

$$(\pi'_D)^n = \beta\pi\beta^{-1} = \pi, \quad \pi'_D \omega' \pi'^{-1} = \beta \cdot \omega^{tq^r} \cdot \beta^{-1} = (\omega')^{qr},$$

so the choice of r does not depend on which root of unity is used. We must still show that r does not depend on the choice of the prime element π_D . Let π' be any prime element of Δ , and suppose that

$$\pi' \cdot \omega \cdot \pi'^{-1} = \omega^{qs}$$

for some s between 1 and n . We may write $\pi' = \gamma\pi_D$ with $\gamma \in u(\Delta)$, and then

$$\omega^{qs} = \gamma\pi_D \cdot \omega \cdot (\gamma\pi_D)^{-1} = \gamma \cdot \omega^{qr} \cdot \gamma^{-1}.$$

Passing to $\bar{\Delta}$ we obtain the equality $\bar{\omega}^{qs} = \bar{\omega}^{qr}$. Therefore $s = r$, since $\bar{\omega}$ is a primitive $(q^n - 1)$ th root of unity. This completes the proof of the theorem.

The above shows that once the complete field K is given, the skewfield D is completely determined by its index n , and by the integer r . Indeed, we first form the field $K(\omega)$, with ω any primitive $(q^n - 1)$ th root of 1. Then we pick any prime $\pi \in R$, and adjoin to the field W an element π_D satisfying the conditions listed in (14.5). This determines the skewfield $D = K(\omega, \pi_D)$ up to K -isomorphism. We call the fraction r/n the *Hasse invariant*[†] of D .

We are still left with the problem of deciding whether each fraction r/n arises from some skewfield.

(14.6) THEOREM. *Let $1 \leq r \leq n$, $(r, n) = 1$. Given the complete field K , there exists a skewfield D with center K , index n , and Hasse invariant r/n .*

Proof. Let $W = K(\omega)$, where ω is a primitive $(q^n - 1)$ th root of 1. If there is such a skewfield D with the desired properties, then W must be a maximal subfield of D , and hence W splits D . Therefore $W \otimes_K D \cong M_n(W)$, and hence each element $d \in D$ is representable by a matrix $d^* \in M_n(W)$. We will therefore try to find a set of matrices in $M_n(W)$ which constitute a skewfield having the desired properties.

Let θ be the automorphism of W for which $\theta(\omega) = \omega^{qr}$, and let π be a prime element of R . For $\alpha \in W$, define

$$\alpha^* = \begin{bmatrix} \alpha & 0 & 0 & \dots & 0 \\ 0 & \theta(\alpha) & 0 & \dots & 0 \\ 0 & 0 & \theta^2(\alpha) & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \theta^{n-1}(\alpha) \end{bmatrix}, \quad \pi_D^* = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ \pi & 0 & 0 & \dots & 0 \end{bmatrix}.$$

The map $\alpha \mapsto \alpha^*$, $\alpha \in W$, gives a K -isomorphism of W onto the field $W^* = K(\omega^*) \subset M_n(K)$, where we identify each $\lambda \in K$ with the scalar matrix $\lambda I_n \in M_n(K)$. It is easily checked that

$$(\pi_D^*)^n = \pi I_n, \quad \pi_D^* \cdot \omega^* \cdot (\pi_D^*)^{-1} = (\omega^*)^{qr}.$$

We now set

$$D = K[\omega^*, \pi_D^*] = \sum_{i,j=0}^{n-1} K(\omega^*)^i (\pi_D^*)^j,$$

[†] Later on, we shall call the fraction r'/n the Hasse invariant of D , where $r' \in \mathbb{Z}$ is chosen so that $rr' \equiv 1 \pmod{n}$, $1 \leq r' \leq n$.

a K -subalgebra of $M_n(W)$. We shall verify that D is the desired skewfield.

Each element $a \in D$ is expressible as a K -linear combination of the n^2 elements $\{(\omega^*)^i \cdot (\pi_D^*)^j\}$. Since $(\omega^*)^i = (\omega^i)^*$, it follows that a is expressible in the form

$$a = \sum_{j=0}^{n-1} \alpha_j^* (\pi_D^*)^j, \quad \alpha_j \in W.$$

Since

$$(\pi_D^*)^j = \begin{bmatrix} 0 & I_{n-j} \\ \pi I_j & 0 \end{bmatrix},$$

we obtain

$$(14.7) \quad a = \begin{bmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} \\ \pi\theta(\alpha_{n-1}) & \theta(\alpha_0) & \theta(\alpha_1) & \dots & \theta(\alpha_{n-2}) \\ \pi\theta^2(\alpha_{n-2}) & \pi\theta^2(\alpha_{n-1}) & \theta^2(\alpha_0) & \dots & \theta^2(\alpha_{n-3}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \pi\theta^{n-2}(\alpha_2) & \pi\theta^{n-2}(\alpha_3) & \pi\theta^{n-2}(\alpha_4) & \dots & \theta^{n-2}(\alpha_1) \\ \pi\theta^{n-1}(\alpha_1) & \pi\theta^{n-1}(\alpha_2) & \pi\theta^{n-1}(\alpha_3) & \dots & \theta^{n-1}(\alpha_0) \end{bmatrix}.$$

Hence if $a = 0$, then each $\alpha_i = 0$. This shows that D is a vector space over W with basis $\{(\pi_D^*)^j : 0 \leq j \leq n-1\}$, and therefore $(D:K) = n^2$.

Next suppose that $a \in D$ is a zero divisor, but that $a \neq 0$. Let a be given as above; after replacing a by $\pi^l a$ with suitable l , we may assume that each $\alpha_j \in o_W$, and that at least one α_j is a unit in o_W . (This depends on the observation that π is also a prime element for o_W .) Now (by Exercise 1.4),

$$\det a \equiv N_{W/K} \alpha_0 \pmod{\pi o_W}.$$

But $\det a = 0$, since a is a zero divisor in D . Therefore $N_{W/K} \alpha_0 \in \pi o_W \cap R$, whence α_0 is not a unit in o_W . Hence we may write $\alpha_0 = \pi \beta_0$ for some $\beta_0 \in o_W$. But then

$$\det a \equiv \pi \cdot N_{W/K} \alpha_1 \pmod{\pi^2 o_W},$$

so also $\alpha_1 = \pi \beta_1$ for some $\beta_1 \in o_W$. Continuing in this way, it follows that each α_j is a multiple of π , which is a contradiction. This proves that D has no zero divisors except 0. Hence for each nonzero $a \in D$, the K -homomorphism $x \rightarrow ax$, $x \in D$, is monic. Since $(D:K)$ is finite, this shows that $D = aD = Da$ for each nonzero $a \in D$, and hence D is a skewfield.

Observe next that W^* is a subfield of D , and that $(W^*:K) = n$. If $a \in D$ commutes with ω^* , then since the diagonal entries $\omega, \theta(\omega), \dots, \theta^{n-1}(\omega)$ of ω^* are pairwise distinct, it follows that a is a diagonal matrix. Hence by

(14.7) we have $a \in W^*$, and so we have shown that W^* is a maximal subfield of D . On the other hand, if a also commutes with π_D^* , then writing $a = \alpha_0^*$ with $\alpha_0 \in W$, it follows at once that $\theta(\alpha_0) = \alpha_0$. Hence $\alpha_0 \in K$, and $a = uI_n$ for some $u \in K$, which shows that K is the center of D . Finally, the equation $(\pi_D^*)^n = \pi I_n$ proves that π_D^* is a prime element for D . Thus D is a skewfield with Hasse invariant r/n , as claimed.

We shall conclude this section by calculating the discriminant $d(\Delta/R)$ of the R -order Δ (see §10) as well as the *different* $\mathfrak{D} = \mathfrak{D}(\Delta/R)$, defined below. To begin with, let $\text{tr}: D \rightarrow K$ be the reduced trace map, and let $\tau: D \times D \rightarrow K$ be the trace form given by $\tau(a, b) = \text{tr}(ab)$, $a, b \in D$. By (9.8), τ is a symmetric nondegenerate associative bilinear form. We may then define

$$\tilde{\Delta} = \{x \in D: \tau(x, \Delta) \subset R\} = \{x \in D: \text{tr}(x\Delta) \subset R\},$$

By Exercise 4.12, $\tilde{\Delta}$ is a full R -lattice in D , and is clearly a two-sided Δ -module. Since $\pi_D^r \tilde{\Delta} \subset \Delta$ for some r , it follows from (13.2) that

$$\tilde{\Delta} = \pi_D^{-m} \cdot \Delta$$

for some integer m , and $m \geq 0$ since $\tilde{\Delta} \supset \Delta$. Call $\tilde{\Delta}$ the *inverse different*, and define the *different* as

$$\mathfrak{D} = \mathfrak{D}(\Delta/R) = \pi_D^m \cdot \Delta.$$

For a nonzero ideal $L = \pi_D^t \Delta$ of Δ , define the *norm*

$$N_{D/K} L = \text{ord}_R(\Delta/L),$$

where ord_R is the R -order ideal (see §4a). We have, as in (4.31 iii),

$$\text{ord}_R(\Delta/\pi_D^t \Delta) = \{\text{ord}_R(\Delta/\pi_D \Delta)\}^t = P^{nt},$$

since $(\tilde{\Delta}: \bar{R}) = n$ in this case. Therefore

$$N_{D/K}(\pi_D^t \Delta) = (N_{D/K} \pi_D)^t \cdot R, \quad N_{D/K} \mathfrak{p} = P^n.$$

(14.8) LEMMA. $d(\Delta/R) = N_{D/K}(\mathfrak{D}(\Delta/R))$.

Proof. Keeping the above notation, we observe that left multiplication by π_D^m gives an R -isomorphism

$$\tilde{\Delta}/\Delta \cong \Delta/\mathfrak{D}.$$

Therefore

$$N_{D/K}(\mathfrak{D}) = \text{ord}_R(\Delta/\mathfrak{D}) = \text{ord}_R(\tilde{\Delta}/\Delta).$$

Now we imitate the proof of (4.35). We may write

$$\Delta = \sum R x_i, \quad \tilde{\Delta} = \sum R y_j, \quad \text{where } \text{tr}(x_i y_j) = \delta_{ij},$$

and the subscripts i, j range from 1 to n^2 . Set $x_i = \sum a_{ij}y_j$, $a_{ij} \in K$. Then $a_{ij} = \text{tr}(x_i x_j)$, and so by Exercise 4.2 we have

$$\text{ord}_R(\tilde{\Delta}/\Delta) = R \cdot \det(a_{ij}) = d(\Delta/R),$$

as claimed.

Let us now calculate $\mathfrak{D}(\Delta/R)$ and $d(\Delta/R)$ explicitly.

(14.9) **Theorem.** *We have*

$$\mathfrak{D}(\Delta/R) = \pi_D^{n-1} \Delta, \quad d(\Delta/R) = P^{n(n-1)}.$$

Proof. The formula for the discriminant follows from that for the different, by taking norms. Let us write $\tilde{\Delta} = \pi_D^{-m} \Delta$; then m is maximal such that $\text{tr } \pi_D^{-m} \Delta \subset R$. Hence we need only show that

$$\text{tr}(\pi_D^{-(n-1)} \Delta) \subset R, \quad \text{tr}(\pi_D^{-n} \Delta) \notin R.$$

Suppose π_D chosen as in (14.5), so that $\pi_D^n = \pi$. Since

$$\Delta = \sum_{j=0}^{n-1} o_W \cdot (\pi_D)^j,$$

we have

$$\pi^{-(n-1)} \Delta = \pi^{-1} \cdot \pi_D \Delta = \sum_{j=1}^{n-1} (\pi^{-1} o_W) \cdot (\pi_D)^j \oplus o_W.$$

Let $a \in D$; to compute $\text{tr } a$, we may use the isomorphism $W \otimes_K D \cong M_n(W)$ to represent $1 \otimes a$ as an element of $M_n(W)$, and then take the trace of the matrix thus obtained. But the isomorphism $W \otimes_K D \cong M_n(W)$ has been exhibited explicitly in (14.7), and hence

$$\text{tr} \left(\sum_{j=0}^{n-1} \alpha_j (\pi_D)^j \right) = T_{W/K} \alpha_0, \quad \alpha_j \in W.$$

Hence we have at once

$$\text{tr}(\pi_D^{-(n-1)} \Delta) = T_{W/K}(o_W) \subset R.$$

On the other hand, if $\text{tr}(\pi_D^{-n} \Delta) \subset R$, then the above argument gives $T_{W/K}(\pi^{-1} o_W) \subset R$, whence $T_{W/K}(o_W) \subset \pi R$. If \bar{T} denotes the trace map from \bar{o}_W to \bar{R} , then since the Galois groups of W/K and \bar{o}_W/\bar{R} are isomorphic, it follows that for each $\lambda \in \bar{o}_W$, $\bar{T}(\bar{\lambda})$ is the image of $T_{W/K}(\lambda)$. We may thus conclude that \bar{T} is the zero map, which contradicts the fact that \bar{o}_W is separable over \bar{R} . This proves that $\text{tr}(\pi_D^{-n} \Delta) \notin R$, and establishes the theorem.

EXERCISES

1. Let D be a skewfield whose center K is infinite. Let $a \in D - K$, $f(X) = \min. \text{pol}_K a$. Show that there are infinitely many elements $a' \in D$ such that $f(a') = 0$. [Hint: For each nonzero $x \in D$, $f(xax^{-1}) = 0$. Since $a \notin K$, there exists an element $y \in D$ which does not commute with a ; the same holds for each $y + \alpha$, $\alpha \in K$. If

$$(y + \alpha)a(y + \alpha)^{-1} = (y + \beta)a(y + \beta)^{-1}, \quad \alpha, \beta \in K, \quad \alpha \neq \beta,$$

then setting $z = y + \beta$, it follows that $z^{-1}(z + \alpha - \beta)$ commutes with a . Hence z commutes with a , a contradiction. Thus $\{(y + \alpha)a(y + \alpha)^{-1} : \alpha \in K\}$ is an infinite set of zeros of $f(X)$].

2. Keep the notation of (14.4) and the discussion preceding it. Show that for each i , $0 \leq i \leq f - 1$, ω^{q^i} is conjugate to ω in D .

3. Let K be the 2-adic completion of the rational field, R its ring of 2-adic integers, and v_K the valuation on K . Let $D = K \oplus Ki \oplus Kj \oplus Kk$ (quaternions over K), and set

$$\Lambda = R + Ri + Rj + Rk + Ra, \quad a = (1 + i + j + k)/2.$$

Show how to extend v_K to a valuation on D , and prove that Λ is its valuation ring. Find the discriminant of Λ , and compute $e(D/K)$, $f(D/K)$, a prime element π_D , the residue class field $\bar{\Delta}$, an R -basis for Δ , and the inertia fields of D over K .

4. Let K be the 3-adic completion of \mathbb{Q} . Show that there exists an element $a \in K$ with $a^2 = -2$. Let $\Phi_4(X) = X^4 + 1$, the cyclotomic polynomial of order 4. Show that

$$\Phi_4(X) = (X^2 - aX - 1)(X^2 + aX - 1) \quad \text{in } K[X],$$

and that each quadratic factor is irreducible in $K[X]$. Let ω be a zero of the first factor in some extension field of K . Prove that ω is a primitive 8th root of unity, and that

$$X^2 - aX - 1 = (X - \omega)(X - \omega^3),$$

$$X^2 + aX - 1 = (X - \omega^5)(X - \omega^7).$$

5. Keeping the notation of (14.5), let W be an inertia field for D . Prove that

$$\text{nr}_{D/K}(\pi_D) = (-1)^{n-1}\pi, \quad \text{nr}_{D/K}(\alpha) = N_{W/K}(\alpha), \quad \alpha \in W.$$

[Hint: Since $X^n - \pi$ is irreducible in $K[X]$ by Exercise 5.1, it follows that $\min. \text{pol}_K \pi_D = X^n - \pi$. But then

$$\text{red. char. pol.}_{D/K} \pi_D = \min. \text{pol}_K \pi_D,$$

by Exercise 9.1. This gives the desired formula for $\text{nr}(\pi_D)$. Next, let $\alpha \in W$ and let $f(X) = \min. \text{pol}_K \alpha$. By Exercise 9.1,

$$\text{red. char. pol.}_{D/K} \alpha = \{f(X)\}^{(W:K(\alpha))}.$$

But also

$$\text{char. pol.}_{W/K} \alpha = \{f(X)\}^{(W:K(\alpha))}$$

(compare degrees !), whence

$$\text{red. char. pol.}_{D/K} \alpha = \text{char. pol.}_{W/K} \alpha, \quad \alpha \in W.$$

This yields the formula for $\text{nr}(\alpha)$.

Another proof can be given by using the matrix representation of π_D and α ($\alpha \in W$) occurring in the proof of (14.6). Then

$$\text{nr}_{D/K} \pi_D = \det \pi_D^* = (-1)^{n-1} \pi,$$

$$\text{nr}_{D/K} \alpha = \det \alpha^* = \prod_{i=0}^{n-1} \theta^i(\alpha) = N_{W/K} \alpha.]$$

6. Let D be a skewfield whose center K is complete with respect to a discrete valuation, with a finite residue class field \bar{R} (as in §14). Let

$$\text{nr } D = \{\text{nr}_{D/K}(d) : d \in D\}.$$

Prove that $\text{nr } D = K$. [Hint: Use the notation and results of the preceding exercise. Then

$$\text{nr } D \supset N_{W/K}(W) = \{x \in K : n | v_K(x)\},$$

by (14.1). But $\text{nr } D$ also contains $(-1)^{n-1} \pi$, whence $\text{nr } D = K$.]

4. Morita Equivalence

We shall need to study the relationship between Λ -modules and $M_n(\Lambda)$ -modules, where as usual $M_n(\Lambda)$ is the ring of all $n \times n$ matrices over the ring Λ . The generalization of this relationship leads to the concept of Morita equivalence, and we sketch here some of the main results of this theory. As references, we cite Bass [1], P. M. Cohn [1], Faith [1]. While the general theory holds for abelian categories, we shall make the simplifying assumption that our categories are in fact categories of modules. Denote by \mathcal{M}_Λ the category of right Λ -modules, by ${}_\Lambda\mathcal{M}_\Lambda$ the category of (Λ, Λ) -bimodules, and so on.

15. PROGENERATORS

We shall use the notation of §2b. Let \mathcal{A} be a category with objects A, A', \dots , and \mathcal{B} a category with objects B, B', \dots . We shall write $A \in \mathcal{A}$ to indicate that A is an object in \mathcal{A} . All functors $F: \mathcal{A} \rightarrow \mathcal{B}$ considered below are assumed to be additive. Unless otherwise stated, functors are taken to be covariant.

Let $F: \mathcal{A} \rightarrow \mathcal{B}$ and $G: \mathcal{A} \rightarrow \mathcal{B}$ be a pair of functors. A *natural transformation* $t: F \rightarrow G$ is a family

$$t = \{t_A: A \in \mathcal{A}\},$$

where for each $A \in \mathcal{A}$,

$$t_A \in \text{Hom}_{\mathcal{B}}(FA, GA),$$

and where for each $\alpha \in \text{Hom}(A, A')$, the diagram

$$\begin{array}{ccc} FA & \xrightarrow{t_A} & GA \\ F\alpha \downarrow & & \downarrow G\alpha \\ FA' & \xrightarrow{t_{A'}} & GA' \end{array}$$

is commutative. If furthermore each t_A is an isomorphism, we call the functors F and G *naturally equivalent*, and write $F \sim G$.

Example. Let $\mathcal{A} = \mathcal{B} = {}_\Lambda\mathcal{M}$, F the identity functor, G the functor $\Lambda \otimes_\Lambda \cdot$. For each $A \in \mathcal{A}$, let $t_A: A \rightarrow \Lambda \otimes_\Lambda A$ be the left Λ -isomorphism given in (2.8). Then t is a natural equivalence from F to G .

Let $\text{id}_{\mathcal{A}}$ be the identity functor on \mathcal{A} . Two categories \mathcal{A} and \mathcal{B} are called *equivalent* if there exist functors F, G :

$$\mathcal{A} \begin{array}{c} \xrightarrow{F} \\ \xleftarrow{G} \end{array} \mathcal{B}$$

such that $GF \sim \text{id}_{\mathcal{A}}$ and $FG \sim \text{id}_{\mathcal{B}}$. For example, if Λ° denotes the opposite ring of Λ (same elements, but multiplication is reversed), then the categories ${}_\Lambda\mathcal{M}$ and ${}_{\Lambda^\circ}\mathcal{M}$ are equivalent.

Now let $F: \mathcal{A} \rightarrow \mathcal{B}$ be any functor. Call F *faithful* if the map

$$(15.1) \quad \alpha \in \text{Hom}(A, A') \rightarrow F\alpha \in \text{Hom}(FA, FA')$$

is injective, that is, if $F\alpha = 0$ implies that $\alpha = 0$. For example, if M is a faithfully flat right Λ -module, then the functor $M \otimes_{\Lambda} \cdot : {}_\Lambda\mathcal{M} \rightarrow \mathcal{A}$ is faithful (see (2.21)).

On the other hand, the functor $F: \mathcal{A} \rightarrow \mathcal{B}$ is *full* if the map in (15.1) is surjective, that is, if each $\beta \in \text{Hom}(FA, FA')$ equals some $F\alpha$. For example, let $\bar{\Lambda} = \Lambda/I$ where I is a two-sided ideal of Λ . Let \mathcal{A} be the category of projective left Λ -modules, \mathcal{B} the corresponding category for $\bar{\Lambda}$, and let $F: \mathcal{A} \rightarrow \mathcal{B}$ be given by $F(M) = M/IM$. Then F is a full functor, since each $\bar{\Lambda}$ -homomorphism $\beta: M/IM \rightarrow N/IN$, where $M, N \in \mathcal{A}$, can be lifted to a Λ -homomorphism $\alpha: M \rightarrow N$, and thus $\beta = F\alpha$.

We recall from (2.14) that an object $X \in \mathcal{A}$ is *projective* if the functor

$$\text{Hom}(X, \cdot) : \mathcal{A} \rightarrow \mathcal{A}$$

is exact. This functor carries $A \in \mathcal{A}$ onto the abelian group $\text{Hom}(X, A)$, and takes each $\alpha \in \text{Hom}(A, A')$ onto

$$\alpha_* : \text{Hom}(X, A) \rightarrow \text{Hom}(X, A'),$$

where $\alpha_* f = \alpha f$, $f \in \text{Hom}(X, A)$.

Whether or not X is projective, let us consider the functor $\text{Hom}(X, \cdot)$. We call X a *generator* of the category \mathcal{A} if $\text{Hom}(X, \cdot)$ is a faithful functor, that is, if $\alpha_* = 0$ implies that $\alpha = 0$. In other words, X is a generator if and only if for each nonzero $\alpha: A \rightarrow A'$ there exists an $f: X \rightarrow A$ such that $\alpha f \neq 0$.

Dually, $X \in \mathcal{A}$ is *injective* if the contravariant functor $\text{Hom}(\cdot, X)$ is exact, while X is a *cogenerator* for \mathcal{A} if $\text{Hom}(\cdot, X)$ is faithful.

(15.2) **THEOREM.** *An object X in the category \mathcal{A} is a generator for \mathcal{A} if and only if every $A \in \mathcal{A}$ is a quotient of a direct sum of copies of X .*

Proof. Let X be a generator, and let $A \in \mathcal{A}$. For each $f \in \text{Hom}(X, A)$, let X_f be a copy of X , and set $Y = \sum_j X_j$. Each X_f maps into A (by means of f),

so there is a map $\eta: Y \rightarrow A$, defined by $\eta = \sum f$. Thus

$$\eta(\sum x_f) = \sum f(x_f), \quad x_f \in X_f.$$

Clearly

$$(15.3) \quad \text{im } \eta = \sum_{f \in \text{Hom}(X, A)} f(X) \subset A.$$

Let us show that $\text{im } \eta = A$; if not, there exists a nonzero map

$$\alpha: A \rightarrow A/\text{im } \eta.$$

Since X is a generator, there must be an $f: X \rightarrow A$ such that $\alpha f \neq 0$. But $(\alpha f)X = \alpha(f(X)) = 0$, since $f(X) \subset \text{im } \eta$. This gives a contradiction, and shows that η is an epimorphism of Y onto A . Therefore A is a quotient of a direct sum of copies of X , as claimed.

Conversely, suppose that for each $A \in \mathcal{A}$ there is an epimorphism $\xi: \sum X_i \rightarrow A$, where each X_i is a copy of X . We must show that X is a generator for \mathcal{A} . Let $\alpha: A \rightarrow A'$ be nonzero; then also $\alpha\xi \neq 0$, since ξ is epic. If we write $\xi = \sum \xi_i$, where $\xi_i: X_i \rightarrow A$, then $\alpha\xi = \sum \alpha\xi_i$. Therefore $\alpha\xi_i \neq 0$ for some i . But $X_i \cong X$, and so there exists an $f: X \rightarrow A$ such that $\alpha f \neq 0$. This proves that X is a generator for \mathcal{A} , as desired.

The construction in (15.3) is of special importance in the following circumstance. Let $X \in {}_\Lambda \mathcal{M}$, and define the *trace ideal* of X as

$$(15.4) \quad \text{trace } X = \sum_{f \in \text{Hom}_\Lambda(X, \Lambda)} f(X) \subset \Lambda.$$

It is easily verified that $\text{trace } X$ is a two-sided ideal of Λ .

(15.5) COROLLARY. *The left Λ -module X is a generator for ${}_\Lambda \mathcal{M}$ if and only if $\text{trace } X = \Lambda$.*

Proof. If $\text{trace } X = \Lambda$, then the proof of the preceding theorem shows that Λ is a quotient module of $\sum X_i$, where each $X_i \cong X$. But every Λ -module A is a quotient of a direct sum $\sum \Lambda_j$, with each $\Lambda_j \cong \Lambda$. Hence A is also a quotient of a direct sum of copies of X , whence X is a generator for ${}_\Lambda \mathcal{M}$ by (15.2).

Suppose conversely that X is a generator. The proof of (15.2) shows that $\text{im } \eta = A$ in (15.3), where A is any Λ -module. Taking $A = {}_\Lambda \Lambda$, we see that the trace ideal of X equals $\text{im } \eta$, and thus coincides with Λ as claimed.

It is clear from (15.2), or directly from the definition of generator, that Λ is itself a generator for the category ${}_\Lambda \mathcal{M}$. Indeed, every nonzero free module is a generator.

Given a possibly infinite family $\{X_\lambda\}$ of objects in \mathcal{A} , we may form their

direct sum $\sum X_\lambda$. There are the usual injection maps $\{i_\lambda\}$ and projection maps $\{p_\lambda\}$, with

$$X_\lambda \xrightarrow[p_\lambda]{i_\lambda} \sum_v X_v.$$

We shall say that a functor $F: \mathcal{A} \rightarrow \mathcal{B}$ preserves direct sums if for each family $\{X_\lambda\}$, there is an isomorphism

$$F\left(\sum_v X_v\right) \cong \sum_v FX_v,$$

induced by the maps $\{Fi_\lambda, Fp_\lambda\}$. For example, tensor product functors preserve direct sums. So also does the functor $\text{Hom}_\Lambda(P, \cdot)$, where P is any finitely generated projective Λ -module (see Exercise 15.3).

(15.6) THEOREM. *Let $F: \mathcal{A} \rightarrow \mathcal{B}$ and $G: \mathcal{A} \rightarrow \mathcal{B}$ be a pair of right exact functors which preserve direct sums. Let $t: F \rightarrow G$ be a natural transformation, and let X be a generator for \mathcal{A} . If $t_X: FX \cong GX$ is an isomorphism in the category \mathcal{B} , then t is a natural equivalence of functors.*

Proof. Since $t = \{t_A: A \in \mathcal{A}\}$ is a natural transformation, each $\alpha: A \rightarrow A'$ gives rise to a commutative diagram

$$\begin{array}{ccc} FA & \xrightarrow{F\alpha} & FA' \\ t_A \downarrow & & \downarrow t_{A'} \\ GA & \xrightarrow{G\alpha} & GA'. \end{array}$$

We are assuming that t_X is an isomorphism, and are trying to prove that each t_A is an isomorphism.

Since X is a generator of \mathcal{A} , each $A \in \mathcal{A}$ is a quotient of a direct sum $\sum X$ of copies of X . Hence there is an \mathcal{A} -exact sequence

$$U \rightarrow V \rightarrow A \rightarrow 0, \quad \text{where } U = \sum X, \quad V = \sum X.$$

But F is right exact, and so the sequence

$$FU \rightarrow FV \rightarrow FA \rightarrow 0$$

is \mathcal{B} -exact. Hence there is a commutative diagram with exact rows:

$$\begin{array}{ccccccc} FU & \longrightarrow & FV & \longrightarrow & FA & \longrightarrow & 0 \\ t_U \downarrow & & t_V \downarrow & & t_A \downarrow & & \\ GU & \longrightarrow & GV & \longrightarrow & GA & \longrightarrow & 0. \end{array}$$

Now $FU \cong \sum FX$, $GU \cong \sum GX$, because F and G preserve direct sums by hypothesis. Since $t_X: FX \cong GX$, it follows that $t_U: FU \cong GU$. Likewise t_V is an isomorphism, and the commutativity of the above diagram shows that t_A is also an isomorphism, as desired.

An object $P \in \mathcal{A}$ is *faithfully projective* if it satisfies the following three conditions:

- (i) P is a projective object in \mathcal{A} .
- (ii) P is a generator for \mathcal{A} .
- (iii) $\text{Hom}(P, \cdot)$ preserves direct sums.

In particular, considering the category ${}_{\Lambda}\mathcal{M}$, we call a left Λ -module P a *progenerator* for ${}_{\Lambda}\mathcal{M}$ if

- (i) P is a finitely generated projective Λ -module, and
- (ii) P is a generator for ${}_{\Lambda}\mathcal{M}$.

Note each such P is faithfully projective, since by Exercise 15.3 $\text{Hom}(P, \cdot)$ necessarily preserves direct sums.

(15.7) THEOREM. *Let P be a faithfully projective object in the category \mathcal{A} , and let*

$$\Lambda = \text{Hom}_{\mathcal{A}}(P, P), \quad \mathcal{B} = {}_{\Lambda}\mathcal{M}.$$

View P as right Λ -module. Then the functor

$$\text{Hom}(P, \cdot) : \mathcal{A} \rightarrow \mathcal{B}$$

gives an equivalence of categories.

Proof. It is clear that Λ is a ring, and that P can be viewed as a right Λ -module. Then for each $A \in \mathcal{A}$, $\text{Hom}_{\mathcal{A}}(P, A)$ is a left Λ -module. Thus the functor $F : \mathcal{A} \rightarrow \mathcal{B}$, given by $F(A) = \text{Hom}(P, A)$, is well defined. Clearly $FP = \Lambda$. Since P is a projective object, the functor F is exact.

In order to show that F is a category equivalence, we use the result of Exercise 15.2. We show first that F is full and faithful, that is, for each pair $A, A' \in \mathcal{A}$, the map

$$(15.8) \quad F : \text{Hom}(A, A') \rightarrow \text{Hom}(FA, FA')$$

given by $\alpha \mapsto F\alpha$, is an isomorphism. Let us first verify this when $A = \sum P_{\lambda}$, where each $P_{\lambda} \cong P$. By (2.7)

$$\text{Hom}(A, A') \cong \prod \text{Hom}(P_{\lambda}, A') \cong \prod_{\lambda} FA',$$

the latter because $\text{Hom}(P_{\lambda}, A') \cong \text{Hom}(P, A') = FA'$. On the other hand, F preserves direct sums since P is faithfully projective, and thus

$$\text{Hom}_{\Lambda}(FA, FA') \cong \text{Hom}_{\Lambda}(\sum FP_{\lambda}, FA') \cong \prod_{\lambda} \text{Hom}_{\Lambda}(\Lambda, FA') \cong \prod_{\lambda} FA'.$$

We have now shown that the map F in (15.8) is an isomorphism whenever A is a direct sum of copies of P .

Now let A and A' be arbitrary, and let

$$U \rightarrow V \rightarrow A \rightarrow 0$$

be an \mathcal{A} -exact sequence in which U and V are direct sums of copies of P . Then the sequence

$$FU \rightarrow FV \rightarrow FA \rightarrow 0$$

is \mathcal{B} -exact, since F is an exact functor. Since Hom is a left exact functor, we obtain a commutative diagram with exact rows

$$\begin{array}{ccccc} 0 \rightarrow \text{Hom}(A, A') & \longrightarrow & \text{Hom}(V, A') & \longrightarrow & \text{Hom}(U, A') \\ & \downarrow F_1 & \downarrow F_2 & & \downarrow F_3 \\ 0 \rightarrow \text{Hom}(FA, FA') & \rightarrow & \text{Hom}(FV, FA') & \rightarrow & \text{Hom}(FU, FA'). \end{array}$$

By the preceding paragraph, both F_2 and F_3 are isomorphisms. Hence so is F_1 , and this completes the proof that $F: \mathcal{A} \rightarrow \mathcal{B}$ is a full and faithful functor. (For another proof see Exercise 15.6.)

In order to deduce that F gives an equivalence of categories, it remains for us to show that every left Λ -module M is of the form FA for some $A \in \mathcal{A}$. Let us first write a Λ -exact sequence

$$X_1 \xrightarrow{\xi} X_0 \rightarrow M \rightarrow 0, \quad X_0, X_1 \quad \Lambda\text{-free.}$$

Since $\Lambda = F(P)$, we may write $X_i = F(U_i)$, with U_i a direct sum of copies of P , $i = 0, 1$. By the preceding paragraphs,

$$\text{Hom}(X_1, X_0) = \text{Hom}(F(U_1), F(U_0)) \cong \text{Hom}(U_1, U_0),$$

so we have $\xi = F\alpha$ for some $\alpha: U_1 \rightarrow U_0$. Let $A = \text{cok } \alpha$, and apply F to the \mathcal{A} -exact sequence

$$U_1 \xrightarrow{\alpha} U_0 \rightarrow A \rightarrow 0,$$

thus obtaining a Λ -exact sequence

$$X_1 \xrightarrow{\xi} X_0 \rightarrow FA \rightarrow 0.$$

Therefore $M \cong FA$, and the proof of the theorem is complete.

(15.9) Corollary. *Let M be a progenerator for the category ${}_{\Delta}\mathcal{M}$, where Δ is a ring, and let $\Lambda = \text{Hom}_{\Delta}(M, M)$ be the endomorphism ring of M . View M as a bimodule ${}_{\Delta}M_{\Lambda}$. Then there is an equivalence of categories*

$$\text{Hom}_{\Delta}(M, \cdot) : {}_{\Delta}\mathcal{M} \rightarrow {}_{\Lambda}\mathcal{M}.$$

EXERCISES

1. Let $F: \mathcal{A} \rightarrow \mathcal{B}$ be an equivalence of categories. Show that A is projective if and only if FA is projective.
2. Let $F: \mathcal{A} \rightarrow \mathcal{B}$ be a full faithful functor such that every $B \in \mathcal{B}$ is the image FA of some $A \in \mathcal{A}$. Prove that F is a category equivalence.
3. Let P be a finitely generated projective left Λ -module. Show that the functor

$$\mathrm{Hom}_{\Lambda}(P, \cdot) : {}_{\Lambda}\mathcal{M} \rightarrow \mathcal{A}\ell$$

preserves direct sums. [Hint: First check the case where $P = \Lambda$, then use the fact that

$$\mathrm{Hom}_{\Lambda}(P + P', \cdot) \sim \mathrm{Hom}_{\Lambda}(P, \cdot) + \mathrm{Hom}_{\Lambda}(P', \cdot).$$

4. Let ${}_{\Lambda}\mathcal{M} \rightarrow {}_{\Delta}\mathcal{M}$ be an equivalence of categories, where Λ and Δ are rings. Show that Λ is left hereditary if and only if Δ is left hereditary. [Hint: Λ is left hereditary if and only if subobjects of projective objects in ${}_{\Lambda}\mathcal{M}$ are projective.]

5. Let $\mathcal{A}\ell^{\circ}$ denote the category which is opposite to $\mathcal{A}\ell$, that is, $\mathcal{A}\ell^{\circ}$ has the same objects as $\mathcal{A}\ell$, but all arrows are reversed.

(i) Prove that direct products in $\mathcal{A}\ell$ correspond to direct sums in $\mathcal{A}\ell^{\circ}$.

(ii) Given an object A' in a category \mathcal{A} , define a functor $G: \mathcal{A} \rightarrow \mathcal{A}\ell^{\circ}$ by setting

$$G(A) = \{\mathrm{Hom}_{\mathcal{A}}(A, A')\}^{\circ} \in \mathcal{A}\ell^{\circ}, \quad \text{for each } A \in \mathcal{A}.$$

(There is an obvious definition of the action of the functor G on maps in \mathcal{A} .) Prove that G is a right exact covariant functor which preserves direct sums!

6. Use Theorem 15.6 to prove that the map F in (15.8) is an isomorphism. [Hint: Keep the notation of the proof of (15.7), so

$$F(A') = \mathrm{Hom}_{\mathcal{A}}(P, A') \quad \text{for each } A' \in \mathcal{A}.$$

Keeping A' fixed, define functors $G, H: \mathcal{A} \rightarrow \mathcal{A}\ell^{\circ}$ by

$$G(A) = \{\mathrm{Hom}_{\mathcal{A}}(A, A')\}^{\circ}, \quad H(A) = \{\mathrm{Hom}_{\mathcal{B}}(FA, FA')\}^{\circ}, \quad A \in \mathcal{A},$$

with obvious definitions of G and H on maps. Since P is a faithfully projective object in \mathcal{A} , the functor F is exact and preserves direct sums. Use this to prove that H is a right exact covariant functor which preserves direct sums.

The functor $F: \mathcal{A} \rightarrow \mathcal{B}$ determines homomorphisms

$$F_{A, A'} : \mathrm{Hom}_{\mathcal{A}}(A, A') \rightarrow \mathrm{Hom}_{\mathcal{B}}(FA, FA'), \quad A, A' \in \mathcal{A}.$$

For each $A \in \mathcal{A}$, define $t_A: HA \rightarrow GA$ by $t_A = \{F_{A, A'}\}^{\circ}$. Prove that $t: H \rightarrow G$ is a natural transformation.

In order to prove that the map F in (15.8) is an isomorphism, it suffices to establish that each t_A is an isomorphism in $\mathcal{A}\ell^{\circ}$. By (15.6), this will follow once we know that t_p is an isomorphism in $\mathcal{A}\ell^{\circ}$. But this is true since

$$GP = \mathrm{Hom}_{\mathcal{A}}(P, A') = FA'$$

$$HP = \mathrm{Hom}_{\mathcal{B}}(FP, FA') = \mathrm{Hom}_{\Lambda}(\Lambda, FA') \cong FA'.]$$

7. Let P_Δ be a progenerator for \mathcal{M}_Δ , and let $G, H: \mathcal{M}_\Delta \rightarrow \mathcal{A}\ell$ be the covariant functors defined by

$$G(L) = \text{Hom}_\Delta(P, L), \quad H(L) = L \otimes_\Delta P^*, \quad L \in \mathcal{M}_\Delta,$$

where $P^* = \text{Hom}_\Delta(P, \Delta)$ (viewed as left Δ -module). Show that the functors G, H are naturally equivalent. [Hint: Prove

- (i) P^* is a finitely generated projective left Δ -module.
- (ii) The functors G and H are exact, and preserve direct sums.
- (iii) There is a natural transformation $t: H \rightarrow G$, given by

$$t_L: H(L) \rightarrow G(L), \quad L \in \mathcal{M}_\Delta,$$

where t_L is defined by the formula

$$\{t_L(l \otimes \varphi)\}x = l \cdot \varphi(x), \quad l \in L, \quad \varphi \in P^*, \quad x \in P.$$

- (iv) $t_\Delta: H(\Delta) \cong G(\Delta)$.

Then use (15.6).]

16. MORITA CORRESPONDENCE

Let M_Δ be a nonzero right Δ -module, and set

$$(16.1) \quad \Lambda = \text{Hom}_\Delta(M, M), \quad M^* = \text{Hom}_\Delta(M, \Delta).$$

Let Λ act on the left on M , so there is a bimodule structure ${}_\Lambda M_\Delta$. By definition,

$$M^* = \text{Hom}_\Delta({}_\Lambda M_\Delta, {}_\Lambda \Delta_\Delta),$$

the set of all *right* Δ -homomorphisms from M to Δ . The left action of Δ on the bimodule ${}_\Lambda \Delta_\Delta$ enables us to make M^* into a left Δ -module. The left action of Λ on the bimodule ${}_\Lambda M_\Delta$ likewise makes M^* a *right* Λ -module (see §2). It is easily verified that M^* is a bimodule ${}_\Lambda M^* {}_\Lambda$.

We define a map

$$(16.2) \quad \mu: M \otimes_\Delta M^* \rightarrow \Lambda, \quad m \otimes f \mapsto (m, f), \quad \text{where } (m, f)m' = m(fm')$$

for $m, m' \in M, f \in M^*$. Likewise, let

$$(16.3) \quad \tau: M^* \otimes_\Lambda M \rightarrow \Delta, \quad f \otimes m' \mapsto [f, m'], \quad \text{where } [f, m'] = fm'.$$

It is easily checked that μ and τ are well defined, μ is a two-sided Λ -homomorphism, and τ a two-sided Δ -homomorphism. Further, one obtains

$$(16.4) \quad (m, f)m' = m[f, m'], \quad g(m, f) = [g, m]f,$$

for $m, m' \in M, f, g \in M^*$. Finally, we note that

$$(16.5) \quad \text{im } \tau = \text{trace } M_\Delta,$$

where “trace” is defined as in (15.4).

(16.6) *Definition.* A *Morita context* consists of a pair of bimodules ${}_A M_\Delta$, ${}_\Delta N_\Lambda$ relative to rings Δ, Λ , and bimodule maps

$$\mu : M \otimes_\Delta N \rightarrow \Lambda, \quad \tau : N \otimes_\Lambda M \rightarrow \Delta,$$

given symbolically by $\mu(m \otimes n) = (m, n)$, $\tau(n \otimes m) = [n, m]$, interrelated by the formulas

$$(m, n)m' = m[n, m'], \quad n(m, n') = [n, m]n',$$

for all $m, m' \in M$, $n, n' \in N$. If both μ and τ are isomorphisms, we call the rings Δ, Λ *Morita equivalent*.

We have just seen how to construct a Morita context by starting with M_Δ , and defining Λ, M^* by (16.1). We call it the Morita context *derived* from the right Δ -module M . We now proceed to investigate this derived context more fully, keeping the notation of (16.1)–(16.5).

(16.7) **THEOREM.** Let M be a nonzero right Δ -module, and let $\Lambda = \text{Hom}_\Delta(M, M)$. Let

$$\mu : M \otimes_\Delta \text{Hom}_\Delta(M, \Delta) \rightarrow \text{Hom}_\Delta(M, M),$$

$$\tau : \text{Hom}_\Delta(M, \Delta) \otimes_\Lambda M \rightarrow \Delta,$$

be the maps defined in (16.2) and (16.3). Then μ is epic if and only if M is a finitely generated projective right Δ -module; in this case, μ is also monic.

On the other hand, τ is epic if and only if M is a generator of the category \mathcal{M}_Δ ; in this case, τ is also monic.

Finally, μ is epic if and only if $1_\Lambda \in \text{im } \mu$, and τ is epic if and only if $1_\Delta \in \text{im } \tau$.

Proof. The last statement in the theorem is obvious, since $\text{im } \mu$ is a two-sided ideal in Λ , and $\text{im } \tau$ a two-sided ideal in Δ .

The identity map 1_M on M is the identity element 1_Λ . Hence if μ is epic, we may write

$$1_M = \sum_{i=1}^r (m_i, f_i), \quad m_i \in M, \quad f_i \in \text{Hom}_\Delta(M, \Delta).$$

Define right Δ -homomorphisms $\Delta^{(r)} \xrightarrow[\beta]{\alpha} M$ by

$$\alpha(a_1, \dots, a_r) = \sum_1^r m_i a_i, \quad \beta(m) = (f_1 m, \dots, f_r m).$$

It is easily seen that $\alpha\beta = 1_M$, whence $M \mid \Delta^{(r)}$, and thus M_Δ is finitely generated and projective. The argument can be reversed, and thus μ is epic if and only if M_Δ is finitely generated and projective.

Next, $\text{im } \tau = \text{trace } M_\Delta$. Hence by (15.5), τ is epic if and only if M is a

generator for \mathcal{M}_Δ . Finally, μ epic implies μ monic, by Exercise 16.1, and likewise for τ . This completes the proof.

The same argument shows

(16.8) **COROLLARY.** *For any Morita context (16.6), we have*

$$1_\Lambda \in \text{im } \mu \implies \mu \text{ epic} \implies \mu \text{ monic},$$

$$1_\Delta \in \text{im } \tau \implies \tau \text{ epic} \implies \tau \text{ monic}.$$

Recall that M_Δ is a *progenerator* of \mathcal{M}_Δ if M is a finitely generated projective Δ -module which is a generator of the category \mathcal{M}_Δ . The preceding results give at once

(16.9) **Corollary.** *The module M_Δ is a progenerator of \mathcal{M}_Δ if and only if both of the maps μ, τ in (16.7) are isomorphisms. If M_Δ is a progenerator, then the Morita context derived from M gives a Morita equivalence between the rings Δ and $\text{Hom}_\Delta(M, M)$.*

Remark. Let M_Δ be a progenerator of \mathcal{M}_Δ . Then M is a projective object in the category \mathcal{M}_Δ , and by (15.9) there is an equivalence of categories

$$(16.10) \quad \text{Hom}_\Delta(M, \cdot) : \mathcal{M}_\Delta \rightarrow \mathcal{M}_\Lambda,$$

where $\Lambda = \text{Hom}_\Delta(M, M)$, and M is viewed as a bimodule ${}_\Lambda M_\Delta$. It is sometimes useful to exhibit this category equivalence in terms of tensor products, rather than Hom. Define M^* as in (16.1); by Exercise 2.5, there is an isomorphism

$$\text{Hom}_\Delta(M, L) \cong L \otimes_\Delta M^*, \quad L \in \mathcal{M}_\Delta,$$

and it is easily verified that this is a right Λ -isomorphism which is natural in L . In other words, there is an equivalence of functors

$$(16.11) \quad \text{Hom}_\Delta(M, \cdot) \sim \cdot \otimes_\Delta M^*.$$

(This also follows from Exercise 15.7.) Hence the equivalence in (16.10) can also be given as

$$\cdot \otimes_\Delta M^* : \mathcal{M}_\Delta \rightarrow \mathcal{M}_\Lambda.$$

We shall show below that every Morita equivalence of rings Δ, Λ is obtained in the manner described above, by means of the Morita context derived from a progenerator M_Δ of category \mathcal{M}_Δ . As a first step in establishing this fact, let us start with an arbitrary Morita context (16.6), not necessarily derived from a Δ -module M , and let us see what conclusions may be drawn if we assume that μ is epic.

(16.12) THEOREM. Suppose that the map μ occurring in the Morita context (16.6) is epic. Then both M_{Δ} and ${}_{\Delta}N$ are finitely generated projective modules, and Λ acts faithfully† on N . Furthermore,

$$M \cong \text{Hom}_{\Delta}(N, \Delta), \quad \Lambda \cong \text{Hom}_{\Delta}(N, N).$$

The first of these is a (Λ, Δ) -bimodule isomorphism, and the second is an isomorphism as rings of right operators on N .

Proof. Let us form the Morita context derived from ${}_{\Delta}N$, by setting

$$\Lambda' = \text{Hom}_{\Delta}(N, N), \quad N^* = \text{Hom}_{\Delta}(N, \Delta).$$

Then Λ' is a ring, and there are bimodule structures ${}_{\Delta}N_{\Lambda'}$, ${}_{\Lambda'}N^*_{\Delta}$, and bimodule homomorphisms

$$\begin{aligned} \mu': N^* \otimes_{\Delta} N &\rightarrow \Lambda', & f \otimes n &\mapsto \{f, n\}, \\ \tau': N \otimes_{\Lambda'} N^* &\rightarrow \Delta, & n \otimes f &\mapsto \langle n, f \rangle = f(n), \end{aligned}$$

where

$$n_1\{f, n\} = \langle n_1, f \rangle n, \quad \{f, n\}g = f\langle n, g \rangle.$$

We may now define a right Δ -homomorphism ψ by

$$\psi: M \rightarrow N^*, \quad m \mapsto [\cdot, m],$$

where we use (\cdot, \cdot) and $[\cdot, \cdot]$ for the maps μ, τ occurring in (16.6). Also define a ring homomorphism

$$\varphi: \Lambda \rightarrow \Lambda', \quad \lambda \mapsto \lambda_R,$$

where λ_R is right multiplication by λ on N . Let us verify that the following diagram is commutative:

$$(16.13) \quad \begin{array}{ccc} M \otimes_{\Delta} N & \xrightarrow{\psi \otimes 1} & N^* \otimes_{\Delta} N \\ \mu \downarrow & & \downarrow \mu' \\ \Lambda & \xrightarrow{\varphi} & \Lambda'. \end{array}$$

To prove equality of two elements of Λ' , we compute their action on an arbitrary element $n' \in N$. We have

$$n'\{(\varphi\mu) \cdot (m \otimes n)\} = n' \cdot (m, n) = [n', m]n,$$

† This means that for $\lambda \in \Lambda$, if $N\lambda = 0$ then $\lambda = 0$.

whereas

$$\begin{aligned} n' \cdot \{(\mu'(\psi \otimes 1) \cdot (m \otimes n)\} &= n' \cdot \{\mu'(\psi m \otimes n)\} = n' \cdot \{\psi m, n\} \\ &= \langle n', \psi m \rangle \cdot n = \{(\psi m)n'\} \cdot n = [n', m] \cdot n. \end{aligned}$$

This shows that (16.13) is commutative.

Up to this point, we have not used our hypothesis that μ is epic. Under this hypothesis, we know from (16.8) that μ is in fact an isomorphism. We shall show that the other maps φ , μ' and $\psi \otimes 1$ in (16.13) are also isomorphisms. We begin by proving that ψ itself is an isomorphism. Choose $z \in M \otimes N$ so that $\mu(z) = 1_\Lambda$; then

$$z = \sum m_i \otimes n_i, \quad 1_\Lambda = \sum (m_i, n_i).$$

If $m \in \ker \psi$, then $[N, m] = 0$, whence

$$m = \sum (m_i, n_i)m = \sum m_i[n_i, m] = 0,$$

and thus ψ is monic. To prove ψ epic, let $f \in N^*$ and set

$$m = \sum m_i \cdot f(n_i).$$

We show that $\psi(m) = f$ by checking that for each $n \in N$, $\{\psi(m)\}n = f(n)$. We have

$$\{\psi(m)\}n = [n, \sum m_i \cdot f(n_i)] = \sum [n, m_i]f(n_i).$$

But f is a Δ -homomorphism, and $[n, m_i] \in \Delta$, whence

$$\{\psi(m)\}n = f(\sum [n, m_i]n_i) = f(\sum n(m_i, n_i)) = f(n).$$

This completes the verification that ψ is an isomorphism. It follows at once that $\psi \otimes 1$ is also an isomorphism.

Now we note that

$$1_\Lambda = \varphi\mu(z) = \mu'(\{\psi \otimes 1\}z),$$

whence by (16.8) μ' is an isomorphism. Since (16.13) commutes, it follows that φ is an isomorphism, as claimed. This in turn implies that Λ acts faithfully on N .

Finally, since μ' is epic, it follows by (16.7) that N is a finitely generated projective left Δ -module. But then N^* is a finitely generated projective right Δ -module, since $(\Delta)^* = \Delta$. We have shown above that $M \cong N^*$, whence we may conclude that M_Δ is finitely generated and projective. This completes the proof.

We called the rings Δ, Λ *Morita equivalent* if there exists a Morita context (16.6) in which both μ and τ are epimorphisms (and hence isomorphisms). We saw in (16.9) that the Morita context derived from a progenerator M_Δ

of \mathcal{M}_Δ always gives a Morita equivalence, and in that special case we constructed an equivalence of categories $\mathcal{M}_\Delta \cong \mathcal{M}_\Lambda$, where $\Lambda = \text{Hom}_\Delta(M, M)$. We now prove that *every* Morita equivalence of rings is derived from a progenerator, and gives an equivalence of categories.

(16.14) **Theorem.** *Let the rings Δ and Λ be Morita equivalent relative to a Morita context ${}_M\Delta, {}_N\Lambda$ as in (16.6). Then*

- (i) *M is a progenerator for both \mathcal{M}_Δ and ${}_\Delta\mathcal{M}$.*
 N is a progenerator for both ${}^M\mathcal{M}$ and \mathcal{M}_Λ .
- (ii) *There are bimodule isomorphisms*

$$N \cong \text{Hom}_\Delta(M, \Delta) \cong \text{Hom}_\Lambda(M, \Lambda), \quad M \cong \text{Hom}_\Lambda(N, \Lambda) \cong \text{Hom}_\Delta(N, \Delta).$$

- (iii) *There are ring isomorphisms*

$$\Lambda \cong \text{Hom}_\Delta(M, M) \cong \text{Hom}_\Lambda(N, N), \quad \Delta \cong \text{Hom}_\Lambda(M, M) \cong \text{Hom}_\Delta(N, N),$$

where $\text{Hom}_\Delta(N, N)$ acts as a ring of right operators on N , and likewise $\text{Hom}_\Lambda(M, M)$ on M .

- (iv) *There are inverse pairs of equivalences of categories*

$$\mathcal{M}_\Lambda \xrightleftharpoons[T]{S} \mathcal{M}_\Delta, \quad {}^M\mathcal{M} \xrightleftharpoons[T']{S'} {}_\Delta\mathcal{M},$$

where

$$S = \cdot \otimes_\Lambda M \sim \text{Hom}_\Lambda(N, \cdot), \quad T = \cdot \otimes_\Delta N \sim \text{Hom}_\Delta(M, \cdot),$$

$$S' = N \otimes_\Lambda \cdot \sim \text{Hom}_\Lambda(M, \cdot), \quad T' = M \otimes_\Delta \cdot \sim \text{Hom}_\Delta(N, \cdot).$$

(v) *The correspondence $J \rightarrow JM$ gives an isomorphism of the lattice of right ideals of Λ and the lattice of submodules of M_Δ , and the two-sided ideals correspond to sub-bimodules of ${}_\Delta M_\Delta$.*

The correspondence $I \rightarrow MI$ gives an isomorphism of the lattice of left ideals of Δ and the lattice of submodules of ${}^M\mathcal{M}$, and the two-sided ideals correspond to sub-bimodules of ${}^M\mathcal{M}_\Delta$.

The correspondence $I \rightarrow \text{Hom}_\Delta(M, MI)$ gives an isomorphism between the lattice of two-sided ideals of Δ and the lattice of two-sided ideals of Λ , once we identify Λ with $\text{Hom}_\Delta(M, M)$.

Proof. By hypothesis both μ and τ in (16.6) are epic, so there exist m 's in M , n 's in N such that

$$(16.15) \quad \sum (m_i, n_i) = 1_\Lambda, \quad \sum [n'_j, m'_j] = 1_\Delta.$$

It is easily checked that for $n \in N$,

$$(\cdot, n) \in \text{Hom}_\Lambda(M, \Lambda), \quad [n, \cdot] \in \text{Hom}_\Delta(M, \Delta).$$

The first equation in (16.15) then asserts that ${}_A M$ has trace ideal Λ , whence ${}_A M$ is a generator of \mathcal{M}_Δ by (15.5). Likewise, the second equation in (16.15) implies that M_Δ is a generator of \mathcal{M}_Δ . Further, since μ is epic, it follows from (16.12) that M_Δ is finitely generated and projective; the same holds for ${}_A M$ since τ is epic. This proves the first part of (i), and the second part follows by symmetry.

The assertions in (ii) and (iii) are immediate consequences of (16.12), using symmetry arguments. (See also Exercise 16.7). To prove (iv) we observe that for each $X \in \mathcal{M}_\Delta$,

$$\begin{aligned} \{(\cdot \otimes N)(\cdot \otimes M)\}X &= (X \otimes_A M) \otimes_\Delta N \cong X \otimes_A (M \otimes_\Delta N) \\ &\cong X \otimes_A \Lambda \cong X, \end{aligned}$$

since $M \otimes_\Delta N \cong \Lambda$ as Λ - Λ -bimodules. All of these isomorphisms are natural in X , and thus $(\cdot \otimes N)(\cdot \otimes M)$ is naturally equivalent to the identity functor on \mathcal{M}_Δ . Analogous arguments hold for the other functors in (iv), so we obtain category equivalences, as claimed. The natural equivalences of the type $\cdot \otimes_A M \sim \text{Hom}_\Delta(N, \cdot)$ follow from (ii) and (16.11).

Finally $S(\Lambda) = M$, so the right ideal J of Λ maps onto $S(J) = J \otimes_A M$. But $J \otimes_A M \cong JM$ as Δ -modules, since ${}_A M$ is projective. This implies the first statement in (v). The second statement follows by symmetry. Finally, if I is a two-sided ideal of Δ , then I corresponds to the sub-bimodule MI of ${}_A M_\Delta$, and this in turn corresponds (via T) to the two-sided ideal $\text{Hom}_\Delta(M, MI)$. This completes the proof.

Let us briefly consider the special case where M_Δ is free on r generators, and where

$$(16.16) \quad \Lambda = \text{Hom}_\Delta(M, M) \cong M_r(\Delta).$$

Clearly M_Δ is a progenerator for \mathcal{M}_Δ , and there is a category equivalence

$$\text{Hom}_\Delta(M, \cdot) : \mathcal{M}_\Delta \rightarrow \mathcal{M}_\Delta.$$

The isomorphism in (16.16) can be described explicitly, once we start with a free Δ -basis $\{m_1, \dots, m_r\}$ of M . Each $f \in \Lambda$ determines a matrix $T_f \in M_r(\Delta)$, such that

$$f(m_1, \dots, m_r) = (m_1, \dots, m_r)T_f.$$

This equation means that

$$(16.17) \quad f(m_j) = \sum_{i=1}^r m_i \tau_{ij}, \quad 1 \leq j \leq r, \quad T_f = (\tau_{ij}).$$

For any two-sided ideal I of the ring Δ , let $M_r(I)$ denote the set of all $r \times r$ matrices with entries in I .

(16.18) COROLLARY. *The map $I \rightarrow M_r(I)$ gives an isomorphism between the lattice of two-sided ideals of Δ and the lattice of two-sided ideals of $M_r(\Delta)$.*

Proof. By (16.14(v)), the map $I \rightarrow \text{Hom}_\Delta(M, MI)$ gives the desired isomorphism, once we identify Λ with $M_r(\Delta)$ as in (16.16). We have

$$M = \sum_{k=1}^r m_k \Delta, \quad MI = \sum_{k=1}^r m_k I,$$

where $\{m_1, \dots, m_r\}$ is a free Δ -basis for M . Let $f \in \Lambda$ correspond to $T_f \in M_r(\Lambda)$, as in (16.17). It is clear that $f \in \text{Hom}_\Delta(M, MI)$ if and only if each τ_{ij} in (16.17) lies in I . Hence the image of $\text{Hom}_\Delta(M, MI)$ in $M_r(\Delta)$ is precisely $M_r(I)$, which proves the corollary.

EXERCISES

1. Keep the notation in (16.1)–(16.5). Prove that if μ is epic, then μ is monic, and likewise for τ . [Hint: It suffices to prove the result for μ , by symmetry. Let μ be epic, and write $1_\Lambda = \sum_1^r (m_i, f_i)$. Let $\sum n_j \otimes g_j \in \ker \mu$, so $\sum (n_j, g_j) = 0$. Then

$$\begin{aligned} \sum_j n_j \otimes g_j &= \sum_{i,j} (m_i, f_i) n_j \otimes g_j = \sum m_i \otimes [f_i, n_j] g_j \\ &= \sum m_i \otimes f_i(n_j, g_j) = 0. \end{aligned}$$

2. Consider an equivalence of categories $\mathcal{M}_\Lambda \xrightleftharpoons{T} \mathcal{M}_\Delta$, where Λ, Δ are rings. Show that this equivalence comes from a Morita context. [Hint: Set $M = T(\Delta)$, $N = S(\Lambda)$. Then there are bimodule structures ${}_A M_\Lambda$, ${}_A N_\Delta$ which give a Morita equivalence between Λ and Δ . Further, the functors S and $\cdot \otimes N$ are naturally equivalent, as are T and $\cdot \otimes M$.]

3. Let M be a free right Δ -module on r generators, and set $\Lambda = \text{Hom}_\Delta(M, M)$. Then M is a progenerator for \mathcal{M}_Δ , and there is an equivalence of categories

$$\mathcal{M}_\Delta \xleftarrow{\cdot \otimes M^*} \mathcal{M}_\Lambda \xrightarrow{\cdot \otimes M}$$

- where $M^* = \text{Hom}_\Delta(M, \Delta)$. What is the two-sided ideal in Λ which corresponds to a given two-sided ideal J in Δ ?

4. Show that Morita equivalent rings have isomorphic centers. [Hint: Identify the center of Λ with the ring of bimodule endomorphisms of ${}_A M_\Lambda$.]

5. Let R be a commutative ring, Λ a left noetherian R -algebra, and M a finitely generated left Λ -module. Suppose that for each maximal ideal P of R , the localization M_P is a generator for the category of left Λ_P -modules. Prove that M is a generator for ${}_\Lambda \mathcal{M}$. Also prove the corresponding statement when “generator” is replaced by “pro-generator”.

6. Let \hat{R} be the completion of the commutative local noetherian ring R , let Λ be a

left noetherian R -algebra, and let M be a finitely generated left Λ -module. Show that M is a generator of ${}_{\Lambda}\mathcal{M}$ if and only if $\hat{R} \otimes_R M$ is a generator of ${}_{\hat{\Lambda}}\mathcal{M}$, where $\hat{\Lambda} = \hat{R} \otimes_R \Lambda$. Prove the corresponding result for progenerators.

7. Show that the isomorphisms in (16.14(ii)) are given as follows:

$$N \cong \text{Hom}_{\Delta}(M, \Delta), n \rightarrow [n, \cdot]; \quad N \cong \text{Hom}_{\Lambda}(M, \Lambda), n \rightarrow (\cdot, n).$$

$$M \cong \text{Hom}_{\Lambda}(N, \Lambda), m \rightarrow (m, \cdot); \quad M \cong \text{Hom}_{\Delta}(N, \Delta), m \rightarrow [\cdot, m].$$

Further, each isomorphism in (16.14(iii)) is given by letting the elements of Λ and Δ act as left or right multiplications on the modules M or N .

8. Show that Morita equivalence of rings is transitive.

9. Let M be a minimal left ideal of the simple left artinian ring Λ . Prove that M is a progenerator for ${}_{\Lambda}\mathcal{M}$. Set $\Delta = \text{Hom}_{\Lambda}(M, M)$, and view M as a bimodule ${}_{\Lambda}M_{\Delta}$. Prove

- (i) Δ is a skewfield.
- (ii) M is a finite dimensional Δ -space.
- (iii) $\Delta \cong \text{Hom}_{\Delta}(M, M)$.

[Hint: Use (15.5) to show that M is a generator for ${}_{\Lambda}\mathcal{M}$. By Schur's Lemma, Δ is a skewfield. Assertions (ii) and (iii) then follow from (16.14). This provides another proof of the harder part of Wedderburn's Theorem (7.4).]

10. Let Δ be a skewfield, $V_{\Delta} = \Delta^{(r)}$ a right Δ -space, and let $\Lambda = \text{Hom}_{\Delta}(V, V)$. Prove that Λ is a simple left artinian ring, and that $\Delta = \text{Hom}_{\Lambda}(V, V)$. [Hint: View V as a bimodule ${}_{\Lambda}V_{\Delta}$. By (16.18), the ring Λ is simple. Its left ideals satisfy the D.C.C., since they are in bijection with the set of Δ -subspaces of V by (16.14). Finally, $\Delta \cong \text{Hom}_{\Lambda}(V, V)$ by (16.14). This proves the easier part of Wedderburn's Theorem (7.4).]

5. Maximal Orders Over Discrete Valuation Rings

Throughout this chapter, R denotes a discrete valuation ring with quotient field K , maximal ideal $P = \pi R \neq 0$, and residue class field $\bar{R} = R/P$. We have already seen in (10.5) that the study of maximal R -orders in separable K -algebras can be reduced to the case of central simple algebras. We shall investigate this case in detail here, by using the results from Chapter III on maximal orders in skewfields, and then applying the Morita equivalence between skewfields and full matrix algebras over skewfields.

We assume throughout that A is a central simple K -algebra, and that V is a minimal left ideal of A . Set $D = \text{Hom}_A(V, V)$, and view ${}_AV_D$ as a bimodule. If $\{v_1, \dots, v_r\}$ is any right D -basis for V , then for each $a \in A$ we may write

$$(17.1) \quad a(v_1, \dots, v_r) = (v_1, \dots, v_r)(\alpha_{ij}), \quad (\alpha_{ij}) \in M_r(D),$$

and the map defined by $a \rightarrow (\alpha_{ij})$ permits us to identify A with $M_r(D)$.

Likewise, if Δ is an R -order in D , we may choose a free Δ -lattice in V , say

$$M = \sum_{i=1}^r m_i \Delta. \text{ For each } a \in \text{Hom}_\Delta(M, M) \text{ we may write}$$

$$(17.2) \quad a(m_1, \dots, m_r) = (m_1, \dots, m_r)(\alpha_{ij}), \quad (\alpha_{ij}) \in M_r(\Delta).$$

The map defined by $a \rightarrow (\alpha_{ij})$ then gives an identification of $\text{Hom}_\Delta(M, M)$ with $M_r(\Delta)$, and this identification is consistent with that obtained from (17.1). Finally, we set

$$(D:K) = n^2, \quad (A:K) = n^2 r^2.$$

17. MAXIMAL ORDERS (COMPLETE LOCAL CASE)

In this section we assume always that R is a complete discrete valuation ring. We know by §12 that the skewfield D contains a unique maximal R -order Δ , which is the integral closure of R in D . Denote by π_D a prime element of Δ , and let $p = \pi_D \Delta$. We have seen in (13.2) that the powers $\{p^m\}$ give all nonzero one-sided ideals of Δ , and that these ideals are necessarily two-sided ideals. We set $\bar{\Delta} = \Delta/p$, a skewfield of finite dimension over the field \bar{R} .

Let $A = M_r(D)$ be a central simple K -algebra. Our aim here is to show that $M_r(\Delta)$, and its conjugates, give all possible maximal R -orders in A . We shall also study the one-sided and two-sided ideals of such orders.

(17.3) **Theorem.** (i) Let $\Lambda = M_r(\Delta)$. Then Λ is a maximal R -order in A , and has a unique maximal two-sided ideal $\pi_D \Lambda$. The powers

$$(\pi_D \Lambda)^m = \pi_D^m \Lambda, \quad m = 0, 1, 2, \dots,$$

give all of the nonzero two-sided ideals of Λ .

(ii) Every maximal R -order in A is of the form $u\Lambda u^{-1}$ for some $u \in u(A)$, and each such ring is a maximal order.

(iii) Every maximal order Λ' is left and right hereditary, and each of its one-sided ideals is principal. The unique maximal two-sided ideal of $u\Lambda u^{-1}$ is $u \cdot \pi_D \Lambda \cdot u^{-1}$, that is, $u\pi_D u^{-1} \cdot u\Lambda u^{-1}$.

Proof. We know by (8.7) that Λ is a maximal order. Keeping the notation (17.2), we set $M = \sum m_i \Delta$; then we may identify Λ with $\text{Hom}_\Delta(M, M)$. Since M_Δ is a progenerator for the category \mathcal{M}_Δ , it follows from (16.9) that Λ is Morita equivalent to Δ , relative to the Morita context derived from M_Δ . By (16.18), the two-sided ideals of Λ are given by $M_r(I)$, with I ranging over the two-sided ideals of Δ . But each nonzero I is some $\pi_D^m \Delta$, by (13.2). This proves (i), once we observe that

$$M_r(\pi_D^m \Delta) = \pi_D^m \cdot M_r(\Delta) = (\pi_D \Lambda)^m.$$

Furthermore, every one-sided ideal of Δ is isomorphic to Δ by (13.2), whence Δ is left and right hereditary. By Exercise 15.4, we may conclude that also Λ is left and right hereditary.

Now let us prove that every right ideal of Λ is principal,[†] that is, has the form $x\Lambda$ for some $x \in \Lambda$. By (16.14), every right ideal of Λ can be written as $\text{Hom}_\Delta(M, L)$ for some Δ -submodule L of M . However, M is Δ -free, and every right ideal of Δ is principal, and is isomorphic to Δ . Hence by (2.44) we may write $L = \sum_{j=1}^s l_j \Delta$, a free Δ -module on s generators, where necessarily $s \leq r$.

Let $\Delta^{s \times r}$ denote the set of $s \times r$ matrices with entries in Δ . There is then a bijection $\text{Hom}_\Delta(M, L) \leftrightarrow \Delta^{s \times r}$, given by $f \leftrightarrow U_f$, where

$$f(m_1, \dots, m_r) = (l_1, \dots, l_s) U_f.$$

On the other hand, there is a unique $B \in \Delta^{r \times s}$ such that

$$(l_1, \dots, l_s) = (m_1, \dots, m_r) B,$$

and thus we have

$$f(m_1, \dots, m_r) = (m_1, \dots, m_r) \cdot B U_f.$$

Comparing this with (17.2), it follows that $\text{Hom}_\Delta(M, L)$ can be identified with the right ideal $B \cdot \Delta^{s \times r}$ of $M_r(\Delta)$. But for each $U \in \Delta^{s \times r}$, we have

[†] Caution: A principal ideal $x\Lambda$ is not isomorphic to Λ , except when $x \in u(A)$.

$$B \cdot U = [B \ 0] \begin{bmatrix} U \\ * \end{bmatrix},$$

where the right-hand expression is a product of two $r \times r$ matrices. Therefore

$$B \cdot \Delta^{s \times r} = [B \ 0] \cdot M_r(\Delta),$$

and so we have shown that the given right ideal of Λ is principal, with generator $[B \ 0]$. A corresponding statement holds for left ideals of Λ , by symmetry. (A rather different proof of these facts is given in (18.7).)

Turning next to the proof of (ii), let Λ' be another maximal order in A . Then $\Lambda'\Lambda$ is a full right Λ -lattice in A , so there exists a nonzero $\alpha \in R$ such that $\alpha\Lambda'\Lambda \subset \Lambda$. Then $\alpha\Lambda'\Lambda$ is a right ideal of Λ , hence is principal by the above, and so $\Lambda'\Lambda = u\Lambda$ for some $u \in A$. Clearly $A = uA$, whence $u \in u(A)$ by (6.4). Therefore

$$u\Lambda = \Lambda'\Lambda = \Lambda' \cdot \Lambda'\Lambda = \Lambda' \cdot u\Lambda \supset \Lambda'u,$$

and thus $\Lambda' \subset u\Lambda u^{-1}$. But $u\Lambda u^{-1}$ is also an order, and hence $\Lambda' = u\Lambda u^{-1}$ since Λ' is maximal.

Finally, the inner automorphism of A given by $x \rightarrow uxu^{-1}$, $x \in A$, carries Λ onto Λ' . The assertions about Λ' follow at once from those about Λ , and the proof is complete.

(17.4) COROLLARY. *Let $A = \text{Hom}_D(V, V)$, where D is a skewfield with center K , and where V is a simple left A -module which is a right vector space over D . Let Δ be the maximal R -order in D , and let Λ be any maximal R -order in A . Then there exists a full free Δ -lattice M in V such that $\Lambda = \text{Hom}_\Delta(M, M)$. Conversely, each such Λ is maximal.*

Proof. Let N be any free Δ -lattice spanning V , and set $\Lambda' = \text{Hom}_\Delta(N, N)$. By the above theorem, there exists $u \in u(A)$ such that $\Lambda = u\Lambda' u^{-1}$. But then choose $M = uN$, and we have

$$\text{Hom}_\Delta(uN, uN) = u \cdot \text{Hom}_\Delta(N, N) \cdot u^{-1} = \Lambda,$$

as desired. Note that since N_Δ is free, so is M_Δ . The fact that each $\text{Hom}_\Delta(M, M)$ is maximal has already been observed in (17.3(i)).

Another important consequence of (17.3) is

(17.5) COROLLARY. *For every maximal R -order Λ in A , we have*

$$\text{rad } \Lambda = \pi_D \Lambda, \quad \Lambda/\text{rad } \Lambda \cong M_r(\Delta/\text{rad } \Delta),$$

where “rad” denotes Jacobson radical, and where $\Delta/\text{rad } \Delta$ is a skewfield.

Proof. By (17.4) we may choose $\Lambda = M_r(\Delta)$. We may write $\text{rad } \Lambda = \pi_D^m \Lambda$ for some $m > 0$. If $m > 1$, then $\Lambda/\text{rad } \Lambda$ contains the nonzero nilpotent ideal $\pi_D \Lambda / \text{rad } \Lambda$, which is impossible since $\Lambda/\text{rad } \Lambda$ is semisimple. Thus $m = 1$, and

$$\Lambda/\text{rad } \Lambda \cong M_r(\Lambda/\pi_D \Delta) = M_r(\Delta/\text{rad } \Delta).$$

This finishes the proof.

Now let X be any full R -lattice in A , and define its left and right orders as in (8.1), (8.2).

(17.6) THEOREM. $O_l(X)$ is a maximal order if and only if $O_r(X)$ is a maximal order.

Proof. Let $\Lambda = O_r(X)$ be maximal, and set $\Lambda' = O_l(X)$. Then X is a right Λ -lattice in A , so as in (17.3) we may write $X = u\Lambda$ for some $u \in u(A)$. Then

$$u\Lambda u^{-1} \cdot X \subset X,$$

whence $u\Lambda u^{-1} \subset \Lambda'$. Since $u\Lambda u^{-1}$ is a maximal order, we obtain $u\Lambda u^{-1} = \Lambda'$, and so Λ' is maximal, as claimed.

Keeping the notation of (17.3), let us determine all one-sided ideals of Λ , and especially the maximal such ideals. We begin with an easy result.

(17.7) THEOREM. Every matrix with entries in Δ can be diagonalized by means of elementary row and column operations. Given any $x \in \Delta^{s \times r}$, there exist matrices $u \in u(M_s(\Delta))$, $v \in u(M_r(\Delta))$, such that

$$uxv = \text{diag}(\pi_D^{a_1}, \dots, \pi_D^{a_s}), \quad 0 \leq a_1 \leq \dots \leq a_s$$

The integers a_1, \dots, a_s are uniquely determined by x . (Possibly some of the $\{a_i\}$ are infinite, and we interpret π_D^∞ as 0.)

Proof. One can imitate the usual proof for the case where Δ is a (commutative) principal ideal domain. Indeed, the argument is even simpler in this case, since Δ is a local ring without zero divisors, and the fact that multiplication in Δ is non-commutative does not cause any difficulties. We shall not give the details of the proof. For more general theorems of this type, see Knebusch [1].

(17.8) THEOREM. (i) Set $\bar{\Lambda} = \Lambda/\text{rad } \Lambda \cong M_r(\bar{\Delta})$. There is a one-to-one correspondence $J \rightarrow \bar{J}$ between maximal right ideals of Λ and those of $\bar{\Lambda}$. Here, \bar{J} is the image of J in $\bar{\Lambda}$, and $\Lambda/J \cong \bar{\Lambda}/\bar{J}$. The module Λ/J is a simple Λ -module.

(ii) Let $x_1 = \text{diag}(\pi_D, 1, \dots, 1) \in M_r(\Delta)$. Then $x_1 \Lambda$ is a maximal right ideal of Λ , and its conjugates

$$\{u \cdot x_1 \Lambda \cdot u^{-1} : u \in u(\Lambda)\}$$

give all of the maximal right ideals of Λ .

(iii) For $x \in \Lambda$, the right ideal $x\Lambda$ is maximal if and only if the left ideal Λx is maximal.

Proof. Each maximal right ideal J of Λ contains $\text{rad } \Lambda$, by (6.3) and (6.6). Therefore

$$\Lambda/J \cong (\Lambda/\text{rad } \Lambda)/(J/\text{rad } \Lambda) = \bar{\Lambda}/\bar{J}.$$

Since J is maximal, Λ/J is a simple Λ -module, whence $\bar{\Lambda}/\bar{J}$ is a simple $\bar{\Lambda}$ -module. Therefore \bar{J} is also maximal. Conversely for each maximal right ideal Y of $\bar{\Lambda}$, the kernel of the epimorphism $\Lambda \rightarrow \bar{\Lambda}/Y$ is a maximal right ideal J of Λ such that $\bar{J} = Y$. This proves (i).

Next, we have

$$1 - \bar{x}_1 = e_{11} = \text{diag}(1, 0, \dots, 0) \in \bar{\Lambda},$$

whence

$$\bar{\Lambda}/\bar{x}_1\bar{\Lambda} = \bar{\Lambda}/(1 - e_{11})\bar{\Lambda} \cong e_{11}\bar{\Lambda}.$$

But e_{11} is a primitive idempotent in $\bar{\Lambda}$, so $e_{11}\bar{\Lambda}$ is a simple $\bar{\Lambda}$ -module. Thus $x_1\Lambda$ is a maximal right ideal of Λ , as claimed. The same argument shows that Λx_1 is a maximal left ideal of Λ .

By (17.3), every maximal right ideal of Λ has the form $x\Lambda$ for some $x \in \Lambda$. As in (17.7), choose $u, v \in u(\Lambda)$ so that

$$uxv = \text{diag}(\pi_D^{a_1}, \dots, \pi_D^{a_r}), \quad 0 \leq a_1 \leq \dots \leq a_r.$$

But if $0 \leq b_i \leq a_i$, $1 \leq i \leq r$, then

$$uxv \cdot \Lambda = \text{diag}(\pi_D^{a_1}, \dots, \pi_D^{a_r}) \cdot \Lambda \subset \text{diag}(\pi_D^{b_1}, \dots, \pi_D^{b_r}) \cdot \Lambda \subset \Lambda.$$

Since $x\Lambda$ is maximal, so is $uxv \cdot \Lambda$, because left multiplication by u carries Λ onto itself, and carries $x\Lambda$ onto $uxv \cdot \Lambda$. Hence we have $a_1 = \dots = a_{r-1} = 0$, $a_r = 1$, and thus

$$uxv = \text{diag}(1, \dots, 1, \pi_r) = x_r,$$

say. But $x_r = tx_1t'$ for some $t, t' \in u(\Lambda)$, and thus $uxv = tx_1t'$, so

$$x\Lambda = u^{-1}t \cdot x_1\Lambda = (u^{-1}t) \cdot x_1\Lambda \cdot (u^{-1}t)^{-1}.$$

This completes the proof of (ii).

Finally, let $x\Lambda$ be maximal. By the above, we may write $x = u'x_1v'$ for some $u', v' \in u(\Lambda)$. Then $\Lambda x = \Lambda x_1 \cdot v'$, whence Λx is a maximal left ideal of Λ , as claimed. This proves the theorem.

18. MAXIMAL ORDERS (LOCAL CASE)

Keeping the notation introduced at the beginning of this chapter, let R

be a discrete valuation ring, not necessarily complete. Let \hat{R} denote the P -adic completion of R , and \hat{K} the quotient field of \hat{R} . Given any separable K -algebra B , we may form the \hat{K} -algebra $\hat{B} = \hat{K} \otimes_K B$, which is a separable \hat{K} -algebra by Exercise 7.13. Of course, when B is a central simple K -algebra, we know from (7.8) that \hat{B} is a central simple \hat{K} -algebra. However, if B is merely assumed separable over K , then it may well happen that \hat{B} will have more simple components than B . This may occur even when B is a field (see Exercise 7.7, for example). Even in the case where B is central simple over K , the full matrix algebras B, \hat{B} may consist of different size matrices. Despite these precautionary remarks, however, we can obtain results on R -orders in B by using the theorems in §17 on \hat{R} -orders in \hat{B} .

If Γ is any R -order in B , then setting $\hat{\Gamma} = \hat{R} \otimes_R \Gamma$, we obtain an \hat{R} -order $\hat{\Gamma}$ in \hat{B} . If M is any Γ -module, then $\hat{M} = \hat{R} \otimes_R M$ is a $\hat{\Gamma}$ -module. We shall use such notation hereafter without further comment. By (11.5), Γ is a maximal order in B if and only if $\hat{\Gamma}$ is a maximal order in \hat{B} .

(18.1) THEOREM. *Every maximal R -order Γ in a separable K -algebra B is left and right hereditary.*

Proof. By (10.5), the maximal \hat{R} -order $\hat{\Gamma}$ is expressible as a ring direct sum $\sum \Lambda_i$ of maximal R_i -orders in central simple algebras, where each R_i is a complete discrete valuation ring in the center of some simple component of \hat{B} . Each of these direct summands Λ_i is hereditary by (17.3), and thus $\hat{\Gamma}$ itself is hereditary. Therefore also Γ is hereditary, by §3d.

(18.2) THEOREM. *Let Λ be any R -algebra, finitely generated as R -module, and let $\bar{\Lambda} = \Lambda/\pi\Lambda$.*

(i) *For each $s \geq 1$, there is a ring isomorphism*

$$\Lambda/\pi^s \Lambda \cong \bar{\Lambda}/\pi^s \bar{\Lambda}.$$

(ii) *There are ring isomorphisms*

$$\Lambda/\text{rad } \Lambda \cong \bar{\Lambda}/\text{rad } \bar{\Lambda} \cong \bar{\Lambda}/\text{rad } \bar{\Lambda}.$$

(iii) *Let M, N be finitely generated left Λ -modules. Then $M \cong N$ as Λ -modules if and only if $\hat{M} \cong \hat{N}$ as $\hat{\Lambda}$ -modules.*

Proof. Assertion (i) follows immediately from Exercise 5.7. Taking $s = 1$ in (i), we have $\bar{\Lambda} \cong \bar{\Lambda}/\pi \bar{\Lambda}$. We then obtain (ii) by applying (6.15) twice, once for the R -order Λ and once for the \hat{R} -order $\hat{\Lambda}$.

To prove (iii), we note that if $M \cong N$, then obviously $\hat{M} \cong \hat{N}$. Conversely, let $\varphi : \hat{M} \cong \hat{N}$, and let $\psi = \varphi^{-1}$. Since \hat{R} is a flat R -module (see (2.23) or Exercise 5.3), it follows at once by (2.38) that

$$\hat{R} \otimes_R \text{Hom}_\Lambda(M, N) \cong \text{Hom}_{\hat{\Lambda}}(\hat{M}, \hat{N}).$$

Thus we may view $\text{Hom}_{\hat{\Lambda}}(\hat{M}, \hat{N})$ as the P -adic completion of $\text{Hom}_{\Lambda}(M, N)$. But $\text{Hom}_{\Lambda}(M, N)$ is dense in its completion (see §5, or (6.16)), and so we can find an $f \in \text{Hom}_{\Lambda}(M, N)$ such that

$$f \equiv \varphi \pmod{\pi \cdot \text{Hom}_{\Lambda}(\hat{M}, \hat{N})}.$$

Likewise, we may choose $g \in \text{Hom}_{\Lambda}(N, M)$ such that $g \equiv \psi \pmod{\pi}$. Then $gf \in \text{Hom}_{\Lambda}(M, M)$ is such that

$$m - (gf)m \in \pi\hat{M}, \quad m \in M.$$

However, $M \cap \pi\hat{M} = \pi M$ by Exercise 5.7, and thus $m - (gf)m \in \pi M$ for all $m \in M$. This gives

$$M = (gf)M + \pi M.$$

But $\text{rad } R = \pi R$, and M is a finitely generated R -module, so by Nakayama's Lemma it follows from the above that $M = (gf)M$. Therefore gf is a Λ -automorphism of M , by (6.3a). Likewise, fg is a Λ -automorphism of N . Thus both f and g are isomorphisms, which shows that $M \cong N$, and completes the proof of the theorem.

(18.3) **Theorem.** *Let Λ be a maximal R -order in a central simple K -algebra A . Then Λ has a unique maximal two-sided ideal \mathfrak{P} , given by $\mathfrak{P} = \Lambda \cap \text{rad } \hat{\Lambda}$. Then $\text{rad } \Lambda = \mathfrak{P}$, and every nonzero two-sided ideal of Λ is a power of \mathfrak{P} . Further, $\text{rad } \hat{\Lambda}$ is the P -adic completion of $\text{rad } \Lambda$.*

Proof. Since $\hat{\Lambda}$ is a maximal \hat{R} -order in the central simple \hat{K} -algebra $\hat{\Lambda}$, the ring $\hat{\Lambda}/\text{rad } \hat{\Lambda}$ is simple. Hence also $\Lambda/\text{rad } \Lambda$ is simple, by (18.2). But every maximal two-sided ideal of Λ contains $\text{rad } \Lambda$ by (6.13), and thus $\text{rad } \Lambda$ is the unique maximal two-sided ideal of Λ . Furthermore, (18.2(ii)) implies at once that

$$\text{rad } \Lambda = \Lambda \cap \text{rad } \hat{\Lambda}, \quad \hat{R} \otimes_{\hat{R}} \text{rad } \Lambda = \text{rad } \hat{\Lambda}.$$

Next, since A is simple, every nonzero two-sided ideal M of Λ is such that $KM = A$. Thus $M \supseteq \pi^s \Lambda$ for some s , and hence M is the inverse image of a two-sided ideal of $\Lambda/\pi^s \Lambda$. But $\Lambda/\pi^s \Lambda \cong \hat{\Lambda}/\pi^s \hat{\Lambda}$, and all two-sided ideals of $\hat{\Lambda}/\pi^s \hat{\Lambda}$ are images of powers of $\text{rad } \hat{\Lambda}$. It follows at once that M itself is a power of \mathfrak{P} , as claimed. This completes the proof of the theorem.

We next give a criterion, due to Auslander-Goldman [1], for an order to be maximal.

(18.4) **THEOREM.** *Let Λ be an R -order in the central simple K -algebra A . Then Λ is maximal if and only if Λ is hereditary, and $\text{rad } \Lambda$ is its unique maximal two-sided ideal.*

Proof. Maximal orders have the indicated properties, by (18.1) and (18.3). Conversely, let Λ be hereditary, with unique maximal two-sided ideal $\text{rad } \Lambda$, and let Γ be an order properly containing Λ . Then Γ is a left Λ -lattice, hence is a finitely generated projective left Λ -module by (10.7). It follows then from (16.7) that the map

$$\mu : \text{Hom}_{\Lambda}(\Gamma, \Lambda) \otimes_{\Lambda} \Gamma \rightarrow \text{Hom}_{\Lambda}(\Gamma, \Gamma)$$

is epic, where

$$\mu(f \otimes \gamma) = (f, \gamma), \quad \gamma'(f, \gamma) = [\gamma', f]\gamma,$$

and $[\gamma', f]$ is f evaluated at γ' . Suppose that $\mu\{\sum f_i \otimes \gamma_i\} = 1$. Then $\sum \gamma(f_i, \gamma_i) = \gamma$ for all $\gamma \in \Gamma$, that is,

$$\sum [\gamma, f_i]\gamma_i = \gamma, \quad \gamma \in \Gamma.$$

Now consider the trace ideal T of the left Λ -module Γ (see (15.4)). Then T is the two-sided ideal of Λ spanned by

$$\{[\gamma, f] : \gamma \in \Gamma, f \in \text{Hom}_{\Lambda}(\Gamma, \Lambda)\},$$

so the above equation implies that $T\Gamma = \Gamma$. Let us show that T is a proper ideal of Λ . If $T = \Lambda$, then Γ is a progenerator of ${}_{\Lambda}\mathcal{M}$. This gives (by (16.14))

$$\Lambda = \text{Hom}_{\Omega}(\Gamma, \Gamma), \quad \text{where } \Omega = \text{Hom}_{\Lambda}(\Gamma, \Gamma),$$

and where ${}_{\Lambda}\Gamma_{\Omega}$ is viewed as a bimodule. But then $\Omega = \Gamma$, since every Λ -endomorphism of ${}_{\Lambda}\Gamma$ is given by right multiplication by an element of Γ . Therefore we obtain $\Lambda = \text{Hom}_{\Omega}(\Gamma, \Gamma) = \Gamma$, a contradiction.

We have now shown that T is a proper ideal of Λ , and thus T is contained in the unique maximal two-sided ideal $\text{rad } \Lambda$ of Λ . Since $T\Gamma = \Gamma$, it follows that $(\text{rad } \Lambda)\Gamma = \Gamma$, which is impossible by Nakayama's Lemma. This shows that Λ is a maximal order, and completes the proof of the theorem.

We are going to show that maximal R -orders in separable K -algebras are principal ideal rings, that is, every one-sided ideal is principal. Theorems 10.5 and 18.2 will enable us to reduce this question to the case of maximal orders in central simple algebras. The key to the proof is the fact that such an order Λ is a *primary ring*, that is, $\Lambda/\text{rad } \Lambda$ is a simple artinian ring. We begin with a result on primary algebras.

(18.5) THEOREM. *Let B be a primary finite dimensional algebra over a field k , and let M, N be finitely generated projective left B -modules. Then $M \cong N$ if and only if $(M:k) = (N:k)$.*

Proof. Let $\bar{B} = B/\text{rad } B$, a simple artinian ring, and let $b \in B$ map onto $\bar{b} \in \bar{B}$.

Suppose that

$$B = Be_1 \oplus \cdots \oplus Be_n$$

is a decomposition of B into a direct sum of indecomposable left ideals, where the $\{e_i\}$ are primitive idempotents in B . By (6.21), $Be_i \cong Be_j$ if and only if $\bar{B}e_i \cong \bar{B}e_j$, and the modules $\{\bar{B}e_i\}$ are minimal left ideals of \bar{B} . Since \bar{B} is simple artinian, the $\{\bar{B}e_i\}$ are mutually isomorphic. Therefore $Be_i \cong Be_1$ for all i . But M and N are direct summands of $B^{(s)}$ for some s , whence by the Krull-Schmidt Theorem (Exercise 6.6), both M and N are direct sums of copies of Be_1 . Hence $M \cong N$ if and only if M and N have the same k -dimension.

We need one more preliminary result:

(18.6) THEOREM. *Let Λ be any R -order in a finite dimensional K -algebra $K\Lambda$, and let M, N be projective left Λ -lattices. Set $\bar{\Lambda} = \Lambda/\pi\Lambda$, $\bar{M} = M/\pi M$, $\bar{N} = N/\pi N$. Then $M \cong N$ as Λ -modules if and only if $\bar{M} \cong \bar{N}$ as $\bar{\Lambda}$ -modules.*

Proof. Clearly $M \cong N$ implies that $\bar{M} \cong \bar{N}$. Conversely, let $\varphi: \bar{M} \cong \bar{N}$ be a $\bar{\Lambda}$ -isomorphism. Since both M and N are Λ -projective, we may find Λ -homomorphisms α, β lifting φ, φ^{-1} , respectively, making the following diagram commute:

$$\begin{array}{ccc} M & \xrightleftharpoons[\beta]{\alpha} & N \\ \downarrow & & \downarrow \\ \bar{M} & \xrightleftharpoons[\varphi^{-1}]{\varphi} & \bar{N}. \end{array}$$

For $m \in M$, we have $(\beta\alpha)m - m \in \pi M$. Hence $M = \beta\alpha M + \pi M$, so $M = \beta\alpha M$ by Nakayama's Lemma. Then $\beta\alpha$ is an automorphism of M by (6.3a). Likewise, $\alpha\beta$ is an automorphism of N , and so $\alpha: M \cong N$, as desired.

There is a generalization of the above theorem, in which the hypothesis on M and N is dropped. The general version states: If $K\Lambda$ is K -separable, then there exists a positive integer q depending on Λ , such that for any pair of Λ -lattices M, N , we have $M \cong N$ if and only if $M/\pi^q M \cong N/\pi^q N$. Indeed, q may be chosen so that $\pi^{q-1}R$ is the Higman ideal of Λ (see Curtis-Reiner [1, Th. 75.11], where the Higman ideal is denoted by $i(\Lambda)$).

We are now ready to generalize (17.3)–(17.6) to the present case, in which R need not be complete.

(18.7) **Theorem.** Let Λ be a maximal R -order in a central simple K -algebra A .

(i) Let M and N be left Λ -lattices. Then $M \cong N$ if and only if M and N have the same R -rank.

(ii) Every one-sided ideal of Λ is principal.

(iii) Every maximal R -order in A is a conjugate $u\Lambda u^{-1}$ of Λ , where $u \in u(A)$.

(iv) Let $\hat{A} = \hat{K} \otimes_K A \cong M_t(E)$, where E is a skewfield with center \hat{K} , and let Ω be the unique maximal \hat{R} -order in E . Then

$$\Lambda/\text{rad } \Lambda \cong M_t(\Omega/\text{rad } \Omega),$$

and $\Omega/\text{rad } \Omega$ is a skewfield.

Proof. Since Λ is hereditary, M is Λ -projective by (10.7). Thus $\bar{M} = M/\pi M$ is $\bar{\Lambda}$ -projective, since if $M \mid \Lambda^{(r)}$ then $\bar{M} \mid \bar{\Lambda}^{(r)}$. Now let M, N be any left Λ -lattices. Then by (18.6), $M \cong N$ if and only if $\bar{M} \cong \bar{N}$ as $\bar{\Lambda}$ -modules. Since $\hat{\Lambda}/\text{rad } \hat{\Lambda}$ is a simple artinian ring by (17.5), it follows from (18.2) that $\bar{\Lambda}$ is a primary ring. Hence by (18.5), $\bar{M} \cong \bar{N}$ if and only if $(\bar{M} : \bar{R}) = (\bar{N} : \bar{R})$. Finally, we note that $(\bar{M} : \bar{R}) = \text{rank}_R M$. This proves that $M \cong N$ if and only if M and N have the same R -rank.

Suppose next that M is a left ideal of Λ . Then KM is a left ideal of the simple artinian ring A , whence $KM = Ae = K \cdot \Lambda e$ for some idempotent $e \in A$. Hence $\Lambda e \cong M$ by (i); if this isomorphism maps e onto m , then $M = \Lambda m$. This completes the proof of (ii). It should be pointed out that this proof is completely independent of that given for the corresponding statement in (17.3(iii)), and so constitutes another proof of that statement.

The argument in (17.3) which proves that every maximal order is conjugate to Λ , carries over unchanged to the present case. It remains for us to prove (iv). Keeping the notation of (iv), we showed in (17.5) that

$$\hat{\Lambda}/\text{rad } \hat{\Lambda} \cong M_t(\Omega/\text{rad } \Omega).$$

Thus the desired formula for $\Lambda/\text{rad } \Lambda$ holds by virtue of (18.2). This completes the proof of the theorem.

(18.8) **Remarks.** (i) The integer t occurring in (18.7(iv)) is called the *capacity* of $\text{rad } \Lambda$. If $A \cong M_r(D)$, where D is a skewfield, and if

$$\hat{D} = \hat{K} \otimes_K D \cong M_s(E)$$

for some skewfield E , then

$$\hat{A} \cong M_r(\hat{D}) \cong M_{rs}(E).$$

This E is the same as that which occurs in (18.7(iv)), and $t = rs$.

(ii) The statements and proofs of (17.4) and (17.6) carry over unchanged to the present case where R need not be complete.

(iii) If Λ is a maximal order in a skewfield D with center K , (18.2) shows that

$$\Delta/\text{rad } \Delta \cong \hat{\Delta}/\text{rad } \hat{\Delta}.$$

Here, $\hat{\Delta}$ is a maximal \hat{R} -order in the central simple \hat{K} -algebra \hat{D} . But if \hat{D} is not a skewfield, then $\hat{\Delta}/\text{rad } \hat{\Delta}$ is certainly *not* a skewfield. Indeed, in terms of the notation of the first remark above, we have

$$\hat{\Delta}/\text{rad } \hat{\Delta} \cong M_s(\Omega/\text{rad } \Omega),$$

where Ω is the maximal \hat{R} -order in E .

Generalizing (17.8), we have

(18.9) THEOREM. *Let Λ be a maximal R -order in a central simple K -algebra A .*

(i) *There is a one-to-one correspondence $J \rightarrow \bar{J}$ between the set of maximal right ideals J of Λ , and the set of maximal right ideals \bar{J} of $\Lambda/\text{rad } \Lambda$.*

(ii) *All maximal right ideals of Λ are mutually conjugate under inner automorphisms by units of Λ .*

(iii) *If $x\Lambda$ is a maximal right ideal of Λ , then Λx is a maximal left ideal of Λ .*

Proof. The proof of (i) is exactly the same as in (17.8). Next, let $x\Lambda$ and $y\Lambda$ be maximal right ideals of Λ . Since $\Lambda/x\Lambda$ is an R -torsion module, it follows from Exercise 5.7 that there is a right Λ -isomorphism $\Lambda/x\Lambda \cong \hat{\Lambda}/x\hat{\Lambda}$, whence $x\hat{\Lambda}$ is a maximal right ideal in $\hat{\Lambda}$. But then $\hat{\Lambda}x$ is a maximal left ideal in $\hat{\Lambda}$ by (17.8), and so Λx is a maximal left ideal in Λ . This proves (iii).

Next, by (17.8) there exists $u \in u(\hat{\Lambda})$ such that $y\hat{\Lambda} = u \cdot x\hat{\Lambda}$. Choose $v \in \Lambda$ with $v \equiv u \pmod{\pi\hat{\Lambda}}$; since v, u have the same image in $\Lambda/\pi\Lambda$, and since $\pi\Lambda \subset \text{rad } \Lambda$, it follows from Exercise 6.2 that $v \in u(\Lambda)$. But then $y\Lambda$ and $v\Lambda$ are a pair of maximal right ideals of Λ , having the same image in $\Lambda/\text{rad } \Lambda$. It follows from (i) that $y\Lambda = v\Lambda = v \cdot x\Lambda \cdot v^{-1}$ as desired, which completes the proof.

(18.10) THEOREM. *Let Λ be a maximal R -order in a separable K -algebra A . Then every one-sided ideal of Λ is principal. If M and N are left Λ -lattices, then $M \cong N$ if and only if $KM \cong KN$ as left A -modules.*

Proof. If $M \cong N$, then clearly $KM \cong KN$. Conversely if $KM \cong KN$ then $\hat{K}\hat{M} \cong \hat{K}\hat{N}$ as left $\hat{\Lambda}$ -modules. If we decompose $\hat{\Lambda}$ into simple components, then there are corresponding decompositions

$$\hat{\Lambda} = \sum \Lambda_i, \quad \hat{M} = \sum \Lambda_i \hat{M}_i,$$

and each Λ_i is a maximal R_i -order in a central simple algebra, as in the proof of (18.1). From the isomorphism $\hat{K}\hat{M} \cong \hat{K}\hat{N}$ it follows that $\hat{K} \cdot \Lambda_i \hat{M} \cong \hat{K} \cdot \Lambda_i \hat{N}$

for each i , whence by (18.7(i)) we may conclude that $\Lambda_i \hat{M} \cong \Lambda_i \hat{N}$ for each i . Hence $\hat{M} \cong \hat{N}$, and so $M \cong N$ by (18.2(iii)).

Finally, if M is a left ideal of Λ , then $KM = Ae = K \cdot \Lambda e$ for some idempotent e in the semisimple ring A . Thus $M \cong \Lambda e$ by the first part of this proof, and the theorem is established.

EXERCISES

Unless otherwise stated, R denotes a discrete valuation ring, not necessarily complete.

1. Let Δ be a maximal R -order in a skewfield D with center K . Show that every left Δ -lattice is free. [Hint: Since Δ is hereditary, each left Δ -lattice M is isomorphic to a direct sum of ideals of Δ . Each such ideal is principal, hence is isomorphic to Δ .]

2. Prove (18.9(ii), (iii)) without using the results for the case where R is complete. [Hint: Let $\bar{\Lambda} = \Lambda/\text{rad } \Lambda$, and let $x\Lambda, y\Lambda$ be maximal right ideals of Λ . Then $\bar{x}\bar{\Lambda}, \bar{y}\bar{\Lambda}$ are maximal right ideals of the simple ring $\bar{\Lambda}$. By Exercise 7.12, there exists $u \in u(\bar{\Lambda})$ such that $u \cdot \bar{x}\bar{\Lambda} \cdot u^{-1} = \bar{y}\bar{\Lambda}$. Choose $v \in \Lambda$ with $\bar{v} = u$; then $v \in u(\Lambda)$ by Exercise 6.2. Therefore $v \cdot x\Lambda \cdot v^{-1} = y\Lambda$, since these maximal right ideals have the same image in $\bar{\Lambda}$.

Further, $\bar{\Lambda}\bar{x}$ is a maximal left ideal of $\bar{\Lambda}$, by Exercise 7.12. Therefore Λx is a maximal left ideal of Λ .]

3. In this exercise, R denotes a semilocal Dedekind domain, that is, a Dedekind domain with only a finite number of maximal ideals $\{P_1, \dots, P_n\}$. Let Λ be an R -order in a separable K -algebra A , and let M, N be left Λ -lattices. Show that $M \cong N$ if and only if $M_{P_i} \cong N_{P_i}$, $1 \leq i \leq n$. [Hint: Let $f_i: M_{P_i} \cong N_{P_i}$, $1 \leq i \leq n$. Replacing f_i by αf_i , $\alpha \in R - P_i$, we may assume that each $f_i \in \text{Hom}_R(M, N)$. Choose $\beta_1, \dots, \beta_n \in R$ such that $\beta_i \equiv 1 \pmod{P_i}$, $\beta_j \equiv 0 \pmod{P_j}$, $j \neq i$. Set $f = \sum \beta_i f_i$, and show that $f: M \rightarrow N$ is an epimorphism, by verifying that $f_{P_i}: M_{P_i} \rightarrow N_{P_i}$ is epic for $1 \leq i \leq n$. Deduce from this that f is an isomorphism.]

4. Which of the results of this section remain true when R is assumed to be a semilocal Dedekind domain, rather than a discrete valuation ring?

19. IDEALS

Throughout this section, let Λ be a maximal R -order in a central simple K -algebra A , where R is a discrete valuation ring, not necessarily complete. We shall study here the factorization properties of one-sided ideals of Λ , and begin with a number of definitions.

For a pair of full R -lattices M, N in A , define their product $M \cdot N$ in the usual way, as the full R -lattice consisting of all finite sums $\sum m_i n_i$, $m_i \in M$, $n_i \in N$. Call M a *normal ideal* in A if both $O_l(M)$ and $O_r(M)$ are maximal orders. By (17.6) and (18.8(ii)), if one of these orders is maximal, then so is the other. Call these orders *similar*; by (18.7), they are necessarily conjugate in A . The normal ideal M is *two-sided* if $O_l(M) = O_r(M)$. In the special case where

$A = K$, the normal ideals are precisely the fractional R -ideals of K (see §4a), and are of course two-sided.

An *integral ideal* in A is a normal ideal M such that $M \subset O_r(M)$.

(19.1) THEOREM. *If M is a normal ideal such that $M \subset O_l(M)$, then also $M \subset O_r(M)$, and conversely.*

Proof. Let $\Lambda = O_l(M)$, so M is a left ideal of Λ . Hence $M = \Lambda x$ for some $x \in u(A)$, and clearly

$$(19.2) \quad O_r(M) = O_r(\Lambda x) = x^{-1}\Lambda x.$$

Since $x \in \Lambda$, we have $x\Lambda \subset \Lambda$, whence

$$M = x^{-1} \cdot x\Lambda \cdot x \subset x^{-1}\Lambda x = O_r(M).$$

This completes the proof.

If M is a two-sided normal ideal with $\Lambda = O_l(M) = O_r(M)$, we shall also refer to M as a *two-sided Λ -ideal* in A .

(19.3) THEOREM. *The set of two-sided Λ -ideals in A is an infinite cyclic group with generator $\text{rad } \Lambda$ and identity element Λ , relative to the usual multiplication of lattices.*

Proof. Let $\mathfrak{P} = \text{rad } \Lambda$, so by (18.3) every nonzero two-sided ideal of Λ is a power of \mathfrak{P} . In particular we have $\pi\Lambda = \mathfrak{P}^m$ for some m . Define $\mathfrak{P}^{-1} = \pi^{-1}\mathfrak{P}^{m-1}$, a two-sided Λ -ideal in A . Then $\mathfrak{P} \cdot \mathfrak{P}^{-1} = \mathfrak{P}^{-1} \cdot \mathfrak{P} = \Lambda$. If X is any two-sided Λ -ideal in A , then for some s , $\pi^s X$ is a two-sided ideal in Λ , and so $X = \pi^{-s}\mathfrak{P}^k$ for some k . Thus X is a power of \mathfrak{P} , and $X^{-1} = \pi^s(\mathfrak{P}^{-1})^k$. This completes the proof.

An integral ideal M will be called a *maximal integral ideal* if M is a maximal left ideal in $O_l(M)$. (Some authors refer to such ideals as *indecomposable* ideals, but we shall not use this terminology here.)

(19.4) THEOREM. *If the normal ideal M is a maximal left ideal of $O_l(M)$, then M is a maximal right ideal in $O_r(M)$, and conversely.*

Proof. Let $M = \Lambda x$ be a maximal left ideal in Λ , where $\Lambda = O_l(M)$. By (19.2), $O_r(M) = x^{-1}\Lambda x = \Lambda'$, say. By (18.9), $x\Lambda$ is a maximal right ideal in Λ . Therefore $x^{-1} \cdot x\Lambda \cdot x$ is a maximal right ideal in $x^{-1}\Lambda x$. This proves that M is a maximal right ideal in Λ' , as claimed. We also remark for future use that conjugation by x^{-1} yields an isomorphism of R -modules:

$$(19.5) \quad \frac{\Lambda}{\Lambda x} \cong \frac{x^{-1}\Lambda x}{x^{-1} \cdot \Lambda x \cdot x} = \frac{\Lambda'}{\Lambda' x}.$$

We have thus proved that the property of an integral ideal being maximal does not depend on whether we consider it as a left ideal in its left order, or a right ideal in its right order. We may also conclude that *all* maximal integral ideals in A are mutually conjugate, since each pair of maximal orders are conjugate, and for a given maximal order Λ , any two maximal left ideals of Λ are conjugate by (18.9).

Let M, N be any pair of full R -lattices in A . We say that their product $M \cdot N$ is *proper* if $O_r(M) = O_l(N)$. Likewise, a product $M_1 \cdot M_2 \cdots M_k$ is *proper* if $O_r(M_i) = O_l(M_{i+1})$, $1 \leq i \leq k-1$.

(19.6) THEOREM. *Let M be a proper left ideal of the maximal order Λ , such that the Λ -module Λ/M has a composition series of length k . Then M is expressible as a proper product of k maximal integral ideals*

$$M = M_1 M_2 \cdots M_k,$$

with

$$O_l(M) = O_l(M_1), \quad O_r(M) = O_r(M_k).$$

Proof. Use induction on k , the result being trivial when $k = 1$. Assume that $k > 1$, and that the theorem is known for the case $k - 1$. We can choose a maximal left ideal Λx of Λ such that $M \subset \Lambda x \subset \Lambda$, and then $\Lambda x/M$ has composition length $k - 1$. Let $\Lambda' = x^{-1}\Lambda x$; then Λ' is a maximal order, and there is a bijection $W \rightarrow x^{-1}W$ between the set of Λ -modules W and the set of Λ' -modules $x^{-1}W$. Therefore $x^{-1}M$ is a left ideal of Λ' , and $x^{-1}\Lambda x/x^{-1}M$ has composition length $k - 1$ as left Λ' -module. It follows from the induction hypothesis that we may write $x^{-1}M = M_2 \cdots M_k$, a proper product of maximal integral ideals, with

$$O_l(M_2) = O_l(x^{-1}M) = x^{-1}\Lambda x = \Lambda'.$$

If we set $M_1 = \Lambda x$, then M_1 is a maximal integral ideal such that $O_r(M_1) = \Lambda'$. Therefore the factorization

$$M = \Lambda x \cdot x^{-1}M = M_1 M_2 \cdots M_k$$

expresses M as a proper product of maximal integral ideals. Once such a factorization is known, then there are obvious inclusions

$$O_l(M) \supset O_l(M_1), \quad O_r(M) \supset O_r(M_k).$$

Since all of these orders are maximal, equality must hold. This completes the proof.

(19.7) COROLLARY. Let $\text{rad } \Lambda$ have capacity t , that is,

$$\Lambda/\text{rad } \Lambda \cong M_t(S)$$

for some skewfield S . Then $\text{rad } \Lambda$ is expressible as a proper product of t maximal integral ideals.

Proof. $M_t(S)$ is a direct sum of t simple left Λ -modules, and hence $\Lambda/\text{rad } \Lambda$ has composition length t .

EXERCISES

1. Show that in a proper product of maximal integral ideals, the factors need not commute with one another. [Hint: Suppose that $M_1 \cdot M_2 = M_2 \cdot M_1$, where M_1, M_2 are maximal integral ideals. If the algebra A is $M_n(D)$, where $n > 1$, then M_1 is not a two-sided $O_i(M_1)$ -ideal. Therefore

$$O_i(M_1 M_2) = O_i(M_1), \quad O_i(M_2 M_1) = O_i(M_2) = O_r(M_1) \neq O_i(M_1).]$$

2. Show that in some cases an integral ideal may be expressed in more than one way as a proper product of maximal integral ideals. [Hint: Let $A = M_2(K)$, $\Lambda = M_2(R)$, $x_1 = \begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix}$, $x_2 = \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}$, where π is a prime element of R . Then x_1, x_2 commute, and

$$\pi\Lambda = \Lambda x_1 \cdot x_1^{-1}(\Lambda x_2)x_1 = \Lambda x_2 \cdot x_2^{-1}(\Lambda x_1)x_2$$

gives two different factorizations of $\pi\Lambda$.]

20. DIFFERENT, DISCRIMINANT

Throughout this section, R denotes a discrete valuation ring, not necessarily complete, and Λ a maximal R -order in a central simple K -algebra A . Let $\text{tr}_{A/K}$ denote the reduced trace map, and $\tau_{A/K}: A \times A \rightarrow K$ the bilinear reduced trace form defined by $\tau(a, b) = \text{tr}(ab)$. We shall drop the subscript A/K when there is no danger of confusion.

We define

$$\tilde{\Lambda} = \{x \in A: \tau(x, \Lambda) \subset R\} = \{x \in A: \text{tr}(x\Lambda) \subset R\}.$$

By Exercise 4.12, $\tilde{\Lambda}$ is a full R -lattice in A , and is clearly a two-sided Λ -module containing Λ (by (10.1)). Let $\mathfrak{P} = \text{rad } \Lambda$; then by (19.3) we have $\tilde{\Lambda} = \mathfrak{P}^{-m}$ for some $m \geq 0$. Call $\tilde{\Lambda}$ the *inverse different*, and define the *different*

$$\mathfrak{D} = \mathfrak{D}(\Lambda/R) = \mathfrak{P}^m.$$

(20.1) THEOREM. If \hat{R} is the P -adic completion of R , then

$$\mathfrak{D}(\tilde{\Lambda}/\hat{R}) = \hat{R} \otimes_R \mathfrak{D}(\Lambda/R).$$

Proof. By (9.29), $\text{tr}_{\hat{A}/\hat{R}}$ extends the map $\text{tr}_{A/K}$. Hence for each $x \in A$ we have

$$\mathrm{tr}_{A/K}(x\Lambda) \subset R \iff \mathrm{tr}_{\hat{A}/\hat{R}}(x\Lambda) \subset \hat{R} \iff x \in \tilde{\Lambda}.$$

This proves that $\tilde{\Lambda} = A \cap \tilde{\Lambda}$. If $\mathfrak{P} = \mathrm{rad} \Lambda$, then $\mathfrak{P} = A \cap \hat{\mathfrak{P}}$, where $\hat{\mathfrak{P}} = \mathrm{rad} \hat{\Lambda}$. Thus if $\tilde{\Lambda} = \hat{\mathfrak{P}}^{-k}$, then $\tilde{\Lambda} = \mathfrak{P}^{-k}$. This gives the desired result. For later use, we remark that the proof is equally valid for the more general case where A is a separable K -algebra.

(20.2) THEOREM. Let $A = M_r(D)$, where D is a skewfield with center K , and let $\Lambda = M_r(\Delta)$, where Δ is a maximal R -order in D . Then

$$\mathfrak{D}(\Lambda/R) = \mathfrak{D}(\Delta/R) \cdot \Lambda.$$

Proof. Let $x = (d_{ij}) \in M_r(D)$, and let $\lambda = (\beta_{ij}) \in M_r(\Delta)$. Then by Exercise 9.5,

$$\mathrm{tr}_{A/K}(x\lambda) = \sum_{i,j} \mathrm{tr}_{D/K}(d_{ij}\beta_{ji}).$$

Hence if each $d_{ij} \in \tilde{\Lambda}$, then $x \in \tilde{\Lambda}$. On the other hand, let λ have entry β at position (k, l) , and zeros elsewhere, with β variable in Δ . Then $\mathrm{tr}_{A/K}(x\lambda) = \mathrm{tr}_{D/K}(d_{lk}\beta)$, so if $x \in \tilde{\Lambda}$ then $d_{lk} \in \tilde{\Lambda}$. This proves that $\tilde{\Lambda} = M_r(\tilde{\Lambda})$. If $\tilde{\Lambda} = (\mathrm{rad} \Delta)^{-m}$, then

$$\tilde{\Lambda} = M_r((\mathrm{rad} \Delta)^{-m}) = \{M_r(\mathrm{rad} \Delta)\}^{-m} = \{\mathrm{rad} \Lambda\}^{-m},$$

which proves the theorem.

Together, these results yield

(20.3) THEOREM. Let $\hat{K} \otimes_K A \cong M_t(E)$, where E is a skewfield with center \hat{K} and index m , that is, $m^2 = (E:\hat{K})$. Suppose that the residue class field \bar{R} is finite. Then

$$\mathfrak{D}(\Lambda/R) = \mathfrak{P}^{m-1}.$$

Proof. By (20.1) it suffices to prove that $\mathfrak{D}(\hat{\Lambda}/\hat{R}) = \hat{\mathfrak{P}}^{m-1}$. Now $\hat{\Lambda}$ is a maximal \hat{R} -order in $M_t(E)$, so by (17.4) we may write $\hat{\Lambda} = M_t(\Omega)$ for some maximal \hat{R} -order Ω in E . By (20.2) we obtain

$$\mathfrak{D}(\hat{\Lambda}/\hat{R}) = \mathfrak{D}(\Omega/\hat{R}) \cdot \hat{\Lambda}.$$

But $\mathfrak{D}(\Omega/\hat{R}) = (\mathrm{rad} \Omega)^{m-1}$ by (14.9), which completes the proof.

For any left ideal L of Λ , define its *norm* as

$$N_{A/K}(L) = \mathrm{ord}_R \Lambda/L.$$

(20.4) THEOREM. The discriminant $d(\Lambda/R)$ is given by

$$d(\Lambda/R) = N_{A/K}(\mathfrak{D}(\Lambda/R)).$$

Proof. Both the discriminant and the different behave properly under the passage from R to \hat{R} , by (20.1) and Exercise 10.6. So likewise does the norm, and thus it suffices to prove the result for the case where R is complete. But then $\Lambda \cong M_t(\Omega)$ as in the proof of (20.3), and $\mathfrak{D}(\Lambda/R) = \pi_{\Omega}^k \cdot \Lambda$ for some k . Therefore

$$N(\mathfrak{D}(\Lambda/R)) = \text{ord}_R \Lambda / \pi_{\Omega}^k \Lambda = \text{ord}_R \pi_{\Omega}^{-k} \Lambda / \Lambda = \text{ord}_{\hat{R}} \tilde{\Lambda} / \Lambda.$$

The rest of the proof is exactly like that of (14.8).

6. Maximal Orders over Dedekind Domains

Throughout this chapter, R denotes a Dedekind domain with quotient field K , $R \neq K$, and P ranges over the maximal ideals of R . Let R_P be the localization of R at P , and \hat{R}_P the P -adic completion of R . Let \hat{K}_P be the quotient field of \hat{R}_P . For Λ any R -order in the separable K -algebra A , and M any Λ -module, set

$$\hat{\Lambda}_P = \hat{R}_P \otimes_R \Lambda, \quad \hat{M}_P = \hat{R}_P \otimes_R M, \quad \hat{A}_P = \hat{K}_P \otimes_K A.$$

Then $\hat{\Lambda}_P$ is an \hat{R}_P -order in \hat{A}_P , and \hat{M}_P is a $\hat{\Lambda}_P$ -module. It follows from Exercise 7.13 that \hat{A}_P is a separable \hat{K}_P -algebra.

In this chapter we shall generalize the theorems obtained in Chapters III and V. There are two ways of accomplishing this. In the first approach, followed in §§ 21–22, we use the local results from Chapter V, together with the techniques of § 5a, to obtain global results. The second approach, given in § 23, is independent of the first, and also yields the basic theorems for the global case. In this second method, we give some straightforward generalizations of some of the familiar proofs in algebraic number theory. Indeed, this same dichotomy already occurs in algebraic number theory. One can develop the ideal theory of Dedekind domains either from the standpoint of valuation theory (first approach), or by manipulations with the ideals themselves (second approach). Just as in algebraic number theory, however, we cannot in the long run avoid the use of P -adic completions. Many of the deeper results depend on the interrelations between the global and local theories. Indeed, we have already seen in (20.3) that when R is a discrete valuation ring, we may calculate the different $\mathfrak{D}(\Lambda/R)$ by passing to completions.

21. BASIC RESULTS

Let Λ be an R -order in the separable K -algebra A , and suppose that there are decompositions

$$(21.1) \quad \hat{A}_P = \sum^* A_i \text{ (simple components)}, \quad \hat{\Lambda}_P = \sum^* \Lambda_i,$$

where Λ_i is an \hat{R}_P -order in A_i . Let K_i be the center of A_i , and R_i the integral closure of \hat{R}_P in K_i . By (10.5), the maximal \hat{R}_P -orders in A_i coincide with the maximal R_i -orders in A_i . In particular, if Λ is a maximal R -order in A , then

by (11.6) $\hat{\Lambda}_P$ is a maximal \hat{R}_P -order in \hat{A}_P , and so by (10.5) there is a decomposition $\hat{\Lambda}_P = \sum \Lambda_i$, with each Λ_i a maximal R_i -order in the central simple K_i -algebra A_i . We may then apply the results of Chapter V, on maximal orders in central simple algebras over complete fields, to the orders Λ_i .

Conversely, if the order $\hat{\Lambda}_P$ is known to have a decomposition as in (21.1) for each P , and if each Λ_i is a maximal order in A_i , then we may conclude from (10.5) that Λ is necessarily a maximal order in A . As an illustration of these remarks, we prove a number of basic results.

(21.2) **Theorem.** *Let M be a full R -lattice in A . Then $O_l(M)$ is a maximal R -order in A if and only if $O_r(M)$ is a maximal R -order in A .*

Proof. We know that \hat{R}_P is R -flat, by (2.22) or Exercise 5.4. As in the proof of (8.5), it follows that

$$(21.3) \quad O_r(\hat{M}_P) = \hat{R}_P \otimes_R O_r(M),$$

and likewise for left orders. Now suppose that $\Lambda = O_l(M)$ is maximal, and let $\Gamma = O_r(M)$. Keeping the notation of (21.1), there is also a decomposition $\hat{M}_P = \sum M_i$, where M_i is a full \hat{R}_P -lattice in A_i , and where $\Lambda_i = O_l(M_i)$. But then there is a decomposition

$$\hat{\Gamma} = \sum \Gamma_i, \quad \text{where } \Gamma_i = O_r(M_i).$$

Since Λ is maximal, so is each Λ_i , whence so is each Γ_i by (17.6). Therefore Γ is maximal, by the remarks preceding the theorem, and the proof is complete.

(21.4) **Theorem.** *Maximal orders are left and right hereditary.*

Proof. Let Λ be a maximal R -order in A , and use the notation of (21.1). Each Λ_i is hereditary by (17.3), whence $\hat{\Lambda}_P$ is hereditary for each P . Thus Λ is itself hereditary, by (3.24) and (3.30).

(21.5) **COROLLARY.** *Let Λ be a maximal order. Then every left Λ -lattice M is Λ -projective. Further, M is indecomposable if and only if KM is a simple A -module.*

Proof. Since Λ is hereditary, M is projective by (10.7). If M decomposes, so does KM . Conversely, let W be any A -submodule of KM , and set $N = M \cap W$. Then N is a Λ -submodule of M , and by (4.0) the Λ -module M/N is an R -lattice. Hence M/N is Λ -projective, and so the Λ -exact sequence

$$0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$$

is split. This gives a decomposition of M , unless $W = 0$ or $W = KM$, which completes the proof.

We are now ready to determine *all* maximal R -orders in A . We have seen that it suffices to handle the case of central simple algebras. We prove

(21.6) Theorem. *Let $A = \text{Hom}_D(V, V)$ be a simple algebra, where V is a right vector space of dimension r over the skewfield D with center K . Let Δ be some fixed maximal R -order in D , and let M be any full right Δ -lattice in V . Then $\text{Hom}_\Delta(M, M)$ is a maximal R -order in A . If Λ' is any maximal R -order in A , then there exists a full right Δ -lattice N in V such that $\Lambda' = \text{Hom}_\Delta(N, N)$.*

Proof. Letting $\Lambda = \text{Hom}_\Delta(M, M)$, we have

$$\Lambda_P = R_P \otimes_R \Lambda = \text{Hom}_{\Delta_P}(M_P, M_P)$$

for each P . By (18.7) every right ideal of Δ_P is principal, whence M_P is Δ_P -free. Hence by (8.7) Λ_P is a maximal R_P -order. This holds for each P , and so Λ is maximal by (11.2).

Now let Λ' be any maximal R -order in A . Since Λ and Λ' are a pair of full R -lattices in A , we have $\Lambda'_P = \Lambda_P$ a.e., say except at P_1, \dots, P_n . By (18.7), for each P there exists an element $u_P \in u(A)$ such that $\Lambda'_P = u_P \Lambda_P u_P^{-1}$, and we may take $u_P = 1$ for $P \neq P_1, \dots, P_n$. For each P , set $X(P) = u_P M_P$; then we have

$$\Lambda'_P = \text{Hom}_{\Delta_P}(X(P), X(P)).$$

If we define $N = \bigcap_P X(P)$, then by (4.22) N is a full right Δ -lattice in A , such that $N_P = X(P)$ for all P . But then Λ' and $\text{Hom}_\Delta(N, N)$ are a pair of full R -lattices in A , with the same localizations for each P . Therefore $\Lambda' = \text{Hom}_\Delta(N, N)$ by Exercise 3.2, and the theorem is proved.

(21.7) COROLLARY. *Keeping the above notation, every maximal order in A is Morita equivalent to Δ .*

Proof. Every maximal order Λ in A is of the form $\Lambda = \text{Hom}_\Delta(M, M)$, where M is some full right Δ -lattice in V . Since Δ is hereditary, it is clear that M is a finitely generated projective Δ -module. We wish to show that M is a progenerator for the category \mathcal{M}_Δ , and so we must verify that $\text{Hom}_\Delta(M, \cdot)$ is a faithful functor. But for each Δ -module L , we know that

$$\{\text{Hom}_\Delta(M, L)\}_P \cong \text{Hom}_{\Delta_P}(M_P, L_P)$$

for each P . Since M_P is Δ_P -free by Exercise 18.1, it follows from §15 that $\text{Hom}_{\Delta_P}(M_P, \cdot)$ is a faithful functor. Therefore $\text{Hom}_\Delta(M, \cdot)$ is also faithful,

and so we have proved that M_Δ is a progenerator for \mathcal{M}_Δ . Hence Λ and Δ are Morita equivalent, by (16.9), and the result is established.

EXERCISES

1. Let Λ be a maximal R -order in a separable K -algebra A , and let M be any left Λ -lattice. Show that the endomorphism ring $\text{End}_\Lambda M$ is a maximal R -order in the separable K -algebra $\text{End}_A KM$.

[Hint: It suffices to prove the result when A is a central simple K -algebra, and where R is a discrete valuation ring. Set $\Gamma = \text{End}_\Lambda M$, $B = \text{End}_A KM$, and let V be a simple left A -module. Then $D = \text{End}_A V$ is the skewfield part of A . We have $KM \cong V^{(t)}$ for some t , whence $B \cong \text{End}_A V^{(t)} \cong M_t(D)$. Thus B is also a central simple K -algebra.]

Now choose a left Λ -lattice L in V such that $KL = V$. Then $KM \cong (KL)^{(t)}$, whence $M \cong L^{(t)}$ by (18.10). Therefore

$$\Gamma = \text{End}_\Lambda M \cong \text{End}_\Lambda L^{(t)} \cong M_t(\Delta),$$

where $\Delta = \text{End}_\Lambda L$ is a maximal R -order in D . Hence Γ is a maximal R -order in B , as claimed.]

22. IDEAL THEORY

In this section we shall develop the theory of one-sided and two-sided ideals in maximal orders over a Dedekind ring R with quotient field K , by using the results of §§18, 19 for the local case. Let P, Q, \dots denote prime ideals of R , *always assumed to be nonzero*. To begin with, let Λ be any R -order in a separable K -algebra A .

A *prime ideal* of Λ is a proper two-sided ideal \mathfrak{P} in Λ , such that $K \cdot \mathfrak{P} = A$, and such that for every pair of two-sided ideals S, T in Λ ,

$$(22.1) \quad S \cdot T \subset \mathfrak{P} \implies S \subset \mathfrak{P} \quad \text{or} \quad T \subset \mathfrak{P}.$$

There is no loss of generality in imposing this condition only for the special case where both S and T contain \mathfrak{P} ; for if (22.1) holds in this special case, then in the general case we have

$$\begin{aligned} S \cdot T \subset \mathfrak{P} &\implies (S + \mathfrak{P})(T + \mathfrak{P}) \subset \mathfrak{P} \implies S + \mathfrak{P} \subset \mathfrak{P} \quad \text{or} \quad T + \mathfrak{P} \subset \mathfrak{P} \\ &\implies S \subset \mathfrak{P} \quad \text{or} \quad T \subset \mathfrak{P}. \end{aligned}$$

Hence (22.1) is equivalent to the following condition: for each pair of two-sided ideals J, J' in Λ/\mathfrak{P} ,

$$(22.2) \quad J \cdot J' = 0 \implies J = 0 \quad \text{or} \quad J' = 0.$$

(22.3) **THEOREM.** *The prime ideals of Λ coincide with the maximal two-sided ideals of Λ . If \mathfrak{P} is a prime ideal of Λ , then $P = \mathfrak{P} \cap R$ is a (nonzero) prime ideal*

of R , and $\bar{\Lambda} = \Lambda/\mathfrak{P}$ is a finite dimensional simple algebra over the field R/P .

Proof. Let \mathfrak{P} be a prime ideal of Λ , and set $P = \mathfrak{P} \cap R$, $\bar{\Lambda} = \Lambda/\mathfrak{P}$. Since \mathfrak{P} is a full R -lattice in Λ , we have $P \neq 0$. On the other hand, $P < R$ since $1 \notin \mathfrak{P}$. If $\alpha, \beta \in R$, then

$$\begin{aligned}\alpha\beta \in P &\implies \alpha\Lambda \cdot \beta\Lambda \subset \mathfrak{P} \implies \alpha\Lambda \subset \mathfrak{P} \quad \text{or} \quad \beta\Lambda \subset \mathfrak{P} \\ &\implies \alpha \in P \quad \text{or} \quad \beta \in P.\end{aligned}$$

Thus P is a prime ideal of R , and $\bar{\Lambda}$ is a finite dimensional algebra over the field R/P .

Next we observe that $\text{rad } \bar{\Lambda}$ is nilpotent, since $\bar{\Lambda}$ is artinian. Thus $\text{rad } \bar{\Lambda} = 0$ by (22.2), and so $\bar{\Lambda}$ is semisimple. However, the simple components of $\bar{\Lambda}$ are two-sided ideals of $\bar{\Lambda}$ which annihilate one another. Hence by (22.2) there is only one simple component, that is, $\bar{\Lambda}$ is a simple algebra. Therefore $\bar{\Lambda}$ has no nontrivial two-sided ideals, whence \mathfrak{P} is a maximal two-sided ideal of Λ .

Conversely, let \mathfrak{P} be any maximal two-sided ideal of Λ . Then (22.1) automatically holds true when S and T contain \mathfrak{P} , since the only possibilities for S and T are \mathfrak{P} and Λ . This shows that \mathfrak{P} is a prime ideal, and establishes the theorem.

Keeping the above notation, we prove.

(22.4) THEOREM. *Let Λ be a maximal R -order in a central simple K -algebra A . There is a one-to-one correspondence $\mathfrak{P} \leftrightarrow P$ between the set of prime ideals \mathfrak{P} of Λ , and the set of prime ideals P of R , given by*

$$P = R \cap \mathfrak{P}, \quad \mathfrak{P} = \Lambda \cap \text{rad } \Lambda_P.$$

Further, $\mathfrak{P} \cdot \Lambda_P = \text{rad } \Lambda_P$, the unique prime ideal of Λ_P . For each prime ideal Q of R different from P , we have $\mathfrak{P}_Q = \Lambda_Q$.

Proof. Let \mathfrak{P} be a prime ideal of Λ , and set $\bar{\Lambda} = \Lambda/\mathfrak{P}$, $P = R \cap \mathfrak{P}$. Then $\text{ann}_R \bar{\Lambda} = P$, so by (3.6) it follows that

$$\bar{\Lambda} \cong R_P \otimes_R \bar{\Lambda} \cong \Lambda_P / \mathfrak{P} \cdot \Lambda_P.$$

But $\bar{\Lambda}$ is a simple ring, and hence $\mathfrak{P} \cdot \Lambda_P$ is a maximal two-sided ideal of Λ_P . By (18.3), all two-sided ideals of Λ_P are powers of $\text{rad } \Lambda_P$. Therefore

$$\mathfrak{P}_P = \mathfrak{P} \cdot \Lambda_P = \text{rad } \Lambda_P,$$

as claimed. Furthermore, Λ/\mathfrak{P} is torsionfree relative to the multiplicative set $R - P$, so by (3.10) we obtain

$$\mathfrak{P} = \Lambda \cap \mathfrak{P}_P = \Lambda \cap \text{rad } \Lambda_P.$$

Finally, for $Q \neq P$ we have $R_Q \otimes_R (\Lambda/\mathfrak{P}) = 0$, and thus $\mathfrak{P}_Q = \Lambda_Q$.

Conversely, given a prime ideal P of R , we may form the two-sided ideal $P\Lambda$ of Λ . Then $P\Lambda \neq \Lambda$, since Λ is an R -lattice, and so there exists a maximal two-sided ideal \mathfrak{P} of Λ with $P\Lambda \subset \mathfrak{P}$. Clearly $P = R \cap \mathfrak{P}$, since the intersection is a prime ideal of R containing P . The preceding discussion shows that $\mathfrak{P} = \Lambda \cap \text{rad } \Lambda_P$, so P uniquely determines \mathfrak{P} . This completes the proof of the theorem.

Now let L be any full R -lattice in the separable K -algebra A , and define
(22.5)
$$L^{-1} = \{x \in A : L \cdot x \cdot L \subset L\}.$$

Clearly

$$(22.6) \quad L^{-1} = \{x \in A : L \cdot x \subset O_l(L)\} = \{x \in A : x \cdot L \subset O_r(L)\}.$$

If $\Lambda = O_r(L)$, then $\alpha\Lambda \subset L \subset \beta\Lambda$ for some nonzero $\alpha, \beta \in R$. Therefore $\alpha^{-1}\Lambda \supset L^{-1} \supset \beta^{-1}\Lambda$, since

$$\alpha^{-1}\Lambda = \{x \in A : \alpha\Lambda \cdot x \subset \Lambda\} \supset \{x \in A : L \cdot x \subset \Lambda\} = L^{-1},$$

and likewise for the other inclusion. Thus L^{-1} is also a full R -lattice in A . We shall call L a *full left Λ -lattice* in A , to indicate that L is a left Λ -module which is a full R -lattice in A . Then L^{-1} is a full right Λ -lattice in A .

We may identify L^{-1} with $\text{Hom}_\Lambda(L, \Lambda)$, where L, Λ are viewed as left Λ -modules. For each prime ideal P of R , L_P is a full left Λ_P -lattice in A . By (3.18) we have

$$(L^{-1})_P = R_P \otimes_R \text{Hom}_\Lambda(L, \Lambda) \cong \text{Hom}_{\Lambda_P}(L_P, \Lambda_P) = (L_P)^{-1}.$$

Hereafter, we shall identify $(L^{-1})_P$ with $(L_P)^{-1}$. Likewise, we identify

$$\hat{R}_P \otimes_R L^{-1} \quad \text{and} \quad (\hat{L}_P)^{-1},$$

where \hat{R}_P, \hat{L}_P are P -adic completions of R, L , respectively.

(22.7) **THEOREM.** *Let L be a full left Λ -lattice in A , where Λ is a maximal R -order in a separable K -algebra A . Then*

$$L \cdot L^{-1} = \Lambda, \quad L^{-1} \cdot L = O_r(L), \quad (L^{-1})^{-1} = L.$$

Proof. In order to prove that $L \cdot L^{-1} = \Lambda$, it suffices by Exercise 3.2 to prove that

$$L_P \cdot (L_P)^{-1} = \Lambda_P$$

for each P . By (18.10) we may write $L_P = \Lambda_P y$ for some $y \in A$. Then $A = Ay$, which implies by (6.3a) that $y \in u(A)$. Therefore

$$(L_P)^{-1} = \{x \in A : \Lambda_P y \cdot x \subset \Lambda_P\} = y^{-1}\Lambda_P.$$

This gives $L_P \cdot L_P^{-1} = \Lambda_P y \cdot y^{-1} \Lambda_P = \Lambda_P$, as desired, and shows that $L \cdot L^{-1} = \Lambda$. The argument also yields the formula

$$(L_P)^{-1} \cdot L_P = y^{-1} \Lambda_P y = O_r(L_P)$$

for each P , whence $L^{-1} \cdot L = O_r(L)$. Likewise $(L^{-1})^{-1} = L$, since this holds locally at each P , and the theorem is established.

(22.8) COROLLARY. *Keeping the above notation, we have*

$$O_l(L^{-1}) = O_r(L), \quad O_r(L^{-1}) = O_l(L).$$

Proof. The first equality holds locally:

$$O_l(L_P^{-1}) = O_l(y^{-1} \Lambda_P) = y^{-1} \Lambda_P y = O_r(L_P).$$

Thus the first assertion is correct, and the second follows in the same way.

We now repeat several definitions, which were first given in the local case in §19. All ideals considered below are full R -lattices in A . Call a full R -lattice M a *normal ideal* if both $O_l(M)$ and $O_r(M)$ are maximal orders. An *integral ideal* of A is a normal ideal M such that $M \subset O_l(M)$.

(22.9) THEOREM. *If M is a normal ideal such that $M \subset O_l(M)$, then also $M \subset O_r(M)$, and conversely.*

Proof. It suffices to establish the result after localizing at an arbitrary prime ideal P of R . But the local result has already been proved in (19.1). (See also Exercise 22.9.)

If M is a normal ideal with $O_l(M) = O_r(M) = \Lambda$, we shall also refer to M as a *two-sided Λ -ideal* in A .

(22.10) THEOREM. *Let Λ be a maximal R -order in the central simple K -algebra A . Then the set of two-sided Λ -ideals in A is the free abelian group generated by the prime ideals of Λ . The group operation is the usual multiplication of lattices, the identity element is Λ , and inverses are given by (22.5).*

Proof. Let $\mathfrak{P}_1, \mathfrak{P}_2$ be distinct prime ideals of Λ , and let $P_i = \mathfrak{P}_i \cap R$, so $P_1 \neq P_2$. For Q any prime ideal of R , we have

$$(22.11) \quad (\mathfrak{P}_i)_Q = \begin{cases} \Lambda_Q, & Q \neq P_i, \\ (\mathfrak{P}_i)_Q, & Q = P_i. \end{cases}$$

But then $\mathfrak{P}_1 \cdot \mathfrak{P}_2 = \mathfrak{P}_2 \cdot \mathfrak{P}_1$, since this is true locally at every Q .

Now let M be a two-sided Λ -ideal in A . Then for each Q , M_Q is a two-sided

Λ_Q -ideal in A , and so by (19.3) we have

$$M_Q = \mathfrak{Q}_Q^{m_Q} \text{ for some } m_Q \in \mathbb{Z},$$

where \mathfrak{Q} is the prime ideal of Λ corresponding to Q . It should be pointed out that the definition of \mathfrak{Q}_Q^{-1} given in (19.3) agrees with the definition of inverse given in (22.6). Furthermore, $m_Q = 0$ a.e., since $M_Q = \Lambda_Q$ a.e. It follows at once that

$$M = \prod_Q \mathfrak{Q}^{m_Q},$$

since this result holds everywhere locally. Indeed, for any P we have

$$M_P = \mathfrak{P}_P^{m_P} = \prod_Q \mathfrak{Q}_P^{m_Q},$$

by (22.11). Finally, the ideal group is free abelian on the generators $\{\mathfrak{P}\}$, since the ideal M uniquely determines the exponents in the factorization of M . This completes the proof.

(22.12) COROLLARY. *The preceding theorem is valid for the more general case where Λ is a maximal R -order in a separable K -algebra A .*

Proof. Let A and Λ be decomposed into components as in (10.5). Then every two-sided Λ -ideal M in A decomposes into a direct sum $\sum M_i$, where M_i is a two-sided Λ_i -ideal in the central simple K_i -algebra A_i . In particular, each maximal two-sided ideal of Λ is of the form

$$(22.13) \quad \Lambda_1 \oplus \cdots \oplus \Lambda_{j-1} \oplus \mathfrak{P}_j \oplus \Lambda_{j+1} \oplus \cdots \oplus \Lambda_t$$

for some j , $1 \leq j \leq t$, and some prime ideal \mathfrak{P}_j in Λ_j . Conversely, each such expression is a prime ideal of Λ . It follows at once that if we express M_j as a power product of prime ideals of Λ_j , then

$$(22.13a) \quad \Lambda_1 \oplus \cdots \oplus \Lambda_{j-1} \oplus M_j \oplus \Lambda_{j+1} \oplus \cdots \oplus \Lambda_t$$

is a power product of the corresponding prime ideals of Λ of the form (22.13). Since M is the product (for $1 \leq j \leq t$) of the expressions in (22.13a), it is clear that M is a power product of prime ideals of Λ . It is then also obvious that the prime ideals of Λ generate a free abelian group, and so the result is proved.

We have at our disposal all of the information necessary to describe how a prime ideal P of R behaves in a maximal R -order in a simple K -algebra:

(22.14) THEOREM. *Let A be a central simple L -algebra, and let L be a finite separable extension of K . Let S denote the integral closure of R in L . Given a prime ideal P of R , let P_1, \dots, P_d be the distinct primes of S dividing P , and set*

$e_i = e(P_i, L/K)$. Each P_i determines a prime ideal \mathfrak{P}_i of Λ by (22.4), and we may write

$$P_i \Lambda = \mathfrak{P}_i^{m_i}, \quad 1 \leq i \leq d,$$

for some positive integers $\{m_i\}$.

(i) The factorization of $P\Lambda$ into prime ideals of Λ is given by

$$P\Lambda = \prod_{i=1}^d \mathfrak{P}_i^{e_i m_i}.$$

(ii) For each i , m_i is the ramification index of the skewfield part of the central simple \hat{L} -algebra \hat{A} , where $\hat{\cdot}$ denotes P_i -adic completion.

(iii) If the residue class field R/P is finite, then for each i , m_i is the index of the skewfield part of \hat{A} .

Proof. From (4.27) we have $PS = \prod P_i^{e_i}$, whence

$$P\Lambda = \prod (P_i \Lambda)^{e_i} = \prod \mathfrak{P}_i^{e_i m_i}$$

as claimed. Now keep i fixed, and let \hat{L} , $\hat{\Lambda}$, \hat{A} denote P_i -adic completions. Since $\hat{\Lambda}$ is a maximal \hat{S} -order in \hat{A} , by (17.3) we may write

$$\hat{A} = M_r(D), \quad \hat{\Lambda} = M_r(\Delta),$$

where D is a skewfield with center \hat{L} , and Δ is the maximal \hat{S} -order in D . If m denotes the ramification index of D over \hat{L} , then by §13 we have

$$\hat{P}_i \Delta = (\pi_D \Delta)^m,$$

where π_D is a prime element of Δ . Therefore

$$\hat{P}_i \hat{\Lambda} = M_r(\hat{P}_i \Delta) = \pi_D^m \hat{\Lambda} = (\text{rad } \hat{\Lambda})^m.$$

On the other hand, $\text{rad } \hat{\Lambda}$ is the P_i -adic completion of \mathfrak{P}_i by (18.3). Therefore when we take completions on both sides of the equation $P_i \Lambda = \mathfrak{P}_i^{m_i}$ we obtain $\hat{P}_i \hat{\Lambda} = (\text{rad } \hat{\Lambda})^{m_i}$. This shows that $m_i = m$, and establishes (ii). Assertion (iii) follows from (i), by virtue of (14.3).

Let us turn next to the theory of one-sided ideals in a separable K -algebra A . A normal ideal M is called a *maximal integral ideal* in A if M is a maximal left ideal in its left order $O_l(M)$.

(22.15) THEOREM. For each maximal left ideal M of a maximal R -order Λ in a separable K -algebra A , there is a unique prime ideal \mathfrak{P} of Λ such that

$$(22.16) \quad \mathfrak{P} \subset M \subset \Lambda, \quad \mathfrak{P} = \text{ann}_{\Lambda} \Lambda/M = \{x \in \Lambda : x\Lambda \subset M\}.$$

We say that M belongs to \mathfrak{P} . Then Λ/M is a simple left module over the simple ring Λ/\mathfrak{P} . Conversely, each \mathfrak{P} determines a maximal left ideal M of Λ which belongs to \mathfrak{P} .

Proof. Given a maximal ideal M of Λ , we can decompose M and Λ according to the decomposition of A into simple components. It is then sufficient to prove the result when A is a central simple K -algebra. Now let $\mathfrak{P} = \text{ann}_\Lambda \Lambda/M$, a two-sided ideal of Λ . Choose a nonzero $\alpha \in R$ such that $\alpha\Lambda \subset M$; then $\alpha \in \mathfrak{P}$, so $\alpha\Lambda \subset \mathfrak{P}$, and thus Λ/\mathfrak{P} is an artinian ring. But Λ/M is a faithful left (Λ/\mathfrak{P}) -module, and is a simple module. Therefore the ring Λ/\mathfrak{P} is a simple artinian ring, and so \mathfrak{P} is a prime ideal of Λ , as claimed. Clearly $\mathfrak{P} = \mathfrak{P}\Lambda \subset M$. Furthermore, if \mathfrak{Q} is any two-sided ideal of Λ contained in M , then $\mathfrak{Q} \subset \text{ann}_\Lambda \Lambda/M = \mathfrak{P}$. Thus there is a unique prime ideal of Λ contained in M .

Conversely, given a prime ideal \mathfrak{P} of Λ , by Zorn's Lemma there exists a maximal left ideal M of Λ such that $\mathfrak{P} \subset M \subset \Lambda$. Then $\mathfrak{P} \subset \text{ann}_\Lambda \Lambda/M$, so equality must hold, and thus M belongs to \mathfrak{P} . This completes the proof.

(22.17) THEOREM. *Let M be a normal ideal in the separable K -algebra A . If M is a maximal left ideal of $O_l(M)$, then M is a maximal right ideal of $O_r(M)$, and conversely.*

Proof. As remarked above, it suffices to prove the result for the special case where A is a central simple K -algebra. Let $\Lambda = O_l(M)$, and let \mathfrak{P} be the prime ideal of Λ to which M belongs. Setting $P = R \cap \mathfrak{P}$, it is clear that $\text{ann}_R \Lambda/M = P$, whence by (3.6) we have $\Lambda_P/M_P \cong \Lambda/M$. Thus M_P is a maximal left ideal of Λ_P . If we set $\Lambda' = O_r(M)$, it then follows from (19.4) that M_P is a maximal right ideal of Λ'_P .

On the other hand, let Q be any prime ideal of R different from P . Then $\mathfrak{P}_Q = M_Q = \Lambda_Q$, and so

$$\Lambda'_Q = O_r(M_Q) = \Lambda_Q = M_Q.$$

Now let $M \subset N \subset \Lambda'$, where N is any right ideal of Λ' . Then $M_Q = N_Q$ for $Q \neq P$, whereas N_P is either M_P or Λ'_P . In the former case we see that $N = M$, while in the latter case $N = \Lambda'$. Thus M is a maximal right ideal of Λ' , and the theorem is proved.

Let M, N be any pair of full R -lattices in the separable K -algebra A . Their product $M \cdot N$ is *proper* if $O_r(M) = O_l(N)$. Likewise, a product $M_1 M_2 \cdots M_k$ is called *proper* if

$$O_r(M_i) = O_l(M_{i+1}), \quad 1 \leq i \leq k-1.$$

Generalizing (19.6), we prove

(22.18) Theorem. *Let M be a full left ideal of the maximal R -order Λ in the separable K -algebra A , and suppose that the Λ -module Λ/M has composition length k . Then M is expressible as a proper product of k maximal integral ideals $M_1 \cdots M_k$, such that*

$$O_l(M) = O_l(M_1), \quad O_r(M) = O_r(M_k).$$

Proof. Use induction on k , the result being trivial when $k = 1$. Assume that $k > 1$, and that the theorem is known for the case $k - 1$. We can choose a maximal left ideal N of Λ such that $M \subset N \subset \Lambda$, and then N/M has composition length $k - 1$ as left Λ -module. Both M and N are normal ideals, with left order Λ . By (22.7) we have

$$N \cdot N^{-1} = \Lambda, \quad N^{-1} \cdot N = O_r(N) = \Lambda' (\text{say}).$$

Now there is a bijection $W \rightarrow N^{-1}W$ between the set of left Λ -submodules W of N , and the set of left Λ' -submodules $N^{-1}W$ of Λ' , with the inverse mapping given by $N^{-1}W \rightarrow N(N^{-1}W)$. Therefore $N^{-1}M$ is a left ideal of Λ' , and the quotient $\Lambda'/N^{-1}M$ has composition length $k - 1$ as left Λ' -module. It follows from the induction hypothesis that we may write

$$N^{-1}M = M_2 \cdots M_k,$$

a proper product of $k - 1$ maximal integral ideals, with

$$O_l(M_2) = O_l(N^{-1}M) = \Lambda', \quad O_r(M_k) = O_r(N^{-1}M) = O_r(M).$$

But then $M = NM_2 \cdots M_k$ is the desired proper product of k maximal integral ideals, and the theorem is proved.

We shall next prove the non-commutative analogue of the algebraic number theory dictum "To contain is to divide" (see H. Cohn [1]). In the proof, it will be convenient to use the notation $N = N_{ij}$ to indicate that the normal ideal N has left order Λ_i and right order Λ_j . Thus a proper product might be written as $N_{12}N_{23}$, where Λ_1, Λ_2 and Λ_3 need not be distinct. From (22.8) we obtain

$$(N_{ij})^{-1} = (N^{-1})_{ji}, \quad N \cdot N^{-1} = \Lambda_i, \quad N^{-1} \cdot N = \Lambda_j.$$

(22.19) THEOREM. (i) A proper product of integral ideals is integral.

(ii) Let M_{12}, N_{14} be normal ideals with the same left order Λ_1 . Then $M \subset N$ if and only if $M_{12} = N_{14} \cdot C_{42}$ for some integral ideal C .

(iii) Let M_{12}, N_{34} be normal ideals. Then $M \subset N$ if and only if M is a proper product

$$(22.20) \quad M_{12} = B_{13} N_{34} C_{42}$$

for some integral ideals B, C .

Proof. To prove (i), we show by induction on k that

$$M_{12} M_{23} \cdots M_{k,k+1} \subset \Lambda_{k+1},$$

if the M 's are integral ideals. The result is clear for $k = 1$, so let $k > 1$, and assume the result for $k - 1$ factors. Then

$M_{12} \cdots M_{k-1,k} M_{k,k+1} \subset \Lambda_k M_{k,k+1} = M_{k,k+1} \subset \Lambda_{k+1}$,
as desired.

We next prove (iii), since (ii) will then follow as a special case. If (22.20) holds with B, C integral, then

$$M_{12} \subset \Lambda_3 N_{34} \Lambda_4 = N_{34},$$

as claimed. Conversely, let $M_{12} \subset N_{34}$, and set

$$B_{13} = M_{12}(\Lambda_3 M_{12})^{-1}, \quad C_{42} = (N_{34})^{-1} M_{12}.$$

It is easily verified that B, C are normal ideals with the indicated orders. Next, the normal ideals M and $\Lambda_3 M$ have the same right order, and $M \subset \Lambda_3 M$, so by (22.6) we obtain $M^{-1} \supset (\Lambda_3 M)^{-1}$. Therefore $B \subset M \cdot M^{-1} = \Lambda_1$, and hence B is integral. Further, $C = N^{-1} M \subset N^{-1} N = \Lambda_4$, so C is also integral. Finally,

$$\begin{aligned} B_{13} N_{34} C_{42} &= M(\Lambda_3 M)^{-1} \cdot N \cdot N^{-1} M = M(\Lambda_3 M)^{-1} \cdot \Lambda_3 M \\ &= M \cdot \Lambda_2 = M, \end{aligned}$$

which completes the proof of (iii). To prove (ii), note that when $\Lambda_1 = \Lambda_3$, we obtain $B = M(\Lambda_1 M)^{-1} = \Lambda_1$ in the above. This establishes the theorem. Of course, the analogue of (ii) holds for a pair of normal ideals with the same right order.

Let us now investigate the uniqueness properties of the factorization of an integral ideal into a proper product of maximal integral ideals. As we have already seen in Exercises 19.1 and 19.2, the factors need not commute, and there may be more than one possible factorization. To some extent, the difficulty arises from the fact that we must consider not just one maximal order, but the sequence of maximal orders associated with the successive factors. Let us prove some results on change of orders.

(22.21) THEOREM. *Let Λ_1, Λ_2 be a pair of maximal R -orders in the separable K -algebra A . Then there exists a normal ideal $M = M_{12}$. If $I(\Lambda_j)$ denotes the group of two-sided Λ_j -ideals in A ($j = 1, 2$), there is an isomorphism*

$$\varphi_{12}: I(\Lambda_1) \cong I(\Lambda_2), \quad \text{where } \varphi_{12}(X) = M^{-1} X M, \quad X \in I(\Lambda_1).$$

The map φ_{12} is independent of the choice of M_{12} .

Proof. The product $M = \Lambda_1 \cdot \Lambda_2$ is a normal ideal with left order Λ_1 and right order Λ_2 . It is clear that φ_{12} carries $I(\Lambda_1)$ into $I(\Lambda_2)$, taking Λ_1 onto Λ_2 . If N_{12} is another normal ideal, then $MN^{-1} \in I(\Lambda_1)$. Since $I(\Lambda_1)$ is abelian, it follows that MN^{-1} commutes with each $X \in I(\Lambda_1)$, and hence $M^{-1} XM = N^{-1} X N$. Therefore φ_{12} does not depend on the choice of the normal ideal

M_{12} used to define φ_{12} . Finally, φ_{12} is an isomorphism since it has an inverse φ_{21} , given by $\varphi_{21}(Y) = MYM^{-1}$, $Y \in I(\Lambda_2)$. This completes the proof.

(22.22) COROLLARY. Let M_{12} be a maximal integral ideal which belongs to the prime ideal \mathfrak{P}_1 of Λ_1 , and to the prime ideal \mathfrak{P}_2 of Λ_2 . Then $\mathfrak{P}_2 = \varphi_{12}(\mathfrak{P}_1)$.

Proof. It is clear from (22.21) that $\varphi_{12}(\mathfrak{P}_1)$ is a prime ideal of Λ_2 , and that $\varphi_{12}(\mathfrak{P}_1) = M^{-1}\mathfrak{P}_1 M$. We have

$$\mathfrak{P}_1 \subset M \Rightarrow M^{-1} \subset \mathfrak{P}_1^{-1} \Rightarrow M^{-1}\mathfrak{P}_1 M \subset \mathfrak{P}_1^{-1}\mathfrak{P}_1 M = M.$$

Thus $\varphi_{12}(\mathfrak{P}_1)$ is a prime ideal of Λ_2 contained in M , whence M belongs to $\varphi_{12}(\mathfrak{P}_1)$. This completes the proof.

(22.23) COROLLARY. Let M_{23} be a maximal integral ideal belonging to the prime ideal \mathfrak{P}_2 of Λ_2 . Then for each normal ideal $B = B_{12}$, the quotient $B_{12}/B_{12}M_{23}$ is a simple left Λ_1 -module, and

$$\text{ann}_{\Lambda_1} B/BM = \{x \in \Lambda_1 : xB \subset BM\} = \varphi_{21}(\mathfrak{P}_2).$$

Proof. If $BM \subset X \subset B$ is a chain of left Λ_1 -modules, then $M \subset B^{-1}X \subset \Lambda_2$ is a chain of left Λ_2 -modules. Thus $B^{-1}X$ is either M or Λ_2 , whence X is either BM or B . This shows that B/BM is a simple left Λ_1 -module. As in the proof of (22.15), $\text{ann}_{\Lambda_1} B/BM$ is a prime ideal of Λ_1 . But $\varphi_{21}(\mathfrak{P}_2) = B\mathfrak{P}_2 B^{-1}$ is a prime ideal of Λ_1 which annihilates B/BM . Therefore $\text{ann}_{\Lambda_1} B/BM = \varphi_{21}(\mathfrak{P}_2)$, and the corollary is established.

Let $\varphi_{12}: I(\Lambda_1) \cong I(\Lambda_2)$ be the isomorphism described in (22.21). For $X \in I(\Lambda_1)$, we call the ideals X and $\varphi_{12}(X)$ similar. Thus, by (22.22), each maximal integral ideal determines a pair of similar prime ideals. We may caution that the converse need not hold, that is, given a pair of similar prime ideals \mathfrak{P}_1 and \mathfrak{P}_2 , it is not necessarily true (even in the complete local case) that there exists a maximal integral ideal M_{12} belonging to both \mathfrak{P}_1 and \mathfrak{P}_2 (see Exercise 22.1).

We are now ready to deal with the uniqueness properties of factorizations into proper products of maximal integral ideals, still assuming that A is any separable K -algebra.

(22.24) THEOREM. In any factorization of an integral ideal L into a proper product of maximal integral ideals, the number of factors is uniquely determined by L , and the prime ideals to which these factors belong are uniquely determined up to similarity and order of occurrence.

Proof. Let $L = L_1$, be an integral ideal, and suppose that

$$(22.25) \quad L_{1r} = M_{12} M_{23} \cdots M_{kr},$$

where each $M_{i,i+1}$ is a maximal integral ideal, and $M_{k,k+1}$ is interpreted to be M_{kr} . By (22.23), the chain of left Λ_1 -modules

$$(22.26) \quad \Lambda_1 \supset M_{12} \supset M_{12} M_{23} \supset \cdots \supset M_{12} M_{23} \cdots M_{kr} = L_{1r}$$

is strictly decreasing, and is unrefinable. The factor modules

$$(22.27) \quad \Lambda_1 / M_{12}, M_{12} / M_{12} M_{23}, \dots,$$

are therefore the composition factors of the left Λ_1 -module Λ_1 / L . By the Jordan–Hölder Theorem, these composition factors are uniquely determined by L , up to Λ_1 -isomorphism and order of occurrence.

There are k such factor modules, so L determines k uniquely. Furthermore, let \mathfrak{P}_i denote the prime ideal of Λ_i to which $M_{i,i+1}$ belongs, $1 \leq i \leq k$. Then by (22.23) we have

$$\mathfrak{P}_1 = \text{ann}_{\Lambda_1} \Lambda_1 / M_{12}, \quad \varphi_{21}(\mathfrak{P}_2) = \text{ann}_{\Lambda_1} M_{12} / M_{12} M_{23}, \dots.$$

Thus L uniquely determines the set of prime ideals of Λ_1

$$\{\mathfrak{P}_1, \varphi_{21}(\mathfrak{P}_2), \dots, \varphi_{k1}(\mathfrak{P}_k)\}.$$

This completes the proof of the theorem.

As already remarked in Exercises 19.1 and 19.2, the individual factors $M_{i,i+1}$ occurring in (22.25) are not uniquely determined (except in special cases). Indeed, even the set of maximal orders $\{\Lambda_2, \dots, \Lambda_k\}$ is not an invariant of L . We now prove, however, that the order of occurrence of the composition factors of Λ_1 / L in (22.27) may be specified in advance.

(22.28) **THEOREM.** *Let L be a left ideal of the maximal R -order Λ in a separable K -algebra A , and let $\{S_1, \dots, S_k\}$ be the composition factors of the Λ -module Λ / L , arranged in any preassigned order. Then there is a factorization (22.25) of L into a product of maximal integral ideals, such that the factor modules in (22.27) are precisely S_1, \dots, S_k , in that order.*

Proof. Any composition series for the left Λ -module Λ / L lifts to an unrefinable chain of left ideals of Λ , and this chain can be expressed in the form (22.26) for some choice of M 's (by (22.19)). Hence it suffices to prove that Λ / L has a composition series in which the composition factors occur in the preassigned order S_1, \dots, S_k . Furthermore, a decomposition of A into simple components yields corresponding decompositions of Λ and L , and hence of Λ / L . It is therefore sufficient to deal with the case where A is a central simple K -algebra.

Let us set $T = \Lambda / L$, an R -torsion finitely generated left Λ -module, and let

$\mathfrak{A} = \text{ann}_\Lambda T$. Then \mathfrak{A} is a two-sided ideal of Λ , and so we may write $\mathfrak{A} = \prod_1^n \mathfrak{P}_i^{a_i}$, where the $\{\mathfrak{P}_i\}$ are distinct prime ideals of Λ . Then T is a left (Λ/\mathfrak{A}) -module. But

$$\Lambda/\mathfrak{A} \cong \sum_1^n \Lambda/\mathfrak{P}_i^{a_i},$$

whence there is a decomposition $T = \sum_1^n T_i$, with

$$T_i = \{x \in T : \mathfrak{P}_i^{a_i} x = 0\} = \{x \in T : \mathfrak{P}_i^m x = 0 \text{ for some } m\}.$$

(Call T_i the \mathfrak{P}_i -primary component of T .)

It suffices to show that the left Λ -module T_i has a composition series in which the factors occur in a preassigned order. Each composition factor X of T_i is a simple left Λ -module, hence as in (22.15), $\text{ann}_\Lambda X$ is a prime ideal of Λ . But then $\text{ann}_\Lambda X = \mathfrak{P}_i$, since we already know that $\mathfrak{P}_i^{a_i} X = 0$. Hence X is a simple left (Λ/\mathfrak{P}_i) -module. Since Λ/\mathfrak{P}_i is a simple artinian ring, there is only one isomorphism class of such modules X . Thus all of the composition factors of T_i are mutually isomorphic. This proves that T_i has a composition series with preassigned order of composition factors (indeed, any composition series of T_i will do), and thus the same holds true for Λ/L . The theorem is thus established.

To conclude this section, we observe that the collection of normal ideals in a separable K -algebra forms a groupoid, according to the following definition. A *groupoid* G is a collection of elements, certain of whose products are defined and lie in G , such that

- (i) For each $a_{ij} \in G$, there exist unique elements $e_i, e_j \in G$ such that $e_i a_{ij} = a_{ij} = a_{ij} e_j$, where all indicated products are defined. Further, $e_i e_i = e_i$, $e_j e_j = e_j$. Call e_i the *left unit* of a_{ij} , and e_j the *right unit* of a_{ij} .
- (ii) $a_{ij} b_{kl}$ is defined if and only if $j = k$, that is, if and only if the right unit of a_{ij} equals the left unit of b_{kl} .
- (iii) If ab and bc are defined, so are $(ab)c$ and $a(bc)$, and these are equal.
- (iv) For each $a_{ij} \in G$, there exists an $a_{ij}^{-1} \in G$ with left unit e_j , right unit e_i , such that

$$a_{ij} \cdot a_{ij}^{-1} = e_i, \quad a_{ij}^{-1} \cdot a_{ij} = e_j.$$

- (v) Given any pair of units $e, e' \in G$, there is an element $a_{ij} \in G$ with left unit e , right unit e' .

The collection of all normal ideals in A , relative to proper multiplication, is the *Brandt groupoid* associated with A . The units are the maximal orders in A ; the inverse of a normal ideal M is the normal ideal M^{-1} . If Λ and Λ' are maximal orders, the normal ideal $\Lambda \cdot \Lambda'$ has left unit Λ , right unit Λ' .

EXERCISES

Unless otherwise stated, Λ denotes a maximal R -order in a separable K -algebra A .

1. Let R be a complete discrete valuation ring with prime element π , and let

$$\Lambda_1 = M_3(R), \quad \Lambda_2 = y\Lambda_1 y^{-1}, \quad \text{where } y = \text{diag}(1, 1, \pi) \in \Lambda_1.$$

Show that no maximal left ideal of Λ_1 can be a maximal right ideal of Λ_2 . Deduce from this that the prime ideals $\pi\Lambda_1$, $\pi\Lambda_2$ are similar, but that there is no maximal integral ideal M_{12} which belongs to both $\pi\Lambda_1$ and $\pi\Lambda_2$. [Hint: Let $\Lambda_1 x$ be a maximal left ideal of Λ_1 , and suppose that $O_r(\Lambda_1 x) = \Lambda_2$. Then $\Lambda_2 = x^{-1}\Lambda_1 x$, so

$$(xy) \cdot \Lambda_1 \cdot (xy)^{-1} = \Lambda_1.$$

Therefore (see Exercise 38.5) $xy = \pi^k u$ for some $k \geq 1$ and some $u \in u(\Lambda_1)$. But then x has elementary divisors $\{\pi^{k-1}, \pi^k, \pi^k\}$, which contradicts (17.8).]

2. Let M, N be normal ideals in A . Prove that $M \cdot N$ is a proper product if and only if replacing either factor by a larger R -lattice (in A) increases the product. [Hint: Let $M = M_{12}$, $N = N_{34}$, in the notation introduced just before (22.19). Suppose that increasing either factor increases the product MN . Then

$$MN = M\Lambda_2 \cdot N = M \cdot \Lambda_2 N \implies N = \Lambda_2 N \implies \Lambda_2 = \Lambda_3.$$

Conversely, let $\Lambda_2 = \Lambda_3$ and let $M'N = MN$, where M' is an R -lattice properly containing M . Then

$$M' \subset M'\Lambda_2 = M' \cdot NN^{-1} = M \cdot NN^{-1} = M,$$

a contradiction.]

3. Let $\mathfrak{P}_1, \dots, \mathfrak{P}_n$ be distinct prime ideals of Λ . Let

$$\mathfrak{A} = \prod_1^n \mathfrak{P}_i^{a_i}, \quad \mathfrak{B} = \prod_1^n \mathfrak{P}_i^{b_i}, \quad a_i, b_i \in \mathbb{Z}.$$

Prove

(i) $\mathfrak{A} \supset \mathfrak{B}$ if and only if $a_i \leq b_i$, $1 \leq i \leq n$.

(ii) $\mathfrak{A} + \mathfrak{B} = \prod_1^n \mathfrak{P}_i^{\min(a_i, b_i)}$.

(iii) $\mathfrak{A} \cap \mathfrak{B} = \prod_1^n \mathfrak{P}_i^{\max(a_i, b_i)}$.

(iv) If each $a_i \geq 0$, then there is a ring isomorphism

$$\Lambda/\mathfrak{A} \cong \sum_{i=1}^n \Lambda/\mathfrak{P}_i^{a_i}.$$

4. Show that each finitely generated R -torsion left Λ -module X is expressible as a finite direct sum $\sum \Lambda/J_i$, where each J_i is a left ideal of Λ of the same R -rank as Λ . [Hint: As in the proof of (22.28), the problem reduces to the case where R is a complete discrete valuation ring, and where $\Lambda = M_k(\Delta)$ for some maximal R -order Δ in a skewfield. By means of the Morita correspondence, the problem further reduces to that of finding R -torsion Δ -modules. Now use (17.7).]

5. Any simple left Λ -module is of the form Λ/M , where M is a maximal left ideal of Λ . Let $P = R \cap M$. Show that P is a prime ideal of R , and that $P = \text{ann}_R \Lambda/M$. [Hint: Use (22.3).]

6. Let M_{23} be a maximal integral ideal, and B_{12} any normal ideal. Prove that

$$\text{ann}_R \Lambda_2 / M_{23} = \text{ann}_R B_{12} / B_{12} M_{23}.$$

[Hint: If $P = \text{ann}_R \Lambda_2 / M$, then $PB^{-1}B = P\Lambda_2 \subset M_{23}$, whence $PB \subset BM$.]

7. Keeping the notation of (22.28), let $\mathfrak{P}_i = \text{ann}_\Lambda S_i$, $P_i = \mathfrak{P}_i \cap R = \text{ann}_R S_i$, $1 \leq i \leq k$. Let P_1, \dots, P_n be the distinct prime ideals of R among $\{P_1, \dots, P_k\}$. Show that we can express L as a proper product

$$L = N^{(1)} \cdot N^{(2)} \cdots N^{(n)},$$

where each $N^{(i)}$ is an integral ideal such that

$$(N^{(i)})_{P_i} = L_{P_i}, \quad (N^{(i)})_P = \text{maximal order} \quad (P \neq P_i),$$

for $1 \leq i \leq n$.

8. Let L, M be left ideals in Λ such that

$$\text{ann}_R \Lambda/L + \text{ann}_R \Lambda/M = R.$$

Show that there exists a left ideal N such that

$$\Lambda/N \cong \Lambda/L \dot{+} \Lambda/M.$$

[Hint: Define a left Λ -homomorphism

$$f: \Lambda \rightarrow \Lambda/L \dot{+} \Lambda/M$$

by $f(\lambda) = (\lambda + L, \lambda + M)$, $\lambda \in \Lambda$. For each prime ideal P of R , either $(\Lambda/L)_P = 0$ or $(\Lambda/M)_P = 0$. Thus f_P is epic for each P , whence also f is epic. Now choose $N = \ker f$.]

9. Prove (22.9) directly. [Hint: $M \subset O_r(M) \Rightarrow M \cdot M \subset M \Rightarrow M \subset O_r(M)$.]

10. Verify that the definition of inverses in (19.3) agrees with the definition in (22.6).

11. Show that any two maximal orders Λ_1, Λ_2 in A are Morita equivalent. [Hint: (1) Reduce to central simple case, then use (21.7) and transitivity of Morita equivalence; or (2) Let $M = M_{12}$ be a normal ideal, and identify $\text{Hom}_{\Lambda_1}(M, \Lambda_1)$ with the module of right multiplications by elements of M^{-1} . The formula $M \cdot M^{-1} = \Lambda_1$ is then equivalent to the assertion that

$$\mu: M \otimes_{\Lambda_2} \text{Hom}_{\Lambda_1}(M, \Lambda_1) \rightarrow \Lambda_1$$

is an epimorphism. Likewise,

$$\tau: \text{Hom}_{\Lambda_1}(M, \Lambda_1) \otimes_{\Lambda_1} M \rightarrow \Lambda_2$$

is epic. Hence Λ_1 and Λ_2 are Morita equivalent by §16.]

12. Let Γ be an arbitrary R -order in a central simple K -algebra A . Show that Γ is a maximal order if and only if Γ is hereditary, and for each prime ideal P of R there is a unique prime ideal of Γ containing P . [Hint: To prove Γ maximal, it suffices to prove Γ_P maximal for each P . There is a one-to-one correspondence between the

prime ideals of Γ containing P , and the prime ideals of Γ_P . Now use (18.4).]

13. Let P be a prime ideal of R , and let $P\Lambda = \prod \mathfrak{P}_i^{e_i}$, where the \mathfrak{P}_i are prime ideals of the maximal order Λ . Let $f_i = (\Lambda/\mathfrak{P}_i : R/P)$. Prove that

$$\sum e_i f_i = (A : K).$$

[Hint: Consider the \bar{R} -algebra $\Lambda/P\Lambda$, where $\bar{R} = R/P$, and imitate the proof of (4.30).]

23. ALTERNATE APPROACH TO GLOBAL IDEAL THEORY

In §§21–22, we derived results on ideals and orders in the global case by making use of the local theorems from Chapter V. In this section we shall give an alternate approach to some of the global theorems obtained in §§21–22. The direct global approach given below generalizes some of the standard arguments of algebraic number theory. We shall not use any of those results from the preceding sections, whose proofs were based on localization techniques. This section may be skipped if desired without affecting the continuity of the exposition.

As usual, let A be a separable K -algebra, where K is the quotient field of the Dedekind domain R . In §22, we defined prime ideals of an R -order Λ in A , and showed that these coincide with the maximal two-sided ideals of Λ . We now recall some other definitions from §22. All ideals M considered below are assumed to be full R -lattices in A . Call M a *normal ideal* if $O_i(M)$ is a maximal R -order. An *integral ideal* is a normal ideal M such that $M \subset O_i(M)$. A *maximal integral ideal* is an integral ideal M which is a maximal left ideal in $O_i(M)$. (We shall eventually remedy this asymmetry in the definitions (see (23.2), (23.10), and (23.11).) Let us write $M = M_{ij}$ to indicate that M is an ideal with

$$O_i(M_{ij}) = \Lambda_i, \quad O_r(M_{ij}) = \Lambda_j.$$

Our aim is to derive the factorization properties of one-sided and two-sided ideals. We begin with

(23.1) **LEMMA.** *Let Λ be any R -order in A . Then every two-sided ideal in Λ contains a product of prime ideals.*

Proof. If not, then the set of two-sided ideals which do not contain such products is non-empty, hence has a maximal element J since Λ is noetherian. Clearly J is not a prime ideal, so by (22.2) there exist two-sided ideals B, C of Λ , properly containing J , such that $J \supset BC$. But both B and C contain products of prime ideals, whence so does J . This yields a contradiction, and proves the lemma.

(23.2) **LEMMA.** *Let M_{ij} be a full R -lattice in A . Then $M_{ij} \subset \Lambda_i$ if and only if $M_{ij} \subset \Lambda_j$.*

Proof. Let $M_{ij} \subset \Lambda_i$; then

$$M_{ij} \cdot M_{ij} \subset \Lambda_i \cdot M_{ij} = M_{ij} \implies M_{ij} \subset O_r(M_{ij}) = \Lambda_j.$$

This completes the proof.

For any full R -lattice $L = L_{ij}$ in A , define L^{-1} as in (22.5). Then for $x \in L^{-1}$,

$$Lx \subset \Lambda_i \implies L \cdot x\Lambda_i \subset \Lambda_i \implies x\Lambda_i \subset L^{-1},$$

whence L^{-1} is a right Λ_i -module. Thus we obtain

$$(23.3) \quad O_r(L_{ij}^{-1}) \supset \Lambda_i, \quad O_l(L_{ij}^{-1}) \supset \Lambda_j.$$

Our next step is to develop the theory of two-sided ideals, and we now prove

(23.4) **LEMMA.** *Let M be a two-sided ideal in the maximal order Λ . If $M < \Lambda$, then $M^{-1} > \Lambda$.*

Proof. It is clear from (23.3) that M^{-1} is a two-sided Λ -ideal in A , and obviously $M^{-1} \supset \Lambda$. Let us assume that $M^{-1} = \Lambda$, and obtain a contradiction. Since $M < \Lambda$, we can choose a prime ideal \mathfrak{P} of Λ with $M \subset \mathfrak{P} \subset \Lambda$. Let α be a nonzero element of $R \cap \mathfrak{P}$ (such exist, since \mathfrak{P} is a full R -lattice in A). Then by (23.1) $\alpha\Lambda$ contains a product of prime ideals, and so we may write

$$\mathfrak{P} \supset \alpha\Lambda \supset \mathfrak{P}_1 \mathfrak{P}_2 \cdots \mathfrak{P}_r,$$

where the \mathfrak{P}_i are prime ideals, and where r is minimal. Since $\mathfrak{P} \supset \mathfrak{P}_1 \cdots \mathfrak{P}_r$ and \mathfrak{P} is a prime ideal, it follows that \mathfrak{P} contains some factor \mathfrak{P}_j , and then of course $\mathfrak{P} = \mathfrak{P}_j$. Thus we may write

$$\mathfrak{P} \supset \alpha\Lambda \supset B\mathfrak{P}C,$$

where B, C are two-sided ideals of Λ . We then obtain

$$\begin{aligned} \alpha^{-1} B\mathfrak{P}C \subset \Lambda &\implies B \cdot \alpha^{-1} \mathfrak{P}C \cdot B \subset B \implies \alpha^{-1} \mathfrak{P}CB \subset O_r(B) \\ &\implies \alpha^{-1} CB \subset \mathfrak{P}^{-1} \subset M^{-1} = \Lambda \implies CB \subset \alpha\Lambda. \end{aligned}$$

This shows that $\alpha\Lambda$ contains a product CB of $r - 1$ prime ideals, which contradicts the minimality of r , and completes the rather mystifying proof.

(23.5) **THEOREM.** *Let M be a full R -lattice in A such that $O_r(M)$ is a maximal order. Then*

$$M \cdot M^{-1} = O_r(M).$$

Proof. Let $\Lambda = O_r(M)$ be maximal, and set $B = M \cdot M^{-1}$, a two-sided ideal in Λ . Then

$$\begin{aligned} BB^{-1} \subset \Lambda &\implies M \cdot M^{-1}B^{-1} \subset \Lambda \implies M^{-1}B^{-1} \subset M^{-1} \\ &\implies B^{-1} \subset O_r(M^{-1}). \end{aligned}$$

But $O_r(M^{-1}) \supset O_r(M) = \Lambda$ by (23.3), whence $O_r(M^{-1}) = \Lambda$. Therefore $B^{-1} \subset \Lambda$, so $B = \Lambda$ by (23.4). This completes the proof.

The preceding result is the key step in this chain of arguments. Using it, we prove

(23.6) **THEOREM.** *Let Λ be a maximal order. For each two-sided ideal M in Λ , we have*

$$(23.7) \quad M \cdot M^{-1} = M^{-1} \cdot M = \Lambda, \quad (M^{-1})^{-1} = M.$$

Furthermore, every two-sided ideal in Λ is uniquely expressible as a product of prime ideals of Λ , and multiplication of prime ideals is commutative.

Proof. The first two equalities in (23.7) are immediate consequences of (23.5). To establish the last formula, choose a nonzero $\alpha \in R$ such that $\alpha M^{-1} \subset \Lambda$. Then αM^{-1} is a two-sided ideal of Λ , whence

$$(\alpha M^{-1})(\alpha M^{-1})^{-1} = \Lambda.$$

But

$$(\alpha M^{-1})^{-1} = \alpha^{-1}L, \quad \text{where } L = (M^{-1})^{-1}.$$

Therefore $M^{-1} \cdot L = \Lambda$, whence

$$L = \Lambda L = MM^{-1} \cdot L = M\Lambda = M.$$

We shall now show that every two-sided ideal N of Λ is a product of prime ideals (an “empty” product, if $N = \Lambda$.) If the result is false, let N be a largest counterexample. Surely N is not prime, and so there exists a prime ideal \mathfrak{P} with $N < \mathfrak{P} < \Lambda$, and hence

$$N \subset N\mathfrak{P}^{-1} \subset \Lambda.$$

If $N = N\mathfrak{P}^{-1}$, then $\mathfrak{P}^{-1} \subset O_r(N) = \Lambda$, which is impossible by (23.4). Thus $N < N\mathfrak{P}^{-1}$, whence $N\mathfrak{P}^{-1}$ is a product of prime ideals $\mathfrak{P}_1 \dots \mathfrak{P}_r$. This gives $N = \mathfrak{P}_1 \dots \mathfrak{P}_r \mathfrak{P}$, a contradiction. We have thus established that every two-sided ideal of Λ is a product of prime ideals.

Now let $\mathfrak{P}, \mathfrak{P}'$ be distinct prime ideals of Λ . Then

$$\mathfrak{P}^{-1}\mathfrak{P}'\mathfrak{P} \subset \mathfrak{P}^{-1}\Lambda\mathfrak{P} = \Lambda,$$

and

$$\mathfrak{P}(\mathfrak{P}^{-1}\mathfrak{P}'\mathfrak{P}) = \mathfrak{P}'\mathfrak{P} \subset \mathfrak{P}'.$$

Thus \mathfrak{P}' contains the product $\mathfrak{P}(\mathfrak{P}^{-1}\mathfrak{P}'\mathfrak{P})$ of a pair of two-sided ideals of Λ , and consequently $\mathfrak{P}' \supset \mathfrak{P}^{-1}\mathfrak{P}'\mathfrak{P}$. Therefore $\mathfrak{P}'\mathfrak{P} \supset \mathfrak{P}'\mathfrak{P}$. Since the reverse

inclusion follows by symmetry, we obtain $\mathfrak{P}\mathfrak{P}' = \mathfrak{P}'\mathfrak{P}$, as desired. It remains to prove uniqueness (up to order of occurrence of the factors), so let

$$(23.8) \quad \mathfrak{P}_1 \cdots \mathfrak{P}_r = \mathfrak{Q}_1 \cdots \mathfrak{Q}_s,$$

where the \mathfrak{P} 's and \mathfrak{Q} 's are prime ideals. Then $\mathfrak{P}_1 \supset \prod \mathfrak{Q}_i$ implies that $\mathfrak{P}_1 = \mathfrak{Q}_k$ for some k . Multiplying (23.8) by \mathfrak{P}_1^{-1} and repeating the argument, we see that the $\{\mathfrak{P}_i\}$ coincide with the $\{\mathfrak{Q}_j\}$, apart from order of occurrence. This establishes the theorem.

It is easily deduced from the above that the set of two-sided Λ -ideals in A is the free abelian group generated by the prime ideals of Λ . We leave the obvious proofs to the reader.

Remark. The method of proof of (23.5) can be applied to more general situations, and leads to the theory of Asano orders in arbitrary rings. As in Jacobson [1, Ch. 6], one first generalizes the concepts of orders and fractional ideals. Then one defines an *Asano order* to be an order whose fractional two-sided ideals form a multiplicative group. For the theory of Asano orders, the reader may consult Jacobson [1] as basic reference. Further developments are given in Asano [1, 2], Harada [6], Michler [1], and Robson [1, 2].

(23.9) COROLLARY. *If M is a proper left ideal of the maximal order Λ , then $M^{-1} > \Lambda$.*

Proof. Let $M \subset N \subset \Lambda$, where N is a maximal left ideal of Λ . Then $M^{-1} \supset N^{-1} \supset \Lambda$, and so it suffices to prove that $N^{-1} > \Lambda$. Let us set

$$\mathfrak{P} = \text{ann}_{\Lambda} \Lambda/N.$$

As in the proof of (22.15), we find that \mathfrak{P} is a prime ideal of Λ , and Λ/N is a simple left module over the simple ring $\bar{\Lambda} = \Lambda/\mathfrak{P}$. Hence N is the inverse image, under the map $\Lambda \rightarrow \bar{\Lambda}$, of some maximal left ideal of $\bar{\Lambda}$. Therefore (see Exercise 7.12) we may write

$$N = \Lambda(1 - e) + \mathfrak{P},$$

where $e \in \Lambda$ is such that its image \bar{e} is a primitive idempotent in $\bar{\Lambda}$. Set $L = e\Lambda + \mathfrak{P}$, a right ideal in Λ . Since $(1 - e)e \in \mathfrak{P}$, it follows that $N \cdot L \subset \mathfrak{P}$. On the other hand, $N \cdot L$ is a two-sided ideal of Λ containing \mathfrak{P}^2 . It follows from (23.6) that NL is either \mathfrak{P} or \mathfrak{P}^2 . If $NL = \mathfrak{P}^2$, then $\mathfrak{P}e \subset \mathfrak{P}^2$; multiplying by \mathfrak{P}^{-1} , we deduce that $e \in \mathfrak{P}$, which is impossible. This shows that $NL = \mathfrak{P}$.

Now choose a nonzero $\alpha \in R \cap \mathfrak{P}$, and write $\alpha\Lambda$ as a product of prime ideals of Λ . Since $\alpha\Lambda \subset \mathfrak{P}$, one of the factors must equal \mathfrak{P} , and so we may write

$$\alpha\Lambda = \mathfrak{P}\mathfrak{Q} = NL\mathfrak{Q},$$

where \mathfrak{Q} is some two-sided ideal of Λ . If $N^{-1} = \Lambda$, then

$$\begin{aligned}\alpha^{-1}L\mathfrak{Q} \subset N^{-1} = \Lambda &\implies L\mathfrak{Q} \subset \alpha\Lambda \implies L\Lambda \subset \alpha\Lambda \cdot \mathfrak{Q}^{-1} = \mathfrak{P} \\ &\implies L \subset \mathfrak{P}.\end{aligned}$$

But $L = e\Lambda + \mathfrak{P}$, so the last inclusion is impossible. This shows that $N^{-1} > \Lambda$, and completes the proof of the theorem.

We are finally ready to prove

(23.10) THEOREM. *Let M be a full R -lattice in A . Then $O_l(M)$ is a maximal order if and only if $O_r(M)$ is a maximal order.*

Proof. Let $\Lambda = O_l(M)$ be maximal. Replacing M by αM if need be, where $\alpha \in R$, $\alpha \neq 0$, we may hereafter assume that $M \subset \Lambda$. When $M = \Lambda$, then $O_r(M) = \Lambda$, so we may restrict ourselves to the case where $M < \Lambda$. If the theorem is false, let M be a maximal counterexample, and choose a left ideal L of Λ such that

$$M < L \subset \Lambda, \quad L/M = \text{simple left } \Lambda\text{-module.}$$

(Possibly $L = \Lambda$.) Then $O_l(L) = \Lambda$, and since M is assumed to be a maximal counterexample, it follows that $O_r(L) = \Lambda'$ is a maximal order. Then $L \cdot L^{-1} = \Lambda$ by (23.5). But the analogue of (23.5), obtained by reversing “left” and “right”, is also true. This analogue yields the equality $L^{-1} \cdot L = \Lambda'$, since $O_r(L)$ is a maximal order.

Each left ideal X of Λ' maps onto a Λ -submodule LX of L , and the correspondence $X \leftrightarrow LX$ is one-to-one, since $X = L^{-1} \cdot LX$. Set $N = L^{-1}M$; then

$$N = L^{-1}M \subset L^{-1}L = \Lambda'.$$

It follows that N is a maximal left ideal of Λ' , since M is a maximal Λ -submodule of L . Consequently we obtain

$$N^{-1} > \Lambda', \quad N \cdot N^{-1} = \Lambda', \quad N^{-1} \cdot N \subset O_r(N),$$

by (23.9) and (23.5).

Next, for $x \in A$ we have

$$Nx \subset N \implies LNx \subset LN \implies x \in O_r(M),$$

$$Mx \subset M \implies L^{-1}Mx \subset L^{-1}M \implies x \in O_r(N).$$

Therefore $O_r(N) = O_r(M)$. Since M is assumed to be a counterexample to the theorem, it follows that $O_r(N)$ is not a maximal order. Thus $O_r(N) < \Lambda''$ for some maximal order Λ'' . We observe next that $N\Lambda''N^{-1}$ is an order, since

$$N\Lambda''N^{-1} \cdot N\Lambda''N^{-1} \subset N\Lambda'' \cdot O_r(N) \cdot \Lambda''N^{-1} \subset N\Lambda''N^{-1}.$$

But also

$$N\Lambda''N^{-1} \supset N \cdot N^{-1} = \Lambda',$$

and hence $N\Lambda''N^{-1} = \Lambda'$, since Λ' is a maximal order. Consequently there is a chain of left Λ' -ideals

$$N \subset N\Lambda'' \subset N\Lambda''N^{-1} = \Lambda'.$$

Since N is a maximal left ideal in Λ' , it follows that $N\Lambda''$ is either N or Λ' . If $N\Lambda'' = N$, then $\Lambda'' \subset O_r(N)$, which is impossible. Hence $N\Lambda'' = \Lambda'$, and thus

$$\Lambda' = N\Lambda'' \cdot N^{-1} = \Lambda'N^{-1}.$$

Therefore $N^{-1} = \Lambda'$, which is also impossible. This proves that there can be no counterexample to the theorem, and so the result is established.

We have now shown, without the use of local results, that for a normal ideal M , both $O_l(M)$ and $O_r(M)$ are maximal orders. We have also shown that

$$M \cdot M^{-1} = O_l(M), \quad M^{-1} \cdot M = O_r(M)$$

for any normal ideal M , and furthermore, $M \subset O_l(M)$ if and only if $M \subset O_r(M)$. The proofs of Theorems 22.18 and 22.19 carry over unchanged, since they depend only upon the above-stated results, rather than any localization arguments. We are left with the task of proving (22.17) without using results from Chapter V.

(23.11) THEOREM. *Let $M = M_{12}$ be a normal ideal. Then M is a maximal left ideal in Λ_1 if and only if M is a maximal right ideal in Λ_2 .*

Proof. Let M be a maximal left ideal in Λ_1 . Then $M \subset \Lambda_2$, by (23.2). If $M = \Lambda_2$, then $\Lambda_1 = O_l(M) = \Lambda_2 = M$, which is impossible. Suppose that M is not a maximal right ideal of Λ_2 . Then there exists a normal ideal $N = N_{32}$ such that

$$M_{12} < N_{32} < \Lambda_2.$$

Surely $N_{32} < \Lambda_3$, since otherwise $\Lambda_2 = \Lambda_3 = N$. It follows from (22.19) that we may write $M_{12} = B_{13} \cdot N_{32}$ for some integral ideal B_{13} . The product $B \cdot N$ is a proper product, whence by Exercise 22.2 we obtain

$$M = B \cdot N < B \cdot \Lambda_3 = B \subset \Lambda_1.$$

Therefore $B = \Lambda_1$, and so $\Lambda_3 = O_r(B) = \Lambda_1$, which implies that $M = B \cdot N = \Lambda_3 \cdot N_{32} = N$. This is a contradiction and the theorem is proved.

At this point we have established all of the major results of §22 without the use of localization arguments. We shall not proceed further with the program

of obtaining global results directly however, and merely observe that the remaining theorems in §22 can be derived readily from the results so far established in this section.

24. NORMS OF IDEALS

Throughout this section let A be a separable K -algebra. As in the preceding sections, M_{12} denotes an ideal in A with left order Λ_1 and right order Λ_2 . We shall define norms and reduced norms of normal ideals of A , so as to generalize the concept of relative norm in algebraic number theory described in (4.31 iii). To begin with, let $M = M_{12}$ be an integral ideal of A , and define its *norm* by

$$(24.1) \quad N_{A/K}(M_{12}) = \text{ord}_R \Lambda_1 / M_{12}.$$

When there is no danger of confusion, we shall omit the subscripts A/K and R . Since M_{12} is a full R -lattice in its left order Λ_1 , the quotient Λ_1 / M_{12} is a finitely generated torsion R -module. Thus $\text{ord } \Lambda_1 / M$ is a nonzero ideal of R , and equals R if and only if $M = \Lambda_1$.

We shall soon remove the asymmetry in the definition of norm, and we begin with some easy results.

(24.2) THEOREM. (i) Let M be an integral ideal of A . Then

$$N(M_P) = \{N(M)\}_P$$

for each prime ideal P of R .

(ii) For each maximal R -order Λ in A ,

$$N(\Lambda a) = R \cdot Na = N(a\Lambda), \quad a \in \Lambda \cap u(A).$$

Proof. (i) Let $\Lambda = O_i(M)$, so $\Lambda_P = O_i(M_P)$ by (8.5). Therefore

$$N(M_P) = \text{ord}_{R_P} \Lambda_P / M_P = R_P \otimes_R \text{ord}_R \Lambda / M = \{N(M)\}_P,$$

using (4.20 ii).

(ii) We have

$$N(\Lambda a) = \text{ord } \Lambda / \Lambda a = R \cdot Na,$$

by Exercise 10.7. In order to compute $N(a\Lambda)$, we set

$$\Lambda' = O_i(a\Lambda) = a\Lambda a^{-1}.$$

Then

$$N(a\Lambda) = \text{ord } \Lambda' / a\Lambda = \text{ord } a\Lambda a^{-1} / a\Lambda.$$

However, there is an R -isomorphism

$$a\Lambda a^{-1} / a\Lambda \cong \Lambda / \Lambda a, \quad \text{given by } \lambda \rightarrow a^{-1}\lambda a, \quad \lambda \in a\Lambda a^{-1}.$$

Thus by Exercise 10.7,

$$\text{ord } \Lambda'/a\Lambda = \text{ord } \Lambda/\Lambda a = R \cdot Na.$$

This completes the proof.

Using this result, we obtain a number of important consequences.

(24.3) THEOREM. *Let M_{12} be an integral ideal of A . Then*

$$\text{ord}_R \Lambda_1/M_{12} = \text{ord}_R \Lambda_2/M_{12},$$

so that the norm of M can be computed by using either the left order of M or the right order of M .

Proof. In order to prove the equality of a pair of order ideals, it suffices to establish the equality after replacing R by each of its localizations R_P , with P an arbitrary prime ideal of R (see Exercise 3.2). Changing notation, assume now that R is a discrete valuation ring. By (18.10) we may write $M = \Lambda_1 a$ for some $a \in u(A)$, and then $\Lambda_2 = O_r(M) = a^{-1} \Lambda_1 a$. The formula, which we are trying to prove, thus becomes

$$\text{ord } \Lambda_1/\Lambda_1 a = \text{ord } a^{-1} \Lambda_1 a/\Lambda_1 a.$$

But we have already established this result in the proof of (24.2), and so the theorem is proved.

(24.4) THEOREM. *Let $L \cdot M$ be a proper product of integral ideals. Then*

$$N(L \cdot M) = N(L) \cdot N(M).$$

Proof. Let $L = L_{12}$, $M = M_{23}$. By (4.17), the exact sequence of left Λ_1 -modules

$$0 \rightarrow L/LM \rightarrow \Lambda_1/LM \rightarrow \Lambda_1/L \rightarrow 0$$

gives rise to the equality

$$N(LM) = N(L) \cdot \text{ord } L/LM.$$

Thus it suffices to show that $\text{ord } L/LM = N(M)$. As in the proof of (24.2), it is enough to prove this when R is a discrete valuation ring. But then $L = x\Lambda_2$ for some $x \in u(A)$, and so

$$L/LM = x\Lambda_2/xM \cong \Lambda_2/M,$$

where the indicated isomorphism is an R -isomorphism. This implies at once that $\text{ord } L/LM = N(M)$, and the theorem is proved.

We are now in a position to extend our definition of norm from integral

ideals to normal ideals. For each normal ideal J , choose a nonzero $\alpha \in R$ such that αJ is integral, and let

$$N^*(J) = \alpha^{-n} N(\alpha J), \quad \text{where } n = (A : K).$$

Let us show at once that $N^*(J)$ does not depend on the choice of α . If also $\beta J \subset \Lambda = O_i(J)$, then $\alpha\beta J = \alpha\Lambda \cdot \beta J = \beta\Lambda \cdot \alpha J$,

and both of the indicated products are proper products. Hence

$$N(\alpha\Lambda) N(\beta J) = N(\beta\Lambda) N(\alpha J)$$

by (24.4). But $N(\alpha\Lambda) = R \cdot \alpha^n$, $N(\beta\Lambda) = R \cdot \beta^n$, whence

$$\alpha^{-n} N(\alpha J) = \beta^{-n} N(\beta J),$$

as claimed. In particular, if J is an integral ideal, we may choose $\alpha = 1$, and thus $N^*(J) = N(J)$.

(24.5) THEOREM. *The above-defined norm N^* satisfies*

$$N^*(J \cdot J') = N^*(J) \cdot N^*(J')$$

for each proper product $J \cdot J'$ of normal ideals. Further

$$N^*(J^{-1}) = N^*(J)^{-1}.$$

Proof. Choose a nonzero $\alpha \in R$ such that both αJ and $\alpha J'$ are integral. Then $\alpha J \cdot \alpha J'$ is a proper product of integral ideals, and so

$$N(\alpha J) N(\alpha J') = N(\alpha^2 JJ') = \alpha^{2n} N^*(JJ').$$

This implies at once that $N^*(JJ') = N^*(J) N^*(J')$. Further, if $\Lambda = O_i(J)$ then $J \cdot J^{-1} = \Lambda$, whence

$$R = N(\Lambda) = N^*(J) \cdot N^*(J^{-1}).$$

This completes the proof of the theorem.

Hereafter we shall write N instead of N^* , so we have now defined the norm $N(J)$ of each normal ideal J of A . If J_1 is a two-sided Λ_1 -ideal in A , where Λ_1 is a maximal order, then for each normal ideal $L = L_{12}$, the proper product $L^{-1} J_1 L$ is a two-sided Λ_2 -ideal J_2 . We have called J_1 and J_2 *similar* (see §22). It follows at once that

$$N(J_2) = N(L^{-1} J_1 L) = N(J_1),$$

so similar ideals have the same norm.

Let \mathfrak{P} be any prime ideal of the maximal order Λ , and set $P = R \cap \mathfrak{P}$, $\bar{R} = R/P$. We define the *inertial degree* of \mathfrak{P} as

$$f = f(\mathfrak{P}, \Lambda/R) = (\Lambda/\mathfrak{P} : \bar{R}).$$

Since $\Lambda/\mathfrak{P} \cong \bar{R}^{(f)}$ as R -modules, we obtain

$$(24.6) \quad N(\mathfrak{P}) = \text{ord}_R \Lambda/\mathfrak{P} = P^f.$$

Define the *capacity* κ of \mathfrak{P} by the condition

$$\Lambda/\mathfrak{P} \cong M_\kappa(S), \quad S = \text{skewfield}.$$

(24.7) THEOREM. *Similar prime ideals have the same inertial degree, capacity, and norm.*

Proof. Let \mathfrak{P}_1 be a prime ideal of the maximal order Λ_1 , and let $\mathfrak{P}_2 = L^{-1}\mathfrak{P}_1 L$ be a similar prime ideal in Λ_2 , where $L = L_{12}$ is a normal ideal. Clearly $\mathfrak{P}_1 \cap R = \mathfrak{P}_2 \cap R = P$, and by the proof of (22.4) we have

$$\Lambda_i/\mathfrak{P}_i \cong (\Lambda_i)_P / (\mathfrak{P}_i)_P, \quad i = 1, 2.$$

To prove the theorem, it suffices to show that there is an isomorphism of R/P -algebras $\Lambda_1/\mathfrak{P}_1 \cong \Lambda_2/\mathfrak{P}_2$, under the assumption that R is a discrete valuation ring. But in this case, $L = \Lambda_1 x$ for some $x \in u(A)$, so

$$\Lambda_2/\mathfrak{P}_2 = x^{-1}\Lambda_1 x / x^{-1}\mathfrak{P}_1 x \cong \Lambda_1/\mathfrak{P}_1.$$

This completes the proof.

(24.8) COROLLARY. *Let M be a maximal integral ideal, belonging to a prime ideal of inertial degree f and capacity κ . Then*

$$N(M) = P^{f/\kappa}, \quad \text{where } P = R \cap M.$$

Proof. Let $\Lambda = O_r(M)$, and let M belong to the prime ideal \mathfrak{P} of Λ . Then $\Lambda/\mathfrak{P} \cong (\Lambda/M)^{(\kappa)}$ as left Λ -modules, whence

$$P^f = N(\mathfrak{P}) = \text{ord}_R \Lambda/\mathfrak{P} = \{\text{ord}_R \Lambda/M\}^\kappa = N(M)^\kappa.$$

This proves the theorem. It should be pointed out that if $\Lambda' = O_r(M)$, then M also belongs to a prime ideal \mathfrak{P}' of Λ' . However, \mathfrak{P} and \mathfrak{P}' are similar by (24.22), and they have the same P, f, κ by (24.7), so the assertion of the theorem holds equally well when we work with \mathfrak{P}' rather than \mathfrak{P} .

We shall next give another interpretation of norms, which relates norms of ideals with norms of elements.

(24.9) THEOREM. *Let J be a normal ideal of A , and let N denote $N_{A/K}$. Then*

$$N(J) = R\text{-ideal generated by } \{N(x) : x \in J\}.$$

Proof. It suffices to prove the result when R is a discrete valuation ring, and an obvious argument shows that we may restrict ourselves to the case where J is an integral ideal. Then $J = \Lambda a$ for some $a \in u(A)$, where $\Lambda = O_i(J)$, and so $N(J) = R \cdot Na$ by Exercise 10.7. On the other hand,

$$\sum_{x \in J} R \cdot N(x) = \sum_{\lambda \in \Lambda} R \cdot N(\lambda) N(a) = R \cdot N(a),$$

since $N(\lambda) \in R$ for each $\lambda \in \Lambda$. This completes the proof.

(24.10) COROLLARY. *Let K be a finite separable extension of the field E , and let R be the integral closure in K of the Dedekind domain S with quotient field E . Then*

$$N_{K/E}(N_{A/K}J) = N_{A/E}J$$

for each normal ideal J of A .

Proof. Let J be a normal ideal of A , and set $\Lambda = O_i(J)$. Then Λ is a maximal S -order in A , as well as a maximal R -order in A . To prove the stated equality of S -ideals in E , we need only prove the result when S is replaced by its localizations at prime ideals of S . Changing notation, we assume that S is a discrete valuation ring. Then $J = \Lambda x$ for some $x \in u(A)$, and so

$$N_{A/E}J = S \cdot N_{A/E}x, \quad N_{A/K}J = R \cdot N_{A/K}x.$$

But by (24.2), for each nonzero $\alpha \in R$ we have

$$N_{K/E}(R\alpha) = S \cdot N_{K/E}\alpha.$$

Therefore

$$N_{K/E}(N_{A/K}J) = S \cdot N_{K/E}(N_{A/K}x) = S \cdot N_{A/E}x$$

by Exercise 1.5. This completes the proof.

We shall now define reduced norms of normal ideals, and in order to avoid cumbersome notation, we shall restrict our attention to the central simple case. For the remainder of this section, let A denote a central simple K -algebra, and let $(A : K) = n^2$ hereafter. Denote by “nr” the reduced norm map $\text{nr}: A \rightarrow K$, so by (9.7) we have

$$N_{A/K}a = (\text{nr } a)^n, \quad a \in A.$$

(24.11) THEOREM. *For each normal ideal J in the central simple K -algebra A , the norm $N(J)$ is the n -th power of an R -ideal $\text{nr } J$, called the reduced norm of J . For each proper product $J \cdot J'$ of normal ideals in A , we have*

$$\text{nr } (J \cdot J') = (\text{nr } J)(\text{nr } J').$$

Proof. To prove that $N(J)$ is an n th power, it suffices to show that for each prime ideal P of R , $N(J_P)$ is an n th power. Changing notation, we may assume that R is a discrete valuation ring. But then $J = \Lambda a$ for some $a \in u(A)$, where $\Lambda = O_l(J)$, and thus

$$N(J) = R \cdot N_{A/K} a = (R \cdot \text{nr } a)^n.$$

Finally, N is multiplicative on proper products by (24.5), whence so is “nr”. This completes the proof.

As a direct consequence of (24.9) and (24.11), we obtain

(24.12) COROLLARY. *For each normal ideal J in A , $\text{nr } J = R$ -ideal generated by $\{\text{nr } x : x \in J\}$.*

We shall now establish the following important result:

(24.13) THEOREM. *Let M be a maximal integral ideal of the central simple K -algebra A , and set $P = M \cap R$, $\bar{R} = R/P$. If \bar{R} is a finite field, then*

$$\text{nr } M = P, \quad N(M) = P^n, \quad (A : K) = n^2.$$

Proof. Let $\Lambda = O_l(M)$, and let \mathfrak{P} be the prime ideal of Λ to which M belongs. By (24.8)

$$\text{nr } M = P^{f/\kappa n},$$

where f is the inertial degree of \mathfrak{P} and κ is the capacity of \mathfrak{P} . Letting \hat{R} denote the P -adic completion of R , we have

$$\hat{\Lambda}/\hat{\mathfrak{P}} \cong \Lambda_P/\mathfrak{P}_P \cong \Lambda/\mathfrak{P}$$

by (18.2) and (22.4). Further, \hat{A} is a central simple \hat{K} -algebra and $(\hat{A}:\hat{K}) = (A:K) = n^2$. Thus we can compute f , κ , n by working with the case where the underlying ring is \hat{R} , rather than R .

Let us write $\hat{A} \cong M_r(D)$, where D is a skewfield with center \hat{K} and index m . Then $\hat{\Lambda} \cong M_r(\Delta)$, where Δ is the maximal \hat{R} -order in D , and we have

$$\hat{\Lambda}/\hat{\mathfrak{P}} \cong M_r(\Delta/\text{rad } \Delta).$$

Further, $\Delta/\text{rad } \Delta$ is a skewfield of dimension m over \bar{R} , by (14.3). Hence we obtain

$$f = (\hat{\Lambda}/\hat{\mathfrak{P}}:\bar{R}) = r^2m, \quad \kappa = r, \quad n^2 = (\hat{A}:\hat{K}) = r^2m^2.$$

This gives

$$f/\kappa n = r^2m/r \cdot rm = 1,$$

and completes the proof.

(24.14) **Corollary.** Let M be an integral ideal of the central simple K -algebra A , and assume that R/P is finite for each maximal ideal P of R . Then $\text{nr } M$ is the product of the R -annihilators of the Λ -composition factors of the left Λ -module Λ/M , where $\Lambda = O_i(M)$.

Proof. Let $\{S_i\}$ be the set of Λ -composition factors of Λ/M , and write $S_i \cong \Lambda/M_i$, with M_i a maximal left ideal of Λ . Then $\text{ann}_R S_i = M_i \cap R = P_i$ (say), and $N(M_i) = P_i^n$ by (24.13). Hence by (4.17) we have

$$N(M) = \text{ord}_R \Lambda/M = \prod \text{ord}_R S_i = \prod N(M_i) = (\prod P_i)^n.$$

Since $N(M) = (\text{nr } M)^n$, we obtain $\text{nr } M = \prod P_i$, as desired.

EXERCISES

In Exercises 1–3, A is a separable K -algebra, M is a normal ideal in A , and $\Lambda = O_i(M)$.

1. Let \hat{R} be the P -adic completion of R , where P is a prime ideal of R . Show that $\hat{R} \otimes_R N(M) = N(\hat{M})$. [Hint: It suffices to prove the result when M is integral. But

$$\hat{R} \otimes_R \text{ord}_R \Lambda/M = \text{ord}_{\hat{R}} \hat{\Lambda}/\hat{M}$$

by Exercise 4.4.]

2. If M is integral, prove that

$$\text{ord}_R \Lambda/M = \text{ord}_R M^{-1}/\Lambda.$$

[Hint: After localizing, write $M = \Lambda x$. Then

$$M^{-1}/\Lambda = x^{-1}\Lambda/\Lambda \cong \Lambda/\Lambda x.$$

Now use (24.2).]

3. Let M be integral, and let $K = \mathbf{Q}$, $R = \mathbf{Z}$. Prove that

$$N(M) = (\text{card } \Lambda/M) \cdot \mathbf{Z}.$$

Call $\text{card } \Lambda/M$ the *counting norm* or *absolute norm* of M .

4. Let Λ be a maximal order in a central simple K -algebra A , and let J be a proper two-sided ideal of Λ . Define a J -adic valuation w on A as follows: for $a \in A$, $a \neq 0$, let $w(a)$ be the least integer such that

$$\Lambda \cdot a \cdot \Lambda = J^{w(a)} BC^{-1},$$

where B and C are two-sided ideals of Λ such that $B + C = \Lambda$ and J does not divide B . Set $w(0) = +\infty$. Prove that

$$w(a + b) \geq \min(w(a), w(b)), \quad w(ab) \geq w(a) + w(b), \quad a, b \in A.$$

Now give A the J -adic topology, in which two elements $a, b \in A$ are near each other if $w(a - b)$ is large. Let \hat{A}_J denote the J -adic completion of A , and $\hat{\Lambda}_J$ the completion of Λ . Show that each element of $\hat{\Lambda}_J$ is representable by a sequence $\{a_n\}$ from Λ , with

$$a_{n+1} \equiv a_n \pmod{J^n}, \quad n = 1, 2, \dots.$$

Let $J = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$, where the $\{\mathfrak{P}_i\}$ are distinct prime ideals of Λ , and each $e_i \geq 1$. Using Exercise 22.3 (iv), show that

$$\hat{\Lambda}_J \cong \sum_{i=1}^r \hat{\Lambda}_{\mathfrak{P}_i}.$$

Prove further that if $P_i = R \cap \mathfrak{P}_i$, then

$$\hat{\Lambda}_{\mathfrak{P}_i} \cong \hat{\Lambda}_{P_i} \cong \hat{R}_{P_i} \otimes_R \Lambda.$$

Calculate the completion $\hat{\Lambda}_{\alpha\Lambda}$, where α is any ideal of R .

5. Let Λ be a maximal order in a central simple K -algebra A , and let M be a left ideal in Λ , and J a two-sided ideal in Λ . Call M and J relatively prime if $M + J = \Lambda$. Prove that the following are equivalent:

- (i) M and J are relatively prime.
- (ii) For each prime \mathfrak{P} of Λ dividing J , $\hat{M}_{\mathfrak{P}} = \hat{\Lambda}_{\mathfrak{P}}$.
- (iii) For each prime P of R , either $J_P = \Lambda_P$ or $M_P = \Lambda_P$.
- (iv) $N_{A/K} M + N_{A/K} J = R$.

(See also Exercise 27.5.)

25. DIFFERENT, DISCRIMINANT

Through this section let Λ be a maximal R -order in the separable K -algebra A , and let $\text{tr}: A \rightarrow K$ be the reduced trace map. By “ideal” we mean, as usual, a full R -lattice in A . Given a two-sided Λ -ideal J in A , define its *complementary ideal* as

$$\tilde{J} = \{x \in A : \text{tr } xJ \subset R\}.$$

Then \tilde{J} is also a two-sided Λ -ideal in A . In particular, we call $\tilde{\Lambda}$ the *inverse different* of Λ , and define the *different* of Λ as

$$\mathfrak{D} = \mathfrak{D}(\Lambda/R) = \tilde{\Lambda}^{-1}.$$

Since $\tilde{\Lambda} \supset \Lambda$, it is clear that \mathfrak{D} is a two-sided ideal of Λ . As in the proofs of (4.35) and (20.1), it is easily verified that the process of forming complementary ideals commutes with localization or completion at prime ideals of R . Furthermore, as explained in Exercise 25.1, the calculation of $\mathfrak{D}(\Lambda/R)$ can always be reduced to the central simple case.

(25.1) THEOREM. *Keeping the above notation, we have*

$$\tilde{J} = \tilde{\Lambda} \cdot J^{-1}.$$

Proof. It suffices to prove the result locally, when R is a discrete valuation

ring. But then $J = y\Lambda$ for some $y \in u(A)$, and so $\text{tr } xJ = \text{tr } xy\Lambda$. Thus $x \in \tilde{J}$ if and only if $xy \in \tilde{\Lambda}$. Therefore

$$\tilde{J} = \tilde{\Lambda}y^{-1} = \tilde{\Lambda} \cdot J^{-1},$$

which completes the proof.

The *discriminant* $d(\Lambda/R)$ is the ideal of R generated by

$$\{\det(\text{tr } x_i x_j)_{1 \leq i, j \leq n} : x_1, \dots, x_n \in \Lambda\},$$

where $n = (A : K)$. As in Exercises 4.13 and 10.6, forming discriminants commutes with localization or completion at a prime ideal of R .

(25.2) THEOREM.

$$d(\Lambda/R) = N_{A/K}(\mathfrak{D}(\Lambda/R)).$$

Proof. It suffices to prove the result locally, since the norm behaves properly under localization by (24.2). We have

$$N(\mathfrak{D}) = \text{ord}_R \Lambda/\mathfrak{D} = \text{ord}_R \tilde{\Lambda}/\Lambda$$

by Exercise 24.2. Now let $\Lambda = \sum_{i=1}^n Rx_i$; as in the proof of (4.35), we have

$$d(\Lambda/R) = R \cdot \det(\text{tr } x_i x_j)_{1 \leq i, j \leq n}.$$

On the other hand, choose a dual basis $\{y_j\}$ of A so that $\text{tr } x_i y_j = \delta_{ij}$. Then $\tilde{\Lambda} = \sum Rx_j$, and if we set $x_i = \sum \alpha_{ij} y_j$, $\alpha_{ij} \in K$, then

$$\text{ord}_R \tilde{\Lambda}/\Lambda = R \cdot \det(\alpha_{ij})$$

by Exercise 4.2. But $\alpha_{ij} = \text{tr } x_i x_j$, so the proof is completed.

(25.3) THEOREM. *The discriminant $d(\Lambda/R)$ is independent of the choice of the maximal order Λ .*

Proof. Let Γ be another maximal R -order in A , and choose a normal ideal L in A with left order Γ and right order Λ . Then $\Gamma = L\Lambda L^{-1}$, and $\mathfrak{D}(\Gamma) = L \cdot \mathfrak{D}(\Lambda) \cdot L^{-1}$. Taking norms, we obtain $d(\Gamma) = d(\Lambda)$, as claimed.

We next prove the non-commutative analogue of (4.37).

(25.4). THEOREM. *Let \mathfrak{P} be a prime ideal of the maximal R -order Λ in a separable K -algebra A . Set $P = \mathfrak{P} \cap R$, $\bar{R} = R/P$, and write $P\Lambda = \mathfrak{P}^e \mathfrak{Q}$, where $e \geq 1$ and \mathfrak{Q} is a two-sided ideal of Λ not divisible by \mathfrak{P} . Then $\mathfrak{P}^{e-1} \mid \mathfrak{D}(\Lambda/R)$. If $e = 1$, then $\mathfrak{P} \mid \mathfrak{D}(\Lambda/R)$ if and only if the center of the simple \bar{R} -algebra Λ/\mathfrak{P} is inseparable over \bar{R} .*

Proof. Step 1. We show first that the proof can be reduced to the case where

A is simple, and R is a complete discrete valuation ring. Indeed, starting with the general case, let \hat{R} be the P -adic completion of R . If we replace each ideal by its P -adic completion, then the hypotheses are unchanged. (In this connection, note that from the relation $\mathfrak{P} + \mathfrak{Q} = \Lambda$ it follows that $\hat{\mathfrak{P}} + \hat{\mathfrak{Q}} = \hat{\Lambda}$, so $\hat{\mathfrak{P}}$ does not divide $\hat{\mathfrak{Q}}$.) Since $\mathfrak{D}(\hat{\Lambda}/\hat{R})$ is the P -adic completion of $\mathfrak{D}(\Lambda/R)$, we know that

$$\mathfrak{P}^k | \mathfrak{D}(\Lambda/R) \text{ if and only if } \hat{\mathfrak{P}}^k | \mathfrak{D}(\hat{\Lambda}/\hat{R}).$$

Hence it suffices to prove the desired result for the case where R is complete.

Changing notation, we assume for the remainder of this proof that R is a complete discrete valuation ring. If we write A as a direct sum $\sum_{i=1}^t A_i$ of simple components, then correspondingly $\Lambda = \sum \Lambda_i$, with Λ_i a maximal R -order in A_i . Renumbering the $\{A_i\}$ if need be, we may take

$$\mathfrak{P} = \mathfrak{P}_1 \oplus \Lambda_2 \oplus \cdots \oplus \Lambda_t,$$

where $\mathfrak{P}_1 = \text{rad } \Lambda_1$ is the unique prime ideal of Λ_1 . Then \mathfrak{Q} must have the form

$$\mathfrak{Q} = \Lambda_1 \oplus \mathfrak{Q}_2 \oplus \cdots \oplus \mathfrak{Q}_t, \quad \mathfrak{Q}_j = \text{two-sided ideal in } \Lambda_j,$$

and likewise there is a decomposition

$$\mathfrak{D}(\Lambda/R) = \mathfrak{D}_1 \oplus \cdots \oplus \mathfrak{D}_t, \quad \mathfrak{D}_i = \mathfrak{D}(\Lambda_i/R).$$

Then we have $P\Lambda_1 = \mathfrak{P}_1^e$, and $\mathfrak{P}^k | \mathfrak{D}(\Lambda/R)$ if and only if $\mathfrak{P}_1^k | \mathfrak{D}_1$. Changing notation once more, we may thus assume for the remainder of the proof that A is a simple separable K -algebra and that $\mathfrak{Q} = \Lambda$, that is, $P\Lambda = \mathfrak{P}^e$.

Step 2. We now show that if $P\Lambda = \mathfrak{P}^e$ then $\mathfrak{P}^{e-1} | \mathfrak{D}$, where $\mathfrak{D} = \mathfrak{D}(\Lambda/R)$. Consider the \bar{R} -algebra $\bar{\Lambda} = \Lambda/P\Lambda$; since an R -basis of Λ maps onto an \bar{R} -basis of $\bar{\Lambda}$, we may conclude (as in the proof of formula (4.38)) that

$$(25.5) \quad \overline{\text{char. pol.}}_{A/K} a = \text{char. pol.}_{\bar{\Lambda}/\bar{R}} \bar{a}, \quad a \in \Lambda,$$

where bars denote reduction mod P . For each $a \in \mathfrak{P}$ we have $\bar{a}^e = 0$ in $\bar{\Lambda}$, and so $\text{char. pol. } \bar{a}$ is a power of X . But then by (25.5), $\text{char. pol. } a$ (taken mod P) is a power of X . Since $\text{char. pol. } a$ is a power of $\text{red. char. pol. } a$ by (9.24), we conclude that also $\text{red. char. pol. } a$ (taken mod P) is a power of X .

But we have

$$\text{red. char. pol. } a = X^n - (\text{tr } a) X^{n-1} + \cdots + (-1)^n \text{nr } a,$$

and so we have now shown that

$$\text{tr}_{A/K} \mathfrak{P} \subset P.$$

Therefore $\mathfrak{P} \subset P \cdot \mathfrak{D}^{-1}$, whence $\mathfrak{P}^{e-1} | \mathfrak{D}$ as claimed.

Step 3. For the rest of the proof let $e = 1$, so that $P\Lambda = \mathfrak{P}$ is the prime ideal of Λ . Let $A = M_r(D)$, where D is a skewfield with center L , and let S be the integral closure of R in L . We set $(D:L) = n^2$, $(L:K) = k$. Then Λ is also a maximal S -order in A , and by (17.4) we may identify Λ with a full matrix ring $M_r(\Delta)$ over the unique maximal S -order Δ in D . From (17.5) and the formula

$$\mathfrak{P} = P\Lambda = M_r(P\Delta) = M_r(PS \cdot \Delta),$$

it follows that PS is the prime ideal of S , and $P\Delta$ is the prime ideal of Δ . Therefore $\bar{\Delta} = \Delta/P\Delta$ is a skewfield; since $\Lambda/\mathfrak{P} \cong M_r(\bar{\Delta})$, the skewfield $\bar{\Delta}$ has the same center C as does the \bar{R} -algebra Λ/\mathfrak{P} . Furthermore,

$$\mathfrak{D}(\Lambda/R) = M_r(\mathfrak{D}(\Delta/R))$$

by (20.2). Thus we need to prove that $P\Delta \mid \mathfrak{D}(\Delta/R)$ if and only if C is inseparable over \bar{R} , so we have now reduced the problem to the case of skewfields.

Step 4. Keeping the notation of the preceding step, let $a \in \Delta$ map onto $\bar{a} \in \bar{\Delta}$, and let

$$f(X) = \text{red. char. pol.}_{D/K} a, \quad m(X) = \text{min. pol.}_{\bar{R}} \bar{a}.$$

Then $f(X)$ has degree nk , whereas

$$\text{degree of } m(X) = (\bar{R}(\bar{a}): \bar{R}) = d,$$

say. Since $\bar{\Delta}$ is a skewfield, $m(X)$ must be irreducible over \bar{R} , and hence $\text{char. pol.}_{\bar{R}/K} \bar{a}$ is a power of $m(X)$. It then follows from (25.5) that $\bar{f}(X)$ is a power of $m(X)$, whence $d \mid nk$. Furthermore, we obtain

$$(25.6) \quad \bar{\text{tr}}_{D/K} a = (nk/d) \cdot T(\bar{a}), \quad a \in \Delta,$$

where T is the ordinary trace from the field $\bar{R}(\bar{a})$ to \bar{R} .

We shall now show that if C (= the center of $\bar{\Delta}$) is inseparable over \bar{R} , then $\bar{\text{tr}}_{D/K} a = 0$ for each $a \in \Delta$. This will imply that $\text{tr}_{D/K} \Delta \subset P$, whence $P^{-1}\Delta \subset \mathfrak{D}(\Delta/R)^{-1}$, and so $P\Delta \mid \mathfrak{D}(\Delta/R)$ as asserted. Let $p = \text{char } \bar{R}$, so $p \in P$. If \bar{a} is inseparable over \bar{R} then $T(\bar{a}) = 0$, so by (25.6) we obtain $\bar{\text{tr}} a = 0$ as desired. On the other hand, suppose that \bar{a} is separable over \bar{R} . Since C is inseparable over \bar{R} , there exists an element $b \in \Delta$ such that $\bar{b} \in C$ and \bar{b} is inseparable over $\bar{R}(\bar{a})$. Then $\bar{R}(\bar{a}, \bar{b})$ is a finite algebraic extension of \bar{R} , so by the “Theorem of the primitive element” (see van der Waerden [1]), there exists an element $c \in \Delta$ such that $\bar{R}(\bar{a}, \bar{b}) = \bar{R}(\bar{c})$. Therefore

$$(\bar{R}(\bar{c}): \bar{R}) = (\bar{R}(\bar{a}, \bar{b}): \bar{R}(\bar{a}))(\bar{R}(\bar{a}): \bar{R}) = (p^s d') \cdot d$$

for some $s \geq 1$, where $(\bar{R}(\bar{a}, \bar{b}): \bar{R}(\bar{a})) = p^s d'$ and where $d = (\bar{R}(\bar{a}): \bar{R})$ as before. However, $(\bar{R}(\bar{c}): \bar{R})$ is the degree of $\text{min. pol.}_{\bar{R}} \bar{c}$, and thus divides nk by the remarks in the preceding paragraph. This proves that $p^s \cdot d \mid nk$, and so

$p^s \mid (nk/d)$. Therefore $\bar{\text{tr}}_{D/K} a = 0$ whenever \bar{a} is separable over \bar{R} . We have thus established that $P\Delta \nmid \mathfrak{D}(\Delta/R)$ whenever C is inseparable over \bar{R} .

Step 5. Suppose finally that C is separable over \bar{R} , and that $e = 1$ as before. Since PS is the prime ideal of S , it follows that $\bar{S} = S/PS$ is a field, and $(\bar{S}:\bar{R}) = (L:K) = k$ by (5.6).

$$\begin{array}{ccc} D & \xrightarrow{\quad} & \bar{\Delta} \\ n^2 \downarrow & & \downarrow m^2 \\ L & \xrightarrow{\quad} & C \\ k \downarrow & & t^2 \\ K & \xrightarrow{\quad} & \bar{S} \\ & & k \\ & & \bar{R} \end{array}$$

Further, $(\bar{\Delta}:\bar{S}) = (\Delta/P\Delta:\bar{S}) = (D:L) = n^2$.

Set $(\bar{\Delta}:C) = m^2$; then

$$n^2 = (\bar{\Delta}:\bar{S}) = m^2(C:\bar{S}),$$

so $(C:\bar{S}) = t^2$ for some integer t . We show next that $C = \bar{S}$, that is, $t = 1$. By (7.15) there exists a maximal subfield E of the skewfield $\bar{\Delta}$, with the property that E is a separable extension of C . Then E is a separable field extension of \bar{R} , and so $E = \bar{R}(\bar{c})$ for some $\bar{c} \in \bar{\Delta}$. Since $(E:C) = m$ by (7.15), we obtain

$$(\bar{R}(\bar{c}):\bar{R}) = (E:C)(C:\bar{S})(\bar{S}:\bar{R}) = mt^2k.$$

But on the other hand $(\bar{R}(\bar{c}):\bar{R})$ is a divisor of nk , by the first paragraph of Step 4. Thus $mt^2k \mid mtk$, whence $t = 1$ and $C = \bar{S}$.

It now follows that for each $a \in \Delta$, both of the polynomials

$$\overline{\text{red. char. pol.}}_{D/K} a, \quad \overline{\text{red. char. pol.}}_{\bar{\Delta}/\bar{R}} \bar{a}$$

have degree nk . Both of them are powers of the irreducible polynomial $\min. \text{pol.}_{\bar{R}} \bar{a}$, and hence they are equal. This shows that

$$\bar{\text{tr}}_{D/K} a = \text{tr}_{\bar{\Delta}/\bar{R}} \bar{a}, \quad a \in \Delta.$$

But by hypothesis $\bar{\Delta}$ is a separable \bar{R} -algebra, and so there exists an element $a \in \Delta$ such that $\text{tr}_{\bar{\Delta}/\bar{R}} \bar{a} \neq 0$. This shows that $\bar{\text{tr}}_{D/K} \Delta \not\subset P$, and hence it follows that $P\Delta \nmid \mathfrak{D}(\Delta/R)$. This completes the proof of the theorem.

If A is a central simple K -algebra, and $(A:K) = n^2$, then we have

$$d(\Lambda/R) = N_{A/K}(\mathfrak{D}(\Lambda/R)) = (\text{nr } \mathfrak{D})^n.$$

We call $\text{nr } \mathfrak{D}$ the *ground ideal* of Λ . It is an ideal of R , and is independent of the choice of the maximal order Λ .

For each prime ideal P of R , the P -adic completion \hat{A}_P is isomorphic to a full matrix algebra $M_{\kappa_P}(S)$, where S is a skewfield with center \hat{K}_P and index m_P . We shall call m_P the *local index* of A at P , and κ_P the *local capacity* of A at P .

Now suppose that K is a global field. Then of course each residue class field R/P is a finite field, and has no inseparable extensions. Hence for each prime ideal \mathfrak{P} of the maximal order Λ , we have

$$\mathfrak{P} \mid \mathfrak{D}(\Lambda/R) \quad \text{if and only if} \quad \mathfrak{P}^2 \mid P\Lambda, \quad \text{where } P = \mathfrak{P} \cap R.$$

In fact, we have the more precise statement:

(25.7) **Theorem.** *Let A be a central simple K -algebra, where K is a global field, and let Λ be a maximal R -order in A . For each P , let m_P be the local index of A at P , and let \mathfrak{P} be the prime ideal of Λ corresponding to P . Then $m_P = 1$ a.e., and*

$$(25.8) \quad P\Lambda = \mathfrak{P}^{m_P}, \quad \mathfrak{D}(\Lambda/R) = \prod_P \mathfrak{P}^{m_P - 1}.$$

Proof. Since K is a global field, the first of the above equalities follows from (22.14). As remarked at the start of this section, for each P we have

$$(25.9) \quad \mathfrak{D}(\hat{\Lambda}/\hat{R}) = \hat{R} \otimes_R \mathfrak{D}(\Lambda/R),$$

where \hat{R} , $\hat{\Lambda}$ denote P -adic completions. The left hand expression equals $\hat{\mathfrak{P}}^{m_P - 1}$ by (20.3), since K is a global field. On the other hand, $\mathfrak{D}(\Lambda/R)$ is an ideal in Λ , so $\mathfrak{D}_P = \Lambda_P$ a.e., whence $\mathfrak{D}(\hat{\Lambda}/\hat{R}) = \hat{\Lambda}$ a.e. by (25.9). This shows that $m_P = 1$ a.e. It also establishes the second equality in (25.8) since that equality holds at each P -adic completion (see (5.2)).

We may remark that in the above situation, the power of \mathfrak{P} in $\mathfrak{D}(\Lambda/R)$ is precisely \mathfrak{P}^{e-1} , where $P\Lambda = \mathfrak{P}^e$. Thus (25.4) is in a sense best possible.

(25.10) **COROLLARY.** *Keeping the above notation, we have*

$$\text{nr } \mathfrak{D}(\Lambda/R) = \prod_P P^{(m_P - 1)\kappa_P}, \quad d(\Lambda/R) = \{\text{nr } \mathfrak{D}(\Lambda/R)\}^n$$

where $n^2 = (A : K)$, and κ_P denotes the local capacity of A at P .

Proof. Let P be any prime ideal of R , \mathfrak{P} the corresponding prime ideal of Λ , and M a maximal left ideal of Λ belonging to \mathfrak{P} . Then $\text{nr } M = P$ by (24.13). On the other hand, the proof of (24.8) shows that

$$N(\mathfrak{P}) = N(M)^{\kappa_P}.$$

Since the ordinary norm is the n th power of the reduced norm, this gives

$$(25.11) \quad \text{nr } \mathfrak{P} = P^{\kappa_P}.$$

The formulas in (25.10) for the ground ideal $\text{nr } \mathfrak{D}$, and for the discriminant $d(\Lambda/R)$, now follow directly from (25.8) by taking reduced norms.

EXERCISES

Let Λ be a maximal R -order in the separable K -algebra A .

- Using the notation of (10.5), show that

$$\mathfrak{D}(\Lambda/R) = \sum' \mathfrak{D}(\Lambda_i/R),$$

and that

$$\mathfrak{D}(\Lambda_i/R) = \mathfrak{D}(\Lambda_i/R_i) \cdot \mathfrak{D}(R_i/R).$$

Here, $\mathfrak{D}(R_i/R)$ is the different defined as in §4d. [Hint: Imitate the proof of Exercise 4.11, using (9.15).]

- Keeping the above notation, show that

$$d(\Lambda/R) = \prod d(\Lambda_i/R),$$

and that

$$d(\Lambda_i/R) = \{N_{K_i/K} d(\Lambda_i/R_i)\} \{d(R_i/R)\}^{(A_i:K_i)},$$

where $d(R_i/R)$ is the discriminant of R_i with respect to R (see §4d). [Hint: By (25.2) and Exercise 1,

$$d(\Lambda/R) = N_{A/K} \mathfrak{D}(\Lambda/R) = \prod N_{A_i/K} \mathfrak{D}(\Lambda_i/R) = \prod d(\Lambda_i/R).$$

Further,

$$d(\Lambda_i/R) = N_{A_i/K} \mathfrak{D}(\Lambda_i/R) = \{N_{A_i/K} \mathfrak{D}(\Lambda_i/R_i)\} \{N_{A_i/K} \mathfrak{D}(R_i/R)\}.$$

By Exercise 1.5,

$$N_{A_i/K} \mathfrak{D}(\Lambda_i/R_i) = N_{K_i/K} \{N_{A_i/K_i} \mathfrak{D}(\Lambda_i/R_i)\} = N_{K_i/K} d(\Lambda_i/R_i).$$

Likewise

$$\begin{aligned} N_{A_i/K} \mathfrak{D}(R_i/R) &= N_{K_i/K} \{N_{A_i/K_i} \mathfrak{D}(R_i/R)\} \\ &= \{N_{K_i/K} \mathfrak{D}(R_i/R)\}^{(A_i:K_i)} = \{d(R_i/R)\}^{(A_i:K_i)}. \end{aligned}$$

This yields the desired formulas for $d(\Lambda/R)$ and $d(\Lambda_i/R)$.]

- Let $M = M_{12}$ be a normal ideal of A , and define its *complementary ideal* by

$$\tilde{M} = \{x \in A : \text{tr } xM \subset R\}.$$

Show that $\tilde{M} = (\tilde{M})_{21}$ is also a normal ideal of A , and that $\tilde{M} = M$ (compare Exercise 4.12). Prove further that

$$\tilde{M} = \tilde{\Lambda}_2 \cdot M^{-1} = M^{-1} \cdot \tilde{\Lambda}_1.$$

[Remark: Manipulations of this type can be used to give another proof of the fact that $O_r(M)$ is maximal if and only if $O_r(M)$ is maximal; see Deuring [1, p. 84].]

3. An element $a \in u(A)$ is called an *R-unit* if both a and a^{-1} are integral over R . Prove that if a is integral over R , then a is an *R-unit* if and only if $N_{A/K} a \in u(R)$. [Hint: Let a be integral over R , and let Λ be a maximal R -order in A containing $R[a]$. If $Na \in u(R)$, then $\text{ord}_R \Lambda/\Lambda a = R$, so $\Lambda = \Lambda a$. Therefore $1 = xa$ for some $x \in \Lambda$, and clearly $x = a^{-1}$.]

4. Let $\Gamma \subset \Gamma'$ be R -orders in A , and let $x \in \Gamma$. Show that $x \in u(\Gamma)$ if and only if $x \in u(\Gamma')$. [Remark: The result is clear from Exercise 3. Alternate proof (A. Dress): if $x \in \Gamma \cap u(\Gamma')$, then x^{-1} is integral over R , whence $x^{-1} \in R[x] \subset \Gamma$; thus $x \in u(\Gamma)$.]

26. IDEAL CLASSES; JORDAN-ZASSENHAUS THEOREM

Throughout this section let R denote a Dedekind domain whose quotient field K is a global field. As shown in the references listed in §4, the ring $R/R\alpha$ is finite for each nonzero $\alpha \in R$. Let us set

$$|\alpha| = \text{card } R/R\alpha, \quad \alpha \neq 0; \quad |0| = 0.$$

Let Λ be an R -order in a K -algebra A . By a *left Λ -ideal* in A we shall mean, as usual, a left Λ -lattice M in A such that $KM = A$. We may partition the set of left Λ -ideals in A into ideal classes, by placing two such ideals M, N in the same class if $M \cong N$ as left Λ -modules. Each such isomorphism extends to a left A -isomorphism $KM \cong KN$, hence is given by right multiplication by some $x \in u(A)$. Thus the *ideal class* containing M consists of all ideals $\{Mx : x \in u(A)\}$. We shall show that under suitable hypotheses, the number $b(\Lambda)$ of ideal classes of Λ is finite. This result will be a special case of the more general Jordan-Zassenhaus Theorem proved below, and will be valid for all orders, not just for maximal orders. As we shall see, the general case reduces quickly to the case of ideals. We shall follow the treatment in Swan-Evans [1]; another approach is given in Curtis-Reiner [1].

Given an R -order Λ , we shall say that the *Jordan-Zassenhaus condition* $JZ(\Lambda)$ holds true if for each positive integer t , there are only finitely many Λ -isomorphism classes of left Λ -lattices of R -rank at most t . We intend to prove that JZ holds for all R -orders in semisimple K -algebras. Exercise 26.6 shows that the restriction to semisimple algebras cannot be omitted.

Our first lemma shows that in order to test whether $JZ(\Lambda)$ holds true, it suffices to test for $JZ(\Delta)$, with Δ ranging over orders in skewfields.

(26.1) LEMMA. *Let Λ be an R -order in the semisimple K -algebra A , let D_i be the skewfield part of the i -th simple component of A , and let Δ_i be an R -order in D_i . If $JZ(\Delta_i)$ holds for each i , then $JZ(\Lambda)$ also holds true.*

Proof. To begin with, let Γ be another R -order in A such that $\Gamma \subset \Lambda$. Any

two left Λ -lattices M, N are also left Γ -lattices, and

$$K \otimes_R \text{Hom}_\Gamma(M, N) \cong \text{Hom}_A(KM, KN) \cong K \otimes_R \text{Hom}_\Lambda(M, N).$$

Thus $M \cong N$ as Λ -lattices if and only if there exists an A -isomorphism $\varphi: KM \cong KN$ such that $\varphi(M) = N$. Since this condition is independent of Λ , it follows that M and N are Λ -isomorphic if and only if they are Γ -isomorphic.

Now let t be any positive integer, and let $\{M_i\}$ be a collection of left Λ -lattices of R -rank at most t . If $JZ(\Gamma)$ holds true, then there are only a finite number of Γ -isomorphism classes among the $\{M_i\}$. Hence there are only finitely many Λ -isomorphism classes among the $\{M_i\}$, which shows that $JZ(\Lambda)$ is also true.

We show conversely that if $JZ(\Lambda)$ holds, then so does $JZ(\Gamma)$. Given t , let $\{L_1, \dots, L_f\}$ be a full set of representatives of the isomorphism classes of left Λ -lattices of R -rank at most t . For any Γ -lattice M of R -rank at most t , we may view M as embedded in KM , and then we may form the Λ -lattice ΛM . Since ΛM has the same R -rank as M , it follows that $\Lambda M \cong L_i$ for some i , $1 \leq i \leq f$. Replacing M by a Γ -isomorphic copy, we may assume that $\Lambda M = L_i$. Choose a nonzero $\alpha \in R$ such that $\alpha\Lambda \subset \Gamma$; then

$$\alpha L_i = \alpha \cdot \Lambda M \subset M \subset L_i.$$

But L_i is a finitely generated R -module, and thus $L_i/\alpha L_i$ is a finite group, since $R/\alpha R$ is finite for each nonzero $\alpha \in R$. However, $M/\alpha L_i$ is an R -submodule of $L_i/\alpha L_i$, and thus there are only a finite number of possible M 's. We have therefore shown that the conditions $JZ(\Lambda)$ and $JZ(\Gamma)$ are equivalent whenever $\Gamma \subset \Lambda$.

If Ω is any R -order in A , then $\Omega \cap \Lambda$ is also an R -order in A . Both $JZ(\Lambda)$ and $JZ(\Omega)$ are equivalent to $JZ(\Omega \cap \Lambda)$, and hence are equivalent to each other. This proves that if $JZ(\Lambda)$ holds for one R -order Λ in A , then it holds for every R -order in A .

Now let $A = \sum M_{n_i}(D_i)$, let Δ_i be an R -order in D_i , and choose $\Lambda_i = M_{n_i}(\Delta_i)$, $\Lambda = \sum \Lambda_i$. Each left Λ -lattice M decomposes into a direct sum $\sum M_i$, with M_i a left Λ_i -lattice. If $\{M^{(\alpha)}\}$ is some family of left Λ -lattices, then for each α we may write

$$M^{(\alpha)} = \sum M_i^{(\alpha)}, \quad M_i^{(\alpha)} = \text{left } \Lambda_i\text{-lattice.}$$

Clearly

$$R\text{-rank } M^{(\alpha)} = \sum_i R\text{-rank } M_i^{(\alpha)} \quad \text{for each } \alpha.$$

Hence the set of positive integers $\{R\text{-rank } M^{(\alpha)}\}$ is bounded above if and only if for each i , the set $\{R\text{-rank } M_i^{(\alpha)}\}$ is bounded above. We shall usually abbreviate this statement by omitting the superscript α , and shall say "The

R -rank of M is bounded if and only if for each i , the R -rank of M_i is bounded". Thus $JZ(\Delta)$ holds true if and only if $JZ(\Delta_i)$ holds for each i . By §16, Δ_i is Morita equivalent to Δ_i , and there exists a (Δ_i, Δ_i) -bimodule L such that the correspondence $M \rightarrow L \otimes_{\Delta_i} M$ gives a one-to-one isomorphism-preserving correspondence between the set of left Δ_i -modules M and the set of left Δ_i -modules $L \otimes M$. This bimodule L is a projective right Δ_i -module, and thus if M is an R -lattice, so is $L \otimes M$. Further, $\text{rank}_R M$ is bounded if and only if $\text{rank}_R L \otimes M$ is bounded. It follows at once that $JZ(\Delta_i)$ holds true if and only if $JZ(\Delta_i)$ holds true. This completes the proof of the theorem.

(26.2) **LEMMA.** *Let Δ be an R -order in a skewfield D over K . Then $JZ(\Delta)$ holds if and only if the number $h(\Delta)$ of ideal classes of Δ is finite.*

Proof. If $JZ(\Delta)$ holds, then clearly $h(\Delta)$ is finite. Conversely, suppose $h(\Delta)$ is finite. If D is separable over K , then we can show quickly that $JZ(\Delta)$ holds true. Namely, by the proof of (26.1), we may assume that Δ is a maximal R -order in D . Then Δ is hereditary, so every left Δ -lattice M is isomorphic to a direct sum of left ideals of Δ . If $\text{rank}_R M$ is bounded, so is the number of summands. Up to isomorphism, there are only $h(\Delta)$ possible choices for each summand, whence the number of non-isomorphic M 's of bounded R -rank is finite. Thus $JZ(\Delta)$ holds in this case.

Still assuming that $h(\Delta)$ is finite, let us drop the assumption that D is separable over K . By (10.6), each left Δ -lattice M may be embedded in a free Δ -lattice $\Delta^{(n)}$, where $KM = D^{(n)}$, and then

$$\text{rank}_R M = (KM : K) = n \cdot (D : K).$$

Let $d = (D : K)$. We show by induction on t that there are only finitely many non-isomorphic left Δ -lattices of R -rank td ; this of course implies that $JZ(\Delta)$ holds true.

The result is clear for $t = 1$, since we have assumed that $h(\Delta)$ is finite. Let $t > 1$, and assume the result holds for lattices of R -rank $(t - 1)d$. If M is any left Δ -lattice of R -rank td , then by the method of proof of (2.44), there is a Δ -exact sequence

$$O \rightarrow N \rightarrow M \rightarrow J \rightarrow O,$$

where J is a left ideal of Δ , and where $\text{rank}_R N = (t - 1)d$. Up to isomorphism, there are finitely many choices for N and J . Hence (see §2d) we need only show that for each fixed choice of N and J , the group $\text{Ext}_{\Delta}^1(J, N)$ is finite. This group is a finitely generated R -module by (2.34), so in view of our assumptions on R , we need only prove that it is an R -torsion module, that is,

$$K \otimes_R \text{Ext}_{\Delta}^1(J, N) = 0.$$

The left-hand expression equals $\text{Ext}_D^1(KJ, KN)$ by (2.43), and hence is zero by (2.28 v) since KJ is free as left D -module. This completes the proof of the lemma.

(26.3) LEMMA. Suppose that R is either \mathbf{Z} or a polynomial domain $k[X]$ over a finite field k . Let D be a skewfield over the quotient field K of R . Then $JZ(\Delta)$ holds true for every R -order Δ in D .

Proof. By the preceding lemma, it suffices to prove the finiteness of the number of isomorphism classes of left ideals of Δ . Since R is a principal ideal domain, we may write

$$\Delta = \sum_{i=1}^n Rx_i, \quad x_j x_i = \sum \alpha_{ijl} x_l, \quad \alpha_{ijl} \in R.$$

Let $x = \sum \lambda_i x_i \in \Delta$, $\lambda_i \in R$. Then

$$x_j x = \sum_{i,l} \lambda_i \alpha_{ijl} x_l.$$

Hence if $x \neq 0$, then by Exercise 26.3 we obtain

$$\text{card } \Delta/\Delta x = |N_{D/K} x| = |\det(\sum_i \lambda_i \alpha_{ijl})_{1 \leq j, l \leq n}|,$$

where for nonzero $\alpha \in R$, $|\alpha| = \text{card } R/R\alpha$. But the indicated determinant is a homogeneous polynomial of degree n in the λ 's, with coefficients in R . It follows from Exercise 26.1 that there exists a positive constant c such that

$$|\lambda_1| \leq t, \dots, |\lambda_n| \leq t \Rightarrow |N_{D/K}(\sum \lambda_i x_i)| \leq c \cdot t^n.$$

Now let M be any proper left ideal of Δ . Then Δ/M is a finite group, since it is a finitely generated torsion R -module. Let s be the greatest integer such that $s^n \leq \text{card } \Delta/M$, and let $\lambda_1, \dots, \lambda_n$ range independently over all elements $\lambda \in R$ with $|\lambda| \leq s+1$. By Exercise 26.1 there are at least $(s+1)^n$ such n -tuples $(\lambda_1, \dots, \lambda_n)$, and thus $\sum \lambda_i x_i$ ranges over more than $\text{card } \Delta/M$ distinct elements of Δ . Hence two such sums must be congruent mod M , and therefore M contains a nonzero element

$$x = \sum_{i=1}^n \lambda_i x_i,$$

where $\lambda_i \in R$, and $|\lambda_i| \leq 2(s+1)$ for each i .

Therefore $\Delta x \subset M \subset \Delta$, and

$$\text{card } \Delta/\Delta x = |N_{D/K}(\sum \lambda_i x_i)| \leq c \cdot 2^n(s+1)^n,$$

while $\text{card } \Delta/M \geq s^n$. Hence

$$\begin{aligned} \text{card } M/\Delta x &= \{\text{card } \Delta/\Delta x\}/\{\text{card } \Delta/M\} \\ &\leq c \cdot 2^n(s+1)^n/s^n = c \cdot 2^n(1+s^{-1})^n \leq c \cdot 4^n. \end{aligned}$$

We have thus shown that every proper left ideal M of Δ contains a nonzero element x such that $\text{card } M/\Delta x \leq c \cdot 4^n$. The same holds when $M = \Delta$, just choosing $x = 1$. Consider now all R -modules T having at most $c \cdot 4^n$ elements. Since R is a principal ideal domain, we may express T as a finite direct sum $\sum R/R\alpha_i$ where $\text{card } R/R\alpha_i \leq c \cdot 4^n$ for each i . Then each $\alpha_i \neq 0$ since R is infinite, and so $|\alpha_i| \leq c \cdot 4^n$ for each i . The number of possible choices for the $\{\alpha_i\}$ is therefore finite, by Exercise 26.1, and thus there exists a nonzero $\beta \in R$ such that $\beta T = 0$ for each T . Note that β does not depend on T .

In particular, we have $\beta M \subset \Delta x$ always, and so

$$\beta \cdot \Delta x \subset \beta M \subset \Delta x.$$

Therefore

$$\beta \Delta \subset M \cdot \beta x^{-1} \subset \Delta.$$

But β was chosen independently of M , and $\Delta/\beta\Delta$ is finite. Hence the number of choices for $M \cdot \beta x^{-1}$ is also finite. Since $M \cong M \cdot \beta x^{-1}$ as left Δ -modules, it follows that the number of isomorphism classes of left ideals of Δ is finite, and the proof is complete.

We are now ready to prove the fundamental result

(26.4) **Theorem** (Jordan–Zassenhaus). *Let R be any Dedekind domain whose quotient field K is a global field. Then for each R -order Λ in a semisimple K -algebra A , and for each positive integer t , there are only finitely many isomorphism classes of left Λ -lattices of R -rank at most t .*

Proof. We are trying to prove that JZ holds for R -orders in semisimple K -algebras. We shall first establish the existence of a Dedekind domain R_0 with quotient field K , such that $R_0 \subset R$, and such that JZ holds for R_0 -orders. When K is an algebraic number field, we choose $R_0 = \text{alg. int.}\{K\}$, the integral closure of \mathbf{Z} in K . Since $\mathbf{Z} \subset R$, and R is integrally closed, it follows that $R_0 \subset R$. By (26.1) and (26.3), JZ holds for \mathbf{Z} -orders. Hence it also holds for R_0 -orders, by Exercise 26.4.

On the other hand, suppose that K is a function field. By definition, we may write $K = k(x_1, \dots, x_n)$ for some elements x_1, \dots, x_n , where k is a finite field, and where K has transcendence degree 1 over k . Each x_i is expressible as $x_i = y_i/z_i$ with $y_i, z_i \in R$, and therefore $K = k(y_1, z_1, \dots, y_n, z_n)$. By a theorem of F. K. Schmidt (see Zariski–Samuel [1, Th. 31, p. 105]), we may choose one of the elements $y_1, z_1, \dots, y_n, z_n$ (call the chosen element X), such that $k(X)$ is purely transcendental over k and K is a finite separable extension of $k(X)$. Of course $X \in R$, from the manner in which X was chosen. Furthermore, the prime field \mathbf{F} of k lies in R , and every element of k is integral over \mathbf{F} . Therefore $R \supset k[X]$, and hence also $R \supset R_0$, where R_0 is the integral

closure of $k[X]$ in K . By (26.1) and (26.3), JZ holds for $k[X]$ -orders. Hence by Exercise 26.4, JZ also holds for R_0 -orders.

Now let Λ be any R -order in a semisimple K -algebra, where K is either an algebraic number field or a function field. We have shown above that R contains a Dedekind domain R_0 with quotient field K , such that JZ holds for R_0 -orders. By (8.8), there exists an R_0 -order Λ_0 in A such that $\Lambda = R\Lambda_0$. Further, each left Λ -lattice may be expressed as RM_0 , for some left Λ_0 -lattice M_0 . Clearly, the R -rank of RM_0 equals the R_0 -rank of M_0 . Since $JZ(\Lambda_0)$ holds true, it follows at once that $JZ(\Lambda)$ is also true. This completes the proof of the theorem.

It is worth pointing out another approach to the proof of the Jordan-Zassenhaus Theorem. Once the theorem is established for R_0 -orders, it follows for arbitrary R -orders by Exercise 26.5, since it can be shown (see Swan-Evans [1, pp. 226–227]) that $R = S^{-1}R_0$ for some multiplicative subset S of R_0 .

Finally, keeping the notation of (26.4), let L be any finite separable extension of K , and let R' be any R -order in L . Even if R' is not a Dedekind domain, the condition $JZ(\Lambda')$ is meaningful for R' -orders Λ' in semisimple L -algebras. The discussion in Exercise 26.4 remains valid, and shows that $JZ(\Lambda')$ holds for each such Λ' .

We shall now consider the special case

$$(26.5) \quad A = \mathbf{Q} \oplus \mathbf{Qi} \oplus \mathbf{Qj} \oplus \mathbf{Qk}, \quad \Lambda = \mathbf{Z} \oplus \mathbf{Zi} \oplus \mathbf{Zj} \oplus \mathbf{Zk}, \\ a = (1 + i + j + k)/2,$$

where Λ is a maximal \mathbf{Z} -order in the rational quaternion algebra A . By Exercise 25.3, $u(\Lambda)$ consists of the 24 elements

$$\pm 1, \quad \pm i, \quad \pm j, \quad \pm k, \quad (\pm 1 \pm i \pm j \pm k)/2.$$

It follows readily that for each $x \in \Lambda$, there exists a unit $u \in u(\Lambda)$ such that $ux \in \mathbf{Z} \oplus \mathbf{Zi} \oplus \mathbf{Zj} \oplus \mathbf{Zk}$.

We shall prove that $h(\Lambda) = 1$, and indeed that Λ is a euclidean domain, though not commutative. Let $x, y \in \Lambda$, $y \neq 0$, and write

$$xy^{-1} = q + r, \quad q = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k, \quad r = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k,$$

where $\alpha_v \in \mathbf{Z}$, $\beta_v \in \mathbf{Q}$. We may choose q so that each $|\beta_v| \leqslant 1/2$. Further, if it turns out that each $|\beta_v| = 1/2$, we may change our choice of q and r so that $q \in \Lambda$ and $r = 0$. Hence we can always pick $q \in \Lambda$, $r \in A$, such that

$$\text{nr } r = \beta_0^2 + \beta_1^2 + \beta_2^2 + \beta_3^2 < 1.$$

Therefore we may write

$$x = qy + t, \quad \text{where } q, t \in \Lambda, \quad \text{and } 0 \leqslant \text{nr } t < \text{nr } y.$$

This shows that Λ has a euclidean algorithm, and consequently every left ideal in Λ is principal, and is generated by an element of smallest reduced norm. Therefore $h(\Lambda) = 1$, as claimed.

For orders of class number 1, we can obtain a factorization theory for elements, rather than for ideals. Let Λ be any maximal order in a separable K -algebra, with $h(\Lambda) = 1$. Let $x \in \Lambda \cap u(A)$; we call x *indecomposable* if x is a non-unit of Λ which cannot be expressed as a product of non-units. We claim that x is indecomposable if and only if Λx is a maximal left ideal of Λ . If Λx is not maximal, then $\Lambda x < \Lambda m < \Lambda$ for some m , and then there is a factorization $x = ym$ into non-units. The procedure can be reversed, and the claim is established.

Now let $x \in \Lambda \cap u(A)$ be arbitrary, and let

$$\Lambda x = \Lambda x_1 < \Lambda x_2 < \cdots < \Lambda x_n = \Lambda$$

be an unrefinable chain of left ideals of Λ , where $x = x_1$ and $x_n = 1$. Then $x_i = u_i x_{i+1}$ for some $u_i \in \Lambda$, and

$$\Lambda x_{i+1} / \Lambda x_i \cong \Lambda / \Lambda u_i,$$

so each u_i is indecomposable. The equation

$$x = u_1 u_2 \cdots u_{n-1}$$

expresses x as a product of $n - 1$ indecomposable elements. The prime ideals of Λ associated with these elements are uniquely determined by x , up to similarity and order of occurrence (see (22.24)).

Returning to the case of quaternions, we use the preceding discussion to prove

(26.6) **THEOREM.** *Every positive rational integer is expressible as a sum of four squares.*

Proof. Keep the notation of (26.5), and let p be any rational prime. Then there exists a maximal left ideal $M = \Lambda m$ such that $p\Lambda \subset M \subset \Lambda$. Since A is a central simple \mathbf{Q} -algebra, it follows from (24.13) that

$$(\text{nr } m)\mathbf{Z} = \text{nr } M = p\mathbf{Z}.$$

Therefore $p = \text{nr } m$, since $\text{nr } m > 0$.

Now set $m = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$; replacing m by um if need be, where $u \in u(\Lambda)$, we may assume that each $\alpha_v \in \mathbf{Z}$. But then

$$p = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2,$$

a sum of four squares.

Finally, let $r = \prod p_v^{a_v}$ be any positive rational integer, where the $\{p_v\}$

are primes, and let

$$p_v = \text{nr } m_v, \quad m_v \in \mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}j \oplus \mathbf{Z}k.$$

Then

$$r = \prod p_v^{a_v} = \prod \text{nr}(m_v^{a_v}) = \text{nr} \prod m_v^{a_v}.$$

This proves that r is a sum of four squares of rational integers, and the theorem is established.

EXERCISES

1. Let $R = \mathbf{Z}$ or $R = k[X]$, where $\text{card } k = q$. For nonzero $\alpha \in R$, let $|\alpha| = \text{card } R/R\alpha$, and set $|0| = 0$. Prove that $|\alpha|$ is finite for all $\alpha \in R$, and

$$(i) |\alpha\beta| = |\alpha||\beta|, \quad |\alpha + \beta| \leq |\alpha| + |\beta|, \quad \alpha, \beta \in R.$$

- (ii) For each positive integer n , the number of elements $\alpha \in R$ with $|\alpha| \leq n$ is finite, and is at least n . [Hint: Let $\deg \alpha$ denote the degree of a polynomial $\alpha \in k[X]$, with $\deg 0 = -\infty$. Then $|\alpha| = q^{\deg \alpha}$, which yields (i). Further, $|\alpha| \leq n$ if and only if $\deg \alpha \leq \log_q n$. The number of such α 's equals q^{1+r} , where r is the greatest integer such that $r \leq \log_q n$.]

2. Keeping the above notation, let $N \subset M$ be free R -modules, where

$$M = \sum_{i=1}^d Rm_i, \quad N = \sum_{j=1}^d Rn_j, \quad n_j = \sum a_{ij} m_i, \quad a_{ij} \in R.$$

Prove that $\text{card } M/N = |\det(a_{ij})|$. [Hint: R is a principal ideal domain. After basis changes in M and N , which leave $|\det(a_{ij})|$ unchanged, we may assume that $(a_{ij}) = \text{diag}(b_1, \dots, b_d)$. Then

$$\text{card } M/N = \prod \text{card } R/Rb_i = \prod |b_i| = |\det(a_{ij})|.$$

Compare with Exercise 4.2.]

3. Keep the above notation, and let Λ be an R -order in a K -algebra A . Then for each $x \in \Lambda$ such that $x \in u(A)$, we have

$$\text{card } \Lambda/\Lambda x = |N_{A/K} x|,$$

where in this case the norm $N_{A/K}$ must be computed by letting x act by right multiplication on an R -basis of Λ .

4. Let L be a finite separable extension of K , and let R' be the integral closure of R in L . Show that if $JZ(\Lambda)$ holds for R -orders Λ in semisimple K -algebras, then $JZ(\Lambda')$ holds for R' -orders Λ' in semisimple L -algebras. [Hint: Since R' is a finitely generated R -module, each such Λ' is also an R -order. Further, for each Λ' -lattice M ,

$$\text{rank}_{R'} M = (L:K) \cdot \text{rank}_R M.]$$

5. Let $R' = S^{-1}R$ be a ring of quotients of R . Show that if JZ holds for R -orders (in semisimple K -algebras), then JZ also holds true for R' -orders. [Hint: Let the R' -order Λ' have R' -generators $\{x_i\}$, and let $x_i x_j = \sum \alpha_{ijl} x_l$, α 's in R' . Choose $s \in S$ so

that each $s\alpha_{ij} \in R$, and set $\Lambda = R + \sum R(sx_i)$. Then Λ is an R -order such that $R'\Lambda = \Lambda'$. Likewise, if $M' = \sum \Lambda'm_i$ is a Λ' -lattice, then $M = \sum \Lambda m_i$ is a Λ -lattice such that $\Lambda'M = M'$, and $\text{rank}_R M = \text{rank}_{R'} M'$. Deduce that if $JZ(\Lambda)$ holds, then so does $JZ(\Lambda')$. See also Exercise 3.5.]

6. Let $A = \mathbf{Q} \oplus \mathbf{Q}v$, where $v^2 = 0$, and let $\Lambda = \mathbf{Z} \oplus \mathbf{Z}v$ be a \mathbf{Z} -order in A . For $r \geq 1$, let M_r be the unital Λ -lattice $\mathbf{Z} + \mathbf{Z}$, where

$$v(a, b) = (0, rb), \quad (a, b) \in M_r.$$

Show that if $M_r \cong M_s$, then $r = s$. (Consider M_r/vM_r .) Thus $JZ(\Lambda)$ cannot hold in this case.

7. Suppose that $JZ(\Lambda)$ holds true for the R -order Λ in the semisimple K -algebra A , and let $h(\Lambda)$ be the number of classes of left Λ -ideals M in A such that $KM = A$. Prove

- (i) If $\Lambda \subset \Lambda' = R$ -order, then $h(\Lambda) \geq h(\Lambda')$.
- (ii) If Λ and Λ' are maximal orders, then $h(\Lambda) = h(\Lambda')$.
- (iii) If Λ is maximal, then $h(\Lambda)$ equals the number of classes of right Λ -ideals in A .
- (iv) $h(\Lambda') \leq h(\Lambda)$ if Λ' is a localization or completion of Λ at a prime ideal of R .

8. Let Λ be a maximal R -order in a separable K -algebra A . For $x \in u(A)$, we call the maximal order $x\Lambda x^{-1}$ conjugate to Λ . Show that if $JZ(\Lambda)$ holds true, then there are finitely many conjugacy classes of maximal R -orders in A .

9. Let $L = \mathbf{Q}(\sqrt{2})$, $R = \mathbf{Z}[\sqrt{2}]$, $S = \mathbf{Z}[2\sqrt{2}]$. Show that $R = \text{alg. int. } \{L\}$, and that R, S are \mathbf{Z} -orders in L . Prove that $h(S) > h(R) = 1$. [Hint: $h(R) = 1$ since R has a Euclidean algorithm (see Exercise 30.4). Show that the ideal $2S + 2\sqrt{2}S$ is not a principal ideal of S , so $h(S) \geq 2$.]

27. GENUS

Throughout this section let R denote a Dedekind domain with quotient field K . Let Λ be an R -order in a K -algebra A . Two left Λ -lattices M, N are in the same genus (notation: $M \vee N$) if for each prime ideal P of R , there is a Λ_P -isomorphism $M_P \cong N_P$.

(27.1) THEOREM. *Let M, N be left Λ -lattices. Then $M \vee N$ if and only if for each nonzero ideal I of R , the condition*

$$(27.2) \quad 0 \rightarrow M \rightarrow N \rightarrow T \rightarrow 0, \quad I + \text{ann}_R T = R,$$

holds for some Λ -exact sequence for some Λ -module T .

Proof. If the condition (27.2) holds when $I = P$, then $P + \text{ann}_R T = R$, whence $T_P = 0$ by (4.20). Since

$$0 \rightarrow M_P \rightarrow N_P \rightarrow T_P \rightarrow 0$$

is Λ_P -exact, it follows that $M_P \cong N_P$. Thus if (27.2) holds when I ranges over the prime ideals of R , then $M \vee N$.

Conversely, assume that $M \vee N$, and let I be a preassigned nonzero ideal of R . Let P_1, \dots, P_n be the distinct prime ideals dividing I . By the method of proof of Exercise 18.3, there exists $\varphi \in \text{Hom}_\Lambda(M, N)$ such that $\varphi_{P_i}: M_{P_i} \cong N_{P_i}$, $1 \leq i \leq n$. Since

$$(\ker \varphi)_{P_i} = \ker \varphi_{P_i} = 0,$$

and $\ker \varphi$ is R -torsionfree, it follows that $\ker \varphi = 0$. Consider the Λ -exact sequence

$$0 \rightarrow M \xrightarrow{\varphi} N \rightarrow T \rightarrow 0,$$

where $T = \text{cok } \varphi$. Then $T_{P_i} = 0$ for $1 \leq i \leq n$, whence $P_i + \text{ann}_R T = R$ for each i . Therefore $I + \text{ann}_R T = R$, as desired.

It should be remarked that when $I = R$, the preceding proof is valid if we just choose P_1 to be any prime ideal of R .

(27.3) COROLLARY. *Let L, M, N be left Λ -lattices in the same genus. Then there exists a left Λ -lattice L' in the genus, such that*

$$M \dot{+} N \cong L \dot{+} L'.$$

Proof. By (27.1), there exist Λ -exact sequences

$$0 \rightarrow M \xrightarrow{\varphi} L \rightarrow T \rightarrow 0, \quad 0 \rightarrow N \xrightarrow{\psi} L \rightarrow U \rightarrow 0,$$

such that T, U are R -torsion Λ -modules for which

$$\text{ann}_R T + \text{ann}_R U = R.$$

Thus for each prime ideal P of R , either $T_P = 0$ or $U_P = 0$, that is, either $\varphi_P: M_P \cong L_P$ or $\psi_P: N_P \cong L_P$. Now consider the Λ -exact sequence

$$0 \rightarrow L' \rightarrow M \dot{+} N \xrightarrow{(\varphi, \psi)} L \rightarrow 0,$$

where L' is defined to be the kernel of the map (φ, ψ) . The map (φ, ψ) is epic and split, since for each P , the epimorphism $(\varphi, \psi)_P: M_P \dot{+} N_P \rightarrow L_P$ is split. Therefore $M \dot{+} N \cong L \dot{+} L'$, and it remains for us to prove that $L' \vee L$.

Let \hat{R} be the P -adic completion of R , where P is a prime ideal of R , and set $\hat{M} = \hat{R} \otimes_R M$, etc. Then

$$\hat{M} \dot{+} \hat{N} \cong \hat{L} \dot{+} \hat{L}, \quad \hat{M} \cong \hat{L}.$$

Since the Krull–Schmidt Theorem holds for finitely generated $\hat{\Lambda}$ -modules by Exercise 6.6, the above implies (by Exercise 6.7) that $\hat{N} \cong \hat{L}$. Therefore $N_P \cong L_P$ by (18.2), and so $L' \vee L$. This completes the proof.

(27.4) THEOREM. *Let Λ be a maximal R -order in a separable K -algebra, and let M be any left Λ -ideal in A (always subject to the condition that $KM = A$).*

Then M is in the same genus as Λ . Furthermore, given any set of left Λ -ideals M_1, \dots, M_r in A , there exists a left ideal M in Λ such that

$$(27.5) \quad M_1 \dot{+} \cdots \dot{+} M_r \cong \Lambda^{(r-1)} \dot{+} M.$$

Proof. For each P , M_P is a principal Λ_P -ideal by (18.10), and hence $M \vee \Lambda$. By (27.3), we have $M_1 \dot{+} M_2 \cong \Lambda \dot{+} N$ for some left Λ -lattice N such that $N \vee \Lambda$. But by (27.1) we may embed N in Λ , so replacing N by an isomorphic copy, we may assume that N is a left ideal of Λ . Continuing in this way, we find after $r - 1$ steps that (27.5) holds for some left ideal M of Λ .

(27.6) COROLLARY. Let $A = M_r(D)$, where D is a skewfield separable over K , and let Δ be any maximal R -order in D . For each right ideal J of Δ , let $\Delta' = O_l(J)$, and let

$$\Lambda = \begin{bmatrix} \Delta & \dots & \Delta & J^{-1} \\ & \ddots & & \cdot \\ \Delta & \dots & \Delta & J^{-1} \\ J & \dots & J & \Delta' \end{bmatrix}$$

denote the ring of all $r \times r$ matrices (x_{ij}) , where x_{11} ranges over all elements of Δ , \dots, x_{1r} ranges over all elements of J^{-1} , and so on. Then Λ is a maximal R -order in A , and every maximal R -order is of this form, for some right ideal J of Δ .

Proof. By (21.6), each maximal R -order Λ is of the form $\text{Hom}_\Delta(L, L)$, where L is a right Δ -lattice such that $KL \cong D^{(r)}$. Since Δ is hereditary, L can be written as a direct sum of r right ideals of Δ . Hence by (27.4), we may take $L = \Delta^{(r-1)} \dot{+} J$, where J is a right ideal of Δ . But we may identify

$$\text{Hom}_\Delta(\Delta^{(r-1)} \dot{+} J, \Delta^{(r-1)} \dot{+} J)$$

with the indicated ring of matrices, since there are identifications

$$\text{Hom}_\Delta(\Delta, \Delta) = \Delta, \quad \text{Hom}_\Delta(\Delta, J) = J, \quad \text{Hom}_\Delta(J, \Delta) = J^{-1}, \quad \text{Hom}_\Delta(J, J) = \Delta'.$$

This completes the proof.

Let Λ be a maximal R -order in a separable K -algebra A . We shall say that the left ideals M, N of Λ are *relatively prime* if $M + N = \Lambda$.

(27.7) COROLLARY. Let N be any left ideal of Λ . Then every class of left Λ -ideals in A contains an integral ideal relatively prime to N .

Proof. Choose a nonzero $\alpha \in R \cap N$, and let M be any left ideal of Λ . Since

$M \vee \Lambda$, there is an exact sequence

$$0 \rightarrow M \xrightarrow{\varphi} \Lambda \rightarrow T \rightarrow 0$$

with

$$\alpha R + \text{ann}_R T = R,$$

by (27.1). We may write $1 = \alpha\rho + \beta$, with $\rho \in R$, $\beta \in \text{ann}_R T$. Then $\beta\Lambda \subset \varphi(M)$, and $\alpha\rho \in N$, whence $\varphi(M) + N = \Lambda$. But $\varphi(M) = Mx$ for some $x \in u(A)$, and thus $\varphi(M)$ lies in the ideal class of M . This completes the proof.

To conclude this section, we prove

(27.8) THEOREM. *Let Λ be a maximal R -order in a separable K -algebra A , and let X be a left Λ -lattice such that $KX \cong A^{(r)}$ for some positive integer r . Then there exists a left Λ -ideal M in A such that*

$$X \cong \Lambda^{(r-1)} \dot{+} M \quad \text{as } \Lambda\text{-modules.}$$

Proof. By hypothesis, there exists an A -isomorphism $\varphi: KX \cong A^{(r)}$. This isomorphism carries X onto a full R -lattice $\varphi(X)$ in $A^{(r)}$. Since $\Lambda^{(r)}$ is also a full R -lattice in $A^{(r)}$, there exists a nonzero $\alpha \in R$ such that $\alpha \cdot \varphi(X) \subset \Lambda^{(r)}$. Replacing X by the isomorphic Λ -lattice $\alpha \cdot \varphi(X)$, we may hereafter assume that

$$X \subset \Lambda^{(r)}, \quad KX = K \cdot \Lambda^{(r)} = A^{(r)}.$$

(The above reasoning has also been used in the proof of (10.6).)

By (21.4), the maximal order Λ is hereditary. It follows from (2.44) and (2.45 ii) that we may write

$$X = M_1 \dot{+} \cdots \dot{+} M_r,$$

where each M_i is a left ideal of Λ . Since $KX = \sum KM_i = A^{(r)}$, we see that $KM_i = A$ for each i , so each M_i is a left Λ -ideal in A . Hence by (27.4) there exists a left Λ -ideal M in A such that

$$M_1 \dot{+} \cdots \dot{+} M_r \cong \Lambda^{(r-1)} \dot{+} M.$$

This completes the proof of the theorem.

EXERCISES

In the following, Λ denotes an R -order in a separable K -algebra A . Let $\{P_1, \dots, P_n\}$ be the set of all prime ideals P of R such that Λ_P is not a maximal R_P -order.

1. Let M, N be left Λ -lattices such that $KM \cong KN$. Prove that $M \vee N$ if and only if

$$\hat{R}_P \otimes_R M \cong \hat{R}_P \otimes_R N$$

for each P , where \hat{R}_P denotes the P -adic completion of R . [Remark: If this isomorphism holds for even one P , then necessarily $KM \cong KN$. Indeed, the isomorphism implies that

$$\hat{R}_P \otimes_{\hat{R}_P} (\hat{R}_P \otimes_R M) \cong \hat{R}_P \otimes_{\hat{R}_P} (\hat{R}_P \otimes_R N),$$

whence

$$\hat{R}_P \otimes_K KM \cong \hat{R}_P \otimes_K KN.$$

This implies that $KM \cong KN$ by the Noether–Deuring Theorem (see Curtis–Reiner [1, §29].)

2. Let M, N be left Λ -lattices such that $KM \cong KN$. Prove that $M \vee N$ if and only if

$$M_{P_i} \cong N_{P_i}, \quad 1 \leq i \leq n.$$

3. Let $0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$ be an exact sequence of left Λ -lattices. Prove that the sequence splits if and only if for $i = 1, \dots, n$, the sequence

$$0 \rightarrow L_{P_i} \rightarrow M_{P_i} \rightarrow N_{P_i} \rightarrow 0$$

is split.

4. Let M be a left ideal of Λ such that $KM = A$. Show that $\text{ord}_R \Lambda/M \subset M$. [Hint: $\text{ord}_R \Lambda/M \subset \text{ann}_R \Lambda/M$.]

5. Let M_1, M_2 be left ideals of Λ with $KM_i = A$. Show that if

$$\text{ord}_R \Lambda/M_1 + \text{ord}_R \Lambda/M_2 = R,$$

then $M_1 + M_2 = \Lambda$. In particular, if M_1 and M_2 are left ideals in a maximal order Λ , then M_1 and M_2 are “relatively prime” whenever their norms are relatively prime. Is the converse true?

6. Let L, M, N be left Λ -lattices such that $L \vee (M \dotplus N)$. Show that $L \cong X \dotplus Y$, for some Λ -lattices X, Y such that $X \vee M, Y \vee N$. [Hint: By (27.1), there exists an $f \in \text{Hom}_\Lambda(L, M \dotplus N)$ such that

$$f_P: L_P \cong M_P \dotplus N_P, \quad P \in \{P_1, \dots, P_n\}.$$

Let $\pi: M \dotplus N \rightarrow M$ be the projection map, and set $X = \pi f(L)$, $Y = \ker \pi f$. Then

$$0 \rightarrow Y \rightarrow L \rightarrow X \rightarrow 0$$

is an exact sequence of left Λ -lattices. For $P \in \{P_1, \dots, P_n\}$, the sequence

$$0 \rightarrow Y_P \rightarrow L_P \rightarrow X_P \rightarrow 0$$

is Λ_P -split, since

$$L_P \cong M_P \dotplus N_P, \quad X_P = \pi f(L_P) = \pi(M_P \dotplus N_P) = M_P.$$

Therefore, by Exercise 3, $L \cong X \dotplus Y$, and $X \vee M, Y \vee N$.]

7. Let L, M be left Λ -lattices such that $L \vee M^{(n)}$. Then there exist Λ -lattices $M_1, \dots, M_n \vee M$ such that

$$L \cong M_1 \dotplus \cdots \dotplus M_n.$$

Further, given any $M_1, \dots, M_n \vee M$, there exists an $M' \vee M$ such that

$$M_1 \dotplus \cdots \dotplus M_n \cong M^{(n-1)} \dotplus M'.$$

[Hint: The first assertion follows from Exercise 6, the second by repeated use of (27.3).]

7. Crossed-product Algebras

In this chapter we collect a number of important results on Brauer groups, crossed-product algebras, and cyclic algebras. We have included proofs in order to make the subject matter more accessible to the reader who is encountering these topics for the first time. As will be seen below, we work directly with the simple algebras themselves, taking advantage of our earlier results from § 7 and § 14. This enables us to avoid introducing the machinery of cohomology groups.

All of the topics considered below may be found in standard references. Two excellent introductions are Artin–Nesbitt–Thrall [1] and Herstein [1]. For more sophisticated approaches, the reader may consult Albert [1], Bourbaki [1], Cassels–Fröhlich [1], Deuring [1], Jacobson [1, Ch. 5], Weil [1]. The book by Albert has a detailed bibliography of all work on these subjects up to 1938. As additional references on cohomology groups, we cite Babakhanian [1], Gruenberg [1], Neukirch [1], Rotman [1], and Weiss [2].

28. BRAUER GROUPS

Throughout this section let K , L , and E denote fields, with $K \subset L$, and let D denote a skewfield. The symbols A and B will always denote central simple K -algebras. If $A \cong M_n(D)$, we shall refer to D as the *skewfield part* of A . We shall call A and B *similar* (notation: $A \sim B$) if their skewfield parts are K -isomorphic[†]. By Wedderburn's Theorem (7.4), $A \sim B$ if and only if there is an isomorphism of K -algebras[†]

$$A \otimes_K M_r(K) \cong B \otimes_K M_s(K)$$

for some integers r, s .

Let $[A]$ denote the similarity class of A . For each A and B (always assumed to be central simple K -algebras), the tensor product $A \otimes_K B$ is also a central simple K -algebra by (7.6). Let us define multiplication of classes by the formula

$$(28.1) \quad [A][B] = [A \otimes_K B].$$

Then, by (7.7), multiplication of classes is well defined. Clearly

[†]Two K -algebras X, Y are *K -isomorphic* if there exists a ring isomorphism $\varphi: X \cong Y$ such that $\varphi(\alpha x) = \alpha\varphi(x)$, $\alpha \in K$, $x \in X$.

$$[A][B] = [B][A], \quad [A][K] = [A].$$

Finally, we remark that if A is a central simple K -algebra, then so is its opposite ring A° .

(28.2) **THEOREM.** *The classes of central simple K -algebras form an abelian group $B(K)$, called the Brauer group of K , relative to the multiplication defined in (28.1). The identity class is $[K]$, and the inverse of $[A]$ is $[A^\circ]$.*

Proof. Since the associative law holds for tensor products, it also holds for multiplication of similarity classes. Clearly $[K]$ acts as identity, and we need only prove that $[A][A^\circ] = [K]$. We choose $B = A$ in (7.14), so then $B' = K$. By (7.14), we obtain

$$A \otimes_K A^\circ \cong M_n(K), \quad n = (A : K),$$

and thus

$$[A][A^\circ] = [M_n(K)] = [K].$$

This completes the proof.

(28.3) **THEOREM.** *Let $K \subset L$. There is a homomorphism of groups*

$$B(K) \rightarrow B(L), \quad [A] \mapsto [L \otimes_K A], \quad [A] \in B(K).$$

Proof. As usual, let A and B denote central simple K -algebras. Then $L \otimes_K A$ is a central simple L -algebra by (7.8). It is easily verified that

$$A \sim B \implies L \otimes_K A \sim L \otimes_K B,$$

$$L \otimes_K (A \otimes_K B) \cong (L \otimes_K A) \otimes_L (L \otimes_K B), \quad L \otimes_K A^\circ \cong (L \otimes_K A)^\circ,$$

which imply the desired result.

Keeping the above notation, let $B(L/K)$ be the kernel of the homomorphism $B(K) \rightarrow B(L)$. Thus $[A] \in B(L/K)$ if and only if $L \otimes_K A \cong M_r(L)$ for some r . (In this case we say that L splits A , or is a splitting field for A .) There is an exact sequence of groups

$$(28.4) \quad 1 \rightarrow B(L/K) \rightarrow B(K) \rightarrow B(L)$$

whenever $K \subset L$.

The next set of theorems will show that each class $[A'] \in B(L/K)$ contains a representative A in which L is embedded as a maximal subfield. In § 29, we shall see that such algebras A can be described explicitly as crossed-products.

(28.5) **Theorem.** *Let D be a skewfield with center K , and let $m = \sqrt{(D : K)}$ be the index of D . Let E be a finite extension of K .*

- (i) If E splits D , then $m|(E:K)$.
- (ii) There exists a smallest positive integer r for which there is an embedding $E \subset M_r(D)$ as K -algebras. With this choice of r , E splits D if and only if E is a maximal subfield of $M_r(D)$. Furthermore, the centralizer E' of E in $M_r(D)$ is a skewfield, and E is a maximal subfield of $M_r(D)$ if and only if $E = E'$.

Proof. Let $S = E \otimes_K D$, a central simple E -algebra, and let V be a simple right S -module. Then V is a right vector space over the skewfield D , say $(V:D) = r$, and there is an embedding of K -algebras

$$(28.6) \quad E \subset \text{Hom}_D(V, V) \cong M_r(D),$$

since E and D commute elementwise in S . Let us show that this gives an embedding with minimal r . Indeed, given any embedding $E \subset M_t(D)$, there is a right D -space W of dimension t over D , such that $E \subset \text{Hom}_D(W, W)$. By Exercise 28.3, W may be viewed as a right $(E \otimes_K D)$ -module, and hence W is isomorphic to a direct sum of copies of V . Hence t is a multiple of r . This proves that the embedding given in (28.6) has minimal r .

Keeping this notation, let E' be the centralizer† of E in the central simple K -algebra $B = \text{Hom}_D(V, V)$. Each $f \in E'$ is then an $(E \otimes_K D)$ -endomorphism of V , that is, $f \in \text{Hom}_S(V, V)$. Conversely, it is clear that $\text{Hom}_S(V, V) \subset E'$. This shows that $E' = \text{Hom}_S(V, V)$, and the latter is a skewfield by Schur's Lemma (see Exercise 7.1). We have now proved that E' is a skewfield containing E . Let us deduce at once that $E' = E$ if and only if E is a maximal subfield of B . Obviously, if $E' = E$ then E must be a maximal subfield of B . On the other hand, if $E' > E$, choose any $x \in E' - E$. Since E' centralizes E , the element x commutes with each element of E . Therefore $E(x)$ is a field (since it is contained in the skewfield E'), and $E(x) > E$. Thus if $E' > E$, then E is not a maximal subfield of B . We also observe that by (7.13) we have

$$(28.7) \quad (E:K)(E':K) = (B:K) = m^2r^2,$$

whether or not $E' = E$.

After these preliminaries, let us turn to the proof of (i). Suppose that E splits D ; then $S = E \otimes_K D \cong M_m(E)$, so $S \cong V^{(m)}$ as right S -modules. Comparing dimensions as right D -spaces, we obtain

$$(28.8) \quad mr = m(V:D) = (S:D) = (E:K).$$

Therefore $m|(E:K)$, which proves (i). Furthermore, since $E' \supset E$, it follows from (28.7) that $E' = E$. Thus E is a maximal subfield of B , which proves part of (ii).

We now drop the assumption that E splits D , and we show finally that if E is a maximal subfield of B , then necessarily E splits D . Indeed, if E is a maximal

† See pp. 94–95.

subfield of B , then we have seen that $E' = E$. On the other hand, by (7.14) we have

$$B \otimes_K E^\circ \cong M_s(E'), \quad s = (E:K).$$

Since $E = E^\circ = E'$, this shows that E splits B . But $B \cong M_r(D)$, and so E also splits D . This completes the proof of the theorem.

(28.9) *Remarks.* If D is a skewfield with center K and index m , then we know from (7.15) that every maximal subfield of D splits D , and has K -dimension m . Part (i) of the preceding theorem asserts that we cannot find any smaller extensions of K , whether contained in D or not, which split D . Thus (7.15) is a “best possible” result.

The preceding theorem shows that if E splits D , then E can be embedded in a full matrix algebra B over D , in such a way that

$$(B:K) = (E:K)^2,$$

and that E coincides with its centralizer in B . We shall call E a *self-centralizing maximal subfield* of B .

We conclude with some easy consequences of the preceding discussion.

(28.10) **COROLLARY.** *Let A be a central simple K -algebra split by E , where $E \supset K$, and where*

$$(A:K) = (E:K)^2.$$

Then E can be embedded in A as a self-centralizing maximal subfield of A .

Proof. Let D be the skewfield part of A , so E splits D , and let $E \subset M_r(D) = B$ with r minimal, as in (28.5). By (28.9) we have

$$(B:K) = (E:K)^2 = (A:K),$$

whence $A \cong B$. The desired result is now obvious, since E is a self-centralizing maximal subfield of B .

(28.11) **COROLLARY.** *For each central simple K -algebra A' , there exists a finite galois extension L of K which splits A' . Further, $A' \sim A$ for some central simple K -algebra A containing L as a self-centralizing maximal subfield. Finally,*

$$(28.12) \quad B(K) = \bigcup B(L/K),$$

where L ranges over all finite galois extensions of K .

Proof. Given A' , by (7.15) there exists a finite separable extension E of K such that E splits A' . Let L be the normal closure of E over K , that is, the

smallest galois extension of K containing E . Then L is also a splitting field for A' , and L is a finite galois extension of K .

The above shows that $[A'] \in B(L/K)$, which implies at once that (28.12) holds true.

Finally, if D is the skewfield part of A' , then L splits D . As in (28.5), let $L \subset M_r(D)$ be an embedding with minimal r , and set $A = M_r(D)$. By (28.9), L is a self-centralizing maximal subfield of A . Clearly $A' \sim A$, and the proof is complete.

EXERCISES

- Let D be a skewfield with center K , index m . Let E be a finite extension of K which splits D . Then the least value of r for which there is an embedding of K -algebras $E \subset M_r(D)$ is given by $r = (E:K)/m$.
- Let K be a field. Show that the set of subfields of $M_r(K)$ which contain the center K of $M_r(K)$ is in one-to-one correspondence with the set of extension fields E of K for which $(E:K)$ divides r . What are the maximal subfields of $M_r(K)$ containing K ? Show that such maximal subfields are not necessarily self-centralizing.
- Let A and B be K -algebras, and let M be simultaneously a right A -module and a right B -module. We wish to make M into a right $A \otimes_K B$ -module, by defining

$$m(a \otimes b) = mab, \quad a \in A, \quad b \in B, \quad m \in M.$$

Show that this procedure is justified if and only if $A \subset \text{Hom}_B(M, M)$.

29. CROSSED-PRODUCT ALGEBRAS

Throughout this section, L denotes a finite galois extension of the field K , with galois group $\text{Gal}(L/K)$, and E denotes an arbitrary field containing K . Let D be a skewfield with center K . We set $E^* = E - \{0\}$, the multiplicative group of nonzero elements of E .

In § 14 we were concerned with the special case where K is a complete field with a finite residue class field. We showed how to construct a skewfield D with center K and given index n . Recall that we start with a field $W \supset K$ such that $\text{Gal}(W/K)$ is a cyclic group of order n , with generator σ (say). Then

$$D = \sum_{j=0}^{n-1} Wz^j, \quad z^j\alpha = \sigma^j(\alpha)z^j, \quad \alpha \in W, \quad 0 \leq j \leq n-1,$$

and $z^n \in W^*$. Here, W is a maximal subfield of D , and D has a W -basis whose elements correspond to those of $\text{Gal}(W/K)$. This correspondence is such that

$$z^j\alpha z^{-j} = \sigma^j(\alpha), \quad \alpha \in W, \quad 0 \leq j \leq n-1.$$

Further, the set of basis elements $\{z^j\}$ is closed under multiplication, apart

from constant factors from W^* . This construction is a special case of the extremely important concept of crossed-product algebras, which we proceed to define.

Returning to the case of arbitrary K , let $G = \text{Gal}(L/K)$. We shall define an algebra $A = \sum_{\sigma \in G} Lu_\sigma$, having as L -basis a set of symbols $\{u_\sigma : \sigma \in G\}$.

These symbols are to be manipulated according to the formulas

$$(29.1) \quad u_\sigma \cdot x = \sigma(x) \cdot u_\sigma, \quad u_\sigma u_\tau = f_{\sigma, \tau} u_{\sigma\tau}, \quad x \in L, \quad \sigma, \tau \in G,$$

where each $f_{\sigma, \tau} \in L^*$. Note that K is contained in the center of A , but that L is not (if $L \neq K$), since the u_σ 's need not centralize L . The K -algebra A will be associative if and only if $u_\rho(u_\sigma u_\tau) = (u_\rho u_\sigma) u_\tau$ for all $\rho, \sigma, \tau \in G$, or equivalently, if and only if

$$(29.2) \quad \rho(f_{\sigma, \tau}) \cdot f_{\rho, \sigma\tau} = f_{\rho, \sigma} \cdot f_{\rho\sigma, \tau}, \quad \rho, \sigma, \tau \in G.$$

A map $f: G \times G \rightarrow L^*$ satisfying (29.2) is a *factor set* from G to L^* . Given such an f , the algebra A constructed above is called a *crossed-product algebra*, and is denoted by $(L/K, f)$.

If f and g are factor sets, so is fg , where by definition

$$(fg)_{\sigma, \tau} = f_{\sigma, \tau} \cdot g_{\sigma, \tau}, \quad \sigma, \tau \in G.$$

Now let $A = \sum Lu_\sigma$ as above, let $\{c_\sigma : \sigma \in G\}$ be any set of elements of L^* , and put $v_\sigma = c_\sigma u_\sigma$, $\sigma \in G$. Then $A = \sum Lv_\sigma$, and

$$v_\sigma \cdot x = \sigma(x) \cdot v_\sigma, \quad v_\sigma v_\tau = g_{\sigma, \tau} v_{\sigma\tau}, \quad x \in L, \quad \sigma, \tau \in G,$$

where

$$g_{\sigma, \tau} = c_\sigma \cdot \sigma(c_\tau) \cdot c_{\sigma\tau}^{-1} \cdot f_{\sigma, \tau}, \quad \sigma, \tau \in G.$$

The map $\delta c: G \times G \rightarrow L^*$, given by

$$(29.3) \quad (\delta c)_{\sigma, \tau} = c_\sigma \cdot \sigma(c_\tau) \cdot c_{\sigma\tau}^{-1}, \quad \sigma, \tau \in G,$$

is easily found to be a factor set, hereafter called a *principal factor set*. We have thus shown that $g = (\delta c) \cdot f$, and that

$$(29.4) \quad (L/K, f) \cong (L/K, (\delta c) \cdot f)$$

for each $c: G \rightarrow L^*$.

A few definitions are in order. The *trivial* factor set has all values equal to 1. The collection of all factor sets from G to L^* is a multiplicative group $Z^2(G, L^*)$, and the collection of all principal factor sets is a subgroup $B^2(G, L^*)$. We set

$$H^2(G, L^*) = Z^2(G, L^*)/B^2(G, L^*),$$

the *second cohomology group*[†] of G with coefficients in L^* . Call $f, g \in Z^2(G, L^*)$

[†] See Exercise 29.11.

equivalent if f, g have the same image $[f]$ in $H^2(G, L^*)$, that is, if $g = (\delta c)f$ for some c .

It is easily shown that every factor set g is equivalent to a *normalized* factor set f satisfying

$$(29.5) \quad f_{\sigma, 1} = f_{1, \sigma} = 1, \quad \sigma \in G.$$

(See Exercise 29.1.) By (29.4), equivalent factor sets yield isomorphic crossed-product algebras. In particular, if $(L/K, f) = \sum Lu_\sigma$ is a crossed-product algebra in which f is normalized, then u_1 is the unity element of the ring $(L/K, f)$, and each u_σ is a unit in this ring. We shall always identify L with the subring Lu_1 of $(L/K, f)$. Even when f is not necessarily normalized, the preceding remarks show that each u_σ must be a unit in $(L/K, f)$.

(29.6) **THEOREM.** *For each factor set $f: G \times G \rightarrow L^*$, the crossed-product algebra $A = (L/K, f)$ is a central simple K -algebra. The field L is its own centralizer in A , and is a maximal subfield of A . If g is another factor set, then there exists a K -isomorphism*

$$(L/K, f) \cong (L/K, g)$$

if and only if f is equivalent to g .

Proof. Without loss of generality, we may assume that both f and g are normalized. Identify L with $Lu_1 \subset A$. We leave it as an exercise to check that K is the center of A , and that every element of A which commutes with each $x \in L$ must lie in L . Thus L is its own centralizer in A , and is therefore a maximal subfield of A .

To prove that A is simple, let X be a nonzero two-sided ideal of A , and let

$$x = a_{\sigma_1} u_{\sigma_1} + \cdots + a_{\sigma_r} u_{\sigma_r} \in X, \quad x \neq 0,$$

with r minimal. If $r > 1$, choose $b \in L$ with $\sigma_1(b) \neq \sigma_2(b)$. Then $x - \sigma_1(b)^{-1} xb$ is a shorter nonzero element of X . This is impossible, so necessarily $r = 1$, and X contains a unit $a_{\sigma_1} u_{\sigma_1}$ of A . Therefore $X = A$, which shows that A is a central simple K -algebra, as claimed.

Now let $B = \sum Lv_\sigma$, where the $\{v_\sigma\}$ multiply according to the factor set g . Any K -algebra isomorphism $\phi: A \cong B$ must preserve identity elements, so $\phi(u_1) = v_1$. Therefore $\phi(Lu_1) = L'v_1$, where L' is a field K -isomorphic to L . Let $u'_\sigma = \phi(u_\sigma)$, $\sigma \in G$; then $\phi(Lu_\sigma) = L'v_1 \cdot u'_\sigma = L'u'_\sigma$. Therefore

$$(29.7) \quad B = \sum_{\sigma \in G} L'u'_\sigma, \quad u'_\sigma \cdot \phi(x) = \phi(\sigma x) \cdot u'_\sigma, \quad u'_\sigma u'_\tau = \phi(f_{\sigma, \tau}) u'_{\sigma\tau},$$

for $x \in L$, $\sigma, \tau \in G$. On the other hand, $L'v_1$ and Lv_1 are K -isomorphic simple subalgebras of B , so by the Skolem-Noether Theorem (7.21), there is an

inner automorphism θ of B such that $\theta(\phi(x)) = x$, $x \in L$. Applying θ to equations (29.7) and setting $w_\sigma = \theta(u'_\sigma)$, $\sigma \in G$, we obtain

$$B = \sum L w_\sigma; \quad w_\sigma \cdot x = \sigma(x) \cdot w_\sigma, \quad w_\sigma \cdot w_\tau = f_{\sigma, \tau} w_{\sigma\tau}.$$

But for each $\sigma \in G$, $w_\sigma v_\sigma^{-1}$ commutes with each $x \in L$. Since L is its own centralizer in B , this gives $w_\sigma = c_\sigma v_\sigma$ for some $c_\sigma \in L$. The $\{w_\sigma\}$ are an L -basis for B , so each $c_\sigma \neq 0$. Clearly we have $f = (\delta c)g$, so f is equivalent to g . This establishes the theorem, since we have previously remarked that $A \cong B$ whenever f is equivalent to g .

(29.8) COROLLARY. Let $n = (L:K)$. Then $(L/K, f) \cong M_n(K)$ if and only if f is equivalent to the trivial factor set.

Proof. We need only show that $(L/K, 1) \cong M_n(K)$, where 1 denotes the trivial factor set. Now

$$(L/K, 1) = \sum_{\sigma \in G} Lu_\sigma, \quad u_\sigma \cdot x = \sigma(x)u_\sigma, \quad u_\sigma u_\tau = u_{\sigma\tau},$$

for $x \in L$, $\sigma, \tau \in G$. For $x \in L$, let x' denote left multiplication by x acting on L . Then there is an algebra homomorphism

$$\psi: (L/K, 1) \rightarrow \text{Hom}_K(L, L), \quad \text{where } xu_\sigma \mapsto x' \circ \sigma.$$

The kernel is a two-sided ideal of the simple algebra $(L/K, 1)$, hence is zero. Then ψ is monic, and must be an isomorphism since both $(L/K, 1)$ and $\text{Hom}_K(L, L)$ have K -dimension n^2 .

Example. Let $K = \mathbf{Q}$, $L = \mathbf{Q}(i)$, $i^2 = -1$. Then $G = \text{Gal}(L/K)$ is cyclic of order 2, with generator σ , where $\sigma(a + bi) = a - bi$, $a, b \in \mathbf{Q}$. Let $f: G \times G \rightarrow L^*$ be the factor set given by

$$f_{1,1} = f_{\sigma,1} = f_{1,\sigma} = 1, \quad f_{\sigma,\sigma} = -1.$$

Then $A = (L/K, f) = Lu_1 \oplus Lu_\sigma$, where u_1 is the unity element of A , and where

$$u_\sigma \cdot x = \sigma(x)u_\sigma, \quad u_\sigma^2 = -1, \quad x \in L.$$

Thus A is isomorphic to the quaternion algebra $\mathbf{Q} \oplus \mathbf{Qi} \oplus \mathbf{Qj} \oplus \mathbf{Qk}$ over \mathbf{Q} , by identifying $\mathbf{Q} \oplus \mathbf{Qi}$ with L , and j with u_σ .

On the other hand, if we had chosen f normalized, with $f_{\sigma,\sigma} = +1$, then $(L/K, f) \cong M_2(K)$ by (29.8). This completes the example.

(29.9) THEOREM. Let $G = \text{Gal}(L/K)$, and let f, g be factor sets from G to L^* . Then there is a similarity of K -algebras

$$(L/K, f) \otimes_K (L/K, g) \sim (L/K, fg).$$

Proof. Let $C = A \otimes_K B$, where

$$A = (L/K, f) = \sum L u_\sigma, \quad B = (L/K, g) = \sum L v_\sigma.$$

Then C is a central simple K -algebra, by (7.6). We shall find an idempotent $e \in L \otimes_K L \subset C$ such that $eCe \cong (L/K, fg)$. This will yield the desired result, since $C \sim eCe$ by Exercise 29.3.

To begin with, we observe that the subfields $L \otimes 1$ and $1 \otimes L$ of $L \otimes_K L$ commute elementwise. Since L is separable over K , there exists an $a \in L$ such that $L = K(a)$; then $f(x) = \min. \text{pol.}_K a$ has degree n , where $n = (L:K)$. Now define

$$e = \prod (a \otimes 1 - 1 \otimes \sigma a) / \prod (a - \sigma a) \otimes 1,$$

where these products are taken over all $\sigma \in G - \{1\}$. Note that the denominator is not zero, since $a \neq \sigma a$ for each $\sigma \in G - \{1\}$. The numerator is also different from zero in $L \otimes_K L$, since the elements $\{a^r \otimes 1 : 0 \leq r \leq n-1\}$ are linearly independent over $1 \otimes L$. Thus $e \neq 0$ in $L \otimes_K L$.

Next we note that $f(X) = (X - a) \cdot \prod (X - \sigma a)$, where σ ranges over $G - \{1\}$. Therefore

$$(a \otimes 1 - 1 \otimes a) \cdot \prod (a \otimes 1 - 1 \otimes \sigma a) = f(a \otimes 1) = 0.$$

This shows that $(1 \otimes a)e = (a \otimes 1)e$ in $L \otimes L$. Therefore by induction on r , it follows that

$$(a^r \otimes 1)e = (1 \otimes a^r)e, \quad r \geq 0.$$

Since $L = \sum_{r=0}^{n-1} K a^r$, and multiplication in $L \otimes L$ is commutative, we obtain

$$(29.10) \quad (x \otimes 1)e = e(x \otimes 1) = e(1 \otimes x) = (1 \otimes x)e, \quad x \in L.$$

Consequently

$$\begin{aligned} e^2 &= e \cdot \prod (a \otimes 1 - 1 \otimes \sigma a) / \prod (a - \sigma a) \otimes 1 \\ &= e \cdot \prod (a - \sigma a) \otimes 1 / \prod (a - \sigma a) \otimes 1 \\ &= e. \end{aligned}$$

Thus e is an idempotent in $L \otimes_K L$.

It remains for us to prove that $eCe \cong (L/K, fg)$. We have

$$\begin{aligned} eCe &= \sum_{\sigma, \tau \in G} e(L \otimes L) \cdot (u_\sigma \otimes v_\tau) e \\ &= \sum_{\sigma, \tau} e(L \otimes 1) e \cdot e(1 \otimes L) e \cdot e(u_\sigma \otimes v_\tau) e. \end{aligned}$$

But $e(1 \otimes L)e = e(L \otimes 1)e$ by (29.10), and $e(L \otimes 1)e = L'$ is a field

K -isomorphic to L . Let us compute $e(u_\sigma \otimes v_\tau)e$, by using the formulas

$$u_\sigma \cdot x = \sigma(x) u_\sigma, \quad v_\tau \cdot x = \tau(x) \cdot v_\tau, \quad x \in L, \quad \sigma, \tau \in G.$$

Then

$$e(u_\sigma \otimes v_\tau)e = (u_\sigma \otimes v_\tau) \cdot \{\prod (\sigma a \otimes 1 - 1 \otimes \tau \rho a) / \prod (\sigma a - \sigma \rho a) \otimes 1\} \cdot e,$$

where ρ ranges over all elements of $G - \{1\}$. From (29.10), we obtain

$$(29.11) \quad e(u_\sigma \otimes v_\tau)e = (u_\sigma \otimes v_\tau) \cdot e \cdot \prod (\sigma a - \tau \rho a) \otimes 1 / \prod (\sigma a - \sigma \rho a) \otimes 1.$$

If $\sigma \neq \tau$, then $\sigma a - \tau \rho a = 0$ for $\rho = \tau^{-1}\sigma \in G - \{1\}$, and hence $e(u_\sigma \otimes v_\tau)e = 0$. On the other hand, when $\sigma = \tau$ we obtain $e(u_\sigma \otimes v_\sigma)e = (u_\sigma \otimes v_\sigma)e$. An analogous argument proves that $e(u_\sigma \otimes v_\sigma)e = e(u_\sigma \otimes v_\sigma)$.

We have now shown that

$$eCe = \sum_{\sigma \in G} L' w_\sigma,$$

where

$$L' = e(L \otimes 1)e, \quad w_\sigma = e(u_\sigma \otimes v_\sigma)e, \quad \sigma \in G,$$

and have also shown that

$$w_\sigma = (u_\sigma \otimes v_\sigma)e = e(u_\sigma \otimes v_\sigma), \quad \sigma \in G.$$

Clearly $\text{Gal}(L'/K) \cong G$, and we have for $x \in L$,

$$w_\sigma \cdot e(x \otimes 1)e = e(u_\sigma \otimes v_\sigma)(x \otimes 1)e = e(\sigma x \otimes 1)e \cdot w_\sigma.$$

Thus, conjugation by w_σ acts as σ on L' . Further, for $\sigma, \tau \in G$,

$$\begin{aligned} w_\sigma \cdot w_\tau &= e(u_\sigma u_\tau \otimes v_\sigma v_\tau)e = e(f_{\sigma, \tau} u_{\sigma\tau} \otimes g_{\sigma, \tau} v_{\sigma\tau})e \\ &= e(f_{\sigma, \tau} g_{\sigma, \tau} \otimes 1)e \cdot w_{\sigma\tau}. \end{aligned}$$

Thus the w 's multiply according to the factor set fg . This proves that $eCe \cong (L'/K, fg)$, and establishes the theorem.

We are now in a position to relate crossed-product algebras with the Brauer group. We have denoted by $B(L/K)$ the subgroup of the Brauer group $B(K)$ consisting of all classes of central simple K -algebras split by L .

(29.12) **Theorem.** *Let L be a finite galois extension of K , with galois group G . Then*

$$H^2(G, L^*) \cong B(L/K),$$

and the isomorphism is given by mapping $[f] \in H^2(G, L^)$ onto the class $[(L/K, f)] \in B(L/K)$.*

Proof. The indicated map is a well-defined monomorphism of groups, by (29.6) and (29.9). To show that the map is epic, let A' be any central simple K -algebra which is split by L . Then by (28.9) there exists a central simple K -algebra $A \sim A'$, such that L is a self-centralizing maximal subfield of A , and

$$(A:K) = n^2, \quad \text{where } n = (L:K).$$

Of course $[A'] = [A]$ in $B(L/K)$.

For each $\sigma \in G$, the map $\sigma:L \rightarrow L$ is a K -isomorphism of simple subalgebras of A . Hence by the Skolem–Noether Theorem (7.21), there exists $u_\sigma \in u(A)$ such that

$$u_\sigma x u_\sigma^{-1} = \sigma(x), \quad x \in L, \quad \sigma \in G.$$

In order to prove that $A = \sum_{\sigma \in G} Lu_\sigma$, it suffices to show that the right hand expression is a direct sum, for then both sides will have K -dimension n^2 . If the sum is *not* direct, let

$$s = a_{\sigma_1} u_{\sigma_1} + \cdots + a_{\sigma_k} u_{\sigma_k} = 0, \quad a_{\sigma_i} \in L^*,$$

be a relation with minimal k . Surely $k > 1$, since each $u_\sigma \in u(A)$. Choosing $b \in L^*$ such that $\sigma_1(b) \neq \sigma_2(b)$, one easily checks that

$$\sigma_1(b)s - sb = 0$$

gives a shorter nontrivial relation connecting $u_{\sigma_2}, \dots, u_{\sigma_k}$. This is a contradiction, and establishes the formula $A = \sum Lu_\sigma$.

We already know that

$$u_\sigma \cdot x = \sigma(x) \cdot u_\sigma, \quad x \in L, \quad \sigma \in G.$$

Suppose now that $\sigma, \tau \in G$. Then the preceding equation shows that $u_\sigma u_\tau u_{\sigma\tau}^{-1}$ commutes with each $x \in L$. Since L is its own centralizer in A , we obtain

$$u_\sigma u_\tau = f_{\sigma, \tau} u_{\sigma\tau}, \quad f_{\sigma, \tau} \in L^*.$$

The associativity of multiplication in A implies that $f:G \times G \rightarrow L^*$ is a factor set, and thus we have shown that $A \cong (L/K, f)$ for some f . This completes the proof of the theorem.

The preceding theorem shows that every class in the Brauer group $B(K)$ is represented by a crossed-product algebra over K . Hence every skewfield D with center K , such that $(D:K)$ is finite, is similar to some crossed-product algebra $(L/K, f)$. However, as shown by Amitsur [1], there exist skewfields

D which are not isomorphic to crossed-product algebras. (See also Schacher-Small [1]).

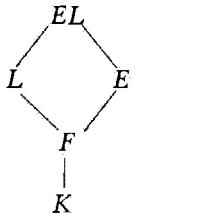
Let us next establish some results on change of fields in crossed-product algebras.

(29.13) THEOREM. *Let L/K be a finite galois extension, and E/K an arbitrary extension. Then*

$$E \otimes_K (L/K, f) \sim (EL/E, f'),$$

where f' is obtained from f by restriction, as described below.

Proof. Let EL be the composite of the fields E and L , in some extension field of K containing both E and L . Let $F = E \cap L$. By galois theory, we know that EL/E is a finite galois extension, and we have a diagram



$$H = \text{Gal}(EL/E) \cong \text{Gal}(L/F) \subset \text{Gal}(L/K) = G.$$

Thus each factor set $f: G \times G \rightarrow L^*$ restricts to a factor set $f': H \times H \rightarrow L^*$, and so we may construct crossed-product algebras $(L/F, f')$ and $(EL/E, f')$. We shall prove

$$(29.14) \quad F \otimes_K (L/K, f) \sim (L/F, f'),$$

$$(29.15) \quad E \otimes_F (L/F, f') \cong (EL/E, f').$$

Together these yield the assertion in the theorem, since

$$E \otimes_K (L/K, f) \cong E \otimes_F (F \otimes_K (L/K, f)).$$

Let F' be the centralizer of F in the central simple K -algebra $A = (L/K, f)$. By (7.14) we have

$$F \otimes_K A \sim F',$$

so (29.14) will be established as soon as we show that

$$F' \cong (L/F, f').$$

Let $\sum_{\sigma \in G} a_\sigma u_\sigma \in F'$, where each $a_\sigma \in L$. Then for all $x \in F$,

$$x \cdot \sum a_\sigma u_\sigma = (\sum a_\sigma u_\sigma) \cdot x = \sum a_\sigma \sigma(x) u_\sigma.$$

Hence whenever $a_\sigma \neq 0$, we must have $\sigma(x) = x$ for all $x \in F$, that is,

$\sigma \in H = \text{Gal}(L/F)$. This shows that

$$F' = \sum_{\sigma \in H} Lu_\sigma = (L/F, f'),$$

so (29.14) is proved.

Now let $B = (L/F, f')$. The F -algebra homomorphism

$$E \otimes_F L \rightarrow EL, \quad x \otimes y \mapsto xy,$$

is an isomorphism (since the map is epic, and both sides have E -dimension $(L:F)$). Therefore

$$E \otimes_F B = \sum_{\sigma \in H} (E \otimes_F L)(1 \otimes u_\sigma) \cong \sum_{\sigma \in \text{Gal}(EL/E)} EL \cdot v_\sigma,$$

where the $\{v_\sigma\}$ multiply according to the factor set f' . This proves (29.15), and establishes the theorem.

(29.16) THEOREM. Let $K \subset L \subset E$, where L/K and E/K are finite galois extensions. Then

$$(L/K, f) \sim (E/K, g),$$

as K -algebras, where g is the inflation of f , as described below.

Proof. By galois theory, there is a diagram

$$\begin{array}{ccc} & E & \\ G & \left| \begin{array}{c} H \\ \vdash \\ L \\ \bar{G} \\ \vdash \\ K \end{array} \right| r & G = \text{Gal}(E/K), \quad H = \text{Gal}(E/L), \quad H \Delta G, \\ & \bar{G} & \bar{G} = G/H \cong \text{Gal}(L/K), \\ & \left| \begin{array}{c} s \\ \vdash \\ r = (E:L), \quad s = (L:K). \end{array} \right| & \end{array}$$

Given a factor set $f: \bar{G} \times \bar{G} \rightarrow L^*$, we define a factor set $g: G \times G \rightarrow L^* \subset E^*$ by the formula

$$g_{\sigma, \tau} = f_{\bar{\sigma}, \bar{\tau}}, \quad \sigma, \tau \in G,$$

where $\bar{\sigma}$ denotes the image of σ in \bar{G} . Call g the *inflation* of f .

Let us set

$$B = (L/K, f) \otimes_K M_r(K),$$

a central simple K -algebra split by L (and hence also split by the field E which contains L). Then

$$(L/K, f) \sim B, \quad (B:K) = (rs)^2, \quad (E:K) = rs.$$

By (28.10), we know that E can be embedded in B as a self-centralizing maximal subfield of B . We shall give a specific such embedding, and shall use it to prove that $B \cong (E/K, g)$, where g is the inflation of f . This will complete the proof of the theorem.

It follows from (29.8) that there is an L -isomorphism

$$(E/L, 1) \cong M_r(L).$$

We shall need to know an explicit form of this isomorphism. Let $E = \sum_{i=1}^r Le_i$, and for each $x \in L$, let $T(x) \in M_r(L)$ describe the action of x by left multiplication on the $\{e_i\}$. Thus

$$x(e_1, \dots, e_r) = (e_1, \dots, e_r) T(x), \quad x \in L.$$

On the other hand, each $\rho \in G$ may be viewed as an element of $\text{Hom}_L(E, E)$, and hence determines a matrix $P_\rho \in M_r(L)$ such that

$$(\rho e_1, \dots, \rho e_r) = (e_1, \dots, e_r) P_\rho, \quad \rho \in G.$$

Let us put $\mathbf{e} = (e_1, \dots, e_r)$. Then the preceding formulas may be written briefly as

$$(29.17) \quad x\mathbf{e} = \mathbf{e}T(x), \quad \rho\mathbf{e} = \mathbf{e}P_\rho, \quad x \in E, \quad \rho \in G.$$

The isomorphism $(E/L, 1) \cong M_r(L)$, given by (29.8), is obtained by the mapping $x \rightarrow T(x)$, $\rho \rightarrow P_\rho$, $x \in E$, $\rho \in H$. Let

$$T(E) = \{T(x) : x \in E\},$$

a field L -isomorphic to E . Then we have

$$(29.18) \quad M_r(L) = \sum_{\rho \in H} T(E)P_\rho.$$

For each matrix X with entries in L , and each $\sigma \in G$, let $\sigma(X)$ be the matrix obtained from X by applying σ to each of its entries. Then

$$(\rho\sigma)\mathbf{e} = \rho(\mathbf{e}P_\sigma) = \mathbf{e}P_\rho \cdot \rho(P_\sigma), \quad \rho, \sigma \in G,$$

whence

$$(29.19) \quad P_{\rho\sigma} = P_\rho \cdot \rho(P_\sigma), \quad \rho, \sigma \in G.$$

On the other hand, for $x \in E$ and $\sigma \in G$ we obtain

$$\begin{aligned} \sigma(x)\sigma(\mathbf{e}) &= \sigma(x\mathbf{e}) = \sigma(\mathbf{e}T(x)) \\ &= \sigma\mathbf{e} \cdot \sigma(T(x)) = \mathbf{e}P_\sigma \cdot \sigma(T(x)). \end{aligned}$$

But also

$$\sigma(x)\sigma(\mathbf{e}) = \sigma(x) \cdot \mathbf{e}P_\sigma = \mathbf{e}T(\sigma(x))P_\sigma.$$

Therefore

$$(29.20) \quad T(\sigma(x)) \cdot P_\sigma = P_\sigma \cdot \sigma(T(x)), \quad x \in E, \quad \sigma \in G.$$

We are now ready to return to the K -algebra B defined above. We may write

$$B = (L/K, f) \otimes_K M_r(K) = \sum_{\tilde{\sigma} \in \tilde{G}} Lu_{\tilde{\sigma}} \otimes M_r(K) \cong \sum_{\tilde{\sigma} \in \tilde{G}} M_r(L)u_{\tilde{\sigma}}.$$

In the above, the symbols $\{u_{\tilde{\sigma}}\}$ multiply according to the normalized factor set f , and in the last summation we have written $u_{\tilde{\sigma}}$ in place of $u_{\tilde{\sigma}} \otimes 1$. From the definition of the crossed-product algebra $(L/K, f)$, we have

$$u_{\tilde{\sigma}} \cdot y = \bar{\sigma}(y) \cdot u_{\tilde{\sigma}}, \quad y \in L, \quad \bar{\sigma} \in \bar{G}.$$

Therefore

$$u_{\tilde{\sigma}} \cdot X = \bar{\sigma}(X) \cdot u_{\tilde{\sigma}}, \quad X \in M_r(L), \quad \bar{\sigma} \in \bar{G}.$$

Let us identify B with $\sum' M_r(L) u_{\tilde{\sigma}}$, and let us use formula (29.18) for $M_r(L)$. Then we may write

$$B = \sum'_{\rho \in H, \tilde{\sigma} \in \bar{G}} T(E) P_\rho u_{\tilde{\sigma}}.$$

We have now exhibited an embedding of E in B , since $E \cong T(E)$. Of course P_1 is the identity matrix in $M_r(L)$, and $u_{\tilde{1}}$ is the unity element of B . We are trying to prove that $B \cong (E/K, g)$.

Let us write $G = H\sigma_1 \cup \dots \cup H\sigma_s$. Each $\sigma \in G$ is uniquely expressible as $\sigma = \rho\sigma_i$, for some $\rho \in H$ and some i between 1 and s . Then $\bar{\sigma} = \bar{\sigma}_i$, and of course $\bar{G} = \{\bar{\sigma}_1, \dots, \bar{\sigma}_s\}$. Now define

$$v_\sigma = P_\sigma u_{\tilde{\sigma}} \in B, \quad \sigma \in G.$$

We shall show that

$$(29.21) \quad B = \sum'_{\sigma \in G} T(E) v_\sigma.$$

Let $\sigma = \rho\sigma_i$, $\rho \in H$, $1 \leq i \leq s$. By (29.19), $P_\sigma = P_\rho \cdot \rho(P_{\sigma_i})$. Since P_{σ_i} has entries in L , and since $\rho \in H$, it follows that $P_\sigma = P_\rho \cdot P_{\sigma_i}$. Furthermore, P_{σ_i} is a unit in the ring $\sum'_{\rho \in H} T(E) P_\rho$. Therefore

$$\begin{aligned} B &= \sum_{i=1}^s \left\{ \sum'_{\rho \in H} T(E) P_\rho \right\} u_{\tilde{\sigma}_i} = \sum_i \left\{ \sum'_{\rho} T(E) P_\rho \right\} P_{\sigma_i} u_{\tilde{\sigma}_i} \\ &= \sum_{i,\rho} T(E) P_{\rho\sigma_i} u_{\tilde{\sigma}_i} = \sum_{\sigma \in G} T(E) v_\sigma, \end{aligned}$$

which establishes formula (29.21).

We are going to prove that $B \cong (T(E)/K, g)$, and so shall first compute $\tilde{G} = \text{Gal}(T(E)/K)$. Since $E \cong T(E)$, it follows that $\tilde{G} = \{\tilde{\sigma} : \sigma \in G\}$, where

$$\tilde{\sigma}(T(x)) = T(\sigma x), \quad x \in E, \quad \sigma \in G.$$

Using this formula, we may now compute the action of v_σ on $T(x)$, for $\sigma \in G$ and $x \in E$. We have

$$v_\sigma \cdot T(x) = P_\sigma u_{\tilde{\sigma}} \cdot T(x) = P_\sigma \cdot \bar{\sigma}(T(x)) \cdot u_{\tilde{\sigma}}.$$

But $\bar{\sigma}(Y) = \sigma(Y)$ for any $Y \in M_r(L)$ and any $\sigma \in G$, since σ acts as $\bar{\sigma}$ on elements

of L . Hence by (29.20) we obtain

$$\begin{aligned} v_\sigma \cdot T(x) &= P_\rho \cdot \sigma(T(x)) \cdot u_{\bar{\sigma}} = T(\sigma(x)) \cdot P_\sigma \cdot u_{\bar{\sigma}} \\ &= T(\sigma(x)) \cdot v_\sigma = \tilde{\sigma}(T(x)) \cdot v_\sigma, \quad x \in E, \quad \sigma \in G. \end{aligned}$$

This proves that v_σ transforms $T(E)$ according to the action of $\tilde{\sigma}$ on $T(E)$.

Finally, we obtain

$$\begin{aligned} v_\sigma v_\tau &= P_\sigma u_{\bar{\sigma}} \cdot P_\tau u_{\bar{\tau}} = P_\sigma \cdot \tilde{\sigma}(P_\tau) \cdot u_{\bar{\sigma}} \cdot u_{\bar{\tau}} \\ &= P_\sigma \cdot \sigma(P_\tau) \cdot f_{\bar{\sigma}, \bar{\tau}} u_{\bar{\sigma}\bar{\tau}} = P_{\sigma\tau} f_{\bar{\sigma}, \bar{\tau}} u_{\bar{\sigma}\bar{\tau}} \\ &= g_{\sigma, \tau} v_{\sigma\tau}, \quad \sigma, \tau \in G. \end{aligned}$$

This establishes that $B \cong (T(E)/K, g)$ as claimed, and completes the proof of the theorem.

Remarks. (i) Let L/K be a finite Galois extension, F an intermediate field, and set

$$G = \text{Gal}(L/K), \quad H = \text{Gal}(L/F).$$

Since H is a subgroup of G , each factor set from G to L^* restricts to a factor set from H to L^* , thereby inducing a homomorphism

$$\text{res}: H^2(G, L^*) \rightarrow H^2(H, L^*).$$

On the other hand, by (28.3) there is a homomorphism

$$F \otimes_K \cdot : B(L/K) \rightarrow B(L/F).$$

Formula (29.14) is equivalent to the assertion that the following diagram commutes:

$$\begin{array}{ccc} H^2(G, L^*) & \xrightarrow{\text{res}} & H^2(H, L^*) \\ \downarrow & & \downarrow \\ B(L/K) & \xrightarrow[F \otimes_K \cdot]{} & B(L/F), \end{array}$$

where the vertical arrows denote the isomorphisms given by (29.12).

(ii) Keeping the above notation, assume further that $H \triangleleft G$, and set $\bar{G} = G/H = \text{Gal}(F/K)$. As in the proof of (29.16), each factor set from \bar{G} to F^* inflates to a factor set from G to L^* , thereby inducing a homomorphism

$$\text{inf}: H^2(\bar{G}, F^*) \rightarrow H^2(G, L^*).$$

On the other hand, each central simple K -algebra split by F is also split by L , so there is a monomorphism $B(F/K) \rightarrow B(L/K)$. Theorem 29.16 is equivalent to the assertion that the following diagram commutes:

$$\begin{array}{ccc} H^2(\bar{G}, F^*) & \xrightarrow{\text{inf}} & H^2(G, L^*) \\ \downarrow & & \downarrow \\ B(F/K) & \longrightarrow & B(L/K), \end{array}$$

where the vertical arrows are the isomorphisms of (29.12).

We conclude this section with a discussion of the relation between the exponent and the index of an element of the Brauer group $B(K)$. For $[A] \in B(K)$, let $\exp [A]$ denote the *exponent* of $[A]$ in $B(K)$, that is, the least positive integer t such that $[A]^t = 1$ in $B(K)$. On the other hand, define the *index* of $[A]$ to be the index of the skewfield part of A . This means that for $[A] \in B(K)$,

$$\text{index } [A] = \text{index } [D] = \sqrt{(D:K)},$$

where D is a skewfield such that $A \sim D$.

(29.22) **Theorem.** *For each $[A] \in B(K)$, we have*

$$[A]^m = 1 \text{ in } B(K), \quad \text{where } m = \text{index } [A].$$

Therefore $\exp [A]$ divides index $[A]$.

Proof. Let $A \sim D$, where D is a skewfield of index m , so $[A] = [D]$ in $B(K)$. By (28.11) there exists a finite galois extension L of K such that L splits A . Then L also splits D . As in the proof of (28.5), using L in place of the field E occurring in that proof, we let V be a simple right $(L \otimes_K D)$ -module, and set $r = (V:D)$. Then there is an embedding

$$L \subset \text{Hom}_D(V, V) = B, \quad B \cong M_r(D),$$

and $(L:K) = mr$ by (28.8). On the other hand, we may view V as left B -module, and then $B \cong V^{(r)}$ as left B -modules. Therefore

$$r(V:L) = (B:L) = (B:K)/(L:K) = mr,$$

and so $(V:L) = m$.

Since L is a self-centralizing maximal subfield of the central simple K -algebra B , it follows as in (29.12) that there exists a factor set $f: G \times G \rightarrow L^*$ such that $B \cong (L/K, f)$. Hence by (29.9) we obtain

$$[A]^m = [B]^m = [(L/K, f^m)] \quad \text{in } B(K).$$

It therefore suffices to prove that f^m is a principal factor set. This will be done by using a technique of Schur, who first proved this theorem. Each $\sigma \in G = \text{Gal}(L/K)$ determines an element $u_\sigma \in (L/K, f)$. We shall identify B with $(L/K, f)$, and then the element u_σ of B acts on the left B -module V . If

$P^{(\sigma)}$ describes the action of u_σ on some specific L -basis of V , then we have obtained a mapping

$$\sigma \in G \rightarrow P^{(\sigma)} \in M_m(L).$$

We shall show that this mapping satisfies the identity

$$(29.23) \quad f_{\sigma, \tau} P^{(\sigma\tau)} = P^{(\sigma)} \cdot \sigma\{P^{(\tau)}\}, \quad \sigma, \tau \in G,$$

where $\sigma\{P^{(\tau)}\}$ is obtained from $P^{(\tau)}$ by applying σ to each of its entries.

To establish the above formula, let us recall that $(V:L) = m$, so we may write $V = \sum_{i=1}^m Lv_i$. For $\sigma \in G$, let us set

$$u_\sigma \cdot v_j = \sum_i p_{ij}^{(\sigma)} v_i, \quad P^{(\sigma)} = (p_{ij}^{(\sigma)}) \in M_m(L).$$

Then

$$(u_\sigma u_\tau) v_j = u_\sigma \left\{ \sum_k p_{kj}^{(\tau)} v_k \right\} = \sum_{i,k} \sigma(p_{kj}^{(\tau)}) \cdot p_{ik}^{(\sigma)} v_i.$$

On the other hand,

$$(u_\sigma u_\tau) v_j = (f_{\sigma, \tau} u_{\sigma\tau}) v_j = f_{\sigma, \tau} \cdot \sum_i p_{ij}^{(\sigma\tau)} v_i.$$

Comparing this formula with the preceding one, we deduce (29.23) at once.

Now take determinants in (29.23), and let $c_\sigma = \det P^{(\sigma)} \in L^*$. Then we obtain

$$(f_{\sigma, \tau})^m \cdot c_{\sigma\tau} = c_\sigma \cdot \sigma(c_\tau), \quad \sigma, \tau \in G.$$

Therefore $f^m = \delta c$, a principal factor set, and so $[A]^m = [B]^m = [(L/K, f^m)] = 1$ in $B(K)$. This completes the proof.

As we shall see in Chapter 8 (see (32.19)),

$$\exp[A] = \text{index}[A], \quad [A] \in B(K),$$

when K is any algebraic number field. For the moment, we content ourselves with a somewhat weaker result, which holds for general K .

(29.24) THEOREM. *For each $[A] \in B(K)$, the integers $\exp[A]$ and $\text{index}[A]$ have the same prime factors, apart from multiplicities.*

Proof. We may assume that A is a skewfield D with center K and index m . Since $\exp[D]$ divides m by (29.22), it suffices for us to prove that each rational prime p dividing m also divides $\exp[D]$. We shall suppose that $p \mid m, p \nmid \exp[D]$, and shall obtain a contradiction.

There exists a finite galois extension L/K such that L splits D , by (28.11). Let $G = \text{Gal}(L/K)$, and let H be a Sylow p -subgroup of G . Then

$$|H| = p^r, r \geq 0, \quad [G:H] = q, \quad p \nmid q.$$

Let E be the subfield of L fixed by H ; then $(E:K) = [G:H] = q$. Since $m \nmid q$, it follows from (28.5i) that E does not split D . Then $S = E \otimes_K D$ is a central simple E -algebra, such that $[S] \neq 1$ in $B(E)$. Consider the diagram

$$\begin{array}{ccccc} & H & & L & \\ G & \downarrow & E & \xrightarrow{p^r} & S \\ & \downarrow & \downarrow & \nearrow m^2 & \\ & K & & \xrightarrow{q} & D \\ & \downarrow & \downarrow & \nearrow m^2 & \end{array}$$

The homomorphism $B(K) \rightarrow B(E)$ defined by $E \otimes_K \cdot$, carries $[D]$ onto $[S]$. Therefore $\exp[S]$ divides $\exp[D]$. Since $p \nmid \exp[D]$, we conclude that $p \nmid \exp[S]$. On the other hand, we have

$$L \otimes_E S = L \otimes_E (E \otimes_K D) \cong L \otimes_K D \cong M_m(L),$$

since L splits D . Therefore L also splits S , and so $n|(L:E)$ by (28.5i), where n is the index of S . Hence n is a power of p . However, by (29.22) we know that $\exp[S]$ divides n , so $\exp[S]$ is also a power of p . But we have shown above that $p \nmid \exp[S]$, and so it follows that $[S] = 1$ in $B(E)$. This is a contradiction, and thus the theorem must be true.

EXERCISES

1. Show that every factor set $f: G \times G \rightarrow L^*$ is equivalent to a normalized factor set. [Hint: Let $c_1 = f_{1,1}^{-1}, c_\sigma = 1$ for $\sigma \in G - \{1\}$. Then $(\delta c)_{\sigma,1} = \sigma(c_1), \sigma \in G$. Set $g = (\delta c)f$, and show first that $g_{1,1} = 1$, then that $g_{\sigma,1} = g_{1,\sigma} = 1$ for all $\sigma \in G$.]
2. Verify that $(L/K, f)$ has center K , and that L is its own centralizer in $(L/K, f)$.
3. Let e be an idempotent of the central simple K -algebra C . Prove that $C \sim eCe$. [Hint: We may take $C = M_r(D)$, D = skewfield with center K . After a suitable change of basis (see Exercise 7.11), we may assume that $e = \text{diag}(1, \dots, 1, 0, \dots, 0)$, where s 1's occur. But then $eCe \cong M_s(D) \sim C$.]
4. Let D be a skewfield with center K , index m . Let E be a finite field extension of K , and let $E \otimes_K D \cong M_r(S)$, where S is a skewfield of index n . Show that S has center E , and that m/n is an integer which divides $(E:K)$. [Hint: This is the *Index Reduction Theorem* of Albert [1]. To prove it, note first that $E \otimes_K D$ is a central simple E -algebra, so S has center E . Next,

$$m^2 = (E \otimes_K D : E) = (M_r(S) : E) = r^2 n^2,$$

so $r = m/n$. Finally, if V is a simple right $M_r(S)$ -module, then $M_r(S) \cong V^{(r)}$. Comparing

right D -dimensions, we obtain

$$(E:K) = r(V:D),$$

so $r|(E:K)$.]

5. Keep the notation of the preceding exercise. Prove that if $(E:K)$ is relatively prime to the index m of D , then $E \otimes_K D$ is a skewfield with center E and index m . [Hint: Using the notation of Exercise 29.4, we see that $r = 1$, since r divides both m and $(E:K)$.]

6. Let D_i be a skewfield with center K , index m_i , $i = 1, 2$, and suppose that $(m_1, m_2) = 1$. Prove that $D_1 \otimes_K D_2$ is a skewfield with center K and index $m_1 m_2$. [Hint: Let $D_1 \otimes_K D_2 \cong M_t(S)$, where S is a skewfield with center K , and let E be a maximal subfield of S . Then E splits S , so

$$[E \otimes_K D_1] [E \otimes_K D_2] = 1 \text{ in } B(E).$$

But under the homomorphism $B(K) \rightarrow B(E)$, $[D_i]$ maps onto $[E \otimes_K D_i]$. Since $[D_i]^{m_i} = 1$, this shows that $[E \otimes_K D_1]$ and $[E \otimes_K D_2]$ have relatively prime orders. Therefore $[E \otimes_K D_i] = 1$ in $B(E)$, $i = 1, 2$, so E splits both D_1 and D_2 . Then $(E:K)$ is divisible by m_1 and m_2 , so $(E:K) \geq m_1 m_2$. Therefore

$$\begin{aligned} (S:K) &= (E:K)^2 \geq m_1^2 m_2^2 = (D_1:K) (D_2:K) \\ &= (D_1 \otimes_K D_2 : K) = (M_t(S):K), \end{aligned}$$

so $S = M_t(S)$. This proves that $t = 1$, and that $(S:K) = m_1^2 m_2^2$.]

7. Let D be a skewfield with center K and index m , where $m = \prod_{i=1}^t p_i^{e_i}$, with the $\{p_i\}$ distinct primes and each $e_i \geq 1$. Prove that there exist skewfields D_1, \dots, D_t with center K , such that D_i has index $p_i^{e_i}$, and

$$(29.25) \quad D \cong D_1 \otimes_K \cdots \otimes_K D_t.$$

[Hint: $\exp[D]$ divides m , and each $p_i|\exp[D]$. We may then write

$$[D] = [A_1] \cdots [A_t] \quad \text{in } B(K),$$

where $\exp[A_i] = p_i^{b_i}$, with $1 \leq b_i \leq e_i$. Let D_i be the skewfield part of A_i . Then

$$[D] = [D_1] \cdots [D_t] = [D_1 \otimes_K \cdots \otimes_K D_t] \quad \text{in } B(K).$$

But index $[D_i] = p_i^{c_i}$ for some $c_i \geq 1$, by (29.22). Hence $D_1 \otimes_K \cdots \otimes_K D_t$ is a skewfield, by Exercise 29.6, and so (29.25) is valid.]

No hints will be given for Exercises 29.8–29.13. The reader may consult the references on cohomology of groups listed at the start of this chapter.

8. Let G be a finite group, and let $\mathbf{Z}G$ be the *integral group ring* consisting of all sums $\{\sum_{g \in G} \alpha_g g : \alpha_g \in \mathbf{Z}\}$ (see beginning of §8, example (iv)). Every additive group M , on which G acts as left operator domain, can be made into a left $\mathbf{Z}G$ -module. Let \mathbf{Z} be the trivial $\mathbf{Z}G$ -module, that is, the additive group \mathbf{Z} on which G acts trivially: $gz = z$, $g \in G$, $z \in \mathbf{Z}$. Let Q_n be the free left $\mathbf{Z}G$ -module having as free basis the collection of all n -tuples $[x_1, \dots, x_n]$ of elements of G . For $n = 0$, interpret Q_0 as the free module on

one generator, with this generator denoted by the empty bracket $[]$. Show that there is a $\mathbf{Z}G$ -exact sequence

$$(29.26) \quad \cdots \rightarrow Q_2 \xrightarrow{d_2} Q_1 \xrightarrow{d_1} Q_0 \xrightarrow{d_0} \mathbf{Z} \rightarrow 0,$$

where

$$d_0[] = 1,$$

$$d_1[x] = x[] - [],$$

$$d_2[x, y] = x[y] - [xy] + [x],$$

$$d_3[x, y, z] = x[y, z] - [xy, z] + [x, yz] - [x, y], \quad x, y, z \in G,$$

and so on. Each map d_i is a left $\mathbf{Z}G$ -homomorphism, that is,

$$d_i\{\xi[x_1, \dots, x_i]\} = \xi d_i[x_1, \dots, x_i], \quad \xi \in \mathbf{Z}G, \quad x_i \in G.$$

9. Given a left $\mathbf{Z}G$ -module M , we apply $\text{Hom}_{\mathbf{Z}G}(\cdot, M)$ to (29.26), obtaining a sequence of additive groups

$$(29.27) \quad 0 \rightarrow \text{Hom}_{\mathbf{Z}G}(\mathbf{Z}, M) \xrightarrow{d_0^*} \text{Hom}_{\mathbf{Z}G}(Q_0, M) \xrightarrow{d_1^*} \text{Hom}_{\mathbf{Z}G}(Q_1, M) \xrightarrow{d_2^*} \cdots,$$

where d_i induces d_i^* as in §2a. Thus

$$d_i^* f = f d_i, \quad f \in \text{Hom}_{\mathbf{Z}G}(Q_i, M).$$

Prove first that $\text{im } d_i^* \subset \ker d_{i+1}^*$. Then define

$$H^0(G, M) = \ker d_1^*, \quad H^n(G, M) = \ker d_{n+1}^*/\text{im } d_n^*, \quad n \geq 1.$$

Call $H^n(G, M)$ the n th cohomology group of G with coefficients in M . Prove that

$$(29.28) \quad H^n(G, M) \cong \text{Ext}_{\mathbf{Z}G}^n(\mathbf{Z}, M), \quad n \geq 0,$$

where on the right, \mathbf{Z} denotes the trivial $\mathbf{Z}G$ -module.

10. Keep the above notation. Each $f \in \text{Hom}_{\mathbf{Z}G}(Q_n, M)$ is determined by its values $\{f[x_1, \dots, x_n]\}$ in M , so we may identify $\text{Hom}_{\mathbf{Z}G}(Q_n, M)$ with the additive group of all maps

$$f : \underbrace{G \times \cdots \times G}_{n \text{ factors}} \rightarrow M.$$

For $n = 0$, identify $\text{Hom}_{\mathbf{Z}G}(G_0, M)$ with M , letting $f \in \text{Hom}_{\mathbf{Z}G}(G_0, M)$ correspond to $f[] \in M$. Prove that

$$(d_1^* f)[x] = f(d_1[x]) = xf[] - f[], \quad \text{where } f:[] \rightarrow M,$$

$$(d_2^* f)[x, y] = xf(y) - f(xy) + f(x), \quad \text{where } f: G \rightarrow M,$$

$$(d_3^* f)[x, y, z] = xf(y, z) - f(xy, z) + f(x, yz) - f(x, y), \quad \text{where } f: G \times G \rightarrow M,$$

and so on. Prove that $H^0(G, M) \cong M^G$ as additive groups, where

$$M^G = \{m \in M : gm = m \text{ for all } g \in G\}.$$

11. Keep the above notation, and let $G = \text{Gal}(L/K)$, where L/K is a finite galois extension. Choose M to be the multiplicative group L^* on which G acts, and view M as $\mathbf{Z}G$ -module. Show that $\ker d_3^*$ consists of all factor sets from G to L^* , and that $\text{im } d_2^*$ consists of all principal factor sets. Deduce that the second cohomology group $H^2(G, L^*)$, defined at the beginning of §29, is a special case of the cohomology groups given in Exercise 29.8.

12. Let $G = \langle \sigma \rangle$ be a finite cyclic group of order n , and let M be a left $\mathbf{Z}G$ -module. Let

$$D = \sigma - 1, \quad N = 1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1} \in \mathbf{Z}G.$$

Prove that there is a $\mathbf{Z}G$ -exact sequence

$$\cdots \xrightarrow{N} \mathbf{Z}G \xrightarrow{D} \mathbf{Z}G \xrightarrow{N} \mathbf{Z}G \xrightarrow{D} \mathbf{Z}G \xrightarrow{\varepsilon} \mathbf{Z} \rightarrow 0,$$

where \xrightarrow{N} means left multiplication by N , \xrightarrow{D} by D , and where ε is the *augmentation map* defined by

$$\varepsilon\left(\sum_{g \in G} \alpha_g g\right) = \sum_{g \in G} \alpha_g, \quad \alpha_g \in \mathbf{Z}.$$

Using this projective resolution of the trivial $\mathbf{Z}G$ -module \mathbf{Z} , deduce that $H^0(G, M) \cong M^G$, and that

$$(29.29) \quad \begin{cases} H^1(G, M) \cong H^3(G, M) \cong H^5(G, M) \cong \cdots \cong \frac{M'}{(\sigma - 1)M}, \\ H^2(G, M) \cong H^4(G, M) \cong H^6(G, M) \cong \cdots \cong \frac{M^G}{(1 + \sigma + \cdots + \sigma^{n-1})M}. \end{cases}$$

Here,

$$M' = \{m \in M : Nm = 0\} = \{m \in M : (1 + \sigma + \cdots + \sigma^{n-1})m = 0\}.$$

13. Let L/K be a finite galois extension, with galois group $G = \langle \sigma \rangle$ cyclic of degree n . Choosing $M = L^*$ in the preceding exercise, show that

$$M^G = \{x \in L^* : \sigma x = x\} = K^*, \quad (1 + \sigma + \cdots + \sigma^{n-1})M = N_{L/K}(L^*),$$

where $N_{L/K}(L^*) = \{N_{L/K} x : x \in L^*\}$. Deduce that

$$(29.30) \quad H^2(G, L^*) \cong K^*/N_{L/K}(L^*).$$

14. Let L/K be a finite galois extension, with galois group G . Prove the *Normal Basis Theorem*:

There exists an $x \in L$ such that $\{\sigma(x) : \sigma \in G\}$ is a K -basis of L .

[Hint (Berger-Reiner [1]): Let $A = (L/K, 1) \cong \text{Hom}_K(L, L)$, as in the proof of (29.8), so L is a left module over the simple ring A . Comparing K -dimensions, it follows that $A \cong L^{(n)}$ as left A -modules. Let

$$A = \sum_{\sigma \in G} Lu_\sigma, \quad B = \sum_{\sigma \in G} Ku_\sigma, \quad u_\sigma u_\tau = u_{\sigma\tau}, \quad \sigma, \tau \in G,$$

where $u_\sigma \cdot x = \sigma(x)u_\sigma$, $\sigma \in G$, $x \in L$.

Then B is a subring of A . If $L = \sum_{i=1}^n Kx_i$, then

$$A = \sum_{\sigma} u_{\sigma} L = \sum_i \{ \sum_{\sigma} Ku_{\sigma} \} x_i \cong B^{(n)}$$

as left B -modules.

Hence $L^{(n)} \cong B^{(n)}$ as left B -modules, whence $L \cong B$ by the Krull–Schmidt Theorem (Exercise 6.6). Therefore $L = Bx$ for some $x \in L$, and

$$Bx = (\sum_{\sigma \in G} Ku_{\sigma})x = \sum_{\sigma \in G} K\sigma(x).$$

30. CYCLIC ALGEBRAS

Throughout this section let L denote a finite galois extension of the field K , and E any extension field of K . The symbol D will always stand for a skewfield. Call L a *cyclic* extension of K if $\text{Gal}(L/K)$ is cyclic; we write $\text{Gal}(L/K) = \langle \sigma \rangle$ to indicate that σ is a generator for $\text{Gal}(L/K)$. Starting with such a cyclic extension L/K , let a be any element of K^* , and form the associative K -algebra

$$(30.1) \quad A = (L/K, \sigma, a) = \sum_{j=0}^{n-1} Lu^j, \quad u \cdot x = \sigma(x) \cdot u, \quad u^n = a, \quad x \in L,$$

where we identify u^0 with the unity element of A . We shall call A a *cyclic* algebra. Obviously A is a crossed-product algebra, with the elements $\{u^j\}$ playing the role of elements $\{v_{\sigma^j} : 0 \leq j \leq n-1\}$ such that

$$v_{\sigma^j} \cdot x = \sigma^j(x) \cdot v_{\sigma^j}, \quad 0 \leq j \leq n-1, \quad x \in L.$$

Thus $A \cong (L/K, f)$ where the factor set f from $\langle \sigma \rangle$ to L^* is given by

$$(30.2) \quad f_{\sigma^i, \sigma^j} = \begin{cases} 1, & i + j < n \\ a, & i + j \geq n \quad 0 \leq i, j \leq n-1. \end{cases}$$

By §29, we know that A is a central simple K -algebra split by L , and that L is a self-centralizing maximal subfield of A .

Conversely, if L/K is cyclic, we show that every crossed-product algebra is a cyclic algebra.

(30.3) THEOREM. Let $G = \text{Gal}(L/K) = \langle \sigma \rangle$ be cyclic of order n , and let $B = (L/K, g)$ be a crossed-product algebra, where $g: G \times G \rightarrow L^*$ is a normalized factor set. Then

$$(L/K, g) \cong (L/K, \sigma, a), \quad a = \prod_{j=0}^{n-1} g_{\sigma^j, \sigma} \in K^*.$$

Proof. We may write

$$B = \sum_{j=0}^{n-1} Lv_{\sigma^j}, \quad v_{\sigma^j} \cdot x = \sigma^j(x) \cdot v_{\sigma^j}, \quad x \in L, \quad v_{\sigma^i} \cdot v_{\sigma^j} = g_{\sigma^i, \sigma^j} v_{\sigma^{i+j}},$$

for $0 \leq i, j \leq n - 1$. Then we obtain

$$\begin{aligned} v_{\sigma}^2 &= v_{\sigma} \cdot v_{\sigma} = g_{\sigma, \sigma} v_{\sigma^2}, & v_{\sigma}^3 &= (g_{\sigma, \sigma} v_{\sigma^2}) v_{\sigma} = g_{\sigma, \sigma} g_{\sigma^2, \sigma} v_{\sigma^3}, \dots, \\ v_{\sigma}^n &= a \cdot v_{\sigma^n} = a. \end{aligned}$$

Therefore

$$B = \sum_{j=0}^{n-1} Lv_{\sigma^j}, \quad v_{\sigma} \cdot x = \sigma(x) \cdot v_{\sigma}, \quad x \in L, \quad v_{\sigma}^n = a.$$

Since v_{σ}^n lies in the center of B , it follows that $a \in K^*$, and the theorem is proved.

Using this result, we may carry over to cyclic algebras the results on crossed-product algebras established in §29. Let us set

$$N_{L/K}(L^*) = \{N_{L/K} x : x \in L^*\}.$$

To begin with, we prove

(30.4) THEOREM. Let $G = \text{Gal}(L/K) = \langle \sigma \rangle$ be cyclic of order n , and let $a, b \in K^*$. Then

- (i) $(L/K, \sigma, a) \cong (L/K, \sigma^s, a^s)$ for each $s \in \mathbb{Z}$ such that $(s, n) = 1$.
- (ii) $(L/K, \sigma, 1) \cong M_n(K)$.
- (iii) $(L/K, \sigma, a) \cong (L/K, \sigma, b)$ if and only if

$$b = (N_{L/K} c)a \text{ for some } c \in L^*.$$

In particular, $(L/K, \sigma, a) \sim K$ if and only if $a \in N_{L/K}(L^*)$.

$$(iv) (L/K, \sigma, a) \otimes_K (L/K, \sigma, b) \sim (L/K, \sigma, ab).$$

Proof. Let

$$(30.5) \quad A = (L/K, \sigma, a) = \sum' Lv^j, \quad B = (L/K, \sigma, b) = \sum' Lv^j,$$

where for all $x \in L$,

$$(30.6) \quad u \cdot x = \sigma(x)u, \quad u^n = a; \quad v \cdot x = \sigma(x)v, \quad v^n = b.$$

If $(s, n) = 1$, then $G = \langle \sigma^s \rangle$ and

$$A = \sum_{j=0}^{n-1} Lw^j, \quad \text{where } w = u^s.$$

It is easily checked that

$$w \cdot x = \sigma^s(x) \cdot w, \quad w^n = a^s, \quad x \in L,$$

so (i) is established.

Assertion (ii) is a special case of (29.8). To prove (iii), note first that for any $c \in L^*$ we have

$$A = \sum_{j=0}^{n-1} L(cu)^j,$$

and

$$\begin{aligned} cu \cdot x &= \sigma(x) \cdot cu, \quad x \in L, \\ (cu)^n &= cu \cdot cu \cdots cu = c \cdot \sigma(c) \cdots \sigma^{n-1}(c) u^n \\ &= (N_{L/K} c)a. \end{aligned}$$

Then $A \cong (L/K, \sigma, a \cdot Nc)$. Conversely, given any K -isomorphism $A \cong B$, we may assume that $A = B$ by using the argument in the proof of (29.6). But then vu^{-1} centralizes L , so $v = cu$ for some $c \in L^*$. Therefore

$$b = v^n = (cu)^n = (N_{L/K} c)a,$$

as claimed.

Analogously, assertion (iv) follows from (29.9). We leave the details as exercise for the reader.

(30.7) COROLLARY. Let $A = (L/K, \sigma, a)$ as above. Then $\exp[A]$ is the least positive integer t such that $a^t \in N_{L/K}(L^*)$. If $\exp[A] = (L:K)$, then A is a skewfield.

Proof. We have $[A]^t = [(L/K, \sigma, a^t)]$ in $B(K)$. Thus $[A]^t = 1$ if and only if a^t is a norm. For the second assertion, let $n = (L:K)$, so $(A:K) = n^2$. If $A \cong M_r(D)$, where D has index m , then $n = mr$. But $[A]^m = 1$ in $B(K)$ by (29.22), whence $\exp[A]$ divides m . Hence if $\exp[A] = n$, it follows that $m = n$ and $r = 1$. Thus A is a skewfield, and the proof is completed.

Let us carry over to the case of cyclic algebras, two further results from §29.

(30.8) THEOREM. Let $G = \text{Gal}(L/K) = \langle \sigma \rangle$ be cyclic of order n , and let $a \in K^*$. Let E be any field containing K , and let EL be the composite of E and L in some larger field containing both E and L . We may write

$$(30.9) \quad H = \langle \sigma^k \rangle = \text{Gal}(L/L \cap E) \cong \text{Gal}(EL/E),$$

where k is the least positive integer such that σ^k fixes $L \cap E$. Then

$$E \otimes_K (L/K, \sigma, a) \sim (EL/E, \sigma^k, a).$$

Proof. The isomorphism given in (30.9) is well known from galois theory,

and we treat it as an identification. Let

$$A = (L/K, \sigma, a) = (L/K, f)$$

where f is normalized and is given by (30.2). If f' denotes the restriction of f to $H \times H$, then by (29.13) we have

$$E \otimes_K A \sim (EL/E, f').$$

Since EL/E is a cyclic extension with galois group $H = \langle \sigma^k \rangle$, it follows from (30.3) that

$$(EL/E, f') = (EL/E, \sigma^k, b),$$

where

$$b = \prod_{r=1}^{m-1} f'_{\sigma^{rk}, \sigma^k}, \quad m = |H| = n/k.$$

From (30.2) we find immediately that $b = a$, which completes the proof of the theorem.

(30.10) THEOREM. *Let $K \subset L \subset E$, where $G = \text{Gal}(E/K) = \langle \sigma \rangle$ is cyclic of finite order t . Let*

$$H = \text{Gal}(E/L), \bar{G} = G/H = \text{Gal}(L/K) = \langle \bar{\sigma} \rangle,$$

where $\bar{\sigma}$ is the image of σ in \bar{G} . Then for any $a \in K^$,*

$$(L/K, \bar{\sigma}, a) \sim (E/K, \sigma, a^{(E:L)}).$$

Proof. Let $A = (L/K, \bar{\sigma}, a) = (L/K, f)$, where

$$f_{\bar{\sigma}^i, \bar{\sigma}^j} = \begin{cases} 1, & i + j < n \\ a, & i + j \geq n, \quad 0 \leq i, j \leq n - 1, \end{cases}$$

and where $n = (L:K)$. By (29.16), we have $A \sim (E/K, g)$, where g is the inflation of f . But from (30.3) we obtain

$$(E/K, g) \cong (E/K, \sigma, b), \quad \text{where } b = \prod_{j=0}^{t-1} g_{\sigma^j, \sigma}.$$

Now $t = (E:K) = (E:L)(L:K) = sn$, where $s = (E:L)$. Further, for $0 \leq j \leq t-1$ we have

$$g_{\sigma^j, \sigma} = f_{\bar{\sigma}^j, \bar{\sigma}} = \begin{cases} a, & j = n - 1, 2n - 1, \dots, sn - 1, \\ 1, & \text{otherwise.} \end{cases}$$

Therefore $b = a^s$, and the theorem is proved.

EXERCISES

1. Let L be a cyclic extension of K . Prove that

$$H^2(G, L^*) \cong B(L/K) \cong K^*/N_{L/K}(L^*)$$

where $G = \text{Gal}(L/K)$. [Hint: Let $G = \langle \sigma \rangle$, and consider the map $K^* \rightarrow B(L/K)$ defined by $a \in K^* \mapsto [(L/K, \sigma, a)] \in B(L/K)$. Show that this gives an epimorphism of groups, with kernel $N_{L/K}(L^*)$. For another proof, see Exercise 29.13.]

2. Let A be a central simple K -algebra split by E , where E is a cyclic extension of K such that $(A:K) = (E:K)^2$. Prove that $A \cong (E/K, \sigma, a)$ for some $a \in K^*$, where $G = \text{Gal}(E/K) = \langle \sigma \rangle$. [Hint: By (28.10), we may embed E in A as a self-centralizing maximal subfield of A . The proof of (29.12) then shows that A is isomorphic to a crossed-product algebra $(E/K, f)$, for some $[f] \in H^2(G, E^*)$. Finally,

$$(E/K, f) \cong (E/K, \sigma, a)$$

for some $a \in K^*$, by (30.3).]

3. Let A' be a central simple K -algebra split by E , where E is a finite cyclic extension of K . Prove that $A' \sim (E/K, \sigma, a)$ for some $a \in K^*$, where $\text{Gal}(E/K) = \langle \sigma \rangle$. [Hint: The proof of (29.12) shows that $A' \sim A$, for some central simple K -algebra A split by E , such that $(A:K) = (E:K)^2$. Now use the preceding exercise.]

4. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, and let $\sigma \in \text{Gal}(L/K)$ be defined by $\sigma(\sqrt{2}) = -\sqrt{2}$. For p an odd prime, let $A = (L/K, \sigma, p)$. Show that $A \cong M_2(K)$ if 2 is a quadratic residue mod p , while A is a skewfield if 2 is not a quadratic residue mod p . [Hint: A is a skewfield if and only if $p \notin N(L^*)$, where N means $N_{L/K}$. Let $R = \mathbb{Z}[\sqrt{2}]$, and show that $R = \text{alg. int. } \{L\}$. Imitating the proof in §26 that the quaternion order has a Euclidean algorithm, show that R is also Euclidean, and hence every ideal of R is principal.

If $p \in N(L^*)$, then there exist integers $a, b, c \in \mathbb{Z}$, not all zero, such that $a^2 - 2b^2 = pc^2$. If $p \nmid a$, then also $p \nmid b$ and $p \nmid c$; after cancellation and repetition of the process, we may assume that $p \nmid a$. Since $a^2 \equiv 2b^2 \pmod{p}$, it follows that 2 is a quadratic residue mod p .

Conversely, if 2 is a quadratic residue mod p , then there exist $a, b \in \mathbb{Z}$ with $p \nmid a$, $p \nmid b$, such that $p \mid (a^2 - 2b^2)$. Then $p \mid (a + b\sqrt{2})(a - b\sqrt{2})$, so pR is not a prime ideal of R . Further, p is unramified in L/K , since p does not divide the discriminant of R over \mathbb{Z} . Hence $pR = P_1P_2$, where the P_i are distinct ideals of R . Therefore $p\mathbb{Z} = N_{L/K}(P_1)$, and if $P_1 = R\alpha$, then $p = \pm N\alpha$. But $u = 1 + \sqrt{2} \in u(R)$, and $N(u) = -1$. Hence p is either $N\alpha$ or $N(u\alpha)$, and so $p \in N(L^*)$.]

31. CYCLIC ALGEBRAS OVER LOCAL FIELDS

Throughout this section let R be a complete discrete valuation ring, with maximal ideal $P = \pi R \neq 0$, and let $\bar{R} = R/P$. Let K be the quotient field of R , and v_K the exponential valuation on K . We assume throughout that the residue class field \bar{R} is finite, and set $\text{card } \bar{R} = q$.

Let D be a skewfield with center K and index m , where by definition

$m = \sqrt{(D:K)}$. Let us recall some details from §14, where we showed that each such skewfield D is isomorphic to a cyclic algebra. Let W' be the unique unramified extension of K of degree m . Then $W = K(\omega)$, where ω is a primitive $(q^m - 1)$ th root of unity over K . The Galois group $\text{Gal}(W/K)$ is cyclic of order m , and has as canonical generator the Frobenius automorphism σ of W/K . Recall that σ is defined by the equation $\sigma(\omega) = \omega^q$. We shall denote the Frobenius automorphism of the extension W/K by $\sigma_{W/K}$; it is defined only for unramified extensions. As in §5b, we use the notation σ_W for the valuation ring of W , p_W for the maximal ideal of σ_W , and \bar{o}_W for the residue class field σ_W/p_W .

We showed in §14 that W may be embedded in D , and that there exists a prime element $z \in D$ such that

$$D = \sum_{j=0}^{m-1} Wz^j, \text{ where } z\alpha z^{-1} = \sigma^r(\alpha), \alpha \in W, \text{ and } z^m = \pi.$$

The integer r is relatively prime to the index m , and D determines $r \bmod m$ uniquely. Further, each pair r, m with $(r, m) = 1$ arises from some D .

In terms of the notation for cyclic algebras introduced in §30, we have $D \cong (W/K, \sigma^r, \pi)$. Choose $s \in \mathbf{Z}$ so that $rs \equiv 1 \pmod{m}$. Then also $(s, m) = 1$, and by (30.4 i),

$$D \cong (W/K, \sigma^r, \pi) \cong (W/K, \sigma^{rs}, \pi^s) = (W/K, \sigma, \pi^s).$$

Furthermore, we could have restricted s to lie in the range $1 \leq s \leq m$. Let $\phi(m)$ denote the number of such integers s . We now prove

(31.1) **THEOREM.** *Let W/K be an unramified extension of degree m , and let σ be the Frobenius automorphism of W/K . Let $\{a_s\}$ be any set of $\phi(m)$ elements of K^* , such that the values $\{v_K(a_s)\}$ are relatively prime to m , and are incongruent mod m . Then the $\phi(m)$ cyclic algebras $\{(W/K, \sigma, a_s)\}$ give a full set of non-isomorphic skewfields with center K and index m .*

Proof. We have already seen that the cyclic algebras

$$\{(W/K, \sigma, \pi^s) : 1 \leq s \leq m, (s, m) = 1\},$$

give a full set of non-isomorphic skewfields with center K and index m . Now let $a \in K^*$, and let

$$N_{W/K}(W^*) = \{N_{W/K}(x) : x \in W^*\}.$$

We showed in (14.1) that $a \in N_{W/K}(W^*)$ if and only if $m | v_K(a)$. On the other hand, from (30.4) we know that for $a, b \in K^*$, we have

$$(31.2) \quad (W/K, \sigma, a) \cong (W/K, \sigma, b) \text{ if and only if } ba^{-1} \in N_{W/K}(W^*).$$

It then follows that

$$(31.3) \quad (W/K, \sigma, a) \cong (W/K, \sigma, b) \quad \text{if and only if} \quad v_K(a) \equiv v_K(b) \pmod{m}.$$

The assertion in the theorem is now obvious.

For each $[A] \in B(K)$, we have denoted by $\exp [A]$ the exponent of $[A]$ in the Brauer group $B(K)$, and by $\text{index } [A]$ the index of the skewfield part of A . An important consequence of the preceding discussion is the following fundamental result:

(31.4) THEOREM. *Let D be a skewfield with center K and index m . Then $m = \exp [D]$. Hence for each $[A] \in B(K)$,*

$$\exp [A] = \text{index } [A].$$

Proof. We may take $D = (W/K, \sigma, \pi^s)$ as in (31.1), with $(s, m) = 1$. Then

$$[D]^t = [(W/K, \sigma, \pi^{st})] \in B(K)$$

by (30.4). But $(W/K, \sigma, 1) \sim K$ by (30.4), and so it follows that $(W/K, \sigma, \pi^{st}) \sim K$ if and only if there is a K -isomorphism

$$(W/K, \sigma, \pi^{st}) \cong (W/K, \sigma, 1).$$

But by (31.3), such an isomorphism exists if and only if $m|st$. This proves that $[D]^t = 1$ in $B(K)$ if and only if $m|st$. Since $(s, m) = 1$, it is clear that $m|st$ if and only if $m|t$. This proves that $\exp [D] = m$. The second assertion in the theorem is immediate.

Whether or not $(s, m) = 1$, we may still form the cyclic algebra $A = (W/K, \sigma, \pi^s)$. By (31.3), the isomorphism class of A depends only on $s \pmod{m}$, that is, on the fraction s/m viewed as an element of the additive group \mathbf{Q}/\mathbf{Z} . Let us find the skewfield part of A ; of course, we already know that A is a skewfield whenever $(s, m) = 1$.

(31.5) THEOREM. *Let W/K be an unramified extension of degree m , with Frobenius automorphism σ , and let $s \in \mathbf{Z}$. Write $s/m = s'/m'$, where $(s', m') = 1$.*

Then $(W/K, \sigma, \pi^s) \sim (W'/K, \sigma', \pi^{s'}) = \text{skewfield of index } m'$,

where W'/K is an unramified extension of degree m' , with Frobenius automorphism σ' .

Proof. Let W' be the subfield of W fixed by $\langle \sigma^{m'} \rangle$, so W'/K is unramified and $(W':K) = m'$. The epimorphism $\text{Gal}(W/K) \rightarrow \text{Gal}(W'/K)$ carries σ onto σ' (see Exercise 31.1). Setting $d = (W:W') = m/m'$, it follows from (30.10) that

$$(W'/K, \sigma', \pi^{s'}) \sim (W/K, \sigma, (\pi^s)^d) = (W/K, \sigma, \pi^s).$$

Since $(s', m) = 1$, we know that $(W'/K, \sigma', \pi^{s'})$ is a skewfield, and the theorem is proved.

(31.6) COROLLARY. *Keep the above notation, and let $a \in K^*$. Then the cyclic algebra $(W/K, \sigma, a)$ is a skewfield if and only if $(m, v_K(a)) = 1$.*

Proof. Let $s = v_K(a)$, so $(W/K, \sigma, a) \cong (W/K, \sigma, \pi^s)$. The result now follows from (31.5).

Let W/K be an unramified extension of degree m , with Frobenius automorphism $\sigma_{W/K}$. Given an integer s , not necessarily prime to m , let us form the cyclic algebra $A = (W/K, \sigma_{W/K}, \pi^s)$. We now define the *Hasse invariant* of A , denoted by $\text{inv } A$, by the formula

$$(31.7) \quad \text{inv} (W/K, \sigma_{W/K}, \pi^s) = s/m \in Q/Z.$$

The skewfield part of A can be calculated by use of (31.5), and it has the same Hasse invariant as A . Therefore $\text{inv } A$ depends only upon the class $[A] \in B(K)$, and we shall write $\text{inv } [A]$ rather than $\text{inv } A$ hereafter. By (31.1), every class in $B(K)$ is represented by some cyclic algebra $(W/K, \sigma_{W/K}, \pi^s)$ with W/K unramified, and hence there is a well defined map

$$\text{inv}: B(K) \rightarrow Q/Z.$$

Caution. Let L/K be a cyclic extension with galois group $\langle \sigma \rangle$ cyclic of order n , and let $a \in K^*$. Then the cyclic algebra $B = (L/K, \sigma, a)$ determines a class $[B]$ in $B(K)$. However, it is *not* necessarily true that $\text{inv } [B] = v_K(a)/n$. Indeed, even when L/K is unramified, the formula is valid only when σ equals the Frobenius automorphism $\sigma_{L/K}$. Further, in the ramified case the Frobenius automorphism $\sigma_{L/K}$ is not even defined. In order to compute $\text{inv } [B]$ when L/K is ramified, we must first write $B \sim (W/K, \sigma_{W/K}, \pi^s) = A$ for some unramified extension W/K , and then we have $\text{inv } [B] = \text{inv } [A] = s/m$.

We are now ready to prove the important result:

$$(31.8) \quad \text{THEOREM. } \text{inv}: B(K) \cong Q/Z.$$

Proof. The map inv is epic, since each element of Q/Z is of the form s/m , with $(s, m) = 1$, $m \geq 1$. Now let $[A] \in B(K)$ be represented by the cyclic algebra

$$A = (W/K, \sigma, \pi^s), \text{ where } W/K \text{ is unramified, } \sigma = \sigma_{W/K}, \text{ and } (W:K) = m.$$

Then $\text{inv } [A] = s/m \in Q/Z$, so $\text{inv } [A] = 0$ if and only if $m|s$, that is, if and only if $A \sim K$. This proves that inv is monic.

Finally, given $[A], [B] \in B(K)$, we may choose W/K unramified so that

$$A = (W/K, \sigma, \pi^s), \quad B = (W/K, \sigma, \pi^t), \quad \sigma = \sigma_{W/K}.$$

Then

$$A \otimes_K B \sim (W/K, \sigma, \pi^{s+t})$$

by (30.4). Therefore

$$\text{inv } [A][B] = \text{inv } [A] + \text{inv } [B],$$

which completes the proof that inv is an isomorphism of groups.

We shall denote inv by inv_K when we need to specify the underlying field K . Our next result, of great importance, describes the effect on inv of a change in ground fields.

(31.9) THEOREM. *Let E be any finite extension of K . The following diagram commutes:*

$$\begin{array}{ccc} B(K) & \xrightarrow{\text{inv}_K} & \mathbf{Q}/\mathbf{Z} \\ \downarrow E \otimes_K & & \downarrow (E:K) \\ B(E) & \xrightarrow{\text{inv}_E} & \mathbf{Q}/\mathbf{Z}, \end{array}$$

where the horizontal maps are isomorphisms, and where the second vertical map is defined to be multiplication by $(E:K)$.

Proof. Let $A = (W/K, \sigma, \pi^s)$ represent a class $[A] \in B(K)$, where W/K is unramified, $\sigma = \sigma_{W/K}$, and $(W:K) = m$. We may view W and E as embedded in some algebraic closure of K , and then we may form their intersection $F = E \cap W$ and their composite EW . If k is the least positive integer such that σ^k fixes F , then F/K is unramified and $(F:K) = k$. By (30.8) we have

$$E \otimes_K A \sim (EW/E, \sigma^k, \pi^s),$$

so it remains for us to compute the Hasse invariant of the right hand expression.

As in §5, let \mathcal{O}_E denote the valuation ring of E , $\bar{\mathcal{O}}_E$ its residue class field, and v_E the exponential valuation on E . Then

$$(E:K) = ef, \quad e = e(E/K), \quad f = f(E/K), \quad v_E = e \cdot v_K \text{ on } K.$$

Note that $m = (W:K) = (\bar{\mathcal{O}}_W:\bar{\mathcal{O}}_K)$. Let us put

$$d = (m, f), \quad m = dm', \quad f = df',$$

where $(m', f') = 1$.

Since d divides both m and f , there is a field $\tilde{o} \subset \bar{\mathcal{O}}_W \cap \bar{\mathcal{O}}_E$ with $(\tilde{o}:\bar{\mathcal{O}}_K) = d$. By (5.9) it follows that there is a field $\tilde{F} \subset W \cap E = F$, such that

$$\tilde{F}/K \text{ is unramified, } (\tilde{F}:K) = (\bar{o}:\bar{o}_K) = d, \quad \bar{o} = \bar{o}_{\tilde{F}}.$$

On the other hand, the field $\bar{o}_{\tilde{F}}$ is contained in both \bar{o}_W and \bar{o}_E , whence $(\bar{o}_{\tilde{F}}:\bar{o}_K)$ divides both m and f , hence divides d . But

$$k = (F:K) = (\bar{o}_F:\bar{o}_K), \quad d = (\tilde{F}:K), \quad F \supset \tilde{F}.$$

Since we have just shown that $k|d$, it follows that $F = \tilde{F}$ and $k = d$. Consequently we obtain

$$f(E/F) = f(E/K)/f(F/K) = f/d = f'.$$

Diagrammatically, we have

$$\begin{array}{ccccc}
 & E \cdot W & & & \\
 & \swarrow \quad \searrow & & & \\
 W & & & E & \\
 & \searrow \quad \swarrow & & & \\
 & m' & & m' & \\
 & \downarrow & & \downarrow & \\
 F = E \cap W & & & & \\
 & k \downarrow & & & \\
 & K & & &
 \end{array}
 \quad \begin{aligned}
 \text{Gal}(EW/E) &\cong \text{Gal}(W/F) = \langle \sigma^k \rangle, \\
 m' &= (W:F) = (EW:E).
 \end{aligned}$$

Now let τ be the Frobenius automorphism of EW/E , and view σ^k as element of $\text{Gal}(EW/E)$. By Exercise 31.1 (iv) we have

$$\tau = (\sigma^k)^{f(E/F)} = \sigma^{kf'}.$$

But $(f', m') = 1$, and $m' = (EW:E)$, so by (30.4 i) we obtain

$$(EW/E, \sigma^k, \pi^s) \cong (EW/E, \sigma^{kf'}, \pi^{sf'}).$$

Therefore

$$E \otimes_K A \sim (EW/E, \tau, \pi^{sf'}),$$

and so

$$\begin{aligned}
 \text{inv}_E [E \otimes_K A] &= v_E(\pi^{sf'})/m' = sf' \cdot v_E(\pi)/m' \\
 &= sf'e/m' = sfe/m = (E:K) \cdot \text{inv}[A].
 \end{aligned}$$

This completes the proof of the theorem.

(31.10) **Corollary.** Let D be a skewfield with center K and index m , and let E be any finite extension of K . Then E splits D if and only if $m|(E:K)$.

Proof. Consider the element $[D] \in B(K)$; then $\text{inv}[D] = s/m$ for some s relatively prime to m . Clearly E splits D if and only if $\text{inv}_E [E \otimes_K D] = 0$.

On the other hand,

$$\text{inv}_E [E \otimes_K D] = (E : K) \cdot s/m.$$

Since $(s, m) = 1$, we conclude that $\text{inv}_E [E \otimes_K D] = 0$ if and only if $m | (E : K)$. This gives the desired result.

As a consequence of the preceding corollary, we obtain the following amazing result:

(31.11) **THEOREM.** *Let D be a skewfield with center K and index m . Then every irreducible m -th degree equation over K has a solution in D .*

Proof. Let $f(X) \in K[X]$ be irreducible, and of degree m . Let $E = K(a)$, where $\min. \text{pol.}_K a = f(X)$. Then $(E : K) = m$, so E splits D by (31.10). It follows from (28.10) that there is a K -embedding of E into D . The image of a is then an element of D which satisfies the equation $f(X) = 0$.

We conclude with a further consequence of (31.8) and (31.9).

(31.12) **Theorem.** *Let E/K be any finite extension of degree n . Then $B(E/K)$ is cyclic of order n .*

Proof. By definition, $B(E/K)$ consists of all classes $[A] \in B(K)$ which are split by E . Hence by (31.9) there is a commutative diagram

$$\begin{array}{ccccc} 1 & \rightarrow & B(E/K) & \rightarrow & B(K) \longrightarrow B(E) \\ & & \downarrow \text{inv}_K & & \downarrow \text{inv}_E \\ Q/Z & \xrightarrow{n} & Q/Z, & & \end{array}$$

where the top row is exact, the bottom map is given by multiplication by n , and the vertical maps are isomorphisms. It follows at once that $B(E/K)$ is isomorphic to the kernel of the bottom map, that is,

$$B(E/K) \cong \frac{1}{n} Z/Z.$$

This completes the proof.

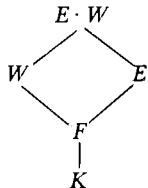
(31.13) **COROLLARY.** *If $(E : K) = n$, then*

$$B(E/K) = \{[A] \in B(K) : [A]^n = 1\}.$$

EXERCISES

The hypotheses and notation given at the beginning of this section remain in force throughout these exercises.

1. Consider the diagram



in which all of the fields indicated are finite extensions of K . We assume that W/K is unramified, and denote its Frobenius automorphism by $\sigma_{W/K}$.

(i) Prove that $\sigma_{W/K} \in \text{Gal}(W/K)$ is characterized by the condition

$$\sigma_{W/K}(x) \equiv x^{\text{card } \bar{o}_K} \pmod{p_W}, \quad x \in o_W.$$

(ii) Prove that F/K is unramified, and that the epimorphism

$$\text{Gal}(W/K) \rightarrow \text{Gal}(F/K)$$

carries $\sigma_{W/K}$ onto $\sigma_{F/K}$. If k is the least positive integer such that

$$(\sigma_{W/K})^k \in \text{Gal}(W/F),$$

prove that

$$(F:K) = k, \quad \sigma_{W/F} = (\sigma_{W/K})^k.$$

(iii) Let $E \cdot W$ be the composite of E and W in some extension field of K . Show that EW/E is an unramified extension, and that

$$\sigma_{EW/E}(\text{restricted to } W) = (\sigma_{W/E})^{f(E/F)} = (\sigma_{W/K}^k)^{f(E/F)},$$

where $f(E/F) = (\bar{o}_E : \bar{o}_F)$.

(iv) When $F = E \cap W$, there is an isomorphism

$$\Psi: \text{Gal}(W/F) \cong \text{Gal}(EW/E),$$

obtained by extending each F -automorphism of W to an E -automorphism of EW . For each $\sigma \in \text{Gal}(EW/E)$, $\Psi^{-1}\sigma$ is just the restriction of σ to W . Deduce from (iii) that

$$\sigma_{EW/E} = \Psi\{(\sigma_{W/K}^k)^{f(E/F)}\}.$$

[Hint: The results are straightforward consequences of the definition of the Frobenius automorphism of an unramified extension. Detailed proofs are available in the references listed at the beginning of §4.]

2. Let L/K be a cyclic extension of degree n , possibly ramified. Prove that $K^*/N_{L/K}(L^*)$ is cyclic of order n . [Hint: Use Exercise 30.1 and Theorem 31.12.]

3. Let $K \subset E \subset F$, where $(F:E) = m$, $(E:K) = n$. We make no assumptions as to ramification, nor do we assume that the extensions are galois extensions. Prove that the sequence of groups

$$1 \rightarrow B(E/K) \xrightarrow{\text{inc}} B(F/K) \xrightarrow{E \otimes_K} B(F/E) \rightarrow 1$$

is exact, where *incl.* is the inclusion map. [Hint: Consider the diagram

$$\begin{array}{ccccccc} 1 & \rightarrow & B(E/K) & \rightarrow & B(F/K) & \rightarrow & B(F/E) \rightarrow 1 \\ & & \downarrow \text{inv}_K & & \downarrow \text{inv}_X & & \downarrow \text{inv}_E \\ 1 & \rightarrow & \frac{1}{n}\mathbf{Z}/\mathbf{Z} & \rightarrow & \frac{1}{mn}\mathbf{Z}/\mathbf{Z} & \rightarrow & \frac{1}{m}\mathbf{Z}/\mathbf{Z} \rightarrow 1. \end{array}$$

Show that the left hand square commutes (use (31.12)), and so does the right hand square (use (31.9)). Then use exactness of the bottom row.]

4. Let L/K be any cyclic extension, with galois group $\langle \sigma \rangle$. Prove that for $s \in \mathbf{Z}$,

$$\text{inv}_K[(L/K, \sigma, \pi^s)] = s \cdot \text{inv}_K[(L/K, \sigma, \pi)].$$

5. Let \mathbf{R} be the real field, \mathbf{C} the complex field,

$$\mathbf{R}^+ = \{x \in \mathbf{R} : x \geq 0\}.$$

Let $N: \mathbf{C} \rightarrow \mathbf{R}$ be the norm map. Prove that $N(\mathbf{C}) = \mathbf{R}^+$.

6. Let D be a skewfield with center \mathbf{C} , such that $(D:\mathbf{C})$ is finite. Prove that $D = \mathbf{C}$. [Hint: Let $a \in D$, and set $\min. \text{pol.}_{\mathbf{C}}(a) = f(X) \in \mathbf{C}[X]$. Then there exist elements $\{\alpha_i\}$ in \mathbf{C} such that $f(X) = \prod(X - \alpha_i)$. Since $\prod(a - \alpha_i) = 0$, and D is a skewfield, some factor $a - \alpha_i$ must be zero.]

7. Let σ be complex conjugation on \mathbf{C} , and let \mathbf{H} be the cyclic algebra

$$\mathbf{H} = (\mathbf{C}/\mathbf{R}, \sigma, -1).$$

Prove that \mathbf{H} is the skewfield consisting of quaternions over \mathbf{R} . [Hint: The least positive integer t such that $(-1)^t \in N_{\mathbf{C}/\mathbf{R}}(\mathbf{C}^*)$ is given by $t = 2$. Thus \mathbf{H} is a skewfield, by (30.7). As in the example following (29.8), we have

$$\mathbf{H} \cong \mathbf{R} \oplus \mathbf{R}i \oplus \mathbf{R}j \oplus \mathbf{R}k,$$

where

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k.$$

8. Prove that if D is a skewfield whose center contains \mathbf{R} , and for which $(D:\mathbf{R})$ is finite, then $D = \mathbf{C}$, \mathbf{R} , or \mathbf{H} . [Hint: If the center of D is \mathbf{C} , then $D = \mathbf{C}$ by Exercise 31.6. Suppose now that D has center \mathbf{R} , and that the index of D is m , where $m > 1$. Then D has a maximal subfield E , with $(E:\mathbf{R}) = m$. Hence $E = \mathbf{C}$, $m = 2$, and by §30 we may write

$$D \cong (\mathbf{C}/\mathbf{R}, \sigma, a), \quad a \in \mathbf{R}^*,$$

where σ is complex conjugation. The isomorphism class of the cyclic algebra $A = (\mathbf{C}/\mathbf{R}, \sigma, a)$ depends only on the coset of a in $\mathbf{R}^*/N(\mathbf{C}^*)$, where N is the norm map from \mathbf{C} to \mathbf{R} . By Exercise 31.5, it follows that A is determined up to isomorphism by the sign of the element a . But we have

$$(\mathbf{C}/\mathbf{R}, \sigma, 1) \cong M_2(\mathbf{R}), \quad (\mathbf{C}/\mathbf{R}, \sigma, -1) = \mathbf{H},$$

so the result follows.]

9. Prove that $[\mathbf{H}] \in B(\mathbf{R})$ has exponent 2.

8. Simple Algebras Over Global Fields

Throughout this chapter let K denote a global field (see §4e). Our aim is to study central simple K -algebras, and ideal class groups of maximal orders in such algebras. As general references for the topics considered below, the reader may consult Albert [1], Cassels–Fröhlich [1], Deuring [1], Roggenkamp [1], Roggenkamp, Huber–Dyson [1], Swan–Evans [1], Weil [1]. We shall state without proof two basic results from class field theory, namely the Hasse Norm Theorem and the Grunwald–Wang Theorem. To include the proofs of these results in this book would require several additional chapters, and would adversely affect the proper balance of the subject matter covered in this book. Apart from these two theorems, however, the rest of the exposition is self-contained.

32. SPLITTING OF SIMPLE ALGEBRAS

Let A be a central simple K -algebra, where K is a global field, and let P range over the primes of K (see §4e). In order to simplify the notation, we shall use K_P (rather than \hat{K}_P) to denote the P -adic completion of K . Then put

$$A_P = K_P \otimes_K A = P\text{-adic completion of } A.$$

By (7.8), A_P is a central simple K_P -algebra; thus the map $[A] \rightarrow [A_P]$ yields a homomorphism of Brauer groups $B(K) \rightarrow B(K_P)$. Suppose that

$$A_P \cong M_{\kappa_P}(S),$$

where S is a skewfield of index m_P over its center K_P . As in §§25, 29, we call m_P the *local index* of A at P , and we write

$$m_P = \text{index } [A_P].$$

We call κ_P the *local capacity* of A at P . Clearly

$$A_P \sim K_P \quad \text{if and only if} \quad m_P = 1.$$

We shall say that A *ramifies* at P , or that P is *ramified* in A , if $m_P > 1$.

The following theorem summarizes some of the main results of Chapter VI (see (22.4), (25.7) and (25.10)).

(32.1) THEOREM. Let R be a Dedekind domain whose quotient field is a global field K , and assume that $R \neq K$. Let Λ be a maximal R -order in the central simple K -algebra A . The nonzero prime ideals P of R , and the prime ideals \mathfrak{P} of Λ , are in one-to-one correspondence, given by

$$P = R \cap \mathfrak{P}, \quad \mathfrak{P} | P\Lambda.$$

Let m_P be the local index of A at P and κ_P the local capacity of A at P . Then

(i) $m_P = 1$ a.e., that is, $A_P \sim K_P$ a.e.

(ii) $P\Lambda = \mathfrak{P}^{m_P}$ for all P .

(iii) Let $\mathfrak{D}(\Lambda/R)$ denote the different of Λ with respect to R , and $d(\Lambda/R)$ the discriminant. Then

$$\mathfrak{D}(\Lambda/R) = \prod_P \mathfrak{P}^{m_P - 1}, \quad d(\Lambda/R) = \left\{ \prod_P P^{(m_P - 1)\kappa_P} \right\}^{\sqrt{(A:K)}}.$$

(iv) We have

$$m_P > 1 \Leftrightarrow P | d(\Lambda/R) \Leftrightarrow \mathfrak{P} | \mathfrak{D}(\Lambda/R) \Leftrightarrow \mathfrak{P}^2 | P\Lambda.$$

In the present discussion, the infinite primes of K will play an important role. Such infinite primes occur only when K is an algebraic number field. In this case, an infinite prime P of K corresponds to an archimedean valuation on K which extends the ordinary absolute value on the rational field \mathbf{Q} . The P -adic completion K_P is either the real field \mathbf{R} (in which case P is called a *real prime*), or else the complex field \mathbf{C} (and P is a *complex prime*).

(32.2) THEOREM. Let A be a central simple K -algebra, and let m_P be the local index of A at an infinite prime P of K .

(i) If P is a complex prime, then

$$A_P \sim K_P \quad \text{and} \quad m_P = 1.$$

(ii) If P is a real prime, then either

$$A_P \sim K_P \quad \text{and} \quad m_P = 1,$$

or else

$$A_P \sim H \quad \text{and} \quad m_P = 2,$$

where H is the skewfield of real quaternions (see Exercise 31.7).

Proof. Clearly $A_P \sim D$, where D is a skewfield with center K_P , and $(D:K_P)$ is finite. If P is complex, then $D = \mathbf{C} = K_P$ by Exercise 31.6. If P is real, then $K_P = \mathbf{R}$, and $D = \mathbf{R}$ or H by Exercise 31.8. This completes the proof.

If P is any finite prime of K , then K_P is a complete field relative to a discrete valuation, and has a finite residue class field. We saw in §31 how to define the

Hasse invariant $\text{inv} [A_P]$ of a central simple K_p -algebra, thereby obtaining an isomorphism $\text{inv}: B(K_p) \cong Q/Z$. We showed in fact (see (31.4) and (31.7)) that

$$(32.3) \quad \begin{cases} \text{inv} [A_p] = s_p/m_p, \text{ where } m_p = \text{index } [A_p], (s_p, m_p) = 1, \\ \exp [A_p] = m_p. \end{cases}$$

We would like to have the same formulas true for the case of infinite primes. First we must define Hasse invariants when P is an infinite prime, and in light of (32.2), it is sufficient to define these invariants for the three cases C , R and H . We set

$$(32.4) \quad \text{inv} [C] = 0, \quad \text{inv} [R] = 0, \quad \text{inv} [H] = \frac{1}{2}.$$

Formulas (32.3) then hold equally well when P is infinite, provided we know that $\exp [H] = \cdot 2$ when $[H]$ is considered as an element of $B(R)$. We have already observed this fact in Exercise 31.9.

Now let A be any central simple K -algebra, and let P be any prime of K (finite or infinite). Clearly,

$$A \sim K \Rightarrow A_p \sim K_p \text{ for all } P.$$

We shall prove the extremely important converse of this implication, by using the Hasse Norm Theorem (see below). First of all, we must review some facts from Galois theory. Some of these results have already been mentioned in §4 and §5c. Proofs are readily available in the references listed at the beginning of §4.

Let L be a finite Galois extension of K , with Galois group $G = \text{Gal}(L/K)$. Let P be a prime of K , finite or infinite. Even when P is a finite prime, it will be convenient to think of P as representing a class of valuations on K , rather than an ideal in some valuation ring. From this point of view, the valuation P extends to a finite set of inequivalent valuations on L , denoted by $p (= p_1), p_2, \dots, p_g$. For each $\sigma \in G$, there is a valuation p^σ on L , defined by the formula

$$p^\sigma(x) = p(\sigma^{-1} x), \quad x \in L.$$

We call p^σ a *conjugate* of p ; if p is a finite prime, then σ carries the valuation ring of p onto the valuation ring of p^σ . Whether or not p is finite, each p_i is of the form p^σ for some $\sigma \in G$.

Keeping the above notation, we set

$$(32.5) \quad G_p = \{\sigma \in G : p^\sigma = p\},$$

and call G_p the *decomposition group* of p relative to the extension L/K . The groups $\{G_{p_i}\}$ are mutually conjugate in G . Each $\sigma \in G_p$ induces a K_p -automorphism $\hat{\sigma}$ of the p -adic completion L_p , since σ maps each Cauchy sequence from L (relative to the p -adic valuation) onto another such sequence. The

map $\sigma \rightarrow \hat{\sigma}$ yields an isomorphism

$$(32.6) \quad G_p \cong \text{Gal}(L_p/K_p).$$

We define

$$(32.7) \quad n_p = (L_p : K_p) = \text{local degree of } L/K \text{ at } P.$$

Then

$$(32.8) \quad n_p = |G_p|, \quad \text{and } n_p | (L : K) \text{ for each } P.$$

It should be remarked that the fields $\{L_{p_i} : 1 \leq i \leq g\}$ are mutually K_p -isomorphic, so n_p does not depend on the choice of the prime p of L which extends P .

The next theorem is of fundamental importance for the entire theory of simple algebras over global fields. The proof depends on class field theory, and is beyond the scope of this book. Proofs may be found in Cassels–Fröhlich [1], Janusz [1], Neukirch [1], and Weil [1].

(32.9) **THEOREM** (Hasse Norm Theorem). *Let L be a finite cyclic extension of the global field K , and let $a \in K$. For each prime P of K , we choose a prime p of L which extends P . Then*

$$a \in N_{L/K}(L) \iff a \in N_{L_p/K_p}(L_p) \text{ for each } P.$$

Remarks. (i) The theorem asserts that a is a *global norm* (from L to K) if and only if at each P , a is a *local norm* (from L_p to K_p).

(ii) If p and p' are primes of L , both of which extend P , then there is a K_p -isomorphism $L_p \cong L_{p'}$, and therefore

$$N_{L_p/K_p}(L_p) = N_{L_{p'}/K_p}(L_{p'}).$$

This shows that in determining local norms at P , it does not matter which prime p of L we use, provided only that p is an extension of the valuation P from K to L .

(iii) By Exercise 32.3, every global norm is also a local norm at each P . The difficult part of the proof of Hasse's Norm Theorem is the converse: if $a \in K$ is a local norm at each P , then a is a global norm. In proving this, it is necessary to know that a is a local norm at *every* prime P of K , including the infinite primes.

(iv) The theorem breaks down if we drop the hypothesis that L/K be cyclic. There are counterexamples even when L/K is abelian (see Cassels–Fröhlich [1], Exercise 5]).

(32.10) **COROLLARY.** *Let $A = (L/K, \sigma, a)$ be a cyclic algebra, where $\text{Gal}(L/K) = \langle \sigma \rangle$ and $a \in K^*$. Then $A \sim K$ if and only if $A_p \sim K_p$ for each prime P of K .*

Proof. By (30.4),

$$A \sim K \Leftrightarrow a \in N_{L/K}(L^*).$$

On the other hand, we showed in (30.8) that for each P ,

$$A_P \sim (L_p/K_p, \sigma^k, a),$$

where σ^k is some generator of $\text{Gal}(L_p/K_p)$. Therefore by (30.4),

$$A_P \sim K_p \Leftrightarrow a \in N_{L_p/K_p}(L_p^*).$$

The desired result now follows from the Hasse Norm Theorem.

Clearly, we could have deduced (32.9) from (32.10), and so the next result may be regarded as a generalization of the Hasse Norm Theorem. Historically, it was first proved by use of (32.10).

(32.11) **Theorem** (Hasse–Brauer–Noether–Albert). *Let A be a central simple K -algebra. Then*

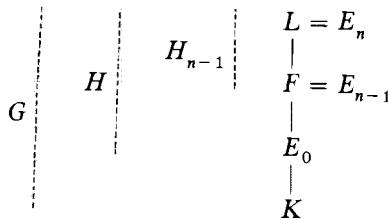
$$A \sim K \Leftrightarrow A_P \sim K_p \text{ for each prime } P \text{ of } K.$$

Proof. If $A \sim K$, then clearly $A_P \sim K_p$ for each P . We shall prove the converse by assuming that $A_P \sim K_p$ for each P , but that $m = \text{index } [A] > 1$, and obtaining a contradiction. By (28.11), there exists a finite galois extension L/K such that L splits A , that is, $L \otimes_K A \sim L$. Let $G = \text{Gal}(L/K)$, let p be some rational prime dividing m , and let H be a Sylow p -subgroup of G . Then $p \nmid [G:H]$, whereas $|H|$ is a power of p .

It is well known from group theory that H has a descending chain of subgroups

$$H = H_0 \supset H_1 \supset \cdots \supset H_n = 1, \quad [H_i : H_{i+1}] = p,$$

with $H_{i+1} \Delta H_i$ for each i . Let E_i be the subfield of L fixed by H_i , so $E_n = L$, and each E_{i+1}/E_i is a cyclic extension of degree p .



Let us set $B = F \otimes_K A$, a central simple F -algebra. Then

$$L \otimes_F B \cong L \otimes_K A \sim L,$$

so L splits B . Hence by Exercise 30.3, B is similar to a cyclic algebra $C = (L/F, \sigma, b)$, where $\text{Gal}(L/F) = \langle \sigma \rangle$ and $b \in F^*$. We intend to show that $B \sim F$, so it suffices for us to prove that $C \sim F$. By (32.10),

$$C \sim F \iff C_p \sim F_p \text{ for every prime } p \text{ of } F.$$

Given a prime p of F , its restriction to K is a prime P of K , and we have

$$\begin{aligned} C_p \sim B_p &= F_p \otimes_F B \cong F_p \otimes_K A \\ &\cong F_p \otimes_{K_P} A_P \sim F_p. \end{aligned}$$

This proves that C splits locally everywhere, whence $C \sim F$, and so $B \sim F$. We have thus shown that F splits the algebra A .

Repeat the argument, using the cyclic extension F/E_{n-2} in place of L/F . Then we find that E_{n-2} also splits A . Continuing in this manner, we see that E_0 splits A . But then $m|(E_0 : K)$ by (28.5). This is impossible, since $p \nmid m$ but $p \nmid (E_0 : K)$, and so the theorem is established.

(32.12) *Remarks* (i) For each prime P of K , there is a homomorphism $B(K) \rightarrow B(K_P)$, defined by $K_P \otimes_K \cdot$. Let $[A] \in B(K)$, and let m_p be the local index of A at P . Then $m_p = 1$ a.e., which means that $[A_p] = 1$ a.e. Hence there is a well defined homomorphism

$$B(K) \rightarrow \sum_p B(K_p).$$

The Hasse–Brauer–Noether–Albert Theorem is precisely the assertion that this map is monic.

(ii) A stronger result, due to Hasse, describes the image of $B(K)$ in $\sum_p B(K_p)$ by means of Hasse invariants. It can be shown (see references) that the following sequence is exact:

$$(32.13) \quad 1 \rightarrow B(K) \rightarrow \sum_p B(K_p) \xrightarrow{\text{inv}} Q/Z \rightarrow 0,$$

where *inv* denotes the Hasse invariant map, computed locally on each component: $\text{inv} = \sum_p \text{inv}_{K_p}$.

It follows from the exactness of (32.13) that

$$(32.13a) \quad \sum_p \text{inv} [A_p] = 0, \quad [A] \in B(K).$$

Of course, $\text{inv} [A_p] = 0$ if P is a complex prime, while $\text{inv} [A_p] = 0$ or $\frac{1}{2}$ if P is a real prime. The exactness of (32.13) also tells us that, other than (32.13a), these are the *only* conditions which the set of local invariants $\{\text{inv} [A_p]\}$ must

satisfy. In other words, suppose that we are given in advance any set of fractions $\{x_P\}$ from Q/Z , such that

$$\begin{cases} x_P = 0 & \text{a.e., } \sum x_P = 0 \\ x_P = 0 & \text{if } P \text{ is complex, } x_P = 0 \text{ or } \frac{1}{2} \text{ if } P \text{ is real.} \end{cases}$$

Then there exists a unique $[A] \in B(K)$ such that

$$\text{inv}[A_P] = x_P \text{ for all } P.$$

(iii) Some authors prove the exactness of (32.13) directly (see Cassels–Fröhlich [1], Neukirch [1]), and then deduce (32.9)–(32.11) as corollaries. To prove that (32.13) is exact, one shows first that the following sequence is exact:

$$(32.14) \quad 1 \rightarrow H^2(G_{L/K}, L^*) \rightarrow \sum_P H^2(G_{L_p/K_p}, L_p^*) \xrightarrow{\text{inv}} \frac{1}{n} Z/Z \rightarrow 0.$$

Here, L/K is any finite *cyclic* extension, and $n = (L:K)$; the direct sum extends over all primes P of K , and for each such P , the prime p is some prime of L extending P . The isomorphism obtained in (29.12) permits one to replace $H^2(G_{L/K}, L^*)$ by $B(L/K)$, and likewise for the terms in the direct sum. Finally, one proves

$$(32.14a) \quad B(K) = \bigcup_L B(L/K),$$

where L ranges over all finite cyclic extensions of K . In (28.12) we proved a weaker version of (32.14a), in which L ranges over all finite *galois* extensions. By (32.20) below, it suffices to consider only cyclic extensions. Formula (32.14a) can also be proved directly, without using the difficult Theorem 32.20. We may remark that if L/K is a finite galois extension, not necessarily cyclic, then the image of *inv* in (32.14) may be a proper subgroup of $(1/n)Z/Z$. For the proofs of the exactness of (32.13) and (32.14), the reader may consult the references listed above.

As a first application of (32.11), we give a simple criterion for deciding whether a finite extension of the global field K splits a given central simple K -algebra.

(32.15) **THEOREM.** *Let A be a central simple K -algebra. For each prime P of K , let $m_P = \text{index } [A_P]$. Let L be any finite extension of K , not necessarily a galois extension. Then L is a splitting field for A if and only if for each prime p of L ,*

$$(32.16) \quad m_p | (L_p : K_p),$$

where P is the restriction of p to K .

Proof. If P is the restriction to K of a prime p of L , then

$$L_p \otimes_{K_P} A_P \cong L_p \otimes_L (L \otimes_K A).$$

Hence if L splits A , then $L \otimes_K A \sim L$, whence $L_p \otimes_{K_P} A_P \sim L_p$, and so L_p splits A_P . Then (32.16) holds, by (28.5).

Conversely, suppose that (32.16) holds for each p . Then (for each p) L_p splits A_P , by (31.10). It follows that the central simple L -algebra $L \otimes_K A$ is split locally at every prime p of L . Hence by the Hasse–Brauer–Noether–Albert Theorem (32.11), $L \otimes_K A \sim L$. Therefore L splits A , as claimed, and the theorem is proved.

A second important consequence of (32.11) is

(32.17) THEOREM. Let A be a central simple K -algebra with local indices $\{m_p\}$, where P ranges over the primes of K . Set

$$m' = \text{L.C.M. } \{m_p\}.$$

Then $\exp [A] = m'$.

Proof. By (32.11),

$$[A]^t = 1 \text{ in } B(K) \iff [A_P]^t = 1 \text{ in } B(K_p) \text{ for each } P.$$

But $\exp [A_P] = m_p$ by (32.3), so $[A_P]^t = 1$ if and only if $m_p | t$. This proves that $[A]^t = 1$ if and only if t is divisible by each m_p . Hence $\exp [A] = m'$, as claimed.

We are going to prove below that whenever K is a global field, we have

$$\text{index } [A] = \exp [A], \quad [A] \in B(K).$$

We shall also prove that each central simple K -algebra A is in fact a *cyclic* algebra, so that (32.10) and (32.11) say exactly the same thing. The proofs will depend on the following result, whose proof is beyond the scope of this book:

(32.18) THEOREM (Grunwald–Wang). Let P_1, \dots, P_s be any set of distinct primes of the global field K . Let $\{m_{P_i} : 1 \leq i \leq s\}$ be positive integers, subject to the conditions: $m_p = 1$ if P is complex, $m_p = 1$ or 2 if P is real, where P ranges over the $\{P_i\}$. Let n be any positive integer divisible by each m_{P_i} , $1 \leq i \leq s$. Then there exists a cyclic extension L/K such that

$$(L:K) = n, \quad (L_p:K_p) = m_{P_i}, \quad P = P_1, \dots, P_s,$$

where p denotes any prime of L extending P .

Remarks. (i) For the proof of the Grunwald–Wang theorem, see Artin–Tate

[1, Ch. 10] or Neukirch [2]. Wang [1] gives the proof for the case where K is an algebraic number field.

(ii) For any Galois extension L/K and any prime P of K , we know that $(L_p : K_p)$ must divide $(L : K)$, by (32.8). Hence if L/K has local degree m_p at P , for $P = P_1, \dots, P_s$, then necessarily $(L : K)$ must be a multiple of m' , where

$$m' = \text{L.C.M.} \{m_{P_1}, \dots, m_{P_s}\}.$$

Hence if we seek a Galois extension L/K with prescribed local degrees $\{m_p\}$ at some preassigned finite set of primes $\{P_i\}$ of K , then m' is the smallest possible value for $(L : K)$. The Grunwald–Wang theorem tells us that not only can we find such a Galois extension L/K of degree m' , but in fact there always exists a cyclic extension of degree m' , with the prescribed local degrees. Further, we can force $(L : K)$ to be any preassigned multiple of m' , if desired.

We are now ready to prove

(32.19) **Theorem.** *Let $[A] \in B(K)$ have local indices $\{m_p\}$. Then*

$$\text{index } [A] = \exp [A] = \text{L.C.M.} \{m_p\}.$$

Proof. We know that $m_p = 1$ except possibly at some finite set of primes $\{P_1, \dots, P_s\}$ of K . We also know that $m_p = 1$ if P is complex, and that $m_p = 1$ or 2 if P is real. Let $m' = \text{L.C.M.} \{m_p\}$, so $m' = \exp [A]$ by (32.17). If $m = \text{index } [A]$, then $m' | m$ by (29.22).

On the other hand, by the Grunwald–Wang Theorem, there exists a cyclic extension L/K such that

$$(L : K) = m', \quad (L_p : K_p) = m_p, \quad P = P_1, \dots, P_s,$$

where as usual p denotes a prime of L extending P . Since the local degree $(L_p : K_p)$ is the same for each such p , and since $m_p = 1$ for $P \neq P_1, \dots, P_s$, it follows from (32.15) that L splits A . But then $m | (L : K)$, by (28.5i). Therefore $m = m'$, and the theorem is proved.

(32.20) **Theorem.** *Every central simple K -algebra is cyclic.*

Proof. Let A be a central simple K -algebra, let $(A : K) = n^2$, and let $\{m_p\}$ be the local indices of A . Since $(A_p : K_p) = n^2$, it follows that $m_p | n$ for each P . Further, $m_p = 1$ except (say) at P_1, \dots, P_s . By (32.18) it follows that we may find a cyclic extension E/K such that

$$(E : K) = n, \quad (E_p : K_p) = m_p, \quad P = P_1, \dots, P_s.$$

Then E splits A , and $(A : K) = (E : K)^2$. Hence, by Exercise 30.2, we may conclude that A is isomorphic to a cyclic algebra $(E/K, \sigma, a)$, where $\text{Gal}(E/K) = \langle \sigma \rangle$ and $a \in K^*$. This completes the proof.

Example. Let us determine some of the local Hasse invariants of the cyclic algebra $A = (L/K, \sigma, a)$, where $\text{Gal}(L/K) = \langle \sigma \rangle$ and $a \in K^*$. Let P denote a prime of K , and \mathfrak{p} an extension of P to L . Then by (30.8) we have

$$A_P \sim (L_{\mathfrak{p}}/K_P, \sigma^k, a),$$

where k is the least positive integer such that σ^k lies in the decomposition group $G_{\mathfrak{p}}$ of \mathfrak{p} relative to L/K . Of course, $\text{inv}[A_P] = 0$ whenever $A_P \sim K_P$.

(i) If P is complex, or if both P and \mathfrak{p} are real, then $A_P \sim K_P$.

(ii) Suppose that P is real, \mathfrak{p} complex. By Exercise 31.8 we have

$$A_P \sim K_P \quad \text{if } a_P > 0,$$

$$A_P \sim H \quad \text{if } a_P < 0,$$

where a_P represents the image of a under the embedding $K \rightarrow K_P$. In the latter case, $\text{inv}[A_P] = \frac{1}{2}$.

(iii) Let P be a finite prime, and assume that P is unramified in the extension L/K . This is equivalent to assuming that $L_{\mathfrak{p}}/K_P$ is unramified. Since $G_{\mathfrak{p}} = \langle \sigma^k \rangle$, we may choose $r \in \mathbb{Z}$ relatively prime to the local degree $n_{\mathfrak{p}} = |G_{\mathfrak{p}}|$, such that σ^{kr} is the Frobenius automorphism of the extension $L_{\mathfrak{p}}/K_P$. By (31.7) we obtain

$$\text{inv}[A_P] = r \cdot v_P(a)/n_{\mathfrak{p}},$$

where v_P is the exponential P -adic valuation. If we reduce the fraction $r \cdot v_P(a)/n_{\mathfrak{p}}$ to lowest terms, then $m_{\mathfrak{p}}$ is the denominator of the fraction thus obtained. In particular, we observe that $m_{\mathfrak{p}} = 1$ whenever $v_P(a) = 0$. Thus, $m_{\mathfrak{p}} = 1$ for every finite prime P , except possibly those primes P which ramify in L/K , or which contain a .

EXERCISES

Throughout these exercises, let A denote a central simple K -algebra, where K is a global field, and let P range over the primes of K .

1. Prove that either $A \sim K$, or else there are at least two primes of K which ramify in A . [Hint: Use (32.13a)].
2. Prove that no infinite primes of K are ramified in A , if index $[A]$ is odd.
3. Let L/K be a galois extension, \mathfrak{p} a prime of L extending the prime P of K . Let $G_{\mathfrak{p}}$ be the decomposition group of \mathfrak{p} relative to L/K , and write

$$G = \bigcup_{i=1}^n G_{\mathfrak{p}} \cdot \sigma_i, \quad n = [G : G_{\mathfrak{p}}].$$

For $x \in L$, let

$$f(x) = \prod_{i=1}^n \sigma_i(x) \in L.$$

Prove that

$$N_{L_p/K_p}(f(x)) = N_{L/K}(x).$$

Deduce that if $a \in K$ is a global norm (from L to K), then a is a local norm (from L_p to K_p) at each P . [Hint:

$$N_{L_p/K_p}(f(x)) = \prod_{\rho \in G_p} \prod_{i=1}^n \rho \sigma_i(x) = \prod_{\sigma \in G} \sigma(x) = N_{L/K}(x).$$

33. REDUCED NORMS

Throughout this section K is assumed to be a global field, unless otherwise stated. Let $\text{nr}_{A/K}: A \rightarrow K$ be the reduced norm map, where A is a central simple K -algebra, and let

$$\text{nr } A = \text{nr}_{A/K}(A) = \{\text{nr}_{A/K} a : a \in A\}.$$

Our aim is to determine the image $\text{nr } A$ explicitly.

Our first result, true for arbitrary fields K , enables us to reduce the problem to the case where A is a skewfield.

(33.1) THEOREM. Let $A = M_r(D)$, where D is a skewfield with center K (not necessarily a global field). Then

- (i) $\text{nr}_{A/K}(A) = \text{nr}_{D/K}(D)$.
- (ii) For $a \in A$, $\text{nr}_{A/K} a = 0$ if and only if a is a nonunit of A .

Proof. We shall omit the subscripts A/K and D/K when there is no danger of confusion. As in Exercise 9.5, let E be a splitting field for D , and let

$$\mu: D \rightarrow E \otimes_K D \cong M_s(E).$$

Then there is an embedding

$$A \rightarrow E \otimes_K A \cong M_{rs}(E),$$

given by

$$a = (\alpha_{ij})_{1 \leq i, j \leq r} \in M_r(D) \rightarrow (\mu(\alpha_{ij})) \in M_{rs}(E).$$

By definition of the reduced norm map, we have

$$\text{nr } a = \det(\mu(\alpha_{ij})), \quad a = (\alpha_{ij}) \in M_r(D).$$

In particular, if $a = (\alpha_{ij})$ is an upper triangular matrix, then

$$(33.2) \quad \text{nr } a = \prod_{i=1}^r \det(\mu(\alpha_{ii})) = \prod_{i=1}^r \text{nr } \alpha_{ii},$$

where $\text{nr } \alpha_{ii}$ means $\text{nr}_{D/K} \alpha_{ii}$. The same holds true if a is lower triangular.

Finally, let $t \in M_r(D)$ be any transposition matrix. From the identity

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix},$$

it follows at once that $\text{nr } t = \text{nr}_{D/K}(-1)$.

By an “elementary matrix” in $M_r(D)$ we shall mean a matrix e which coincides with the $r \times r$ identity matrix, except for having a single nonzero entry off the main diagonal. By (33.2), $\text{nr } e = 1$. Given an arbitrary $a \in A$, we can find matrices $p, q \in A$ which are products of elementary matrices and transpositions, such that

$$paq = \text{diag}(\alpha_1, \dots, \alpha_r), \quad \alpha_i \in D.$$

Note that $a \in u(A)$ if and only if each $\alpha_i \in u(D)$.

Since $\text{nr}_{A/K}$ is multiplicative, and since $\text{nr } p$ and $\text{nr } q$ can only have the values $\text{nr}_{D/K}(\pm 1)$, it follows that

$$\text{nr } a = \text{nr}(\pm \alpha_1 \cdots \alpha_r).$$

This implies (i) immediately. It also proves (ii), since $\text{nr}(\pm \alpha_1 \cdots \alpha_r) = 0$ if and only if some $\alpha_i = 0$.

Let P be a prime of K , and let the subscript P indicate P -adic completion. For any K -algebra A , the embedding

$$A \rightarrow K_P \otimes_K A = A_P$$

carries each $x \in A$ onto an element x_P of A_P . We have at once

(33.3) **THEOREM.** *Let A be a central simple K -algebra, and let P be a prime of K . Then*

$$\text{nr}_{A/K} x = \text{nr}_{A_P/K_P} x_P, \quad x \in A.$$

Proof. Use (9.28), with F replaced by K_P .

We call elements of $\text{nr } A$ *global* reduced norms, and those of $\text{nr } A_P$ *local* reduced norms. The above theorem tells us that every global reduced norm is also a local reduced norm at each P . We shall eventually prove the converse, when K is a global field. As a first step, let us determine which elements are local reduced norms.

(33.4) **Theorem.** *Let P be a prime of the global field K , and let B be any central simple K_P -algebra. Then*

$$\text{nr}_{B/K_P} B = K_P,$$

except for the special case where $K_P = R$ and $B \sim H$. In that case,

$$\text{nr } B = \text{nr } H = R^+ = \{\alpha \in R : \alpha \geq 0\}.$$

Proof. By (33.1) we may assume that B is a skewfield S with center K_P . If P is a finite prime, then $\text{nr } S = K_P$ by Exercise 14.6. If P is an infinite prime, then by (32.2) we have $S = K_P$ (and so also $\text{nr } S = K_P$), except for the special case where $K_P = \mathbf{R}$, $S = \mathbf{H}$. It remains for us to prove that $\text{nr } \mathbf{H} = \mathbf{R}^+$.

Let $a = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \in \mathbf{H}$, $\alpha_v \in \mathbf{R}$. Then (see (9.4)) we have

$$\text{nr}_{\mathbf{H}/\mathbf{R}} a = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \in \mathbf{R}^+.$$

Conversely, each $\alpha \in \mathbf{R}^+$ is expressible in the form α_0^2 , $\alpha_0 \in \mathbf{R}$. This shows that $\text{nr } \mathbf{H} = \mathbf{R}^+$, and completes the proof.

Now let A be a central simple K -algebra, where K is a global field, and let P be a prime of K . For $\alpha \in K$, let α_P denote its image in K_P . By (33.3), we have

$$(33.5) \quad \alpha \in \text{nr } A \implies \alpha_P \in \text{nr } A_P \text{ for each } P.$$

If we are trying to decide whether a given element $\alpha \in K$ is a global reduced norm, we must therefore first check whether α is a local reduced norm at each P . By (33.4), the condition that $\alpha_P \in \text{nr } A_P$ is automatically satisfied for every finite prime P , and also for every infinite prime P as well, except for the special case where $K_P = \mathbf{R}$ and $A_P \sim \mathbf{H}$. This special case can only arise when P is a real prime which is *ramified* in A , using the terminology introduced in §32.

Given the central simple K -algebra A , we define

$$(33.6) \quad U(A) = \{\alpha \in K : \alpha_P > 0 \text{ at each real prime } P \text{ of } K \text{ ramified in } A\}.$$

The preceding discussion then shows that for $\alpha \in K^*$,

$$(33.7) \quad \alpha_P \in \text{nr } A_P \text{ for all } P \iff \alpha \in U(A).$$

We intend to prove that $\alpha \in \text{nr } A$ if and only if $\alpha \in U(A)$, and we begin with two preliminary lemmas which are of interest in themselves.

(33.8) LEMMA. *Let K be any field complete with respect to a valuation $| \cdot |$. Let*

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in K[X]$$

be a separable irreducible polynomial. Set

$$L = K(\xi), \text{ where } \min. \text{ pol.}_K \xi = f(X).$$

Then for any polynomial

$$g(X) = b_1 X^{n-1} + \cdots + b_n \in K[X],$$

for which the values $|b_1|, \dots, |b_n|$ are sufficiently small, the polynomial $f(X) + g(X)$ is also irreducible and separable, and has a zero in L .

Proof. Step 1. The result is obvious when $n = 1$, so assume that $n > 1$ hereafter. Let us first settle the case where the valuation is archimedean, in

which case $K = R$ or C . Since $n > 1$, the only possibility is that $K = R$, $L = C$, and $f(X)$ is a quadratic polynomial with no real zeros. If the coefficients of $g(X)$ are sufficiently small, then also $f(X) + g(X)$ has no real zeros, so $f(X) + g(X)$ is irreducible in $K[X]$, and has a zero in L . Thus the result holds in this case.

Step 2. (Krasner's Lemma). For the rest of the proof, we assume that the valuation is non-archimedean, and that $n > 1$. Let \tilde{K} be an algebraic closure of K containing L , and extend $|\cdot|$ to a valuation on \tilde{K} as in §5b. Two elements γ, γ' in \tilde{K} are *conjugate* (over K) if $\gamma' = \phi(\gamma)$ for some K -automorphism ϕ of \tilde{K} ; this occurs if and only if γ and γ' have the same minimal polynomial over K . It follows from (5.5) that $|\gamma| = |\gamma'|$ whenever γ and γ' are conjugate.

Now let

$$f(X) = (X - \xi_1) \cdots (X - \xi_n), \quad \xi_i \in \tilde{K}, \quad \xi_1 = \xi,$$

and set

$$h = \min \{|\xi_i - \xi| : 2 \leq i \leq n\}.$$

Since $f(X)$ is separable by hypothesis, the elements $\xi_1, \dots, \xi_n \in \tilde{K}$ are distinct, and so $h > 0$. We shall prove that

$$(33.9) \quad \beta \in \tilde{K}, |\beta - \xi| < h \implies \xi \in K(\beta).$$

Suppose that (33.9) is false, and let β be a counterexample, so $\xi \notin K(\beta)$. Let $m(X) = \min_{K(\beta)} \xi$. Then $m(X) | f(X)$, and $m(X)$ has degree greater than 1. Since $f(X)$ has n distinct zeros, namely ξ_1, \dots, ξ_n , it follows that $m(\xi_i) = 0$ for some $\xi_i \neq \xi$. Therefore the elements $\beta - \xi$ and $\beta - \xi_i$ are conjugate over $K(\beta)$, hence over K , and so $|\beta - \xi| = |\beta - \xi_i|$. But then

$$|\xi - \xi_i| \leq \min(|\beta - \xi|, |\beta - \xi_i|) = |\beta - \xi| < h,$$

which contradicts the choice of h . We have thus proved (33.9), which may be rephrased as follows:

If $\beta \in \tilde{K}$ is closer to ξ than any conjugate of ξ , then $\xi \in K(\beta)$.

Step 3. We are now assuming that $n > 1$; it follows that $\xi \neq 0$, since otherwise $f(X)$ is reducible. Hence we may choose $d \in R$ such that

$$0 < d < |\xi|, \quad d \cdot |\xi|^{n-1} < h^n,$$

keeping the notation of Step 2. We shall show that if the coefficients of $g(X)$ are such that

$$|b_j| \leq d^j, \quad 1 \leq j \leq n,$$

then $f(X) + g(X)$ is irreducible, and has a zero in L .

We show first that

$$(33.10) \quad |a_j| \leq |\xi|^j, \quad 1 \leq j \leq n.$$

Indeed, for each such j , the coefficient a_j in $f(X)$ is (apart from sign) the elementary symmetric function of degree j in the quantities $\{\xi_1, \dots, \xi_n\}$. Since these elements are mutually conjugate over K , we have $|\xi_1| = \dots = |\xi_n|$. But then (33.10) follows at once, by using the properties (4.19 i–iv) of the valuation $| \cdot |$. (It should be pointed out that (33.10) is merely a restatement of Lemma 12.9.)

Next, for $1 \leq j \leq n$ we obtain

$$|b_j| \leq d^j < |\xi|^j,$$

whence

$$|a_j + b_j| \leq \max(|a_j|, |b_j|) \leq |\xi|^j.$$

If $\beta \in \tilde{K}$ is any zero of $f(X) + g(X)$, then $f(\beta) + g(\beta) = 0$, and so we conclude that

$$(33.11) \quad |\beta|^n = \left| \sum_{j=1}^n (a_j + b_j)\beta^{n-j} \right| \leq \max_{1 \leq j \leq n} \{|\xi|^j \cdot |\beta|^{n-j}\}.$$

If $|\xi| < |\beta|$, then

$$\max_{1 \leq j \leq n} \{|\xi|^j \cdot |\beta|^{n-j}\} < \max_{1 \leq j \leq n} \{|\beta|^n\} = |\beta|^n,$$

which contradicts (33.11). Therefore $|\beta| \leq |\xi|$. Furthermore,

$$\prod_{i=1}^n (\beta - \xi_i) = f(\beta) = -g(\beta) = -(b_1\beta^{n-1} + \dots + b_n).$$

This gives

$$\left\{ \min_{1 \leq i \leq n} |\beta - \xi_i| \right\}^n \leq \max_{1 \leq j \leq n} \{|b_j| |\beta|^{n-j}\} \leq \max_{1 \leq j \leq n} \{d^j \cdot |\xi|^{n-j}\} = d \cdot |\xi|^{n-1},$$

where the last step follows from the fact that $d < |\xi|$. Since $d \cdot |\xi|^{n-1} < h^n$, we conclude that

$$|\beta - \xi_i| < h \text{ for some } i, \quad 1 \leq i \leq n.$$

Now let ϕ be a K -automorphism of \tilde{K} such that $\phi(\xi_i) = \xi$; then

$$|\phi(\beta) - \xi| = |\beta - \xi_i| < h,$$

and $\phi(\beta)$ is also a zero of $f(X) + g(X)$. Set $\gamma = \phi(\beta)$, so γ is a zero of $f(X) + g(X)$, and $|\gamma - \xi| < h$. By Step 1, it follows that $\xi \in K(\gamma)$. Therefore

$$(K(\gamma):K) \geq (K(\xi):K) = n.$$

On the other hand, γ is a zero of the n th degree polynomial $f(X) + g(X)$. It

follows that this polynomial is irreducible in $K[X]$, and that $K(\gamma) = K(\zeta)$. Thus $\gamma \in L$, and $f(X) + g(X)$ is separable. This completes the proof.

Our second preliminary result is

(33.12) LEMMA. *Let R be a complete discrete valuation ring, with quotient field K and finite residue class field \bar{R} . Let W be an unramified extension of K of degree n . Then for each $\alpha \in u(R)$, there exists an element $y \in W$ such that*

$$N_{W/K} y = \alpha, \quad W = K(y).$$

Proof. The result is obvious when $n = 1$, so take $n > 1$ hereafter. Denote $N_{W/K}$ by N , for brevity. By (14.1) we know that $\alpha = Nx$ for some $x \in W$, and we must modify x so that it generates W . By (5.10) we may set $W = K(\omega)$, where ω is a primitive $(q^n - 1)$ th root of 1 over K , and $\text{card } \bar{R} = q$. Then W/K is a (separable) galois extension; its galois group is cyclic of order n , and is generated by the Frobenius automorphism σ , where $\sigma(\omega) = \omega^q$. Thus there is a one-to-one correspondence between the set of divisors of n , and the set of intermediate fields L between K and W . Consequently there are at most n such intermediate fields.

Let us put

$$L_j = K(x \cdot \omega^{j(q-1)}), \quad 0 \leq j \leq n-1.$$

We have

$$N\omega^{q-1} = \prod_{i=0}^{n-1} \sigma^i(\omega^{q-1}) = \omega^{(q-1)(1+q+\cdots+q^{n-1})} = 1.$$

Therefore

$$N(x \cdot \omega^{j(q-1)}) = Nx = \alpha, \quad 0 \leq j \leq n-1.$$

If $L_j = W$ for some j , then the desired element $y \in W$ such that $Ny = \alpha$, $W = K(y)$, can be chosen as $x \cdot \omega^{j(q-1)}$, and we are through. We shall now assume that each of the n fields L_0, \dots, L_{n-1} is a proper subfield of W , and we shall obtain a contradiction. We saw above that there are at most n fields between K and W , including the extreme cases K and W . Since each of the n fields $\{L_j : 0 \leq j \leq n-1\}$ is assumed to be distinct from W , it follows that two of the L 's must coincide. Suppose that $L_i = L_j$, where $0 \leq i < j \leq n-1$. Since $\alpha \in u(R)$ and $Nx = \alpha$, surely $x \neq 0$. Thus we may form the quotient

$$x \cdot \omega^{j(q-1)} / x \cdot \omega^{i(q-1)} \in L_i,$$

and so L_i contains an element $\omega^{t(q-1)}$, where $0 < t < n-1$. Now $(W:L_i) > 1$ by assumption, and therefore L_i is fixed by some σ^s , with $1 \leq s < n$, $s|n$. Thus $s \leq n/2$. The equation

$$\sigma^s(\omega^{t(q-1)}) = \omega^{t(q-1)}$$

yields the congruence

$$q^s \cdot t(q - 1) \equiv t(q - 1) \pmod{q^n - 1}.$$

Therefore $q^n - 1$ must divide the positive integer

$$\lambda = (q^s - 1)t \cdot (q - 1).$$

But

$$\lambda \leq (q^{n/2} - 1)(q - 1)(n - 2).$$

The reader will easily verify that the right hand expression is always less than $q^n - 1$. This gives the desired contradiction, and completes the proof of the lemma.

(33.13) COROLLARY. *Let R be a complete discrete valuation ring with quotient field K , prime element π , and finite residue class field \bar{R} . Then for each nonzero $\beta \in K$, and each positive integer n , there exists a monic separable irreducible polynomial $f(X) \in K[X]$ of degree n , with constant term $(-1)^n\beta$. Furthermore, if $\beta \in R$ then $f(X)$ may be chosen in $R[X]$.*

Proof. Given $\beta \in K^*$ and $n \geq 1$, we need only show that there exist a separable extension L/K of degree n , and an element $x \in L$ such that

$$\beta = N_{L/K} x, \quad L = K(x).$$

Once this is done, we may pick $f(X) = \min. \text{pol}_K x$. Then $f(X)$ is irreducible and has degree n , since $(L:K) = n$. Further, $f(X)$ is a separable polynomial because L/K is separable. We note also that if $\beta \in R$, then $f(X) \in R[X]$ by virtue of (12.2). The rest of the proof is devoted to showing how to find L and x .

Set $\beta = \pi^r \alpha$, $r \in \mathbf{Z}$, $\alpha \in u(R)$; then $v_K(\beta) = r$, where v_K is the exponential valuation associated with R (see §5b). If $n \nmid r$, then put $s = r/n \in \mathbf{Z}$, and choose W and y as in (33.12). Then

$$N_{W/K}(\pi^s y) = \pi^{ns} \alpha = \beta, \quad W = K(\pi^s y), \quad (W:K) = n.$$

Hence we may choose $L = W$, $x = \pi^s y$, in this case where $n \nmid r$.

We now turn to the case where $n \mid r$, and put

$$d = (n, r), \quad n = md, \quad r = sd, \quad \text{where } (m, s) = 1.$$

Since $n \nmid r$, it follows that $m \neq 1$, and thus that $m > 1$. Now let E/K be an unramified extension of degree d . Since $d \mid r$, we may deduce from the preceding paragraph that there exists an element $y \in E$ such that

$$N_{E/K} y = \beta, \quad E = K(y).$$

Now π is also a prime element for the valuation ring of E , since E/K is

unramified. Therefore by (5.6) we have

$$r = v_K(\beta) = v_E(\beta) = (E:K)v_E(y) = d \cdot v_E(y),$$

which shows that

$$v_E(y) = r/d = s.$$

Let us choose $t = |s| + 1$, and consider the separable polynomial

$$g(X) = X^m + \pi^t X + (-1)^m y \in E[X].$$

Let z be a zero of $g(X)$ in some algebraic closure of E , and set $L = E(z)$. Then L/E is a separable extension, and $(L:E) \leq m$. As in (5.6) we set

$$e = e(L/E), \quad f = f(L/E),$$

so $ef = (L:E) \leq m$, and $v_L(\pi) = e$. Since $g(z) = 0$, we have

$$(33.14) \quad v_L(y) \geq \min \{v_L(z^m), v_L(\pi^t z)\} = \min \{mh, et + h\},$$

where $h = v_L(z)$. If $mh \geq et + h$, then

$$(m - 1)h \geq et > 0.$$

Since $m > 1$, this would give $h > 0$, and then from (33.14) we would obtain

$$es = v_L(y) \geq et + h > et.$$

This is impossible, since $t = |s| + 1$, and so it follows that $mh < et + h$. But then (see (4.19a, (v)), the equation $g(z) = 0$ yields a sharper form of (33.14), namely,

$$es = v_L(y) = \min \{mh, et + h\} = mh.$$

Therefore $m|es$, whence $m|e$ since $(m, s) = 1$. This proves that $m = e$, and therefore L/E is a separable extension of degree m , such that $L = E(z)$. Since $y \in K(z)$ and $E = K(y)$, it follows that

$$L = K(z), \quad (L:K) = md = n, \quad L/K \text{ separable.}$$

Finally,

$$\beta = N_{E/K} y = N_{E/K}(N_{L/E} z) = N_{L/K} z$$

by Exercise 1.5. This completes the proof of the corollary.

With these preliminaries settled, we are now ready to prove the following important result:

(33.15) **Theorem.** (Hasse–Schilling–Maass). *Let A be a central simple K -algebra, where K is a global field, and let $\alpha \in K^*$. Then α is the reduced norm of an element of A if and only if $\alpha_P > 0$ at every infinite prime P of K ramified in A .*

Proof. Step 1. Since $\alpha \in K^*$, it follows from (33.1) that α is a reduced norm if and only if α is the reduced norm of an invertible element of A . We are trying to prove that

$$\text{nr}_{A/K} u(A) = U(A),$$

where $U(A)$ is defined by (33.6). Now

$$\alpha \in \text{nr } A \implies \alpha_P \in \text{nr } A_P \quad \text{for all } P \implies \alpha \in U(A),$$

by (33.5) and (33.7). Hence we need only prove that, conversely, $U(A) \subset \text{nr } A$. In what follows, let $\beta \in U(A)$.

Throughout this proof, let S denote the set of all infinite primes P of K which are ramified in A . Possibly S is the empty set. Choose S' to be a non-empty finite set of finite primes of K , including each finite P ramified in A . Then

$$P \notin S \cup S' \implies A_P \sim K_P.$$

Step 2. Let $(A:K) = n^2$. By (33.13), for each $P \in S'$ we may find a separable polynomial

$$f_P(X) = X^n + a_{1,P}X^{n-1} + \cdots + a_{n-1,P}X + (-1)^n\beta \in K_P[X]$$

such that $f_P(X)$ is irreducible over K_P . If the set S is empty, proceed directly to the next paragraph. If S is non-empty, then some infinite prime of K ramifies in A , so n is even by Exercise 32.2. We then set

$$f_P(X) = X^n + (-1)^n\beta \in K_P[X], \quad P \in S.$$

Given any $\varepsilon > 0$, by (4.11) we can choose a polynomial

$$f(X) = X^n + c_1X^{n-1} + \cdots + c_{n-1}X + (-1)^n\beta \in K[X],$$

such that

$$\begin{cases} \varphi_P(c_i - a_{i,P}) < \varepsilon, & 1 \leq i \leq n-1, \quad P \in S', \\ \varphi_P(c_i) < \varepsilon, & P \in S. \end{cases}$$

By (33.8), if we pick a sufficiently small ε , then $f(X)$ will be irreducible in $K[X]$ for each $P \in S'$. Hence $f(X)$ is also irreducible over K , since S' is non-empty. Furthermore, since $\beta \in U(A)$, we have $\beta_P > 0$ for each $P \in S$. Hence if ε is small enough, we can be sure that for each $P \in S$, the polynomial $f(X)$ has no zeros in the real field K_P .

Step 3. Now choose an element x in an algebraic closure of K , such that $f(x) = 0$, and set $L = K(x)$. Then

$$(L:K) = n, \quad \min. \text{pol}_K x = f(X), \quad N_{L/K} x = \beta.$$

We proceed to calculate the local degrees

$$n_p = (L_p : K_p), \quad P \in S \cup S',$$

where for each $P \in S \cup S'$, the prime p ranges over all primes of L extending P .

For each prime $P \in S$, the polynomial $f(X)$ has no real zeros in K_P . From the discussion in §5c, it follows that each prime p of L which extends P must be complex. Therefore $n_p = 2$ for each such p . On the other hand, for $P \in S'$ the polynomial $f(X)$ is irreducible in $K_P[X]$. Again using §5c, we may conclude that $n_p = n$, and indeed that there is only one p extending P .

Now let $\{m_p\}$ be the set of local indices of the central simple K -algebra A . Then surely $m_p | n$ for each P , and

$$m_p = 1, \quad P \notin S \cup S'; \quad m_p = 2, \quad P \in S.$$

Hence for every prime P of K , and every prime p of L extending P , it follows that $m_p | (L_p : K_p)$. Therefore L is a splitting field for A , by (32.15).

Finally, we note that

$$(A : K) = n^2 = (L : K)^2.$$

Since L splits A , it follows from (28.10) that we may embed L in A as a self-centralizing maximal subfield of A . Therefore

$$\beta = N_{L/K} x = \text{nr}_{A/K} x,$$

by Exercise 9.1, and the proof is finished.

Remark. In the above proof, we used the Strong Approximation Theorem (4.11). It would have been enough to apply a weaker version of (4.11), obtained by deleting from the conclusion of (4.11) the assertion that “ $b \in R_P$ for all $P \neq P_1, \dots, P_n$ ”. This weaker version is called the *Weak Approximation Theorem*, and is true for any domain R (not necessarily a Dedekind domain).

EXERCISES

1. Let K be a field with valuation $| \cdot |$, and $V = \sum_{i=1}^n K v_i$ a finite dimensional K -space. Define a *norm* on V by setting

$$\left\| \sum_{i=1}^n \alpha_i v_i \right\| = \max \{ |\alpha_1|, \dots, |\alpha_n| \}, \quad \alpha_i \in K.$$

Prove the following:

- (i) V is a metric space relative to this norm, with distance between two elements $v, v' \in V$ given by $\|v - v'\|$.
- (ii) This topology on V is independent of the choice of K -basis of V .
- (iii) If K is complete with respect to $| \cdot |$, then V is a complete metric space.

2. Let A be a central simple K -algebra, where K is a field with a valuation $\|\cdot\|$, and define a norm on A as in the preceding exercise. Let $\text{nr}: A \rightarrow K$ be the reduced norm map. Prove that nr is continuous, that is, if $x, y \in A$ are such that $\|x - y\|$ is small, then also $|\text{nr}(x) - \text{nr}(y)|$ is small. [Hint: Choose a field $E \supset K$ such that $(E:K)$ is finite, and E splits A . Extend the valuation $\|\cdot\|$ on K to a norm on E . Then prove that each of the following maps is continuous:

$$A \rightarrow E \otimes_K A, \quad E \otimes_K A \cong M_r(E), \quad \det: M_r(E) \rightarrow E,$$

where $(A:K) = r^2$.]

3. Let A be a central simple K -algebra, P a finite prime of K , R_P the P -adic valuation ring of K_P . Given a finite set of finite primes $\{P_1, P_2, \dots, P_r\}$, show that there exists an element $y \in A$ such that

$$\begin{cases} \text{nr}_{A/K} y = \text{prime element of } R_P, \\ \text{nr}_{A/K} y \in u(R_Q) \text{ for } Q = P_2, \dots, P_r. \end{cases}$$

[Hint: Extend the P -adic valuation φ_P on K_P to a norm $\|\cdot\|_P$ on A and A_P . By (33.4), there exists an $x_P \in A_P$ with $\text{nr } x_P = \pi_P$, a preassigned prime element of R_P . If $y_P \in A_P$ is chosen so that $\|y_P - x_P\|_P$ is sufficiently small, then

$$\text{nr } y_P \equiv \text{nr } x_P \pmod{\pi_P^2 R_P},$$

so $\text{nr } y_P$ is also a prime element of R_P . Now use (4.11) to choose $y \in A$ so that

$$\|y - x_P\|_P < \varepsilon, \|y - 1\|_Q < \varepsilon \text{ for } Q = P_2, \dots, P_r,$$

with ε small. If ε is sufficiently small, then $\text{nr } y$ will have the desired properties.]

4. Let L be a cyclic extension of the algebraic number field K , and let $A = (L/K, \sigma, a)$ be a cyclic algebra. When is A a totally definite quaternion algebra? (See (34.1).)

34. EICHLER'S THEOREM

The following notation remains in force throughout this section:

K = global field

R = Dedekind domain with quotient field K , $R \neq K$

K_P = P -adic completion of K at a prime P of K

φ_P = P -adic valuation on K and K_P (see §4e, 5a)

R_P = P -adic valuation ring in K_P , if P = finite prime
 $= \{x \in K_P : \varphi_P(x) \leq 1\}$

A = central simple K -algebra, $(A:K) = n^2$

m_P = index $[A_P]$ = local index of A at P

S = set of all infinite primes P of K for which $m_P > 1$
 $= \{P : P \text{ an infinite prime of } K \text{ ramified in } A\}$

$U(A) = \{\alpha \in K^* : \alpha_P > 0 \text{ for each } P \in S\}.$

(We remind the reader that the notation K_P, R_P is different from that of the

earlier chapters, where we had previously used R_P to denote the localization of R at a prime ideal P , and \hat{R}_P for the P -adic completion of R .)

According to the Hasse–Schilling–Maass Norm Theorem, we know that

$$\text{nr}_{A/K} u(A) = U(A),$$

a fact which we shall use repeatedly. In this section, we shall present Eichler's refinement of this Norm Theorem. The refinement deals with the problem:

Given a nonzero element $\beta \in R$, does there exist an element $x \in A$ such that $\text{nr}_{A/K} x = \beta$, and x is integral over R ?

In short, we wish to characterize reduced norms of integral elements. Obviously we must assume that $\beta \in U(A)$, since otherwise β cannot be a reduced norm. We shall find that the discussion below proceeds smoothly as long as A satisfies some mild restriction, called the *Eichler condition*. In the exceptional cases, where this condition fails to hold, many of the proofs and results given below are no longer valid. Our first task is to single out these exceptional cases, in which the Eichler condition does not hold. We shall begin with a number of definitions, the significance of which will not become apparent until we are in the middle of the proof of the preliminary Lemma 34.5 below. We shall follow the treatment given in Swan–Evans [1].

(34.1) *Definition.* Let K be an algebraic number field. A central simple K -algebra A is called a *totally definite quaternion algebra* if every infinite prime P of K is ramified in A , and if furthermore $A_P \cong H$ for each such P . Here, H denotes the quaternion skewfield over the real field K_P .

We remark that no complex prime of K can possibly ramify in A . Further, if A is a totally definite quaternion algebra, then

$$(A:K) = (A_P:K_P) = (H:\mathbf{R}) = 4, \quad P \in S.$$

Hence, A is a totally definite quaternion algebra if and only if *all* of the following conditions hold true:

- (i) $(A:K) = 4$,
- (ii) Every infinite prime of K is real,
- (iii) $A_P \cong H$ for every infinite prime P of K .

Equivalently, these mean that $(A:K) = 4$ and that S is the set of *all* infinite primes of K . It is clear that the quaternion algebra over \mathbf{Q} , defined in (9.4), is totally definite.

Totally definite quaternion algebras play the role of exceptions to the theory to be developed in this section. We shall need to find a corresponding class of exceptions for the case where the ground field is a function field. In order to do so, we introduce a bit of non-standard terminology. Let K be any global field, either an algebraic number field or a function field,

and let R be a Dedekind domain with quotient field K . Each nonzero prime ideal P of R gives rise to a prime of K , which we shall also denote by P , and refer to as a “prime of R ”. Those primes of K , which do *not* come from prime ideals of R , will be called “non- R ” primes of K . For example, when K is an algebraic number field and $R = \text{alg. int. } \{K\}$, the ring of all algebraic integers in K (see §4), then the “non- R ” primes of K are precisely the same as the infinite primes of K . (For the proof of this statement, see the references listed in §4.)

It will turn out (see proof of (34.5)) that the central simple K -algebras A , which are “exceptional” relative to R , are those which occur in the following situations:

(34.2) (i) A ramifies at every “non- R ” prime of K , and $(A:K) = 4$, where K is an algebraic number field, or

(ii) A ramifies at every “non- R ” prime of K , where K is a function field.

This leads to the following definition:

(34.3) *Definition.* The central simple K -algebra A satisfies the *Eichler condition relative to R* (notation: $A = \text{Eichler}/R$), if either

(i) K is an algebraic number field, and $(A:K) \neq 4$ if A ramifies at every “non- R ” prime of K , or

(ii) K is a function field, and some “non- R ” prime of K does not ramify in A .

(34.4) *Remark.* In particular, suppose that K is an algebraic number field, and $R = \text{alg. int. } \{K\}$. To say that “ A satisfies the Eichler condition relative to R ” means that either $(A:K) \neq 4$, or else $(A:K) = 4$ but A is not ramified at some infinite prime of K . In other words, in this case we have $A = \text{Eichler}/R$ if and only if A is *not* a totally definite quaternion algebra.

The proofs of the important theorems, given later in this section, will rely heavily on the following rather technical “approximation lemma”. The proof of this lemma requires the hypothesis that A be $\text{Eichler}/R$. We have stated the lemma in a fairly general version, since the extra generality does not make the proof any harder, and will be needed later.

(34.5) *LEMMA.* *We assume that*

(i) A is a central simple K -algebra satisfying the Eichler condition relative to R , with $(A:K) = n^2$,

(ii) S is the set of all infinite primes of K ramified in A ,

(iii) S' is some non-empty finite collection of primes of R , including all those which ramify in A ,

(iv) S'' is any finite collection (possible empty) of primes of R , such that S'' is disjoint from S' ,

- (v) β is a given element of $U(A) \cap R$,
 (vi) For each $P \in S' \cup S''$, we are given a polynomial

$$(34.6) \quad f_P(X) = X^n + b_{1,P}X^{n-1} + \cdots + b_{n-1,P}X + (-1)^n\beta \in R_P[X],$$

such that for each $P \in S'$, $f_P(X)$ is separable and irreducible over K_P .

Then for each $\varepsilon > 0$, there exists a polynomial

$$(34.7) \quad f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + (-1)^n\beta \in R[X],$$

satisfying all of the following conditions:

(C1) For each $P \in S' \cup S''$,

$$\varphi_P(a_i - b_{i,P}) < \varepsilon, \quad 1 \leq i \leq n-1.$$

(C2) For each $P \in S'$, $f(X)$ is irreducible over K_P .

(C3) The polynomial $f(X)$ is separable and irreducible over K .

(C4) For each $P \in S$, $f(X)$ has no zeros in the real field K_P .

Proof. Let $\varepsilon > 0$ be given. After replacing ε by a smaller positive number if need be, we may assume that $\varepsilon < 1$. We may further assume that the conclusion of Lemma 33.8 is valid whenever the coefficients $\{b_i\}$ occurring in (33.8) are subject to the condition that each $\varphi_P(b_i) < \varepsilon$. Our proof now splits into three cases.

Case 1. K = algebraic number field, $n \neq 2$.

For each value of i , $1 \leq i \leq n-1$, we are given a collection of elements

$$\{b_{i,P} \in R_P : P \in S' \cup S''\},$$

which occur as coefficients in the polynomials in (34.6). By the Strong Approximation Theorem (4.11), we may approximate these elements simultaneously by an element $a_i \in K$. Thus we may choose $a_i \in K$ so that

$$\begin{cases} \varphi_P(a_i - b_{i,P}) < \varepsilon & \text{for all } P \in S' \cup S'' \\ \varphi_Q(a_i) \leq 1 & \text{for all primes } Q \text{ of } R \text{ not in } S' \cup S''. \end{cases}$$

Since $\varepsilon < 1$, it follows that for each $P \in S' \cup S''$ we have $a_i - b_{i,P} \in R_P$, and hence also $a_i \in R_P$. But also $a_i \in R_Q$ for every prime Q of R not in $S' \cup S''$. Hence a_i is integral at every prime of R , and so $a_i \in R$.

We shall tentatively define $f(X)$ by formula (34.7), so (C1) surely holds true. By virtue of the restriction placed on ε at the beginning of this proof, it follows from (C1) and (33.8) that $f(X)$ is separable and irreducible over K_P , for each $P \in S'$. Thus (C2) is true, whence (C3) is also true, since S' is non-empty. Unfortunately, however, the polynomial $f(X)$ may fail to satisfy (C4).

If the set S is empty, (C4) is vacuous, and so the lemma is established in this case. Now suppose that S is not empty; then n is even, and hence $n > 2$, since we are considering here the case where $n \neq 2$. Let t be a positive rational integer, and consider the graph of the function $f(x) + tx^2$, where x is a real variable. Since n is even, it follows that by choosing t sufficiently large, we may be certain that the graph lies entirely above the x -axis. At the same time, we can make t divisible by a high power of each prime $P \in S' \cup S''$. Therefore we may choose t so that

$$\begin{cases} \varphi_P(t) < \varepsilon \text{ for all } P \in S' \cup S'', \\ f(X) + tX^2 \text{ has no zero in the real field } K_P, \text{ for each } P \in S. \end{cases}$$

Since $n > 2$, the polynomial $f(X) + tX^2$ is monic. Its coefficients satisfy the same inequalities (C1) as do those of $f(X)$. Hence if we use $f(X) + tX^2$ rather than the original $f(X)$, we have obtained a polynomial which satisfies the conditions (C1)–(C4), as desired.

Case 2. $K =$ algebraic number field, $n = 2$.

Since $n = 2$, and $A = \text{Eichler}/R$ by hypothesis, it follows from (34.3) that there exists at least one “non- R ” prime P_0 of K at which A does not ramify. Thus $P_0 \notin S \cup S' \cup S''$. We shall now imitate the proof given in Case 1, but this time we must use the Very Strong Approximation Theorem (4.40), rather than (4.11). For each value of i , where $1 \leq i \leq n - 1$, we may choose an element $a_i \in K$ such that

$$\begin{cases} \varphi_P(a_i - b_{i,P}) < \varepsilon \text{ for each } P \in S' \cup S'', \\ \varphi_Q(a_i) \leq 1 \text{ for every prime } Q \text{ of } R \text{ not in } S' \cup S'', \\ \varphi_P(a_i) < \varepsilon \text{ for every } P \in S. \end{cases}$$

This application of (4.40) is permissible, since no condition has been imposed on a_i at the prime P_0 .

As in the previous case, it follows that each $a_i \in R$, and we may again define $f(X) \in R[X]$ by formula (34.7). Just as before, $f(X)$ satisfies (C1)–(C3). Furthermore, since $n = 2$, we may write

$$f(X) = X^2 + a_1 X + \beta,$$

and by hypothesis $\beta_P > 0$ for each $P \in S$. Since $\varphi_P(a_1) < \varepsilon$ for each $P \in S$, it is clear that if ε is chosen sufficiently small, then $f(X)$ will have no zero in the real field K_P , for each $P \in S$. Thus $f(X)$ satisfies (C4), and this case is settled.

Case 3. $K =$ function field.

Since $A = \text{Eichler}/R$ by hypothesis, there exists a “non- R ” prime P_0 of K at which A is not ramified. The set S is empty, and $P_0 \notin S' \cup S''$, since $S' \cup S''$

is a collection of primes of R . Given polynomials (34.6) with P ranging over $S' \cup S''$, we use (4.40) to obtain an element $a_i \in K$ such that

$$\begin{cases} \varphi_P(a_i - b_{i,P}) < \varepsilon & \text{for each } P \in S' \cup S'', \\ \varphi_Q(a_i) \leqslant 1 & \text{for every prime } Q \text{ of } R \text{ with } Q \notin S' \cup S''. \end{cases}$$

As in the preceding case, this application of (4.40) is permissible, since we have imposed no condition on a_i at P_0 . We find as before that a_i is integral at every prime of R , and so $a_i \in R$. Now define $f(X)$ by formula (34.7). Just as in Case 1, the polynomial $f(X)$ satisfies (C1)–(C3), while (C4) is vacuous in this case. This completes the proof of the lemma.

As a first application of the preceding lemma, we prove the following result of Eichler:

(34.8) **Theorem.** *If A satisfies the Eichler condition relative to R , then every $\beta \in R \cap U(A)$ is the reduced norm of some element of A integral over R .*

Proof. We may choose S and S' as in (34.5), with S'' empty. Let $\beta \in R \cap U(A)$ be given. For each $P \in S'$, it follows from (33.13) that we may find a separable irreducible polynomial

$$f_P(X) = X^n + b_{1,P}X^{n-1} + \cdots + b_{n-1,P}X + (-1)^n\beta \in R_P[X],$$

with constant term $(-1)^n\beta$. By (34.5), we may then find a separable irreducible polynomial

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + (-1)^n\beta \in R[X],$$

satisfying conditions (C1)–(C4) of (34.5). The discussion in Step 3 of the proof of (33.15) carries over unchanged. It shows that there exists an element $x \in A$ such that

$$f(x) = 0, \quad \beta = \text{nr}_{A/K} x.$$

But then x is integral over R , since $f(x) = 0$, and so the theorem is established.

Before proceeding to the statement and proof of Eichler's Theorem below, we shall recall some definitions from §22. A *normal ideal* in A is a full R -lattice L in A whose left and right orders are maximal R -orders in A . If L is a normal ideal with left order Λ , right order Λ' , then we call L a *principal* ideal if $L = \Lambda x$ for some $x \in A$. In this case,

$$\Lambda' = x^{-1}\Lambda x, \quad L = x\Lambda',$$

so in speaking about principal ideals, it does not matter whether we deal with the left order or the right order of L .

We are now ready to prove the following important result:

(34.9) **Theorem.** (Eichler). *Let A be a central simple K -algebra satisfying the Eichler condition relative to R . Let L be any normal ideal in A . Then L is a principal ideal if and only if its reduced norm $\text{nr}_{A/K} L$ is a principal ideal $R\alpha$ for some $\alpha \in U(A)$.*

Proof. For brevity, we write nr instead of $\text{nr}_{A/K}$. Let L be a normal ideal in A , and let $\Lambda = O_i(L)$, a maximal R -order in A . If L is principal, then $L = \Lambda x$ for some $x \in u(A)$. By (24.12) we obtain

$$\text{nr } L = \text{nr } \Lambda x = R \cdot \text{nr } x,$$

and $\text{nr } x \in U(A)$ by (33.15). We must prove that, conversely, if $\text{nr } L = R\alpha$ for some $\alpha \in U(A)$, then L is principal. We shall assume hereafter that $n > 1$, where $(A:K) = n^2$, since the result is obvious when $n = 1$.

Step 1. Throughout the proof, let $d = d(\Lambda/R)$ be the discriminant of the maximal order Λ (see §25). Then d is a nonzero ideal in R , and for each prime P of R we have (by (32.1))

$$A_P \sim K_P \quad \text{if and only if} \quad P \nmid d.$$

By Exercise 26.8, there are only finitely many conjugacy classes of maximal R -orders in A . Let

$$\Lambda_1 (= \Lambda), \Lambda_2, \dots, \Lambda_\kappa$$

be a full set of representatives of these conjugacy classes. Then each maximal R -order in A is of the form $u\Lambda_i u^{-1}$ for some $u \in u(A)$ and some i between 1 and κ . Choose once and for all a nonzero element $r \in R$ such that $r \notin u(R)$, and

$$(34.10) \quad r\Lambda_i \subset \Lambda, \quad i = 1, \dots, \kappa.$$

We temporarily fix a prime P of R such that $P \nmid rd$, and let M, N be a pair of maximal left ideals of Λ such that $\text{nr } M = \text{nr } N = P$ (see (24.13)). In Step 4, we shall prove that necessarily $M = N\theta$ for some $\theta \in u(\Lambda)$. The remainder of Step 1, and the material in Steps 2 and 3, will be needed in Step 4.

Let us draw some consequences from the hypothesis that $P \nmid rd$. As remarked above, it follows that $A_P \sim K_P$, so $A_P \cong M_n(K_P)$. Since Λ_P is a maximal R_P -order in A_P by (11.5), it follows from (17.3) and (17.5) that

$$\Lambda_P \cong M_n(R_P), \quad \text{rad } \Lambda_P = P \cdot \Lambda_P.$$

Let us set

$$\bar{\Lambda} = \Lambda/P\Lambda \cong \Lambda_P/P\Lambda_P, \quad \bar{R} = R/P \cong R_P/PR_P.$$

Then

$$(34.11) \quad \bar{\Lambda} \cong M_n(\bar{R}) \cong \text{Hom}_{\bar{R}}(V, V),$$

where V is the vector space consisting of all $n \times 1$ column vectors with entries in \bar{R} . We may view V as a simple left $\bar{\Lambda}$ -module.

Since K is a global field, \bar{R} is a finite field, and hence $\bar{\Lambda}$ is a finite ring. Thus we may choose a finite set of elements $\tau_1, \dots, \tau_g \in \Lambda$ such that

$$(34.12) \quad u(\bar{\Lambda}) = \{\bar{\tau}_1, \dots, \bar{\tau}_g\}.$$

Let $\Lambda_{(P)}$ denote the *localization* of Λ at P . By (18.3) we have

$$\text{rad } \Lambda_{(P)} = \Lambda_{(P)} \cap \text{rad } \Lambda_P = \Lambda_{(P)} \cap P \cdot \Lambda_P = P \cdot \Lambda_{(P)}.$$

Since

$$\Lambda_{(P)}/\text{rad } \Lambda_{(P)} = \Lambda_{(P)}/P\Lambda_{(P)} \cong \bar{\Lambda},$$

it follows from Exercise 6.2 that each τ_j is a unit in $\Lambda_{(P)}$. Hence we may choose an element $t \in R - P$ such that

$$(34.13) \quad t \cdot \tau_j^{-1} \in \Lambda, \quad j = 1, \dots, g.$$

For later use, we note that $P \nmid t$.

Step 2. We use the notation of Lemma 34.5, choosing S' to be the set of all primes of R which either ramify in A or which divide the principal ideal $rt \cdot R$. (Possibly some prime divisors of $rt \cdot R$ may ramify in A .) Since $r \notin u(R)$, the set S' is non-empty. We choose S'' to consist of the single prime $\{P\}$, so S'' is disjoint from S' .

We are going to find a collection of polynomials $\{f_Q(X) : Q \in S'\}$ and a polynomial $f_P(X)$, with certain properties. Once this is done, we shall approximate these polynomials by a polynomial in $R[X]$, by using (34.5). To begin with, we claim that for each $Q \in S'$, we may find a polynomial

$$f_Q(X) = X^n + b_{1,Q}X^{n-1} + \cdots + b_{n-1,Q}X + (-1)^n \in R_Q[X],$$

such that

$$(34.14) \quad \begin{cases} f_Q(X) \text{ is separable and irreducible over } K_Q, \\ f_Q(X) \equiv (X - 1)^n \pmod{Q^{nm}}, \end{cases}$$

where Q^m is the power of Q occurring in $rt \cdot R$. (Congruence of polynomials means coefficientwise congruence.)

For each prime $Q \in S'$, we proceed as follows: let $W = K_Q(\omega)$ be an unramified extension of degree n , with Frobenius automorphism σ , where ω is a primitive $(q^n - 1)$ -th root of 1, $q = \text{card } R_Q$. Let π be a prime element of R_Q . By Exercise 34.4, we may choose a positive integer $k \geq nm$ so large that

$$(34.15) \quad u \equiv 1 \pmod{\pi^k R_Q} \implies u = \gamma^n \text{ for some } \gamma \in R_Q, \gamma \equiv 1 \pmod{\pi^{nm} R_Q}.$$

Having done so, we set

$$g(X) = \min. \text{pol.}_{K_Q}(1 + \pi^k \omega) \in R_Q[X].$$

Then $g(X)$ is a separable irreducible polynomial of degree n , and its zeros are $\{1 + \pi^k \omega^{q^i} : 0 \leq i \leq n-1\}$. Therefore $g(X) \equiv (X - 1)^n \pmod{\pi^k}$. Let us write

$$g(X) = X^n + c_1 X^{n-1} + \cdots + c_{n-1} X + (-1)^n u.$$

Since $u \equiv 1 \pmod{\pi^k}$, it follows from (34.15) that $u = \gamma^n$ for some $\gamma \in u(R_Q)$ such that $\gamma \equiv 1 \pmod{\pi^{nn'}}$. We now set

$$\begin{aligned} f_Q(X) &= \gamma^{-n} g(\gamma X) \\ &= X^n + \gamma^{-1} c_1 X^{n-1} + \cdots + \gamma^{-(n-1)} c_{n-1} X + (-1)^n \in R_Q[X]. \end{aligned}$$

Then the polynomial $f_Q(X)$ satisfies conditions (34.14).

Finally, we shall choose $f_P(X) \in R_P[X]$ as in Exercise 34.1, so that $f_P(X)$ is a monic n th degree polynomial whose image $\bar{f}_P(X)$ in $\bar{R}[X]$ has no zeros in the field $\bar{R} = R/P$, and such that $f_P(X)$ has constant term $(-1)^n$.

Step 3. We have thus constructed a set of polynomials $\{f_Q(X) : Q \in S'\}$ and a polynomial $f_P(X)$, all having constant term $(-1)^n$. We apply Lemma 34.5 with $\beta = 1$, and with the sets S, S', S'' as defined in Step 2. Then there exists a separable irreducible polynomial

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + (-1)^n \in R[X],$$

such that $f(X)$ is coefficientwise near $f_Q(X)$ for each $Q \in S' \cup S''$. Now S' includes all primes of R which divide $rt \cdot \bar{R}$, as well as all primes of R ramified in A . If we choose ε in (34.5) sufficiently small, then our polynomial $f(X)$ will satisfy all of the following conditions:

- (i) $\bar{f}(X)$ has no zero in $\bar{R}[X]$, where $\bar{R} = R/P$.
- (ii) $f(X) \equiv (X - 1)^n \pmod{(rt)^n}$.
- (iii) $f(X)$ is irreducible over K_Q , for each $Q \in S'$.
- (iv) $f(X)$ has no zeros in K_Q , for each $Q \in S$.

Now let x be a zero of $f(X)$ in some algebraic closure of K , and set $L = K(x)$. As in the proof of (34.8), we may embed L in A . Then x is an element of A integral over R , and $\text{nr } x = 1$. By Exercise 25.3, x^{-1} is also integral over R . We now set

$$y = (x - 1)/rt \in A.$$

We may write $f(X) = (X - 1)^n + (rt)^n h(X)$, where $h(X) \in R[X]$ by virtue of (ii). Then $f(x) = 0$ implies that $y^n = -h(x) \in R[x]$, and hence by (1.11) y^n is integral over R . Therefore y is also integral over R , and so there exists a maximal R -order in A containing y . Replacing x and y by suitable conjugates if need be, we may assume that $y \in \Lambda_i$ for some choice of i between 1 and κ . Then $ry \in \Lambda$ by (34.10), so also

$$x = 1 + rty \in \Lambda.$$

Since x^{-1} is integral over R , it follows that $x \in u(\Lambda)$.

Let us set

$$(34.16) \quad x_j = \tau_j x \tau_j^{-1} = 1 + \tau_j \cdot r y \cdot t \tau_j^{-1} \in \Lambda, \quad 1 \leq j \leq g,$$

where the fact that $x_j \in \Lambda$ follows from (34.13). Then $\text{nr } x_j = \text{nr } x = 1$, so each $x_j \in u(\Lambda)$.

Step 4. We are now ready to prove the assertion: given any pair of maximal left ideals M, N in the maximal R -order Λ , such that

$$\text{nr } M = \text{nr } N = P, \text{ where } P \nmid rd,$$

then $M = N\theta$ for some $\theta \in u(\Lambda)$. We keep the notation of (34.11), so V is a left $\bar{\Lambda}$ -module, and hence also a left Λ -module. By (2.7) there is a natural isomorphism

$$(34.17) \quad \text{Hom}_\Lambda(\Lambda, V) \cong V, \quad \varphi \mapsto \varphi(1).$$

Recall that the action of an element $\lambda \in \Lambda$ on an element $\varphi \in \text{Hom}_\Lambda(\Lambda, V)$ is given by

$$(\lambda\varphi)\xi = \varphi(\xi\lambda), \quad \xi \in \Lambda.$$

Since $\text{nr } M = P$, it follows from (24.14) that Λ/M is a simple left $\bar{\Lambda}$ -module, and likewise for Λ/N . Hence there exist a pair of Λ -exact sequences

$$0 \rightarrow M \rightarrow \Lambda \xrightarrow{\varphi} V \rightarrow 0, \quad 0 \rightarrow N \rightarrow \Lambda \xrightarrow{\psi} V \rightarrow 0,$$

with

$$M = \ker \varphi, \quad N = \ker \psi, \quad V = \Lambda\varphi(1) = \Lambda\psi(1).$$

Case 1. Suppose that the elements $\varphi(1), \psi(1)$ of the \bar{R} -space V are linearly dependent over \bar{R} . Then there exists an $a \in R - P$ such that $\varphi(1) = a \cdot \psi(1)$. But then $(\varphi - a\psi)(1) = 0$, so by (34.17) we conclude that $\varphi - a\psi = 0$. Therefore $\ker \varphi = \ker \psi$, since $\bar{a} \neq 0$. This gives $M = N$, so the assertion at the start of Step 4 is proved in this case.

Case 2. Now suppose that $\varphi(1)$ and $\psi(1)$ are linearly independent elements of the \bar{R} -space V . In Step 3 we constructed an $x \in \Lambda$ such that $f(x) = 0$. Let \bar{x}_L denote left multiplication by \bar{x} on the $\bar{\Lambda}$ -module V . Then $\bar{f}(\bar{x}_L) = 0$, whence

$$\min. \text{pol.}_{\bar{R}} \bar{x}_L \text{ divides } \bar{f}(X).$$

Since $\bar{f}(X)$ has no zeros in \bar{R} , it follows that the \bar{R} -linear transformation \bar{x}_L on V has no characteristic root in \bar{R} . Hence for each nonzero $v \in V$, the vectors v and $\bar{x}v$ are linearly independent over \bar{R} . Choose a nonzero $v \in V$. Then the pair $\{v, \bar{x}v\}$ are part of an \bar{R} -basis of V . So also are the pair $\{\varphi(1), \psi(1)\}$. Hence there exists an invertible linear transformation T on V such that

$$T: \varphi(1) \rightarrow v, \quad \psi(1) \rightarrow \bar{x}v.$$

Since $\bar{\Lambda} \cong \text{Hom}_{\bar{R}}(V, V)$, T must be given by left multiplication by some unit $\bar{\tau}_j \in u(\bar{\Lambda})$. Therefore

$$\bar{\tau}_j \cdot \varphi(1) = v, \quad \bar{\tau}_j \cdot \psi(1) = \bar{x}v,$$

for some j between 1 and g . These give

$$\psi(1) = \bar{\tau}_j^{-1} \bar{x} \bar{\tau}_j \cdot \varphi(1) = \bar{x}_j \varphi(1),$$

where x_j is defined by (34.16). In view of the natural isomorphism (34.17), we obtain $\psi = x_j \varphi$. Therefore

$$\begin{aligned} N = \ker \psi &= \ker x_j \varphi = \{\xi \in \Lambda : (x_j \varphi)(\xi) = 0\} \\ &= \{\xi : \varphi(\xi x_j) = 0\} = \{\xi : \xi x_j \in M\} = M x_j^{-1}. \end{aligned}$$

This shows that $M = Nx_j$, with $x_j \in u(\Lambda)$, and completes the proof of the assertion made at the beginning of this Step.

Step 5. Suppose to start with that J is any left ideal in the maximal R -order Λ . By (22.18) we may express J as a proper product

$$(34.18) \quad J = M_1 \cdots M_k, \quad M_i = \text{maximal integral ideal}.$$

Then by (24.11),

$$\text{nr } J = (\text{nr } M_1) \cdots (\text{nr } M_k),$$

and each $\text{nr } M_i$ is a prime ideal of R (by (24.13)). Hence the number of factors k is uniquely determined by $\text{nr } J$. Furthermore, if P is a prime of R dividing $\text{nr } J$, then $\text{nr } M_i = P$ for some i , $1 \leq i \leq k$. Indeed, by (22.28) or Exercise 22.7, we can find a factorization of J in which $\text{nr } M_1 = P$. (This important fact may also be proved directly, as follows: given the ideal J , define

$$J^* = \Lambda \cap J_P \cap \bigcap_{Q \neq P} \Lambda_Q,$$

where Q ranges over all primes of R except P . By (5.3) it follows that J^* is a left ideal of Λ such that

$$J^* \supset J, \quad J_P^* = J_P, \quad J_Q^* = \Lambda_Q \quad \text{for all } Q \neq P.$$

Then $\text{nr } J^*$ is a power of P , and $J = J^* \cdot J^{**}$ (proper product) for some integral ideal J^{**} , by (22.19). When we express J^* as a proper product of maximal integral ideals, each factor will have reduced norm P . Hence we obtain a factorization (34.18) in which $\text{nr } M_1 = P$.)

Now let J and J' be any pair of left ideals of Λ . We shall prove that

$$(34.19) \quad \left. \begin{array}{l} \text{nr } J = \text{nr } J' \\ \text{nr } J + rd = R \end{array} \right\} \Rightarrow J' = Jx \text{ for some } x \in u(A).$$

Let P be a prime of R dividing $\text{nr } J$. Then we may write

$$J = M_1 M_2 \cdots M_k, \quad J' = N_1 N_2 \cdots N_k,$$

where

$$\text{nr } M_1 = \text{nr } N_1 = P,$$

and where the M 's and N 's are maximal integral ideals. There are as many factors in J' as in J , since $\text{nr } J' = \text{nr } J$.

We shall establish (34.19) by induction on k . By Step 4, we know that $M_1 = N_1 z$ for some $z \in u(\Lambda)$, which proves the result when $k = 1$. Suppose now that $k > 1$, and that the result holds (for all maximal orders) for products of $k - 1$ maximal integral ideals. We may write

$$J' = N_1 z \cdot (z^{-1} N_2 z) \cdots (z^{-1} N_k z) \cdot z^{-1} = N_1 z \cdot \tilde{J} \cdot z^{-1},$$

where

$$\tilde{J} = (z^{-1} N_2 z) \cdots (z^{-1} N_k z) = z^{-1} (N_2 \cdots N_k) z.$$

It is easily verified that both \tilde{J} and $M_2 \cdots M_k$ are left ideals in the maximal order Λ' , where

$$\begin{aligned} \Lambda' &= O_l(M_2) = O_r(M_1) = O_r(N_1 z) = z^{-1} O_r(N_1) z \\ &= z^{-1} O_l(N_2) z = O_l(z^{-1} N_2 z) = O_l(\tilde{J}). \end{aligned}$$

Furthermore,

$$\text{nr } \tilde{J} = \text{nr } M_2 \cdots M_k, \quad \text{nr } \tilde{J} + rd = R.$$

It follows from the induction hypothesis that

$$\tilde{J} = M_2 \cdots M_k w \quad \text{for some } w \in u(A).$$

Therefore

$$J' = N_1 z \cdot \tilde{J} \cdot z^{-1} = M_1 M_2 \cdots M_k w z^{-1} = J \cdot w z^{-1},$$

which completes the proof of (34.19).

Step 6. We are now ready to prove the theorem. Let L be any normal ideal in A such that $\text{nr } L = R\alpha$, where $\alpha \in U(A)$, and let $\Lambda = O_l(L)$. We must show that $L = \Lambda x$ for some $x \in u(A)$. By (27.7) we can choose $y \in u(A)$ such that

$$Ly \subset \Lambda, \quad Ly + rd\Lambda = \Lambda.$$

Set $L' = Ly$, $\alpha' = \alpha \cdot \text{nr } y$. Then also $\Lambda = O_l(L')$, and $\alpha' \in U(A)$ by (33.15). If we can prove that $L' = \Lambda z$ for some $z \in u(A)$, then $L = \Lambda zy^{-1}$ is also principal.

Changing notation, we may hereafter assume that L is a left ideal of Λ such that

$$L + rd\Lambda = \Lambda, \quad \text{nr } L = R\alpha, \quad \alpha \in R \cap U(A).$$

Let us show that

$$(34.20) \quad R\alpha + rd = R.$$

At each prime P of R dividing rd , we have

$$L_P + rd\Lambda_P = \Lambda_P$$

whence

$$L_P + P\Lambda_P = \Lambda_P.$$

By Nakayama's Lemma, this implies that $L_P = \Lambda_P$. Therefore

$$(\text{nr } L)_P = \text{nr } L_P = \text{nr } \Lambda_P = R_P,$$

which proves that $P \nmid \text{nr } L$. Thus (34.20) is established.

We next observe that since $\alpha \in R \cap U(A)$ it follows from (34.8) that $\alpha = \text{nr } w$ for some $w \in u(A)$ integral over R . If $w \in \Lambda$, then we obtain

$$\text{nr } L = \text{nr } \Lambda w, \quad \text{nr } L + rd = R,$$

and hence $L = (\Lambda w)w'$ for some $w' \in u(A)$, by (34.19). Thus the desired result holds when $w \in \Lambda$. The manipulations which follow are needed to take care of the possibility that $w \notin \Lambda$. By Exercise 10.5, the ring $R[w]$ is contained in some maximal R -order Λ' in A . Consider the normal ideal $(\Lambda'\Lambda)^{-1}$ in A , with the left order Λ and right order Λ' . As in the first paragraph of this step, we may choose an element $z \in u(A)$ such that

$$(\Lambda'\Lambda)^{-1}z \subset \Lambda, \quad \text{nr } \{(\Lambda'\Lambda)^{-1}z\} + rd = R.$$

Let us set

$$M = (\Lambda'\Lambda)^{-1}z, \quad \text{so } M \subset \Lambda, \quad \text{nr } M + rd = R.$$

Then $N(M) + rd = R$ by (24.11), and we have

$$N(M) = \text{ord}_R \Lambda/M \subset M$$

by Exercise 27.4. Hence we may choose an element $\gamma \in N(M)$ such that

$$\gamma R + rd = R,$$

and we note that $\gamma \in R \cap M$. Therefore

$$\gamma \cdot z^{-1}wz \in M \cdot z^{-1}\Lambda'z = M \cdot O_r(M) \subset M \subset \Lambda,$$

and so $L' = \Lambda \cdot \gamma \cdot z^{-1}wz$ is a left ideal of Λ . Also $L\gamma$ is a left ideal of Λ , since $\gamma \in R$. We have

$$\text{nr } L\gamma = (\text{nr } L)(\text{nr } \gamma) = R\alpha\gamma^n,$$

$$\text{nr } L' = R \cdot \text{nr } \gamma \cdot \text{nr } z^{-1}wz = R\gamma^n \cdot \alpha,$$

since $\text{nr } w = \alpha$ by the choice of w . Both α and γ are prime to rd . It follows from (34.19) that $L\gamma = Lx'$ for some $x' \in u(A)$, whence $L = \Lambda x$ for some $x \in u(A)$, as desired. This completes the proof of Eichler's Theorem.

(34.21) COROLLARY. Let Λ be a maximal R -order in A , where $A = \text{Eichler}/R$. Let L, L' be left Λ -ideals in A . Then

$$L = Lx \text{ for some } x \in u(A) \iff \text{nr } L = \alpha(\text{nr } L) \text{ for some } \alpha \in U(A).$$

Proof. If $L = Lx$, then $\text{nr } L = (\text{nr } x)(\text{nr } L)$, and $\text{nr } x \in U(A)$. Conversely, let $\text{nr } L = \alpha(\text{nr } L)$ where $\alpha \in U(A)$. Let $\Lambda' = O_r(L)$, and consider the proper product $L^{-1} \cdot L$. Then

$$\text{nr}(L^{-1} \cdot L) = (\text{nr } L)^{-1} (\text{nr } L) = R\alpha,$$

and $L^{-1}L$ has left order Λ' . By Eichler's Theorem, we may write $L^{-1}L = \Lambda'x$ for some $x \in u(A)$. Then

$$L = LL^{-1} \cdot L = L \cdot \Lambda' x = Lx,$$

as desired. This completes the proof.

Eichler's Theorem (34.9) requires the hypothesis that A be Eichler/ R . Without this hypothesis, Eichler [1] showed that the conclusion of the theorem need not hold true. In his example, A is a totally definite quaternion algebra, and $R = \text{alg. int. } \{K\}$. He proved that (for suitable choice of A) there may exist a non-principal normal ideal L in A , such that $\text{nr}_{A/K} L = R\alpha$ for some $\alpha \in U(A)$.

EXERCISES

1. Let $\bar{R} = R/P$ be a finite field, where P is a prime of R , and let $n > 1$. Show that there exists a polynomial

$$f(X) = X^n + c_1 X^{n-1} + \cdots + c_{n-1} X + (-1)^n \in \bar{R}[X],$$

such that $f(X)$ has no zeros in \bar{R} . [Hint: Let $\text{card } \bar{R} = q$. The number of polynomials

$$h(X) = X^n + c_1 X^{n-1} + \cdots + c_{n-1} X + (-1)^n \in \bar{R}[X]$$

equals q^{n-1} . If $h(X)$ has a zero λ in \bar{R} , then there is a factorization

$$h(X) = (X - \lambda)(X^{n-2} + \cdots + (-1)^{n-1} \lambda^{-1}).$$

There are at most $q - 1$ choices for λ , and at most q^{n-2} choices for the factor of degree $n - 2$. Thus, the number of polynomials $h(X)$ with a zero in \bar{R} is $\leq (q - 1)q^{n-2}$. Hence there are at least

$$q^{n-1} - (q - 1)q^{n-2}$$

polynomials $h(X) \in \bar{R}[X]$ with no zero in \bar{R} . Pick one such $h(X)$, and choose $f(X) \in R[X]$ with $\bar{f} = h$.]

In Exercises 2–4 below, R is a complete discrete valuation ring with exponential valuation v , prime element π , residue class field \bar{R} .

2. Let n be a positive integer, and set $n = \pi^e \alpha$, $\alpha \in u(R)$. Prove that for each positive integer r ,

$$(1 + \pi^r X)^n = 1 + \alpha \pi^{e+r} X + \pi^{2r} g(X),$$

for some $g(X) \in R[X]$.

3. Let $\alpha \in u(R)$, $\beta \in R$, $g(X) \in R[X]$, and let m be a positive integer. Set

$$h(X) = \pi^m g(X) + \alpha X - \beta.$$

Show that $h(X)$ has a zero in R . [Hint: If bars denote passage to \bar{R} , then

$$\bar{h}(X) = \bar{\alpha}X - \bar{\beta} = \alpha(X - \bar{\beta}\bar{\alpha}^{-1}).$$

By Hensel's Lemma, this factorization of $\bar{h}(X)$ lifts to a factorization $h(X) = u(X)v(X)$ in $R[X]$, with $u(X)$ monic, $\bar{u}(X) = X - \bar{\beta}\bar{\alpha}^{-1}$.]

4. Let m, n be positive integers. Show that there exists a positive integer k such that for $u \in R$,

$$u \equiv 1 \pmod{\pi^k} \implies u = \gamma^n \text{ for some } \gamma \in R \text{ such that } \gamma \equiv 1 \pmod{\pi^m}.$$

[Hint (Neukirch [1]): Let $n = \pi^e \alpha$, $\alpha \in u(R)$. We may assume that $m > e$. Choose $k \geq m + e$, and set $u = 1 + \pi^k \beta$, $\beta \in R$, and $\gamma = 1 + \pi^m x$. We need only show that the equation

$$1 + \pi^k \beta = (1 + \pi^m x)^n$$

has a solution with $x \in R$. By Exercise 2, the equation becomes

$$1 + \pi^k \beta = 1 + \alpha \pi^{m+e} x + \pi^{2m} g(x)$$

for some $g(X) \in R[X]$. Hence we must solve

$$\pi^{m-e} g(x) + \alpha x - \beta \pi^{k-(m+e)} = 0, \quad x \in R.$$

Now use Exercise 3.]

35. IDEAL CLASS GROUPS

Throughout this section, let R be a Dedekind domain with quotient field K , and let Λ be a maximal R -order in a central simple K -algebra A . We shall eventually restrict our attention to the case where K is a global field, so as to have available Eichler's Theorem and its consequences, but for the moment K may be arbitrary. We shall define the *ideal class group* of Λ denoted by $\mathrm{Cl} \Lambda$, and shall show how to calculate it. The definition will be such that in the special case where $\Lambda = R$, $\mathrm{Cl} \Lambda$ will coincide with the ideal class group $\mathrm{Cl} R$ defined in §4.

By a *left Λ -ideal* in A we mean, as usual, a left Λ -lattice M in A such that $KM = A$. As in §26, two left Λ -ideals M, N in A are placed in the same *ideal class* if $M \cong N$ as left Λ -modules, or equivalently, if $M = Nx$ for some $x \in u(A)$. Let us attempt to define a group structure on this set of ideal classes. Given any two left Λ -ideals M, N in A , their product $M \cdot N$ is also a left Λ -ideal in A . However, when A is non-commutative, the ideal class of $M \cdot N$ is not necessarily determined by the ideal classes of M and N . Specifically, for each $x \in u(A)$, the ideal Mx is in the same class as M , but possibly $Mx \cdot N$ and $M \cdot N$ are in different classes.

Steinitz's Theorem (4.13) suggests one way of overcoming this difficulty. The theorem states (as a special case) that given any two left R -ideals J, J' in K , then

$$(35.1) \quad J \dot{+} J' \cong R \dot{+} JJ' \text{ as } R\text{-modules,}$$

and furthermore,

$$(35.2) \quad R \dot{+} J \cong R \dot{+} J' \Leftrightarrow \text{class of } J = \text{class of } J' \Leftrightarrow J \cong J'.$$

These results show that the ideal class of the product JJ' can be computed unambiguously from the structure of J and J' as R -modules.

In (27.4) we obtained a partial generalization of Steinitz's Theorem. A special case of (27.4) asserts that given any pair of left Λ -ideals M, M' in A , there exists a left Λ -ideal M'' in A such that

$$(35.3) \quad M \dot{+} M' \cong \Lambda \dot{+} M'' \text{ as } \Lambda\text{-modules.}$$

The isomorphism types of M and M' uniquely determine the isomorphism type of the direct sum $M \dot{+} M'$, and hence that of $\Lambda \dot{+} M''$. This suggests a way of defining a binary operation on ideal classes. It is customary to write this operation additively, so we tentatively define

$$\text{ideal class of } M + \text{ideal class of } M' = \text{ideal class of } M''$$

whenever (35.3) holds true. In order to prove that the operation is well defined, we would need to establish a "cancellation theorem" analogous to (35.2). Specifically, we would need to prove that if M, N are any left Λ -ideals in A , then

$$(35.4) \quad \Lambda \dot{+} M \cong \Lambda \dot{+} N \implies M \cong N.$$

Unfortunately, there are examples in which (35.4) is false (see Swan [1]).

The fact that (35.4) is not always true forces us to introduce a new equivalence relation on the set of Λ -ideals, weaker than isomorphism. It is convenient to define this relation not only for Λ -ideals, but more generally for Λ -modules. Given any two left Λ -modules X, Y , we call X *stably isomorphic*

to Y if there exists a non-negative integer r such that

$$X \dot{+} \Lambda^{(r)} \cong Y \dot{+} \Lambda^{(r)} \text{ as left } \Lambda\text{-modules.}$$

It is easily verified that stable isomorphism is an equivalence relation on the set of all left Λ -modules. Clearly, isomorphism implies stable isomorphism, but not conversely (in general). Let $[X]$ denote the stable isomorphism class of the Λ -module X .

(35.5) THEOREM. *Let $\text{Cl } \Lambda$ denote the set of stable isomorphism classes of left Λ -ideals in A . Define an additive structure on $\text{Cl } \Lambda$ as follows: given any pair of left Λ -ideals M, M' in A , we set*

$$[M] + [M'] = [M''],$$

where M'' is any left Λ -ideal in A such that

$$M \dot{+} M' \cong \Lambda \dot{+} M''.$$

Then $\text{Cl } \Lambda$ is an abelian additive group, with identity element $[\Lambda]$.

Proof. Given M and M' , the existence of an ideal M'' such that (35.3) holds, is guaranteed by (27.4). It is worth pointing out that if M'' is a left Λ -module satisfying (35.3), then in fact M'' is isomorphic to a left Λ -ideal in A (see Exercise 35.1).

Let us show that addition of stable isomorphism classes is well defined. Let N, N' be left Λ -ideals in A such that

$$[M] = [N], \quad [M'] = [N'], \quad N \dot{+} N' \cong \Lambda \dot{+} N''.$$

Then there exists an $s \geq 0$ such that

$$M \dot{+} \Lambda^{(s)} \cong N \dot{+} \Lambda^{(s)}, \quad M' \dot{+} \Lambda^{(s)} \cong N' \dot{+} \Lambda^{(s)}.$$

But then $[M''] = [N'']$, since

$$M'' \dot{+} \Lambda^{(2s+1)} \cong M \dot{+} M' \dot{+} \Lambda^{(2s)} \cong N \dot{+} N' \dot{+} \Lambda^{(2s)} \cong N'' \dot{+} \Lambda^{(2s+1)}.$$

Thus addition is well defined. It is easily verified that addition is associative and commutative, and that

$$[\Lambda] + [M] = [M] \quad \text{for all } [M] \in \text{Cl } \Lambda.$$

It remains to prove the existence of inverses. Any left Λ -ideal M in A is Λ -projective, by (21.5). Hence there exists a left Λ -lattice Y such that

$$M \dot{+} Y \cong \Lambda^{(t)} \text{ for some } t.$$

By Exercise 35.1, Y is isomorphic to a submodule of $\Lambda^{(t-1)}$. Therefore by (27.8) there exists a left Λ -ideal N in A such that

$$Y \cong N + \Lambda^{(t-2)},$$

so we now have

$$M + N + \Lambda^{(t-2)} \cong \Lambda^{(t)}.$$

Let $M + N \cong \Lambda + L$ for some left Λ -ideal L in A ; then $[M] + [N] = [L]$, by the definition of addition of stable isomorphism classes. However,

$$L + \Lambda^{(t-1)} \cong L + \Lambda + \Lambda^{(t-2)} \cong M + N + \Lambda^{(t-2)} \cong \Lambda^{(t)},$$

so $[L] = [\Lambda]$. Thus $[M] + [N] = 0$ in $\text{Cl } \Lambda$, and so inverses exist. This completes the proof that $\text{Cl } \Lambda$ is a group.

It follows at once from (35.1) and (35.2) that when $\Lambda = R$, the group $\text{Cl } \Lambda$ coincides with the class group $\text{Cl } R$ defined in §4. It should also be remarked that when K is a global field and Λ is any maximal R -order, then the ideal class group $\text{Cl } \Lambda$ is necessarily a finite group, by the Jordan–Zassenhaus Theorem (26.4).

For the remainder of this section, we shall restrict our attention to the case where K is a global field. Let us introduce the *ray class group* $\text{Cl}_A R$; this is a modified version of $\text{Cl } R$, with the modification depending on the given central simple K -algebra A . We shall use the following notation:

- $I(R)$ = multiplicative group of R -ideals in K ,
- $P(R)$ = subgroup of principal ideals = $\{R\alpha : \alpha \in K^*\}$,
- $\text{Cl } R = I(R)/P(R)$ = ideal class group of R ,
- S = set of all infinite primes of K ramified in A ,
- $U(A) = \{\alpha \in K^* : \alpha_P > 0 \text{ for each } P \in S\}$,
- $P_A(R) = \{R\alpha : \alpha \in U(A)\}$ = ray group $(\text{mod } S)$,
- $\text{Cl}_A R = I(R)/P_A(R)$ = ray class group $(\text{mod } S)$.

The groups $P_A(R)$ and $P(R)$ may coincide, even when S is non-empty; this certainly occurs when $R = \mathbf{Z}$, for example. In general, $P_A(R)$ is a subgroup of $P(R)$, and there is an epimorphism $\sigma : \text{Cl}_A R \rightarrow \text{Cl } R$. By Exercise 35.2, $\ker \sigma$ is a finite elementary abelian 2-group.

The main result of this section is the fact that the reduced norm map on Λ -ideals induces an isomorphism $\text{Cl } \Lambda \cong \text{Cl}_A R$ if K is an algebraic number field. This isomorphism also holds for the function field case, if we assume that A satisfies the Eichler condition relative to R . Eichler's Theorem (34.9) plays a key role in the proof of these results. We may restate Corollary 34.21 of Eichler's Theorem in our present notation, as follows:

(35.6) THEOREM. *Let K be a global field, and let Γ be a maximal R -order in a central simple K -algebra B , where $B = \text{Eichler}/R$. For each left Γ -ideal L in B , let $v(L)$ denote the class of the R -ideal $\text{nr}_{B/K} L$ in the ray class group $\text{Cl}_B R$.*

Then for each pair of left Γ -ideals L, L' in B , we have

$$L \cong L' \text{ as } \Gamma\text{-modules} \iff v(L) = v(L').$$

A preliminary calculation is necessary before we can apply this result. Given the central simple K -algebra A , we set $B = M_r(A)$, where $r \geq 1$. Then B is also central simple over K , and a prime of K ramifies in B if and only if it ramifies in A . Hence $P_A(R) = P_B(R)$, and the ray class group $\text{Cl}_B R$ coincides with $\text{Cl}_A R$. Let $\Gamma = M_r(\Lambda)$, so by (8.7) Γ is a maximal R -order in B . Each left Γ -ideal L in B determines an element $v(L) \in \text{Cl}_A R$, where

$$(35.7) \quad v(L) = \text{image of } \text{nr}_{B/K} L \text{ in } \text{Cl}_A R.$$

Let us recall from §24 that by definition,

$$\text{nr}_{B/K} L = \{N_{B/K} L\}^{1/s}, \text{ where } (B:K) = s^2.$$

Further, if $L \subset \Gamma$ then

$$N_{B/K} L = \text{ord}_R \Gamma / L.$$

We are now ready to prove

(35.8) **LEMMA.** *Let $r \geq 1$, and let*

$$B = \text{Hom}_A(A^{(r)}, A^{(r)}) \cong M_r(A),$$

where $A^{(r)}$ is viewed as a left A -, right B -bimodule. Let

$$\Gamma = \text{Hom}_\Lambda(\Lambda^{(r)}, \Lambda^{(r)}) \cong M_r(\Lambda).$$

To each left Λ -lattice X in $A^{(r)}$ there corresponds a left Γ -lattice $\varphi(X)$ in B , given by $\varphi(X) = \text{Hom}_\Lambda(\Lambda^{(r)}, X)$. If $X = J_1 + \cdots + J_r$, where each J_i is a left Λ -ideal in A , then

$$(35.9) \quad \text{nr}_{B/K} \varphi(X) = \prod_{i=1}^r \text{nr}_{A/K} J_i.$$

Therefore

$$(35.10) \quad v\{\varphi(X)\} = \prod_{i=1}^r v(J_i) \text{ in } \text{Cl}_A R,$$

where $v(J_i)$ denotes the class of $\text{nr}_{A/K} J_i$ in $\text{Cl}_A R$.

Proof. The left Λ -module $\Lambda^{(r)}$ is a progenerator for the category ${}_\Lambda \mathcal{M}$. Hence by (15.9) or (16.14), there is an equivalence of categories

$$\varphi: {}_\Lambda \mathcal{M} \rightarrow {}_\Gamma \mathcal{M}, \text{ where } \varphi = \text{Hom}_\Lambda(\Lambda^{(r)}, \cdot).$$

Then φ maps $\Lambda^{(r)}$ onto Γ , and carries each Λ -submodule X of $\Lambda^{(r)}$ onto a

left ideal $\varphi(X)$ in Γ . By tensoring with the field K , we find readily that φ carries each Λ -lattice X in $A^{(r)}$ onto a Γ -lattice $\varphi(X)$ in B . The correspondence $X \rightarrow \varphi(X)$ is one-to-one, and preserves isomorphism.

Now let X be any Λ -lattice in $A^{(r)}$ such that $KX = A^{(r)}$. By (27.8) we may write $X = J_1 + \cdots + J_r$, where each J_i is a left Λ -ideal in A . Since the reduced norm is multiplicative, it suffices to prove formulas (35.9) and (35.10) for the case where $X \subset \Lambda^{(r)}$, and each $J_i \subset \Lambda$. We have a commutative diagram

$$\begin{array}{ccc} \varphi(X) = \text{Hom}_\Lambda(\Lambda^{(r)}, X) & \cong & X + \cdots + X \text{ (r copies)} \\ \downarrow & & \downarrow \\ \varphi(\Lambda^{(r)}) = \text{Hom}_\Lambda(\Lambda^{(r)}, \Lambda^{(r)}) & \cong & \Lambda^{(r)} + \cdots + \Lambda^{(r)} \text{ (r copies),} \end{array}$$

where the vertical arrows are inclusions, and the indicated isomorphisms are R -isomorphisms. Therefore

$$N_{B/K} \varphi(X) = \text{ord}_R \varphi(\Lambda^{(r)}) / \varphi(X) = \{\text{ord}_R \Lambda^{(r)} / X\}^r.$$

But

$$\text{ord}_R \Lambda^{(r)} / X = \prod_{i=1}^r \text{ord}_R \Lambda / J_i = \prod_{i=1}^r N_{A/K} J_i.$$

If $(A:K) = n^2$, then $(B:K) = r^2n^2$, and so

$$N_{A/K} = \{\text{nr}_{A/K}\}^n, \quad N_{B/K} = \{\text{nr}_{B/K}\}^{rn}.$$

Hence we obtain

$$\{\text{nr}_{B/K} \varphi(X)\}^{rn} = \left\{ \prod_{i=1}^r \{\text{nr}_{A/K} J_i\}^n \right\}^r,$$

which gives (35.9) at once. Formula (35.10) follows from (35.9) by taking images in $\text{Cl}_A R$, and the proof is complete.

(35.11) COROLLARY. Let K be a global field, and keep the above notation. Let $r \geq 1$, and let

$$X = \sum_{i=1}^r J_i, \quad X' = \sum_{i=1}^r J'_i,$$

where each J_i and J'_i is a left ideal in A . Then

- (i) $X \cong X'$ as Λ -modules if and only if $\varphi(X) \cong \varphi(X')$ as Γ -modules.
- (ii) If $X \cong X'$, then $v\varphi(X) = v\varphi(X')$, that is,

$$(35.12) \quad \prod_{i=1}^r v(J_i) = \prod_{i=1}^r v(J'_i).$$

- (iii) If $A = \text{Eichler}/R$, then $X \cong X'$ if and only if (35.12) holds.

(iv) Let K be an algebraic number field and let $r \geq 2$. Then $X \cong X'$ if and only if (35.12) holds true, even when $A \neq \text{Eichler}/R$.

Proof. Assertion (i) has already been established at the beginning of the proof of (35.8). From (35.8) we also know that

$$v\varphi(X) = \prod_{i=1}^r v(J_i), \quad v\varphi(X') = \prod_{i=1}^r v(J'_i).$$

If $X \cong X'$, then $\varphi(X) = \varphi(X') \cdot b$ for some $b \in u(B)$. Therefore $v\varphi(X) = v\varphi(X')$ since $(\text{nr}_{B/K} b)R \in P_B(R)$, and (ii) is proved.

Suppose for the moment that $A = \text{Eichler}/R$; then also $B = \text{Eichler}/R$. Hence by (35.6) we know that $\varphi(X) \cong \varphi(X')$ if and only if $v\varphi(X) = v\varphi(X')$, and this establishes (iii).

Finally, suppose that K is an algebraic number field and $r \geq 2$. Then $B = \text{Eichler}/R$, whether or not $A = \text{Eichler}/R$. Indeed, if $A \neq \text{Eichler}/R$, then $(A:K) = 4$; but then $(B:K) = 4r^2 > 4$, so necessarily $B = \text{Eichler}/R$. But once we know that $B = \text{Eichler}/R$, we may use (35.6) to deduce that $\varphi(X) \cong \varphi(X')$ if and only if $v\varphi(X) = v\varphi(X')$. This gives assertion (iv) and completes the proof of the corollary.

Let us record an important special case of (35.11).

(35.13) COROLLARY. *Keep the above notation, and let J, J' be left Λ -ideals in A . Let $[J]$ denote the stable isomorphism class of J .*

- (i) *If $A = \text{Eichler}/R$, then $[J] = [J']$ if and only if $J \cong J'$.*
- (ii) *Let K be an algebraic number field. Whether or not $A = \text{Eichler}/R$, we have*

$$[J] = [J'] \iff J + \Lambda \cong J' + \Lambda.$$

Proof. By definition of stable isomorphism, $[J] = [J']$ if and only if $J + \Lambda^{(r)} \cong J' + \Lambda^{(r)}$ for some $r \geq 0$. By (35.10),

$$v\varphi(J + \Lambda^{(r)}) = v(J).$$

Hence if $[J] = [J']$, then $v(J) = v(J')$. Therefore $J \cong J'$ by (35.11 iii), if $A = \text{Eichler}/R$. This proves assertion (i).

Now let K be an algebraic number field. From $v(J) = v(J')$ it follows that

$$v\varphi(J + \Lambda) = v\varphi(J' + \Lambda).$$

Therefore $J + \Lambda \cong J' + \Lambda$ by (35.11 iv), which completes the proof of the corollary.

We are now ready to prove

(35.14) **Theorem** (Swan [1]). *Keep the above notation. If K is an algebraic number field, or if K is a function field and $A = \text{Eichler}/R$, then the reduced norm map induces an isomorphism*

$$\nu : \text{Cl } \Lambda \cong \text{Cl}_A R.$$

Here, $\text{Cl } \Lambda$ is the additive group of stable isomorphism classes of left Λ -ideals in A , and $\text{Cl}_A R$ the multiplicative ray class group (mod S), where S is the set of all infinite primes of K which ramify in A .

Proof. Let J, J' denote left Λ -ideals in A . We shall define the map ν on $\text{Cl } \Lambda$ by setting

$$\nu[J] = \nu(J) = \text{image of } \text{nr}_{A/K} J \text{ in } \text{Cl}_A R.$$

It follows from the proof of (35.13) that ν is well defined on $\text{Cl } \Lambda$, since we showed there that if $[J] = [J']$, then $\nu(J) = \nu(J')$.

Now let $J + J' \cong \Lambda + J''$ for some Λ -ideal J'' . Then $\nu(J)\nu(J') = \nu(J'')$ by (35.11 ii). Therefore

$$\nu\{[J] + [J']\} = \nu[J''] = \nu[J]\nu[J'],$$

so ν is a homomorphism. If $\nu[J] = 1$, then $\nu(J) = \nu(\Lambda)$. By virtue of the hypotheses of this theorem, we may apply (35.13) to conclude that $J + \Lambda \cong \Lambda + \Lambda$. Therefore $[J] = [\Lambda] = 0$ in $\text{Cl } \Lambda$, and thus ν is monic.

Finally, the group $I(R)$ is the free abelian group generated by the nonzero prime ideals P of R . Given P , we may find a maximal integral ideal J of Λ such that $P\Lambda \subset J \subset \Lambda$. Then $\text{nr}_{A/K} J = P$ by (24.13), and so $\nu[J]$ equals the image of P in $\text{Cl}_A R$. This shows that ν is epic, and completes the proof of the theorem.

Remarks. (i) If $A = \text{Eichler}/R$, then there is a one-to-one correspondence between $\text{Cl}_A R$ and the set of isomorphism classes of left Λ -ideals in A .

(ii) Some of the preceding theorems extend to non-maximal orders. We refer the reader to Fröhlich [1], Jacobinski [1, 2], Roggenkamp [1], Swan-Evans [1], Wilson [1]. Fröhlich's article contains a different proof of (35.14), based on an idele-theoretic version of Eichler's Theorem.

EXERCISES

- Let L, M be left Λ -lattices such that $KL \cong A^{(r)}$, $KM \cong A^{(s)}$, and let X be any left Λ -module such that

$$L + M \cong \Lambda + X.$$

Show that X is isomorphic to a left Λ -submodule of $\Lambda^{(r+s-1)}$. [Hint: Since X is isomorphic to a submodule of the Λ -lattice $L + M$, it follows that X is also a Λ -lattice. Tensor the given isomorphism with K , to obtain

$$A^{(r)} \dot{+} A^{(s)} \cong A \dot{+} KX.$$

Hence $KX \cong A^{(r+s-1)}$ by Exercise 6.7. Replacing X by an isomorphic copy, we may assume that $KX = A^{(r+s-1)} = K \cdot \Lambda^{(r+s-1)}$. We may then choose a nonzero $\alpha \in R$ such that $\alpha X \subset \Lambda^{(r+s-1)}$, and surely $X \cong \alpha X$.]

2. Show that the kernel of the epimorphism $\text{Cl}_A R \rightarrow \text{Cl } R$ is a finite elementary abelian 2-group. [Hint: The kernel is isomorphic to $P(R)/P_A(R)$, which is in turn a homomorphic image of $K^*/U(A)$. But there is an exact sequence

$$1 \rightarrow U(A) \rightarrow K^* \xrightarrow{\theta} \prod_{P \in S} \{\pm 1\} \rightarrow 1,$$

where for $a \in K^*$ and $P \in S$, the P -th component of $\theta(a)$ is the sign of a_P in K_P .]

36. K_0 OF MAXIMAL ORDERS

We begin by defining the group $K_0(\Lambda)$ for an arbitrary ring Λ . Let $P(\Lambda)$ denote the category of all finitely generated projective left Λ -modules. Let \mathbf{F} be the free abelian group generated by symbols (M) , one for each isomorphism class of objects $M \in P(\Lambda)$. Let \mathbf{F}_0 be the subgroup of \mathbf{F} generated by all expressions $(L + M) - (L) - (M)$, where $L, M \in P(\Lambda)$. Now set $K_0(\Lambda) = \mathbf{F}/\mathbf{F}_0$. Then $K_0(\Lambda)$ is an abelian additive group, called the *Grothendieck group* of the category $P(\Lambda)$. For $(M) \in \mathbf{F}$, let $[M]$ denote its image in \mathbf{F}/\mathbf{F}_0 . Then every element of $K_0(\Lambda)$ is expressible as a difference $[M] - [N]$, with $M, N \in P(\Lambda)$. For any $L, M \in P(\Lambda)$, we have

$$(36.1) \quad [L + M] = [L] + [M] \text{ in } K_0(\Lambda).$$

Given $M, N \in P(\Lambda)$, we call M *stably isomorphic* to N if $M \dot{+} \Lambda^{(r)} \cong N \dot{+} \Lambda^{(r)}$ for some integer r . By Exercise 36.1, $[M] = [N]$ in $K_0(\Lambda)$ if and only if M is stably isomorphic to N . Hence we may use the symbol $[M]$ to denote both an element of $K_0(\Lambda)$ and the stable isomorphism class of M .

Each ring Λ gives rise to an abelian group $K_0(\Lambda)$. Further, each homomorphism of rings $\varphi: \Lambda \rightarrow \Lambda'$ gives rise to a homomorphism $\varphi_*: K_0(\Lambda) \rightarrow K_0(\Lambda')$ of additive groups. The map φ_* is defined by setting

$$\varphi_*([M] - [N]) = [\Lambda' \otimes_{\Lambda} M] - [\Lambda' \otimes_{\Lambda} N], \quad [M] - [N] \in K_0(\Lambda).$$

In the expression $\Lambda' \otimes_{\Lambda} M$, the ring Λ' is made into a right Λ -module by means of φ . It is easily verified that φ_* is well defined. In the language of category theory, we may view K_0 as a (covariant) functor from the category of rings to the category of abelian groups.

It follows at once from this fact that if $\sum_{i=1}^n \Lambda_i$ is a direct sum of rings ("direct product", in category language), then there is a natural isomorphism

$$(36.2) \quad K_0\left(\sum_{i=1}^n \Lambda_i\right) \cong \sum_{i=1}^n K_0(\Lambda_i).$$

We also note that if the rings Γ and Λ are Morita equivalent (see §16), then the equivalence of categories ${}_\Lambda\mathcal{M} \rightarrow {}_\Gamma\mathcal{M}$ induces an equivalence $P(\Lambda) \rightarrow P(\Gamma)$. This latter equivalence then gives rise to an isomorphism $K_0(\Lambda) \cong K_0(\Gamma)$. We shall use this fact in our discussion below.

We are now ready to investigate K_0 of a maximal order. By (10.5), a maximal order in a separable algebra decomposes as a ring direct sum of maximal orders in central simple algebras. In view of (36.2), it therefore suffices to calculate $K_0(\Lambda)$ for the case where Λ is a maximal R -order in a central simple K -algebra. The aim of this section is to prove that

$$K_0(\Lambda) \cong \mathbf{Z} \dot{+} \text{Cl}\Lambda,$$

where $\text{Cl}\Lambda$ is the ideal class group of Λ defined in §35. We showed in (35.14) that $\text{Cl}\Lambda$ is isomorphic to the ray class group $\text{Cl}_A R$ when K is an algebraic number field, or when K is a function field and $A = \text{Eichler}/R$. Hence in these cases the structure of $K_0(\Lambda)$ is known explicitly.

Our main theorem, which holds whether or not K is a global field, is as follows:

(36.3) THEOREM. *Let R be a Dedekind domain with quotient field K , and let Λ be a maximal R -order in the central simple K -algebra A . There is an exact sequence of additive groups*

$$(36.4) \quad 0 \rightarrow \text{Cl}\Lambda \xrightarrow{\mu} K_0(\Lambda) \xrightarrow{\psi} K_0(A) \rightarrow 0.$$

Furthermore,

$$(36.5) \quad K_0(A) \cong \mathbf{Z}, \quad K_0(\Lambda) \cong \mathbf{Z} \dot{+} \text{Cl}\Lambda.$$

Proof. The inclusion $\Lambda \rightarrow A$ induces $\psi: K_0(\Lambda) \rightarrow K_0(A)$, where

$$\psi[M] = [A \otimes_\Lambda M] = [K \otimes_R \Lambda \otimes_\Lambda M] = [K \otimes_R M]$$

for each $M \in P(\Lambda)$. Since M is a Λ -lattice, we may identify $K \otimes_R M$ with KM .

In order to show that ψ is epic, it suffices to prove that for each finitely generated left A -module W , there exists an $M \in P(\Lambda)$ such that $KM \cong W$. By Exercise 3.5 or Exercise 26.5, there exists a left Λ -lattice M in W such that $KM = W$. But then $M \in P(\Lambda)$, since by (21.5) every Λ -lattice is Λ -projective. Therefore ψ is an epimorphism.

The ideal class group $\text{Cl}\Lambda$ consists of all stable isomorphism classes of left Λ -ideals in A , where a “left Λ -ideal in A ” means a left Λ -lattice M in A such that $KM = A$. Addition in $\text{Cl}\Lambda$ is given by

$$[M] + [M'] = [M''] \quad \text{if } M \dot{+} M' \cong \Lambda \dot{+} M'',$$

where the M 's are left Λ -ideals in A . We define $\mu: \text{Cl } \Lambda \rightarrow K_0(\Lambda)$ by setting

$$\mu[M] = [\Lambda] - [M], \quad [M] \in \text{Cl } \Lambda.$$

Since the element $[M] \in K_0(\Lambda)$ depends only on the stable isomorphism class of M , it is clear that μ is monic. Furthermore,

$$\begin{aligned} M \dot{+} M' \cong \Lambda \dot{+} M'' &\Rightarrow [M] + [M'] = [\Lambda] + [M''] \quad \text{in } K_0(\Lambda) \\ &\Rightarrow [\Lambda] - [M] + [\Lambda] - [M'] = [\Lambda] - [M''] \\ &\Rightarrow \mu[M] + \mu[M'] = \mu[M''] = \mu\{[M] + [M']\}. \end{aligned}$$

Therefore μ is a homomorphism of groups.

For $[M] \in \text{Cl } \Lambda$, we have

$$\psi\mu[M] = [A] - [A] = 0 \quad \text{in } K_0(A),$$

so $\psi\mu = 0$. To prove exactness of the sequence (36.4), it remains to verify that $\ker \psi \subset \text{im } \mu$. Each $x \in K_0(\Lambda)$ may be written as $x = [M] - [N]$, with $M, N \in P(\Lambda)$. If we choose $M' \in P(\Lambda)$ so that $M \dot{+} M' \cong \Lambda^{(r)}$ for some r , then

$$x = [M \dot{+} M'] - [N \dot{+} M'] = [\Lambda^{(r)}] - [L]$$

for some $L \in P(\Lambda)$. Suppose now that $\psi(x) = 0$; then $[KL] = [A^{(r)}]$ in $K_0(A)$. Since A is a simple artinian ring, it follows from Exercise 36.3 that $KL \cong A^{(r)}$ as left A -modules. Hence by (27.8) there exists a left Λ -ideal L_0 in A such that $L \cong \Lambda^{(r-1)} \dot{+} L_0$. Therefore

$$x = [\Lambda^{(r)}] - [\Lambda^{(r-1)} \dot{+} L_0] = [\Lambda] - [L_0] = \mu[L_0].$$

This completes the proof that (36.4) is exact.

Since A is a simple artinian ring, we have $K_0(A) \cong \mathbf{Z}$ by Exercise 36.3. Therefore the sequence (36.4) splits as a sequence of \mathbf{Z} -modules. This shows that $K_0(\Lambda) \cong \mathbf{Z} \dot{+} \text{Cl } \Lambda$, and completes the proof of the theorem.

Let us now compare the sequence (36.4) with that associated with an order Γ which is Morita equivalent to Λ . For simplicity, we treat only the case where $\Gamma \cong M_n(\Lambda)$.

(36.6) **THEOREM.** *Keep the notation of (36.3), and let $n \geq 1$. Set*

$$B = \text{Hom}_A(V, V) \cong M_n(A), \quad \text{where} \quad V = A^{(n)},$$

$$\Gamma = \text{Hom}_\Lambda(L, L) \cong M_n(\Lambda), \quad \text{where} \quad L = \Lambda^{(n)},$$

and where the bimodule structures are given by BV_A , ΓL_Λ . Then there is a commutative diagram with exact rows:

$$(36.7) \quad \begin{array}{ccccccc} 0 & \longrightarrow & \text{Cl } \Lambda & \xrightarrow{\mu} & K_0(\Lambda) & \xrightarrow{\psi} & K_0(A) \longrightarrow 0 \\ & & \downarrow \varphi & & \downarrow L \otimes_{\Lambda} \cdot & & \downarrow V \otimes_A \cdot \\ 0 & \xrightarrow{\sim} & \text{Cl } \Gamma & \xrightarrow{\mu'} & K_0(\Gamma) & \xrightarrow{\psi'} & K_0(B) \longrightarrow 0, \end{array}$$

where the map φ is given by

$$\varphi[M] = [L \otimes_{\Lambda} (\Lambda^{(n-1)} + M)], \quad [M] \in \text{Cl } \Lambda.$$

Each vertical map in (36.7) is an isomorphism.

Proof. Since V_A is a progenerator for \mathcal{M}_A , the ring B is Morita equivalent to A , and there is an equivalence of categories

$$V \otimes_A \cdot : {}_A \mathcal{M} \rightarrow {}_B \mathcal{M}.$$

Likewise, there is an equivalence

$$L \otimes_{\Lambda} \cdot : {}_{\Lambda} \mathcal{M} \rightarrow {}_{\Gamma} \mathcal{M}.$$

The second and third vertical maps in (36.7) are just the isomorphisms induced by these category equivalences. The right hand square in (36.7) is commutative, since both ψ and ψ' are induced by the functor $K \otimes_R \cdot$.

It follows from the Morita equivalence of Γ and Λ that there is a left Γ -isomorphism

$$(36.8) \quad \rho : \Gamma \cong L \otimes_{\Lambda} \Lambda^{(n)},$$

where ${}_L \Lambda$ is a bimodule, and $\Lambda^{(n)}$ is viewed as left Λ -module. For M a left ideal in Λ , we may therefore view $L \otimes_{\Lambda} (\Lambda^{(n-1)} + M)$ as a left ideal in Γ . This readily implies that the stable isomorphism class of M uniquely determines that of $L \otimes_{\Lambda} (\Lambda^{(n-1)} + M)$, and so φ is well defined on $\text{Cl } \Lambda$.

We shall show that the left hand square in (36.7) is commutative. This implies at once that φ is an isomorphism, as claimed. To prove commutativity, we start with an arbitrary $[M] \in \text{Cl } \Lambda$, and make the following calculation in $K_0(\Gamma)$. (In this calculation, we use (36.8), and write \otimes in place of \otimes_{Λ} for brevity.) We have

$$\begin{aligned} \mu' \varphi[M] &= [\Gamma] - [L \otimes (\Lambda^{(n-1)} + M)] = [L \otimes \Lambda^{(n)}] - [L \otimes \Lambda^{(n-1)}] \\ &\quad - [L \otimes M] = [L \otimes \Lambda] - [L \otimes M] = (L \otimes \cdot) \mu[M]. \end{aligned}$$

This shows that the left hand square in (36.7) is commutative, and completes the proof of the theorem.

(36.9) *Remarks.* (i) Keeping the above notation, let S be a simple left A -module. Then $[S]$ is a free \mathbf{Z} -generator for $K_0(A)$, and there is an isomorphism $r_A : K_0(A) \cong \mathbf{Z}$, obtained by setting $r_A[S] = 1$. Since $V \otimes_A S$ is a simple

left B -module, it follows at once that the following diagram commutes:

$$\begin{array}{ccc} K_0(A) & \xrightarrow{r_A} & \mathbf{Z} \\ v \otimes_{\mathcal{A}} \downarrow & & \downarrow 1 \\ K_0(B) & \xrightarrow{r_B} & \mathbf{Z}. \end{array}$$

(ii) Suppose that the hypotheses of (35.14) hold, and keep the above notation. The reduced norm maps induce isomorphisms

$$v: \text{Cl } \Lambda \cong \text{Cl}_A R, \quad v': \text{Cl } \Gamma \cong \text{Cl}_B R,$$

and of course $\text{Cl}_A R = \text{Cl}_B R$. We claim that the diagram

$$(36.10) \quad \begin{array}{ccc} \text{Cl } \Lambda & \xrightarrow{v} & \text{Cl}_A R \\ \varphi \downarrow & & \downarrow 1 \\ \text{Cl } \Gamma & \xrightarrow{v'} & \text{Cl}_A R \end{array}$$

is commutative. Let $[M] \in \text{Cl } \Lambda$, and assume without loss of generality that $M \subset \Lambda$. We need only show that

$$(36.11) \quad \text{nr}_{A/K} M = \text{nr}_{B/K} \{L \otimes (\Lambda^{(n-1)} + M)\},$$

where \otimes means \otimes_{Λ} . If $(A:K) = t^2$, then $(B:K) = t^2 n^2$, so

$$N_{A/K} = (\text{nr}_{A/K})^t, \quad N_{B/K} = (\text{nr}_{B/K})^{tn}.$$

Thus (36.11) holds if and only if

$$\{N_{A/K} M\}^n = N_{B/K} \{L \otimes (\Lambda^{(n-1)} + M)\}.$$

Using (36.8), the right hand expression equals

$$\begin{aligned} \text{ord}_R \frac{L \otimes \Lambda^{(n)}}{L \otimes (\Lambda^{(n-1)} + M)} &= \left\{ \text{ord}_R \frac{\Lambda^{(n)}}{\Lambda^{(n-1)} + M} \right\}^n \\ &= \left\{ \text{ord}_R \frac{\Lambda}{M} \right\}^n = \{N_{A/K} M\}^n. \end{aligned}$$

This completes the proof that the diagram (36.10) is commutative.

EXERCISES

In Exercises 1 and 2, Λ is an arbitrary ring.

1. Let $X, Y \in P(\Lambda)$. Show that $[X] = [Y]$ in $K_0(\Lambda)$ if and only if X is stably isomorphic to Y [Hint: If $X + \Lambda^{(r)} \cong Y + \Lambda^{(r)}$, then $[X] + r[\Lambda] = [Y] + r[\Lambda]$ in $K_0(\Lambda)$, so $[X] = [Y]$. Conversely, if $[X] = [Y]$ in $K_0(\Lambda)$, then $(X) - (Y)$ lies in the subgroup F_0 of F . Hence there exist L 's, M 's in $P(\Lambda)$ such that in F .

$$(X) - (Y) = \sum \{(L_i + L'_i) - (L_i) - (L'_i)\} + \sum \{(M_j + M'_j) - (M_j) - (M'_j)\}.$$

Therefore

$$X + \sum L_i + \sum L'_i + \sum (M_j + M'_j) \cong Y + \sum (L_i + L'_i) + \sum M_j + \sum M'_j.$$

Choose $N \in P(\Lambda)$ so that

$$N + \sum L_i + \sum L'_i + \sum M_j + \sum M'_j \cong \Lambda^{(r)}$$

for some r . Then $X + \Lambda^{(r)} \cong Y + \Lambda^{(r)}$, as desired.]

2. Let $X_i, Y_i \in P(\Lambda)$. Show that $[X_1] - [X_2] = [Y_1] - [Y_2]$ in $K_0(\Lambda)$ if and only if $X_1 + Y_2$ is stably isomorphic to $X_2 + Y_1$.

3. Let A be a semisimple artinian ring with t simple components. Show that

- (i) $P(A)$ consists of all finitely generated left A -modules.
- (ii) For $X, Y \in P(A)$, we have $[X] = [Y]$ in $K_0(A)$ if and only if $X \cong Y$.
- (iii) $K_0(A) \cong \mathbf{Z}^{(t)}$. In fact, if S_1, \dots, S_t are a full set of non-isomorphic simple left A -modules, show that $[S_1], \dots, [S_t]$ form a free \mathbf{Z} -basis for $K_0(A)$.

In Exercises 4–6, let R be a Dedekind domain with quotient field K , and let Λ be a maximal R -order in a central simple K -algebra A .

4. Show that every nonzero left Λ -lattice is a progenerator of the category ${}_{\Lambda}\mathcal{M}$.

5. Show that (36.6) can be generalized, as follows: let L be any nonzero right Λ -lattice, and set

$$\Gamma = \text{Hom}_{\Lambda}(L, L), \quad L^* = \text{Hom}_{\Lambda}(L_{\Lambda}, \Lambda_{\Lambda}),$$

with bimodule structures ${}_{\Gamma}L_{\Lambda}, {}_{\Lambda}(L^*)_{\Gamma}$. Let $V = KL, B = K\Gamma$. Show that the diagram (36.7) is commutative, provided we define $\varphi[M]$ for $[M] \in \text{Cl } \Lambda$ as follows:

$$\varphi[M] = [L \otimes_{\Lambda} \tilde{M}],$$

where \tilde{M} is a left Λ -lattice such that $M + L^* \cong \Lambda + \tilde{M}$. [Hint: The equivalence $L \otimes_{\Lambda} \cdot : {}_{\Lambda}\mathcal{M} \rightarrow {}_{\Gamma}\mathcal{M}$ carries L^* onto Γ . This fact is crucial in proving the commutativity of the left hand square in (36.7).]

6. Keep the notation of the preceding exercise. Show that the analogues of (36.9 i) and (36.9 ii) remain true.

37. PICARD GROUPS

Many of the results in this section are due to Fröhlich [1] (see also Bass [1]). Let R be a commutative ring, Λ any ring (with unity element 1_{Λ}), and let $c(\Lambda)$ denote the center of Λ . We have called Λ an R -algebra if there is a ring homomorphism $R \rightarrow c(\Lambda)$ with $1_R \mapsto 1_{\Lambda}$. In this case, all Λ -modules may be viewed as R -modules. Since every ring is a \mathbf{Z} -algebra, there is no loss of generality in considering algebras rather than rings.

Let Λ, Δ be R -algebras. We shall say that a bimodule ${}_{\Lambda}M_{\Delta}$ is over R if

$$rm = mr \text{ for all } r \in R, m \in M,$$

that is, $(rl_{\Lambda})m = m(r1_{\Delta})$ for all r, m . A bimodule ${}_{\Lambda}M_{\Delta}$ (over R) is invertible if

there exist a bimodule ${}_{\Delta}N_{\Lambda}$ (over R), and a Morita context (16.6), which give a Morita equivalence (over R) of the rings Λ, Δ . We call N the *inverse* of M . As shown in §16, the bimodule isomorphism class (M) uniquely determines the inverse class (N) ; indeed, we have $(N) = (M^{-1})$, where M^{-1} is the bimodule given by

$$(37.1) \quad {}_{\Delta}(M^{-1})_{\Lambda} = \text{Hom}_{\Lambda}({}_{\Lambda}M_{\Delta}, {}_{\Lambda}\Lambda_{\Lambda}) \cong \text{Hom}_{\Delta}({}_{\Lambda}M_{\Delta}, {}_{\Delta}\Delta_{\Delta}).$$

We may restate the definition of invertibility in the following explicit form: the bimodule ${}_{\Lambda}M_{\Delta}$ (over R) is invertible (over R) if there exist a bimodule ${}_{\Delta}N_{\Lambda}$ (over R) and bimodule isomorphisms

$$(37.2) \quad M \otimes_{\Delta} N \cong \Lambda, \quad N \otimes_{\Lambda} M \cong \Delta,$$

making the following diagrams commute:

$$(37.3) \quad \begin{array}{ccc} M \otimes_{\Delta} N \otimes_{\Lambda} M & \rightarrow & \Lambda \otimes_{\Lambda} M \\ \downarrow & & \downarrow \\ M \otimes_{\Delta} \Delta & \rightarrow & M, \end{array} \quad \begin{array}{ccc} N \otimes_{\Lambda} M \otimes_{\Delta} N & \rightarrow & \Delta \otimes_{\Delta} N \\ \downarrow & & \downarrow \\ N \otimes_{\Lambda} \Lambda & \rightarrow & N. \end{array}$$

Let us recall from §16 that every invertible bimodule ${}_{\Lambda}M_{\Delta}$ is a pro-generator for both of the categories ${}_{\Lambda}\mathcal{M}$ and \mathcal{M}_{Δ} . Furthermore,

$$(37.4) \quad \Lambda \cong \text{Hom}_{\Delta}(M, M), \quad \Delta \cong \text{Hom}_{\Lambda}(M, M),$$

where both Δ and $\text{Hom}_{\Lambda}(M, M)$ are viewed as rings of right operators on M . Conversely, progenerators yield Morita equivalences.

(37.5) *Definitions.* (i) Let Λ be an R -algebra. The *Picard group of Λ relative to R* , denoted by $\text{Pic}_R \Lambda$, is the multiplicative group consisting of all bimodule isomorphism classes (M) of invertible bimodules ${}_{\Lambda}M_{\Lambda}$ over R . Multiplication is defined by the formula $(M)(M') = (M \otimes_{\Lambda} M')$. The class (Λ) is the identity element of $\text{Pic}_R \Lambda$, and inverses are given by $(M)^{-1} = (M^{-1})$ with M^{-1} defined as in (37.1), using Λ in place of Δ .

(ii) Let $C = c(\Lambda)$, and view Λ as a C -algebra. We define

$$\text{Picent } \Lambda = \text{Pic}_C \Lambda,$$

so $\text{Picent } \Lambda$ is the subgroup of $\text{Pic}_{\mathbf{Z}} \Lambda$ consisting of all classes of invertible bimodules ${}_{\Lambda}M_{\Lambda}$ such that

$$(37.6) \quad cm = mc \text{ for all } c \in C, m \in M.$$

We remark that the groups $\text{Pic}_R \Lambda$ and $\text{Picent } \Lambda$ need not be commutative. The group $\text{Pic}_{\mathbf{Z}} \Lambda$ is called the *Picard group* of Λ , and the subscript \mathbf{Z} is usually omitted. As we shall see below when we restrict our attention to the case where Λ is an order in a semisimple algebra A over a field, the group

$\text{Picent } \Lambda$ is precisely the group of invertible two-sided Λ -ideals in A , modulo principal ideals generated by units in $c(A)$. From this standpoint, the group $\text{Picent } \Lambda$ is a natural object of investigation.

In Exercise 16.4 we have already noted that Morita equivalent rings have isomorphic centers. Let us give this isomorphism explicitly:

(37.7) THEOREM. *Let Λ, Δ be R -algebras, and let ${}_R M_\Delta$ be an invertible bimodule over R . Then M determines an R -isomorphism $\varphi: c(\Lambda) \cong c(\Delta)$ as follows: for each $c \in c(\Lambda)$, $\varphi(c)$ is the unique element of $c(\Delta)$ such that*

$$(37.8) \quad c \cdot m = m \cdot \varphi(c) \text{ for all } m \in M.$$

Taking $R = \mathbf{Z}$, it follows that Morita equivalent rings have isomorphic centers.

Proof. Since M is invertible, (37.4) shows that each element of Λ (or of Δ) is completely determined by its action on M . For each $c \in C$, the map $m \mapsto cm$, $m \in M$, is a left Λ -endomorphism of M . Hence by (37.4) there is a unique $\varphi(c) \in \Delta$ such that (37.8) holds true. But then for all $x \in \Delta$ and $m \in M$,

$$m(\varphi(c)x) = (cm)x = c(mx) = (mx)\varphi(c) = m(x\varphi(c)).$$

Thus $\varphi(c)$ commutes with each $x \in \Delta$, so $\varphi(c) \in c(\Delta)$. It is easily verified that φ is an R -isomorphism of rings, and the theorem is proved.

Let us show next that Morita equivalent rings have isomorphic Picard groups.

(37.9) THEOREM. *If the R -algebras Λ, Δ are Morita equivalent over R , then $\text{Pic}_R \Lambda \cong \text{Pic}_R \Delta$. If the rings Λ, Λ' are Morita equivalent, then $\text{Picent } \Lambda \cong \text{Picent } \Lambda'$.*

Proof. Let ${}_R M_\Delta$ be an invertible bimodule over R . It is easily verified that the map

$$(X) \rightarrow (M^{-1} \otimes_{\Lambda} X \otimes_{\Lambda} M), \quad (X) \in \text{Pic}_R \Lambda,$$

gives an isomorphism $\text{Pic}_R \Lambda \cong \text{Pic}_R \Delta$. (We should remark that this isomorphism may depend on the choice of M .)

Secondly, let the invertible bimodule ${}_R N_{\Lambda'}$ determine an isomorphism $\varphi: C \cong C'$ as in (37.7), where $C = c(\Lambda)$, $C' = c(\Lambda')$. Then

$$c \cdot n = n \cdot \varphi(c) \text{ for all } c \in C, n \in N.$$

For $(X) \in \text{Picent } \Lambda$ we have $cx = xc$ for all $c \in C$, $x \in X$. Let us deduce from this that $(N^{-1} \otimes_{\Lambda} X \otimes_{\Lambda} N) \in \text{Picent } \Lambda'$. Each element of C' is of the form $\varphi(c)$, for some $c \in C$. Then we have

$$\begin{aligned} (n' \otimes x \otimes n)\varphi(c) &= n' \otimes x \otimes cn = n'c \otimes x \otimes n \\ &= \varphi(c)(n' \otimes x \otimes n), \text{ for all } n' \otimes x \otimes n \in N^{-1} \otimes X \otimes N. \end{aligned}$$

The remaining details of the proof are obvious. A supplement to this theorem is given in Exercise 37.4.

Now let $\text{Aut}_R \Lambda$ be the group of all R -automorphisms of the R -algebra Λ . For each $u \in u(\Lambda)$, let i_u be the inner automorphism defined by

$$(37.10) \quad i_u(x) = uxu^{-1}, \quad x \in \Lambda.$$

The *group of inner automorphisms* of Λ is defined as

$$\text{In } \Lambda = \{i_u : u \in u(\Lambda)\}.$$

Since

$$\alpha \cdot i_u \cdot \alpha^{-1} = i_{\alpha u}, \quad \alpha \in \text{Aut}_R \Lambda, \quad u \in u(\Lambda),$$

it follows that $\text{In } \Lambda$ is a normal subgroup of $\text{Aut}_R \Lambda$. We set

$$(37.11) \quad \text{Out}_R \Lambda = \text{Aut}_R \Lambda / \text{In } \Lambda,$$

the *outer automorphism group of Λ over R* .

(37.12) *Definition.* Let Λ, Δ be R -algebras, ${}_A X_\Delta$ a bimodule over R . Given any automorphisms $f \in \text{Aut}_R \Lambda$, $g \in \text{Aut}_R \Delta$, let ${}_f X_g$ be the bimodule (over R) having the same elements as X , but with the action of Λ “twisted” by f , that of Δ by g . This means that

$$\lambda \circ x \circ \delta \quad (\text{in } {}_f X_g) = f(\lambda) \cdot x \cdot g(\delta) \quad (\text{in } X)$$

for each $x \in X$, $\lambda \in \Lambda$, $\delta \in \Delta$. It is easily verified that

$${}_f({}_g X_{g'}) \cong {}_{fg} X_{gg'} \text{ as bimodules.}$$

(37.13) *LEMMA.* Consider the R -algebra Λ as a (Λ, Λ) -bimodule. For each $f, g \in \text{Aut}_R \Lambda$, there is a (Λ, Λ) -bimodule ${}_f \Lambda_g$ over R . The following bimodule isomorphisms hold true:

$$\begin{aligned} {}_f \Lambda_g &\cong {}_{hf} \Lambda_{hg} \cong {}_1 \Lambda_{f^{-1}g} \cong {}_{g^{-1}f} \Lambda_1, \quad {}_f({}_f \Lambda_g)_{g'} \cong {}_{ff'} \Lambda_{gg'}, \\ {}_f \Lambda_g \otimes {}_f \Lambda_{g'} &\cong {}_f \Lambda_{g f'^{-1} g'}, \quad {}_1 \Lambda_g \otimes {}_1 \Lambda_{g'} \cong {}_1 \Lambda_{gg'}, \\ {}_1 \Lambda_f \otimes {}_f \Lambda_1 &\cong \Lambda \cong {}_f \Lambda_1 \otimes {}_1 \Lambda_f, \end{aligned}$$

where \otimes means \otimes_Λ .

Proof. Exercise for the reader.

(37.14) *THEOREM.* The map $\omega_0 : \text{Aut}_R \Lambda \rightarrow \text{Pic}_R \Lambda$, defined by

$$\omega_0(f) = ({}_1\Lambda_f), \quad f \in \text{Aut}_R \Lambda,$$

is a homomorphism of groups. We have $\ker \omega_0 = \text{In } \Lambda$, the group of inner automorphisms of Λ . Therefore ω_0 induces a monomorphism

$$\omega: \text{Out}_R \Lambda \rightarrow \text{Pic}_R \Lambda,$$

where $\text{Out}_R \Lambda$ is given by (37.11).

Proof. Each $f \in \text{Aut}_R \Lambda$ gives rise to a (Λ, Λ) -bimodule ${}_1\Lambda_f$ over R , and by (37.13), ${}_f\Lambda_1$ is an inverse for ${}_1\Lambda_f$. Thus $\omega_0(f) = ({}_1\Lambda_f) \in \text{Pic}_R \Lambda$. Further, for $f, g \in \text{Aut}_R \Lambda$,

$$\omega_0(fg) = ({}_1\Lambda_{fg}) = ({}_1\Lambda_f)({}_1\Lambda_g)$$

by (37.13), so ω_0 is a homomorphism.

Let us prove that $\ker \omega_0 = \text{In } \Lambda$. We have $\omega_0(f) = 1$ if and only if there exists a bimodule isomorphism $\theta: \Lambda \cong {}_1\Lambda_f$. This occurs if and only if there is a bijection $\theta: \Lambda \rightarrow \Lambda$ such that

$$(37.15) \quad \theta(axb) = a \cdot \theta(x) \cdot f(b) \text{ for all } a, b, x \in \Lambda.$$

Now let $u \in u(\Lambda)$, and let f be the inner automorphism i_u defined by (37.10). Set $\theta(x) = xu^{-1}$, $x \in \Lambda$. Condition (37.15) becomes

$$(axb)u^{-1} = a \cdot xu^{-1} \cdot i_u(b) = a \cdot xu^{-1} \cdot ubu^{-1},$$

which is always true. Therefore $\Lambda \cong {}_1\Lambda_f$ whenever f is inner, and thus $\text{In } \Lambda \subset \ker \omega_0$.

Conversely, let $\theta: \Lambda \rightarrow \Lambda$ be a bijection such that (37.15) holds, and set $u = \theta(1)$. Then

$$\Lambda = \theta(\Lambda) = \theta(\Lambda \cdot 1) = \Lambda\theta(1) = \Lambda u,$$

and likewise $\Lambda = u\Lambda$, so $u \in u(\Lambda)$. Taking $x = b = 1$ in (37.15), we obtain

$$\theta(a) = au \text{ for all } a \in \Lambda.$$

Next choose $a = x = 1$ in (37.15), whence

$$\theta(b) = u \cdot f(b) \text{ for all } b \in \Lambda.$$

Therefore

$$au = \theta(a) = u \cdot f(a) \text{ for all } a \in \Lambda,$$

whence $f = i_{u^{-1}} \in \text{In } \Lambda$. This completes the proof that $\ker \omega_0 = \text{In } \Lambda$, and the remaining assertion in the theorem is now obvious.

The preceding discussion is useful in considering the one-sided modu structure of invertible bimodules. The following result is fundamental:

(37.16) THEOREM. Let $(X), (Y) \in \text{Pic}_R \Lambda$. Then ${}_X \cong {}_Y$ if and only if $(Y) \in (X) \cdot \text{im } \omega$, that is, if and only if $Y \cong {}_1 X_f$ (as bimodules) for some $f \in \text{Aut}_R \Lambda$.

Proof. For each $f \in \text{Aut}_R \Lambda$, there is a (Λ, Λ) -bimodule isomorphism

$${}_1 X_f = X \otimes_{\Lambda} {}_1 \Lambda_f.$$

Hence $(Y) \in (X) \cdot \text{im } \omega$ if and only if $Y \cong {}_1 X_f$ for some f . It is clear that any bimodule isomorphism $Y \cong {}_1 X_f$ is also a left Λ -isomorphism ${}_{\Lambda} Y \cong {}_{\Lambda} X$.

Conversely, let $h: X \cong Y$ be a left Λ -isomorphism. Then h induces an isomorphism h^* of endomorphism rings:

$$h^*: \text{Hom}_{\Lambda}({}_{\Lambda} Y, {}_{\Lambda} Y) \cong \text{Hom}_{\Lambda}({}_{\Lambda} X, {}_{\Lambda} X),$$

given by $h^*(\varphi) = h^{-1} \varphi h$, for $\varphi \in \text{Hom}_{\Lambda}({}_{\Lambda} Y, {}_{\Lambda} Y)$. Since ${}_X \Lambda$ is invertible, each element in $\text{Hom}_{\Lambda}({}_{\Lambda} X, {}_{\Lambda} X)$ is given by a right multiplication $a_r: x \rightarrow xa$, $x \in X$, for some uniquely determined element $a \in \Lambda$. Likewise, every element of $\text{Hom}_{\Lambda}({}_{\Lambda} Y, {}_{\Lambda} Y)$ is of the form $b_r: y \rightarrow yb$, $y \in Y$, for some uniquely determined $b \in \Lambda$. Therefore each $b \in \Lambda$ determines a unique $a \in \Lambda$ such that $h^*(b_r) = a_r$, that is,

$$h^{-1} b_r h = a_r \quad \text{on } X.$$

This gives

$$(h^{-1} b_r h)x = a_r x = xa \quad \text{for all } x \in X,$$

that is,

$$(hx)b = h(xa) \quad \text{for all } x \in X.$$

Setting $a = f(b)$, we obtain the identity

$$(hx)b = h(x \cdot f(b)) \quad \text{for all } x \in X, \quad b \in \Lambda.$$

It follows readily that $f \in \text{Aut}_R \Lambda$, and that the map $h: {}_1 X_f \rightarrow Y$ given by $x \rightarrow h(x)$, $x \in {}_1 X_f$, is a bimodule isomorphism. We have thus shown that if ${}_X \cong {}_Y$, then $Y \cong {}_1 X_f$ (as bimodules) for some $f \in \text{Aut}_R \Lambda$. This completes the proof of the theorem.

Before proceeding with our investigation of $\text{Picent } \Lambda$, let us briefly consider the relation between $\text{Picent } \Lambda$ and $\text{Pic}_R \Lambda$ when Λ is an R -algebra. Let $C = c(\Lambda)$. By (37.7), each invertible ${}_M \Lambda$ over R determines an R -automorphism Φ_M of C , according to the condition that for each $c \in C$,

$$\Phi_M(c) \cdot m = m \cdot c \quad \text{for all } m \in M.$$

It is clear that Φ_M depends only upon the bimodule isomorphism class of M .

Let us calculate Φ_M for the case where $M = {}_1 \Lambda_f$, $f \in \text{Aut}_R \Lambda$. We show that

$$(37.17) \quad M = {}_1 \Lambda_f \implies \Phi_M \text{ is the restriction of } f \text{ to } C.$$

Indeed, let $c \in C$, and let us verify that

$$f(c) \cdot m = m \cdot c \text{ for all } m \in M.$$

Since $M = {}_1\Lambda_f$, this condition becomes

$$f(c) \cdot \lambda = \lambda \cdot f(c) \text{ for all } \lambda \in \Lambda,$$

which certainly holds true since $f(c) \in C$. This establishes (37.17), which we shall need for the next result.

(37.18) THEOREM. *For any R -algebra Λ with center C , there is an exact sequence*

$$(37.19) \quad 1 \rightarrow \text{Picent } \Lambda \rightarrow \text{Pic}_R \Lambda \xrightarrow{\Phi} \text{Aut}_R C.$$

If Λ is commutative, then the sequence

$$(37.20) \quad 1 \rightarrow \text{Picent } \Lambda \rightarrow \text{Pic}_R \Lambda \xrightarrow{\Phi} \text{Aut}_R \Lambda \rightarrow 1$$

is split exact.

Proof. Let $(M), (N) \in \text{Pic}_R \Lambda$, and set $f = \Phi_M$, $g = \Phi_N$. Then for each $c \in C$, we have

$$f(c) \cdot m = mc, \quad g(c) \cdot n = nc, \text{ for all } m \in M, n \in N.$$

Therefore

$$(m \otimes n)c = m \cdot g(c) \otimes n = f(g(c))(m \otimes n) \text{ for all } m \otimes n \in M \otimes_{\Lambda} N.$$

This shows that $\Phi_{M \otimes N} = \Phi_M \circ \Phi_N$, and thus Φ is a homomorphism. Furthermore, $\Phi_M = 1$ if and only if $cm = mc$ for all $m \in M$, $c \in C$, that is, if and only if $(M) \in \text{Picent } \Lambda$. This completes the proof that the sequence (37.19) is exact, once we observe that the mapping of $\text{Picent } \Lambda$ into $\text{Pic}_R \Lambda$ is just the inclusion map.

Now suppose that Λ is commutative, and let ω_0 be the map defined in (37.14). Thus for $f \in \text{Aut}_R \Lambda$, we put $\omega_0(f) = {}_1\Lambda_f \in \text{Pic}_R \Lambda$. Since Λ is commutative, it follows from (37.17) that $\Phi \omega_0(f) = f$. This shows that $\Phi \omega_0$ is the identity map on $\text{Aut}_R \Lambda$, whence by §2a the map Φ is epic, and the exact sequence (37.20) is split. This completes the proof of the theorem.

Remarks. (i) In some cases one can describe explicitly the image of the map Φ occurring in (37.19). Suppose for example that $A = \sum_{i=1}^t A_i$ is semisimple, where for each i the simple component A_i has skewfield part D_i and center K_i . Then $c(A) = \sum K_i$, and each $f \in \text{Aut}_K c(A)$ must permute the $\{K_i\}$. Hence f is completely determined by some permutation π of the set $\{1, \dots, t\}$, together with a collection of K -isomorphisms $f_i: K_i \cong K_{\pi(i)}$,

$1 \leq i \leq t$, where f_i is the restriction of f to K_i . Then $\text{Picent } A \cong \prod \text{Picent } A_i$ by Exercise 37.6, and the exact sequence (37.19) becomes†

$$1 \rightarrow \text{Picent } A \rightarrow \text{Pic}_K A \xrightarrow{\Phi'} \text{Aut}_K c(A).$$

Each $(X) \in \text{Pic}_K A$ yields a Morita equivalence of the K -algebra A with itself. Using this fact, Fröhlich [1] proves that the image of Φ' consists precisely of those elements $f \in \text{Aut}_K c(A)$ such that for $1 \leq i \leq t$, the isomorphism $f_i : K_i \cong K_{\pi(i)}$ can be extended to an isomorphism $D_i \cong D_{\pi(i)}$. We shall see in (37.21) that $\text{Picent } A = 1$, and thus $\text{Pic}_K A \cong \text{im } \Phi'$ in the present case.

(ii) Now let R be a Dedekind domain with quotient field K , and let Λ be a maximal R -order in a separable K -algebra A . Keep the above notation. There is a ring isomorphism

$$\text{Aut}_R c(\Lambda) \cong \text{Aut}_K c(A),$$

given by extending each $f \in \text{Aut}_R c(\Lambda)$ to an $f' \in \text{Aut}_K c(A)$. By using the result that any two maximal orders must be Morita equivalent (see Exercise 22.11), Fröhlich shows that

$$f \in \text{im } \Phi \Leftrightarrow f' \in \text{im } \Phi',$$

where Φ is the map occurring in (37.19). Thus $\text{im } \Phi$ is known also for the case of maximal orders.

(iii) Keep the notation of (i), and consider the exact sequence

$$1 \rightarrow \text{Picent } A_1 \rightarrow \text{Pic}_K A_1 \xrightarrow{\Phi''} \text{Aut}_K K_1.$$

By (i), $\text{im } \Phi''$ consists precisely of those K -automorphisms f of K_1 which can be extended to a K -automorphism of A_1 .

(37.21) **Theorem.** *Let A be any semisimple artinian ring. Then*

$$\text{Picent } A = 1.$$

Proof. We may write $A = \sum_{i=1}^t A_i$, where each A_i is a simple artinian ring. Then

$$\text{Picent } A \cong \prod_{i=1}^t \text{Picent } A_i$$

by Exercise 37.6, so we need only show that each $\text{Picent } A_i = 1$. Changing notation, let A be a simple artinian ring with center K , that is, A is a central simple K -algebra. Let V be a simple left A -module, $D = \text{Hom}_A(V, V) =$ skewfield part of A , and view V as a bimodule ${}_AV_D$ of right D -dimension n . Then

$$A = \text{Hom}_D(V, V) \cong M_n(D).$$

* To clarify the later discussion, we write Φ' rather than Φ .

Now let $(X) \in \text{Picent } A$. Then ${}_A X \cong V^{(k)}$ for some k , and therefore

$$\text{Hom}_A({}_A X, {}_A X) \cong \text{Hom}_A(V^{(k)}, V^{(k)}) \cong M_k(D),$$

where each endomorphism ring is viewed as right operator domain. But $\text{Hom}_A({}_A X, {}_A X) \cong A$ since ${}_A X$ is invertible. Therefore $A \cong M_k(D)$, whence $k = n$. This proves that $X \cong A$ as left A -modules. Hence by (37.16), there exists an $f \in \text{Aut}_K A$ such that $X \cong {}_1 A_f$ as bimodules. But f is an inner automorphism of A , by the Skolem-Noether Theorem. Hence ${}_1 A_f \cong A$ as bimodules, by (37.14). This shows that $(X) = 1$ in $\text{Picent } A$, and completes the proof of the theorem. One may also prove that $\text{Picent } A = 1$ by using Exercise 37.4, since A is an Azumaya K -algebra, and since $\text{Pic}_K K = 1$.

(37.22) Theorem. *Let Λ be a commutative ring such that $\Lambda/\text{rad } \Lambda$ is a direct sum of fields. Then $\text{Picent } \Lambda = 1$. This holds in particular when Λ is a commutative algebra over a local ring R , and Λ is finitely generated as R -module.*

Proof. Set $N = \text{rad } \Lambda$, $\bar{\Lambda} = \Lambda/N$. Clearly $\bar{\Lambda}$ is a commutative ring such that $\text{rad } \bar{\Lambda} = 0$. Thus $\bar{\Lambda}$ is a direct sum of fields if and only if $\bar{\Lambda}$ is an artinian ring.

Any left Λ -module X may be viewed as a bimodule ${}_A X_\Lambda$ over Λ , by defining $x \cdot \lambda = \lambda x$, $\lambda \in \Lambda$, $x \in X$. All bimodules over Λ arise in this way. For each X , let $\bar{X} = X/NX$. We claim that there is a homomorphism $\text{Picent } \Lambda \rightarrow \text{Picent } \bar{\Lambda}$, given by $(X) \mapsto (\bar{X})$. Indeed, given a Morita context where $X \otimes Y \cong \Lambda$, $Y \otimes X \cong \Lambda$, we obtain a new context $\bar{X} \otimes \bar{Y} \rightarrow \bar{\Lambda}$, $\bar{Y} \otimes \bar{X} \rightarrow \bar{\Lambda}$ in which both maps are epic, and hence $(\bar{X}) \in \text{Picent } \bar{\Lambda}$.

Now $\text{Picent } \bar{\Lambda} = 1$ since $\bar{\Lambda}$ is semisimple artinian, and hence for each $(X) \in \text{Picent } \Lambda$ there exists a $\bar{\Lambda}$ -isomorphism $f: \bar{X} \cong \bar{\Lambda}$. In the diagram

$$\begin{array}{ccc} X & \xrightarrow{\quad \varphi \quad} & \Lambda \\ \downarrow \psi & & \downarrow \\ \bar{X} & \xleftarrow{\quad f \quad} & \bar{\Lambda}, \\ & \xleftarrow{\quad f^{-1} \quad} & \end{array}$$

we can find Λ -homomorphisms φ, ψ which lift f, f^{-1} respectively, since X and Λ are Λ -projective. Then $\varphi\psi(a) - a \in N$ for all $a \in \Lambda$, whence $\Lambda = \varphi\psi(\Lambda) + N$. It follows that $\varphi\psi(\Lambda) = \Lambda$, and so φ is epic. Therefore $X = \ker \varphi \oplus X_1$, where $\varphi: X_1 \cong \Lambda$. Consequently $\overline{\ker \varphi} = 0$ in \bar{X} , whence $\ker \varphi = 0$. This proves that $X \cong \Lambda$, as desired. The second assertion in the theorem follows from the first, by use of (6.15).

For the remainder of this section let R be a domain with quotient field K , and let Λ be an R -order in a K -algebra A . If M, N are two-sided Λ -submodules of A such that $MN = NM = \Lambda$, we call M an *invertible* Λ -ideal in A , and N its *inverse*. Then $KM = KN = A$. By Exercise 37.9, M is an invertible

(Λ, Λ) -bimodule, and hence $(M) \in \text{Picent } \Lambda$. The same Exercise shows that $(M)^{-1} = (N)$ in $\text{Picent } \Lambda$. Let us denote by $I(\Lambda)$ the multiplicative group of invertible Λ -ideals in A , with multiplication performed within A . If $C = c(\Lambda)$, then obviously $c(A) = KC$. We prove

(37.23) THEOREM. *There is an exact sequence*

$$1 \rightarrow u(C) \rightarrow u(KC) \xrightarrow{\rho} I(\Lambda) \xrightarrow{\sigma} \text{Picent } \Lambda \xrightarrow{\tau} \text{Picent } A,$$

where $\rho(u) = \Lambda u$, $\sigma(M) = (M)$, $\tau(X) = (KX)$.

Proof. Exactness at $u(KC)$ is clear. By Exercise 37.8, $\ker \sigma = \text{im } \rho$. Finally, $\ker \tau = \text{im } \sigma$ by Exercise 37.10.

(37.24) COROLLARY. *If A is semisimple, then*

$$\text{Picent } \Lambda \cong I(\Lambda)/\{\Lambda u : u \in u(KC)\}.$$

This corollary justifies to some extent our emphasis on the group $\text{Picent } \Lambda$, rather than $\text{Pic}_R \Lambda$. It shows that $\text{Picent } \Lambda$ occurs in a natural way as a class group of invertible Λ -ideals in A .

Let us define

$$\text{Autcent } \Lambda = \text{Aut}_C \Lambda, \quad \text{Outcent } \Lambda = \text{Out}_C \Lambda = \text{Aut}_C \Lambda / \text{In } \Lambda,$$

where $C = c(\Lambda)$. By (37.14), there is a monomorphism

$$\omega: \text{Outcent } \Lambda \rightarrow \text{Picent } \Lambda, \quad f \mapsto ({}_1 \Lambda_f).$$

Now define the *normalizer* of Λ in A as

$$N(\Lambda) = \{x \in u(A) : x\Lambda x^{-1} = \Lambda\}.$$

(37.25) THEOREM. *Let A be a semisimple K -algebra. There is a commutative diagram*

$$\begin{array}{ccc} N(\Lambda)/u(\Lambda) & \xrightarrow{\rho} & \text{Outcent } \Lambda \\ \searrow \omega' & & \downarrow \omega \\ & & \text{Picent } \Lambda, \end{array}$$

where for $x \in N(\Lambda)$,

$$\rho(x) = i_x, \quad \omega'(x) = (\Lambda x),$$

and i_x is the inner automorphism $\lambda \mapsto x\lambda x^{-1}$, $\lambda \in \Lambda$. The map ρ is an isomorphism, and ω' a monomorphism.

Proof. Each $f \in \text{Aut}_C \Lambda$ extends to an $\tilde{f} \in \text{Aut}_{KC} A$. By the Skolem–Noether

Theorem (7.23), $\tilde{f} = i_x$ for some $x \in u(A)$. This shows that ρ is epic. The remaining part of the proof is left as exercise for the reader.

(37.26) COROLLARY. *Let R be a discrete valuation ring.*

- (i) *If Λ is a maximal R -order in a separable K -algebra A , then the maps ρ, ω, ω' in (37.25) are isomorphisms.*
- (ii) *If $\Lambda = M_n(R)$, then $N(\Lambda) = u(\Lambda) \cdot u(K)$.*

Proof. (i) Let $(X) \in \text{Picent } \Lambda$. By (37.24) we may assume that X is a two-sided Λ -ideal in A , such that $KX = A$. Then ${}_A X \cong {}_\Lambda \Lambda$ by (18.10), and hence $(X) \in \text{im } \omega$ by (37.16). This proves that ω is epic, and establishes assertion (i) of the corollary.

(ii) When $\Lambda = M_n(R)$ we have $\text{Picent } \Lambda \cong \text{Picent } R = 1$, and so the second assertion of the corollary follows from the first.

One of our ultimate aims is to evaluate Picent of a maximal order. As a first step in this direction, we treat the complete local case.

(37.27) THEOREM. *Let R be a complete discrete valuation ring, and let Λ be a maximal R -order in a central simple K -algebra A with skewfield part D . Then*

$$\text{Picent } \Lambda \cong \mathbf{Z}/e\mathbf{Z},$$

where $e = e(D/K)$ is the ramification index of D over K . If the discriminant $d(\Lambda/R)$ equals R , then $\text{Picent } \Lambda = 1$.

Proof. Let π be a prime element of R , and let π_D be a prime element of Δ , where Δ is the unique maximal R -order in D (see §12). Then

$$\pi\Delta = (\pi_D\Delta)^e, \quad \text{rad } \Lambda = \pi_D\Delta$$

by §13 and (17.5). Therefore $\pi\Lambda = (\text{rad } \Lambda)^e$. But by (17.3), $I(\Lambda)$ is the infinite cyclic group generated by $\text{rad } \Lambda$. Since

$$\text{Picent } \Lambda \cong I(\Lambda)/\{\pi^k\Lambda : k \in \mathbf{Z}\}$$

by (37.24), we obtain $\text{Picent } \Lambda \cong \mathbf{Z}/e\mathbf{Z}$, as desired.

If $e > 1$, then $(\text{rad } \Lambda)^{e-1}$ divides the different $\mathfrak{D}(\Lambda/R)$, by Step 2 of the proof of (25.4). Therefore $\pi^{e-1}R$ divides the discriminant $d(\Lambda/R)$. Hence if $d(\Lambda/R) = R$, then necessarily $e = 1$ and $\text{Picent } \Lambda = 1$. This completes the proof.

In order to generalize the preceding theorem to the case where R is an arbitrary Dedekind domain, we now prove an important result concerning the relation between global and local Picard groups. This result will be valid for all orders, whether or not they are maximal.

(37.28) **Theorem.** Let Λ be any R -order in a separable K -algebra A , where R is a Dedekind domain with quotient field K , and let $C = c(\Lambda)$. For each maximal ideal P of R , let Λ_P denote the P -adic completion of Λ . Then $\text{Picent } \Lambda_P = 1$ almost everywhere, and there is an exact sequence

$$(37.29) \quad 1 \rightarrow \text{Picent } C \xrightarrow{\tau} \text{Picent } \Lambda \xrightarrow{\varepsilon} \prod_P \text{Picent } \Lambda_P \rightarrow 1.$$

The map τ is given by

$$\tau(L) = (L \otimes_C \Lambda), \quad (L) \in \text{Picent } C.$$

Proof. Step 1. For each maximal ideal P of R , let $R_{(P)}$ denote the localization of R at P (as defined in §3), and let R_P be the P -adic completion of R . We may identify R_P with the completion of the discrete valuation ring $R_{(P)}$ relative to its maximal ideal $P \cdot R_{(P)}$. As pointed out in § 5a, for each finitely generated R -module M , we may form its P -adic completion M_P by first forming the localization $M_{(P)} = R_{(P)} \otimes_R M$, and then passing to completions:

$$M_P = R_P \otimes_{R_{(P)}} M_{(P)} \cong R_P \otimes_R M.$$

Since A is a separable K -algebra, we know from (10.4) that there exists a maximal R -order in A , say Γ . By (11.6), Γ_P is a maximal R_P -order in A_P . But Λ and Γ are a pair of full R -lattices in A , and so by Exercise 4.6 we have $\Lambda_{(P)} = \Gamma_{(P)}$ a.e. Therefore $\Lambda_P = \Gamma_P$ a.e., which proves that for almost all P , Λ_P is a maximal R_P -order in A_P .

Now let $d(\Lambda/R)$ be the discriminant of Λ with respect to R (see §10, §25). Then $d(\Lambda/R)$ is a nonzero ideal of R , since A is a separable K -algebra, and we have

$$d(\Lambda_P/R_P) = \{d(\Lambda/R)\}_P$$

by Exercise 10.6. But $\{d(\Lambda/R)\}_P = R_P$ whenever $P \nmid d(\Lambda/R)$. Since there are only finitely many P 's dividing $d(\Lambda/R)$, it follows that $d(\Lambda_P/R_P) = R_P$ a.e.

Step 2. We have now shown that for all but a finite number of maximal ideals P of R , we have

$$(37.30) \quad \Lambda_P = \text{maximal } R_P\text{-order in } A_P, \quad \text{and} \quad d(\Lambda_P/R_P) = R_P.$$

We claim that $\text{Picent } \Lambda_P = 1$ whenever (37.30) holds true. To verify this, let us write $A_P = \sum A_i$, where each A_i is a central simple algebra over a field K_i containing K_P . Let R_i be the integral closure of R in K_i , so each R_i is a complete discrete valuation ring. By (10.5) we have $\Lambda_P = \sum \Lambda_i$, where for each i , Λ_i is a maximal R_i -order in A_i . Since $d(\Lambda_P/R_P) = R_P$, it follows from Exercise 25.1a that $d(\Lambda_i/R_i) = R_i$ for each i . Hence each $\text{Picent } \Lambda_i = 1$, by (37.27). Therefore

$$\text{Picent } \Lambda_P \cong \prod \text{Picent } \Lambda_i = 1$$

by Exercise 37.6. This shows that $\text{Picent } \Lambda_p = 1$ a.e., as asserted.

Step 3. We shall identify the set of left C -modules with the set of (C, C) -bimodules over C . For each left C -module L , the bimodule structure ${}_A\Lambda_A$ permits us to view $L \otimes_C \Lambda$ as a (Λ, Λ) -bimodule over C . Explicitly we have

$$x(l \otimes \lambda)y = l \otimes x\lambda y, \quad l \in L, \quad x, \lambda, y \in \Lambda.$$

This construction may be visualized more easily as follows: given a C -submodule L of KC , we may form the two-sided Λ -submodule $L\Lambda$ in A . Denote by $I(C)$ the group of invertible C -ideals in KC . Then for each $L \in I(C)$, there is an isomorphism

$$L \otimes_C \Lambda \cong L\Lambda \quad \text{as } (\Lambda, \Lambda)\text{-bimodules.}$$

Furthermore, if $L \in I(C)$ is such that $LL' = C$, then

$$(L\Lambda)(L'\Lambda) = (L\Lambda)(L\Lambda) = \Lambda.$$

Hence for each $L \in I(C)$ we have $L\Lambda \in I(\Lambda)$.

Now let $(L) \in \text{Picent } C$; by (37.24), we may assume that $L \in I(C)$, and the preceding discussion shows that

$$\tau(L) = (L \otimes_C \Lambda) = (L\Lambda) \in \text{Picent } \Lambda.$$

For $L_1, L_2 \in I(C)$ we have $(L_1)(L_2) = (L_1 L_2)$ in $\text{Picent } C$, and hence

$$\tau(L_1) \tau(L_2) = (L_1 \Lambda \cdot L_2 \Lambda) = (L_1 L_2 \cdot \Lambda) = \tau(L_1 L_2).$$

Thus τ is a homomorphism. We must still show that τ is monic.

For any bimodule ${}_A M_\Lambda$, let us set

$$M^\Lambda = \{m \in M : \lambda m = m\lambda \text{ for all } \lambda \in \Lambda\}.$$

Then M^Λ is a C -module, whose isomorphism class depends only upon the class (M) . Obviously

$$(M + N)^\Lambda = M^\Lambda + N^\Lambda, \quad \Lambda^\Lambda = C,$$

if ${}_A N_\Lambda$ is another bimodule. We now verify that for each $(L) \in \text{Picent } C$,

$$(37.31) \quad \{L \otimes_C \Lambda\}^\Lambda = L \otimes_C C \cong L \text{ as } C\text{-modules.}$$

The formula is clearly valid when $L = C$, and hence also for every projective C -module L by (2.17), and hence it holds true whenever $(L) \in \text{Picent } C$.

Suppose now that $(L) \in \text{Picent } C$ is such that $\tau(L) = 1$, that is, $(L \otimes_C \Lambda) = (\Lambda)$. Then there are C -isomorphisms

$$L \cong (L \otimes_C \Lambda)^\Lambda \cong \Lambda^\Lambda = C,$$

and therefore $(L) = 1$ in $\text{Picent } C$. This completes the proof that τ is monic. Another proof of this fact is given in Exercise 37.12.

Step 4. The map τ' in (37.29) is defined by setting

$$\tau'(X) = \prod_P (X_P), \quad (X) \in \text{Picent } \Lambda.$$

It is clear that for each P , the (Λ_P, Λ_P) -bimodule X_P is invertible. Furthermore, $cx = xc$ for all $c \in C, x \in X$, since $(X) \in \text{Picent } \Lambda$. The same equality therefore holds for all $c \in C_P, x \in X_P$. But $C_P = c(\Lambda_P)$ by Exercise 37.14, and hence $(X_P) \in \text{Picent } \Lambda_P$. This shows that $\text{im } \tau' \subset \prod \text{Picent } \Lambda_P$, and obviously τ' is a homomorphism.

We now prove that $\text{im } \tau \subset \ker \tau'$, that is, $(L_P \Lambda_P) = 1$ in $\text{Picent } \Lambda_P$ for each $L \in I(C)$ and each P . Since C is an R -submodule of Λ , C is itself an R -order in KC . Therefore C_P is an R_P -order, whence $\text{Picent } C_P = 1$ by (37.22). Consequently $L_P = C_P u$ for some unit $u \in (KC)_P$, and hence

$$(L_P \Lambda_P) = (u \Lambda_P) = 1 \text{ in } \text{Picent } \Lambda_P.$$

This proves that $\text{im } \tau \subset \ker \tau'$.

To prove the reverse inclusion, suppose that $(X) \in \text{Picent } \Lambda$ is such that $\tau'(X) = 1$, that is, $(X_P) = 1$ in $\text{Picent } \Lambda_P$ for each P . We may assume that $X \in I(\Lambda)$, and so $X_P \in I(\Lambda_P)$ for each P . It follows from Exercise 37.8 that for each P there exists a unit $c_P \in c(A_P)$ such that $X_P = \Lambda_P c_P$. Furthermore, since $X_P = \Lambda_P$ a.e., we may choose $c_P = 1$ a.e. Now set

$$L = KC \cap \left\{ \bigcap_P C_P c_P \right\}, \quad L' = KC \cap \left\{ \bigcap_P C_P c_P^{-1} \right\}.$$

By (5.3), L and L' are C -lattices in KC such that

$$L_P = C_P c_P, \quad L'_P = C_P c_P^{-1} \quad \text{for all } P.$$

Therefore

$$LL' = KC \cap \left\{ \bigcap_P L_P L'_P \right\} = KC \cap \left\{ \bigcap_P C_P \right\} = C,$$

whence L and L' are invertible C -ideals in KC . Thus $(C) \in \text{Picent } C$, and we need only verify that $(X) = \tau(L)$. For each P we have

$$X_P = \Lambda_P c_P = \Lambda_P L_P,$$

and therefore

$$X = A \cap \left\{ \bigcap_P X_P \right\} = A \cap \left\{ \bigcap_P (\Lambda L)_P \right\} = \Lambda L.$$

This proves that $\ker \tau' \subset \text{im } \tau$, and completes the proof that $\text{im } \tau = \ker \tau'$.

Step 5. It remains for us to prove that τ' is epic. Suppose that for each P we are given an element $X(P) \in I(\Lambda_P)$, and we wish to find an $(X) \in \text{Picent } \Lambda$ such

that $\tau'(X) = \prod P X(P)$. Since $\text{Picent } \Lambda_p = 1$ a.e., we may assume that $X(P) = \Lambda_p$ a.e. Now set

$$X = A \cap \left\{ \bigcap_P X(P) \right\}.$$

By (5.3), X is a two-sided Λ -submodule of A such that $X_p = X(P)$ for all P .

For each P , let $Y(P)$ be the inverse of $X(P)$, and set

$$Y = A \cap \left\{ \bigcap_P Y(P) \right\}.$$

Then, as above, Y is also a two-sided Λ -submodule of A such that $Y_p = Y(P)$ for all P . But then $XY = YX = \Lambda$, since these equalities hold locally at all P . This shows that $(X) \in \text{Picent } \Lambda$, and that $\tau'(X) = \prod X(P)$. Hence τ' is epic, and the proof of Theorem 37.28 is finished.

The exactness of the sequence (37.29) shows that the calculation of $\text{Picent } \Lambda$ can be carried out in two steps:

- (i) The determination of the group $\text{Picent } C$ for a commutative order C ,
- (ii) The determination of the groups $\text{Picent } \Lambda_p$ for local orders Λ_p .

There is the further problem of determining the structure of the extension $\text{Picent } \Lambda$, once $\text{Picent } C$ and $\prod \text{Picent } \Lambda_p$ are known. There are as yet no general results concerning this last question.

(37.32) **COROLLARY.** *Let R be a Dedekind domain, and let Λ be a maximal R -order in a central simple K -algebra A . For each maximal ideal P of R dividing the discriminant $d(\Lambda/R)$, let e_p be the ramification index of the skewfield part of A_p over K_p . Then there is an exact sequence of commutative groups*

$$(37.33) \quad 1 \rightarrow \text{Cl } R \rightarrow \text{Picent } \Lambda \rightarrow \prod_{P \mid d(\Lambda/R)} \mathbf{Z}/e_p \mathbf{Z} \rightarrow 1.$$

If K is a global field, then for each P , e_p equals the local index m_p of A at P .

Proof. In this case Λ has center R , and $\text{Picent } R \cong \text{Cl } R$ by (37.24). The group $\text{Picent } \Lambda$ is abelian, since $I(\Lambda)$ is abelian by (22.10). Further, for each P we know that Λ_p is a maximal R_p -order in the central simple K_p -algebra A_p , and $d(\Lambda_p/R_p) = \{d(\Lambda/R)\}_p$. It follows from (37.27) that $\text{Picent } \Lambda_p = 1$ whenever $P \nmid d(\Lambda/R)$, and that $\text{Picent } \Lambda_p \cong \mathbf{Z}/e_p \mathbf{Z}$ whenever $P \mid d(\Lambda/R)$. Then (37.33) is just the exact sequence in (37.29). Finally, $e_p = m_p$ when K is a global field, by (14.3).

It is of interest to compare the groups $\text{Picent } \Lambda$ and $\text{Cl } \Lambda$ when Λ is a maximal order. Most of the remaining material in this section comes from Fröhlich–Reiner–Ullom [1], where non-maximal orders are also considered.

(37.34) THEOREM. Let Λ be a maximal R -order, as in (37.32). There is a homomorphism

$$\theta: \text{Picent } \Lambda \rightarrow \text{Cl } \Lambda,$$

given by $\theta(X) = [X]$, $(X) \in \text{Picent } \Lambda$. If K is a global field and $A = \text{Eichler}/R$ (see Remark 37.41), then

$$\ker \theta \cong \text{Outcent } \Lambda.$$

Proof. The map θ carries the bimodule isomorphism class $(_A X_\Lambda)$ onto the stable isomorphism class $[_A X]$. Now let $(X), (Y) \in \text{Picent } \Lambda$; without loss of generality, we may assume that $X, Y \in I(\Lambda)$ and that $X \subset \Lambda$. Setting $T = \Lambda/X$, we obtain an exact sequence of (Λ, Λ) -bimodules

$$0 \rightarrow X \rightarrow \Lambda \rightarrow T \rightarrow 0,$$

where T is an R -torsion bimodule. Since $_A Y$ is projective, the sequence

$$0 \rightarrow X \otimes Y \rightarrow Y \rightarrow T \otimes Y \rightarrow 0$$

is also exact, where \otimes means \otimes_{Λ} . By (18.10), $Y_P \cong \Lambda_P$ as left Λ_P -modules, for each P . Therefore

$$T \otimes Y \cong \sum_P (T \otimes Y)_P \cong \sum_P T_P \otimes Y_P \cong \sum_P T_P \cong T$$

as left Λ -modules. Since $_A Y$ is projective, we may apply Schanuel's Lemma (see Exercise 2.7) to the above pair of exact sequences, so as to deduce that

$$X + Y \cong \Lambda + X \otimes Y \quad \text{as left } \Lambda\text{-modules.}$$

Hence $[X] + [Y] = [X \otimes Y]$ in $\text{Cl } \Lambda$, which proves that θ is a homomorphism.

Now let K be a global field and let $A = \text{Eichler}/R$. If $(X) \in \text{Picent } \Lambda$ is such that $\theta(X) = 1$, then $[X] = [\Lambda]$, whence $X \cong \Lambda$ as left Λ -modules by (35.13). This latter condition holds if and only if $(X) \in \text{im } \omega$, by (37.16). Therefore $\ker \theta = \text{im } \omega \cong \text{Outcent } \Lambda$, as claimed, and the proof is done.

(37.35) THEOREM. Keep the above notation, and let K be a global field. If K is a function field, assume further that $A = \text{Eichler}/R$. Let $(A:K) = n^2$, and for each maximal ideal P of R , let κ_P be the local capacity of A at P , and m_P the local index. There is a homomorphism

$$t_n: \text{Cl } R \rightarrow \text{Cl}_A R,$$

induced by mapping each R -ideal J in K onto J^n . Then

$$\text{cok } \theta \cong \text{Cl}_A R / W \cdot \text{im } t_n,$$

where W is the subgroup of $\text{Cl}_A R$ generated by the classes of

$$\{P^{\kappa_P} : P \mid d(\Lambda/R)\}.$$

Proof. We have

$$\mathrm{Cl} R = I(R)/P(R), \quad \mathrm{Cl}_A R = I(R)/P_A(R),$$

in terms of the notation preceding (35.6). If no infinite prime of K ramifies in A , then $P(R) = P_A(R)$ and t_n is obviously a homomorphism. On the other hand, if some infinite prime of K does ramify in A , then n must be even, and hence $(Ra)^n \in P_A(R)$ for each $a \in K^*$. Thus t_n is a well defined homomorphism in any case.

By (35.14), the reduced norm map $\mathrm{nr}_{A/K}$ induces an isomorphism $v: \mathrm{Cl} \Lambda \cong \mathrm{Cl}_A R$. Hence

$$\mathrm{cok} \theta \cong \mathrm{Cl}_A R / \{v[X]: X \in I(\Lambda)\}.$$

Each P determines a unique prime ideal \mathfrak{P} of Λ containing P , and these ideals $\{\mathfrak{P}\}$ generate $I(\Lambda)$ as a free abelian group, as proved in (22.10). Furthermore, for each P we have

$$n = m_P \kappa_P, \quad \mathrm{nr}_{A/K} \mathfrak{P} = P^{\kappa_P}$$

by (25.11). Thus $\{v[X]: X \in I(\Lambda)\}$ is the subgroup of $\mathrm{Cl}_A R$ generated by all classes $\{P^{\kappa_P}\}$, P arbitrary. But $\kappa_P = n$ except when $m_P > 1$, that is, except when $P \mid d(\Lambda/R)$. Hence this subgroup is precisely $W \cdot \mathrm{im} t_n$, and the theorem is proved. (Another approach is given in Exercise 37.15)

We shall now compare the maps θ, θ' , where

$$\theta: \mathrm{Picent} \Lambda \rightarrow \mathrm{Cl} \Lambda, \quad \theta': \mathrm{Picent} \Gamma \rightarrow \mathrm{Cl} \Gamma,$$

for the case where Γ is a full matrix ring $M_n(\Lambda)$ over a maximal order Λ . Our main result is

(37.36) THEOREM. *Let Λ be a maximal R -order in a central simple K -algebra A , where K is a global field and $A = \text{Eichler}/R$ (see Remark 37.41). Let $n \geq 1$, and set $E = M_n(R)$, $\Gamma = M_n(\Lambda)$. We may identify Γ with $E \otimes_R \Lambda$. Then*

(i) *There is a commutative diagram of groups, with exact rows:*

$$(37.37) \quad \begin{array}{ccccccc} 1 & \rightarrow & \mathrm{Outcent} \Lambda & \xrightarrow{\alpha} & \mathrm{Picent} \Lambda & \xrightarrow{\beta} & \mathrm{Cl} \Lambda \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\ 1 & \rightarrow & \mathrm{Outcent} \Gamma & \xrightarrow{\alpha'} & \mathrm{Picent} \Gamma & \xrightarrow{\beta'} & \mathrm{Cl} \Gamma, \end{array}$$

where

$$\alpha(f) = 1 \otimes f, \quad \beta(X) = (E \otimes_R X), \quad \gamma[Y] = [E \otimes_R Y].$$

(ii) *Let*

$$(37.38) \quad (\mathrm{Cl} \Lambda)_n = \{\xi \in \mathrm{Cl} \Lambda : n\xi = 0\}, \quad n \cdot \mathrm{Cl} \Lambda = \{n\xi : \xi \in \mathrm{Cl} \Lambda\}.$$

Then

$$\ker \gamma = (\mathrm{Cl} \Lambda)_n, \quad \mathrm{cok} \gamma \cong \mathrm{Cl} \Lambda / n \cdot \mathrm{Cl} \Lambda.$$

(iii) *There is an exact sequence of groups*

$$(37.39) \quad 1 \rightarrow \text{Outcent } \Lambda \xrightarrow{\alpha} \text{Outcent } \Gamma \xrightarrow{\beta} (\text{Cl } \Lambda)_n \rightarrow \text{cok } \theta \rightarrow \text{cok } \theta' \\ \rightarrow \text{Cl } \Lambda/n \cdot \text{Cl } \Lambda \rightarrow 0.$$

Proof. The top row of (37.37) is exact by (37.34). Next we note that $K\Gamma = M_n(A)$, which is also Eichler/ R . Hence we may apply (37.34) to the maximal order Γ , so as to obtain the exact sequence occurring in the bottom row of (37.37). It is clear that (37.37) is a commutative diagram, since all of the maps α, β, γ are induced by $E \otimes_R \cdot$. This establishes assertion (i) of the theorem.

Now let $\varphi: \text{Cl } \Lambda \cong \text{Cl } \Gamma$ be the isomorphism which occurs in the commutative diagram (36.7). We claim that $\gamma = n \cdot \varphi$. Using the notation of (36.7), it suffices to prove that $\mu' \gamma = \mu' \cdot n\varphi$. For $[Y] \in \text{Cl } \Lambda$, we have

$$\mu' \gamma [Y] = \mu' [E \otimes_R Y] = [E \otimes_R \Lambda] - [E \otimes_R Y] \in K_0(\Gamma),$$

whereas

$$\mu' \cdot n\varphi [Y] = n[L \otimes_\Lambda \cdot] \mu [Y] = n\{[L \otimes_\Lambda \Lambda] - [L \otimes_\Lambda Y]\} \in K_0(\Gamma).$$

But in $K_0(\Gamma)$ we have

$$[E \otimes_R \Lambda] = n[L \otimes_\Lambda \Lambda], \quad [E \otimes_R Y] = n[L \otimes_\Lambda Y]$$

by Exercise 37.3. This completes the proof that $\gamma = n\varphi$. Since φ is an isomorphism, it follows at once that $\ker \gamma = (\text{Cl } \Lambda)_n$, and that

$$\text{cok } \gamma = \text{Cl } \Gamma/n \cdot \varphi(\text{Cl } \Lambda) \cong \text{Cl } \Lambda/n \cdot \text{Cl } \Lambda.$$

Finally let us prove (iii). By Exercise 37.2, the map β is an isomorphism. Hence the following diagram is commutative, and has exact rows:

$$\begin{array}{ccccccc} 1 & \rightarrow & \text{Picent } \Lambda & \xrightarrow{\beta} & \text{Picent } \Gamma & \rightarrow & 1 \\ \downarrow & & \downarrow \theta & & \downarrow \theta' & & \downarrow \\ 0 \rightarrow \ker \gamma \rightarrow & \text{Cl } \Lambda & \xrightarrow{\gamma} & \text{Cl } \Gamma & & & \end{array}$$

By the “Snake Lemma” (see Exercise 2.8) there exists an exact sequence

$$1 \rightarrow \ker \theta \rightarrow \ker \theta' \rightarrow \ker \gamma \rightarrow \text{cok } \theta \xrightarrow{\gamma_*} \text{cok } \theta',$$

where γ_* is induced by γ . Then

$$\text{cok } \gamma_* = \{\text{Cl } \Gamma/\text{im } \theta'\}/\gamma_* \{\text{Cl } \Lambda/\text{im } \theta\} \cong \text{cok } \gamma.$$

Hence the sequence

$$\text{cok } \theta \xrightarrow{\gamma_*} \text{cok } \theta' \rightarrow \text{cok } \gamma \rightarrow 0$$

is also exact. This establishes that (37.39) is exact, and completes the proof of the theorem.

(37.40) COROLLARY. Let $\Gamma = M_n(\Lambda)$ as in (37.36), and keep the notation and hypotheses of that theorem. Then

(i) For each $f \in \text{Aut}_R \Gamma$, we have $f^n = (1 \otimes g)\eta$ for some $g \in \text{Aut}_R \Lambda$ and some inner automorphism η of Γ .

(ii) $\text{Out}_R M_n(R) \cong (\text{Cl } R)_n$. Hence for each $f \in \text{Aut}_R M_n(R)$, f^n is an inner automorphism of $M_n(R)$.

Proof. Let ζ be the map occurring in (37.39). Since Γ has center R , we have

$$\text{Aut}_{\text{cent}} \Gamma = \text{Aut}_R \Gamma, \quad \text{Out}_{\text{cent}} \Gamma = \text{Out}_R \Gamma.$$

For $f \in \text{Aut}_R \Gamma$, let \tilde{f} denote its image in $\text{Out}_R \Gamma$. Then $\zeta(\tilde{f}^n) = n \cdot \zeta(\tilde{f}) = 0$, whence $\tilde{f}^n \in \text{im } \alpha$. Hence $f^n = (1 \otimes g)\eta$ for some $g \in \text{Aut}_R \Lambda$ and some $\eta \in \text{In } \Gamma$, which proves (i).

Now let $\Lambda = R$. Then $\ker \theta = 1$, $\text{cok } \theta = 0$, since θ is an isomorphism. The exactness of (37.39) then gives

$$\text{Out}_R \Gamma \cong (\text{Cl } R)_n,$$

as claimed. The remaining assertion in (i) is now clear, and the corollary is proved. The result (ii) is due originally to Rosenberg-Zelinsky [1].

(37.41) *Remark.* As part of the hypotheses of Theorems 37.34, 37.36 and 37.40, we assumed that

$$(37.42) \quad K = \text{global field}, \quad A = \text{Eichler}/R.$$

By (35.13), these assumptions imply that

$$(37.43) \quad [X] = [Y] \text{ in } \text{Cl } \Lambda \Leftrightarrow X \cong Y \text{ as left } \Lambda\text{-lattices.}$$

It was precisely this result, rather than (37.42) itself, which was needed in the proof of (37.34). The other two theorems, (37.36) and (37.40), depend on (37.34). Thus all three theorems remain valid if, in their hypotheses, we replace condition (37.42) by the weaker condition (37.43).

It may well happen that in some cases, (37.43) holds true but (37.42) does not. For example, the quaternion algebra A in (26.5) fails to satisfy the Eichler condition relative to \mathbf{Z} ; nevertheless, (37.43) holds for the maximal \mathbf{Z} -order Λ given in (26.5), since in fact we showed in §26 that every left Λ -ideal in A is principal. Even when K is not a global field, there are cases where (37.43) is valid; an obvious example is that obtained by choosing $A = K$, $\Lambda = R$. In fact, as we shall see in (38.13), stable isomorphism implies isomorphism whenever Λ is a commutative order.

EXERCISES

1. Verify the assertions of (37.13).
2. Let $E = M_n(R)$, where R is a commutative ring and $n \geq 1$. Let Λ be an R -algebra, and $\Gamma = E \otimes_R \Lambda \cong M_n(\Lambda)$. Show that the isomorphism $\text{Pic}_R \Lambda \cong \text{Pic}_R \Gamma$ given in

(37.9), arising from the Morita equivalence of Λ and Γ over R , is also given by the map

$$(X) \rightarrow (E \otimes_R X), \quad (X) \in \text{Pic}_R \Lambda.$$

[Hint: Let $L = R^{(n)} \otimes_R \Lambda$, viewed as bimodule ${}_L L_\Lambda$ after identifying Γ with $\text{Hom}_\Lambda(L, L)$. Let $L^{-1} = \text{Hom}_\Lambda(L, \Lambda)$, viewed as (Λ, Γ) -bimodule. By (37.9), the map defined by

$$(X) \rightarrow (L \otimes_\Lambda X \otimes_\Lambda L^{-1}), \quad (X) \in \text{Pic}_R \Lambda,$$

gives an isomorphism $\text{Pic}_R \Lambda \cong \text{Pic}_R \Gamma$. However, there are two-sided Γ -isomorphisms

$$\begin{aligned} L \otimes_\Lambda X \otimes_\Lambda L^{-1} &\cong \text{Hom}_\Lambda(L, L \otimes_\Lambda X) \\ &\cong \text{Hom}_\Lambda(\Lambda^{(n)}, X^{(n)}) \cong E \otimes_R X. \end{aligned}$$

Therefore $(L \otimes_\Lambda X \otimes_\Lambda L^{-1}) = (E \otimes_R X)$ in $\text{Pic}_R \Gamma$.]

3. Keep the above notation. Show that for each $[Y] \in K_0(\Lambda)$ (see §36),

$$[E \otimes_R Y] = n[L \otimes_\Lambda Y] \quad \text{in } K_0(\Gamma).$$

[Hint: $L \otimes_\Lambda Y \cong R^{(n)} \otimes_R Y$ as left Γ -modules. But E is isomorphic to a direct sum of n copies of the left E -module $R^{(n)}$, and so

$$[E \otimes_R Y] = n[R^{(n)} \otimes_R Y] = n[L \otimes_\Lambda Y],$$

as desired.]

4. An R -algebra E is an *Azumaya R-algebra* (or *central separable R-algebra*) if E has center R , and E is R -separable (see Exercise 7.9). Show that for every R -algebra Λ and every Azumaya R -algebra E , there is an isomorphism

$$\text{Pic}_R \Lambda \cong \text{Pic}_R \Lambda \otimes_R E$$

given by $(X) \rightarrow (X \otimes_R E)$, $(X) \in \text{Pic}_R \Lambda$.

[Hint: (see DeMeyer–Ingraham [1]). Let $E^e = E \otimes_R E^\circ$ be the enveloping algebra of E . Since E is an Azumaya R -algebra, the (E^e, R) -bimodule E is invertible, and E^e is Morita equivalent to R . There are maps

$$\begin{array}{ccccc} \text{Pic}_R \Lambda & \xrightarrow{\psi_1} & \text{Pic}_R \Lambda \otimes E & \xrightarrow{\psi_2} & \text{Pic}_R \Lambda \otimes E \otimes E^\circ \otimes E \\ & & \downarrow \eta & & \downarrow \eta' \\ & & \text{Pic}_R \Lambda & \xrightarrow{\psi_1} & \text{Pic}_R \Lambda \otimes E. \end{array}$$

The diagram commutes, and η, η' are isomorphisms by (37.9) and Exercise 2. Likewise, the maps $\psi_2 \psi_1$ and $\psi_3 \psi_2$ are isomorphisms. Hence also ψ_1 is an isomorphism.]

5. Let Λ be an R -algebra with center C , and keep the notation of (37.11) and (37.19). Show that the following diagram has exact rows and is commutative, and that ω, ω' are monic.

$$\begin{array}{ccccccc} 1 & \rightarrow & \text{Out}_C \Lambda & \rightarrow & \text{Out}_R \Lambda & \rightarrow & \text{Aut}_R C \\ & & \omega \downarrow & & \omega' \downarrow & & 1 \downarrow \\ 1 & \rightarrow & \text{Picent } \Lambda & \rightarrow & \text{Pic}_R \Lambda & \xrightarrow{\Phi} & \text{Aut}_R C. \end{array}$$

6. Let $\Lambda = \sum_{i=1}^t \Lambda_i$ be a direct sum of rings. Prove that

$$\text{Picent } \Lambda \cong \prod_{i=1}^t \text{Picent } \Lambda_i.$$

[Hint: Let $e_1, \dots, e_t \in \Lambda$ be the central idempotents such that $\Lambda_i = \Lambda e_i$. Each $(X) \in \text{Picent } \Lambda$ is such that $e_i X = X e_i$, and thus $(e_i X) \in \text{Picent } \Lambda_i$, $1 \leq i \leq t$. The desired isomorphism is given by $(X) \rightarrow \prod_{i=1}^t (e_i X)$, $(X) \in \text{Picent } \Lambda$.]

7. Let $\Lambda = \sum_{i=1}^t \Lambda_i$ be a direct sum of R -algebras. Show that $\text{Pic}_R \Lambda$ need not be isomorphic to $\prod_{i=1}^t \text{Pic}_R \Lambda_i$.

In Exercises 8–10, let R be a domain with quotient field K , and let Λ be an R -order in a K -algebra A . We write ${}_\Lambda M_\Lambda \subset A$ to indicate that M is a two-sided Λ -submodule of A .

8. Let ${}_\Lambda M_\Lambda \subset A$. Show that there is a bimodule isomorphism $M \cong \Lambda$ if and only if $M = \Lambda c$ for some $c \in u(c(A))$. [Hint: Surely $\Lambda c \cong \Lambda$ for each such c . Conversely, let $\theta: \Lambda \cong M$ be a bimodule isomorphism, and let $c = \theta(1)$. Then θ extends to a bimodule isomorphism $A \cong KM$, so $A = KM = K\Lambda \cdot c$, whence $c \in u(A)$. Further,

$$\theta(1) \cdot a = \theta(a) = a \cdot \theta(1), \quad a \in A,$$

so $c \in u(A)$.]

9. Let ${}_\Lambda M_\Lambda, {}_\Lambda N_\Lambda \subset A$ be such that $MN = NM = \Lambda$. Show that M is an invertible bimodule, and that $(M) \in \text{Picent } \Lambda$, and $(M)^{-1} = (N)$ in $\text{Picent } \Lambda$. [Hint: The maps

$$\mu : M \otimes_\Lambda N \rightarrow MN = \Lambda, \quad v : N \otimes_\Lambda M \rightarrow NM = \Lambda,$$

give a Morita context in which both μ, v are epic, and hence monic.]

10. Let $(X) \in \text{Picent } \Lambda$ be such that $(KX) = 1$ in $\text{Picent } A$. Show that $(X) = (M)$ for some invertible Λ -ideal M in A . [Hint: Since ${}_\Lambda X_\Lambda$ is invertible, ${}_\Lambda X$ is finitely generated and projective as Λ -module, and thus $X \rightarrow KX$ is an embedding. By hypothesis, there is a bimodule isomorphism $f: KX \cong A$. Then $M = f(X) \cong X$, and ${}_\Lambda M_\Lambda \subset A$. Replacing M by rM with suitably chosen $r \in R$, $r \neq 0$, we may assume that $M \subset \Lambda$. If $(X)^{-1} = (Y)$, then likewise $Y \cong N$ for some ${}_\Lambda N_\Lambda \subset \Lambda$. We have a Morita context

$$M \otimes_\Lambda N \cong \Lambda, \quad N \otimes_\Lambda M \cong \Lambda.$$

The map $\theta: M \otimes N \rightarrow MN$ is epic; it is also monic, since each of the maps below is monic:

$$M \otimes N \rightarrow \Lambda \otimes N \rightarrow \Lambda \otimes \Lambda \rightarrow \Lambda.$$

Consequently $MN \cong \Lambda$, $NM \cong \Lambda$. By Exercise 8, we have

$$MN = \Lambda c, \quad NM = \Lambda c' \quad \text{for some } c, c' \in u(c(A)).$$

Then $Nc = Nc'$, and Nc^{-1} is an inverse of M .]

11. Complete the proof of (37.25).
12. Keep the hypotheses and notation of (37.28), and let $L \in I(C)$ be such that $L\Lambda \cong \Lambda$ as (Λ, Λ) -bimodules. Without using (37.28), show that $(L) = 1$ in Picent C . [Hint: By Exercise 8, $L\Lambda = \Lambda c$ for some $c \in u(KC)$. Replacing L by $c^{-1}L$, we may assume that $L\Lambda = \Lambda$. Therefore also $L'\Lambda = \Lambda$, where $L' \in I(C)$ is such that $LL' = C$. We have $L \subset \Lambda \cap KC = C$, and likewise $L' \subset C$. Now C is a commutative R -order in a separable K -algebra, so for each maximal ideal P of R we have Picent $C_P = 1$. Hence we may write $L_P = C_P x_P, (L')_P = C_P y_P$, for some $x_P, y_P \in C_P$. Then $x_P y_P C_P = C_P$, so $x_P \in u(C_P)$ and $L_P = C_P$. This holds for each P , whence $L = C$.]

13. Let A be a K -algebra, where K is a field, and let E be any extension field of K . Prove that

$$c(E \otimes_K A) = E \otimes_K c(A).$$

[Hint: Clearly $c(E \otimes_K A) \supset E \otimes_K c(A)$. The reverse inclusion follows from the first paragraph of the proof of (7.6), if we take $B = E$ in that argument.]

14. Let Λ be an R -order with center C , where R is a Dedekind domain. Prove that Λ_P has center C_P . [Hint: Let $\Lambda^e = \Lambda \otimes_R \Lambda^0$ be the enveloping algebra of Λ (see §7), and view Λ as left Λ^e -module. Then there is an identification

$$C = \text{Hom}_{\Lambda^e}(\Lambda, \Lambda).$$

Therefore by (2.37)

$$C_P = \text{Hom}_{(\Lambda_P)^e}(\Lambda_P, \Lambda_P) = c(\Lambda_P).$$

15. Keep the notation and hypotheses of (37.35). Show that the diagram

$$\begin{array}{ccccccc} 1 & \rightarrow & \text{Cl } R & \rightarrow & \text{Picent } \Lambda & \rightarrow & \prod_p \mathbf{Z}/m_p \mathbf{Z} \rightarrow 1 \\ & & \downarrow t_n & & \downarrow \theta & & \downarrow P \\ 1 & \rightarrow & \text{Cl}_A R & \rightarrow & \text{Cl } \Lambda & \rightarrow & 1 \end{array}$$

is commutative and has exact rows. Deduce from the “Snake Lemma” that the sequence of groups

$$(37.44) \quad 1 \rightarrow \ker t_n \rightarrow \ker \theta \rightarrow \prod_p \mathbf{Z}/m_p \mathbf{Z} \rightarrow \text{cok } t_n \rightarrow \text{cok } \theta \rightarrow 1$$

is exact.

38. NON-MAXIMAL ORDERS

The term “non-maximal order” refers to an order which may be maximal or not. This section is intended to serve as a guide to further study of orders, as well as to indicate some generalizations to non-maximal orders of the material in §§35–37. During the past fifteen years, there have appeared numerous research articles on the theory of orders. There are, however, relatively few books or lecture notes dealing with this topic. The principal ones are as follows:

(i) The lecture notes by Roggenkamp, Huber–Dyson [1] and Roggenkamp [1] contain a systematic treatment of orders. The first of these references contains Chapters I–V of the list below, and overlaps the present book considerably; it also contains an extensive bibliography. The second volume (Chapters VI–X) is devoted to proofs of the major recent developments in the theory of orders, up to 1969. It has a small bibliography, supplementing that of the first volume. The chapter headings are these:

- I. Preliminaries on rings and modules.
- II. Homological algebra.
- III. The Morita theorems and separable algebras.
- IV. Maximal orders.
- V. The Higman ideal and extensions of modules.
- VI. Modules over orders, one-sided ideals over maximal orders.
- VII. Genera of lattices.
- VIII. Grothendieck groups.
- IX. Special types of orders.
- X. The number of indecomposable lattices over orders.

(ii) The lecture notes by Swan–Evans [1] provide an elegant and largely self-contained treatment of many topics in the theory of orders. The authors presuppose a basic knowledge of homological algebra. In a few places, they use some results from Swan [2]. Chapter headings:

1. Introduction.
2. Frobenius functors.
3. Finiteness theorems.
4. Results on K_0 and G_0 .
5. Maximal orders.
6. Orders.
7. K_0 of a maximal order.
8. K_1 and G_1 .
9. Cancellation theorems.
- Appendix.

(iii) The survey article by Reiner [1] contains an extensive summary (without proofs) of the principal results on orders, and a large bibliography. Section headings are as follows:

1. Introduction. Notation and definitions.
2. General remarks. Jordan–Zassenhaus theorem.
3. Extensions.
4. Higman ideal.
5. Representations over local domains.

6. Genus.
7. Maximal orders.
8. Further results on genera.
9. Projective modules and relative projective modules.
10. Grothendieck groups and Whitehead groups.
11. Commutative orders and related results.
12. Divisibility of modules.
13. Hereditary orders.
14. Finiteness of the number of indecomposable representations.
15. Representations of specific groups and orders.
16. Representation rings.
17. Group rings.
18. Algebraic number theory.
19. Krull–Schmidt and Cancellation Theorems.

(iv) Chapter XI of Curtis–Reiner [1], entitled “Integral Representations”, is concerned with the theory of orders.

(v) There are two major references which deal primarily with maximal orders. The first, by Deuring [1], has an extensive bibliography covering research before 1935. The exposition is self-contained but succinct. Chapter headings are:

- I. Grundlagen.
- II. Die Struktursätze.
- III. Darstellungen der Algebren durch Matrizes.
- IV. Einfache Algebren.
- V. Faktorensysteme.
- VI. Theorie der ganzen Größen.
- VII. Algebren über Zahlkörpern. Zusammenhang mit der Arithmetik der Körper.

The second reference is Weil [1]. This work is self-contained, except that familiarity with Haar measure is assumed. Chapters are:

- I. Locally compact fields.
- II. Lattices and duality over local fields.
- III. Places of A-fields.
- IV. Adeles.
- V. Algebraic number fields.
- VI. The theorem of Riemann–Roch.
- VII. Zeta-functions of A-fields.

- VIII. Traces and norms.
- IX. Simple algebras.
- X. Simple algebras over local fields.
- XI. Simple algebras over A-fields.
- XII. Local classfield theory.
- XIII. Global classfield theory.

In the present book, the following sections contain material on non-maximal orders: §§6, 8, 18, 26, 27, 36–41.

We shall now sketch a generalization of the results in §§35–37 to the case of non-maximal orders. For the remainder of this section, let Λ be an R -order, maximal or not, in a separable K -algebra A . As usual, R denotes a Dedekind domain with quotient field K . Since Λ need not decompose into a direct sum of orders in simple algebras, we may no longer restrict our attention to the case of central simple algebras.

Recall from §27 that two left Λ -lattices M, N are in the same *genus* (notation: $M \vee N$) if $M_P \cong N_P$ as left Λ_P -lattices, for each maximal ideal P of R . By (18.2 iii), in this definition it is immaterial whether the subscript P denotes localization or completion. Call M *locally free* (of rank n) if $M \vee \Lambda^{(n)}$. (If Λ is maximal, then by (18.10) *every* left Λ -ideal M in A , such that $KM = A$, is locally free of rank 1. More generally, any left Λ -lattice X , such that $KX \cong A^{(n)}$, is locally free of rank n by (27.8).)

Whether or not Λ is a maximal order, we shall define the *locally free class group* of Λ , denoted by $\text{Cl } \Lambda$, as follows: the elements of $\text{Cl } \Lambda$ are stable isomorphism classes $[M]$ of locally free left Λ -lattices M in A (see Exercise 38.1). As in (35.3), we define addition of classes thus: given $M, M' \vee \Lambda$, by (27.3) there exists an $M'' \vee \Lambda$ such that $M + M' \cong \Lambda + M''$. We then set $[M] + [M'] = [M'']$. To show that inverses exist in $\text{Cl } \Lambda$, we need only modify the proof of (35.5) by using Exercises 27.6 and 27.7 in the parts of the proof where we previously used Theorems 27.4 and 27.8.

The results in (35.6)–(35.14) need not be true for non-maximal orders. Before stating Jacobinski's generalization of these results, we introduce the following definition:

(38.1) *Definition.* Let Λ be an R -order in a separable K -algebra A , where R is a Dedekind domain and K is a global field. For each simple component A_i of A , let R_i denote the integral closure of R in the center of A_i . We say that A *satisfies the Eichler condition relative to R* (notation: $A = \text{Eichler}/R$) if for each i , $A_i = \text{Eichler}/R_i$. This definition extends that given in (34.3).

Remark. Let $R = \text{alg. int. } \{K\}$, where K is an algebraic number field, and let G be a finite group. Set $A = KG$, the group algebra of G over K . Following

the approach in Swan–Evans [1], we may give some *sufficient* conditions that $A = \text{Eichler}/R$. Indeed, if $A \neq \text{Eichler}/R$, then some simple component A_i of A must be a totally definite quaternion algebra over its center L . Since this can never occur if L has any complex primes, we deduce

(i) *If K has any complex primes, then $A = \text{Eichler}/R$.*

Next, suppose that A_i is a totally definite quaternion algebra; then its completion at each real prime of L must be the quaternions \mathbf{H} over the real field \mathbf{R} . Thus the composition of maps

$$KG = A \rightarrow A_i \rightarrow \mathbf{H}$$

gives a homomorphism of G onto a subgroup \bar{G} of $u(\mathbf{H})$, and necessarily \mathbf{H} equals $\mathbf{R}\bar{G}$. Surely \bar{G} must be nonabelian, since \mathbf{H} is a noncommutative ring.

The nonabelian finite subgroups of \bar{G} of $u(\mathbf{H})$ are known explicitly (see Coxeter [1], Coxeter–Moser [1]), and are as follows:

$$\begin{cases} \text{generalized quaternion group of order } 4n, n \geq 2, \\ \text{binary tetrahedral group } \langle 2, 3, 3 \rangle \text{ of order 24,} \\ \text{binary octahedral group } \langle 2, 3, 4 \rangle \text{ of order 48,} \\ \text{binary icosahedral group } \langle 2, 3, 5 \rangle \text{ of order 120.} \end{cases}$$

Hence we conclude

(ii) *$A = \text{Eichler}/R$ if G has no homomorphic image in the above list.*

We now state without proof:

(38.2) THEOREM (Jacobinski [2, 3]). *Let Λ be an R -order in a separable K -algebra A , where K is a global field, and where $A = \text{Eichler}/R$. Let \mathcal{S} be the finite set consisting of all maximal ideals P of R such that Λ_P is not a maximal R_P -order in A_P . Keeping the notation of (38.1), let $C = \sum R_i$, so KC is the center of A . Denote by $I(C, \mathcal{S})$ the multiplicative group of all C -lattices J in KC such that*

$$K \cdot J = KC, \quad J_P = C_P \text{ for all } P \in \mathcal{S}.$$

Let

$$P_\Lambda(C) = \{C \cdot \text{nr}_{A/KC} x : x \in A, x \in u(\Lambda_P) \text{ for all } P \in \mathcal{S}\},$$

a subgroup of $I(C, \mathcal{S})$ consisting of certain principal C -ideals in KC . Then the locally free class group $\text{Cl } \Lambda$ satisfies

$$(38.3) \quad \text{Cl } \Lambda \cong I(C, \mathcal{S})/P_\Lambda(C).$$

Furthermore, if M, N are Λ -lattices in the same genus as Λ , then

$$(38.4) \quad [M] = [N] \text{ in } \text{Cl } \Lambda \iff M \cong N.$$

(38.5) Remarks. (i) if Λ is maximal, the set \mathcal{S} may be taken to be the empty

set. The isomorphism occurring in (38.3) can then be described component-wise, according to the simple components of A . At each simple component, we obtain precisely the isomorphism given in (35.14).

(ii) In the preceding theorem, the subscript P denotes completion. The result holds equally well if we use localizations rather than completions.

(iii) An idele-theoretic version of this theorem, due to Fröhlich [2], holds even when $A \neq \text{Eichler}/R$. See also Wilson [1].

(iv) $\text{Cl}\Lambda$ is a finite group by virtue of the Jordan-Zassenhaus Theorem.

Let us turn next to the material in §36. The definition of $K_0(\Lambda)$ given in §36 holds for all rings Λ , and hence surely for all orders Λ , maximal or not. The map $\mu: \text{Cl}\Lambda \rightarrow K_0(\Lambda)$ occurring in (36.4) is monic, whether or not Λ is maximal. However, the sequence (36.4) need not be exact, and (36.5) need not hold true.

Now let $\Gamma = M_n(\Lambda)$, and keep the notation of (36.6). Most of the proof of (36.6) remains valid when Λ is any R -order in a separable K -algebra. It shows that, in the notation of (36.7), there is a commutative diagram

$$(38.6) \quad \begin{array}{ccc} \text{Cl}\Lambda & \xrightarrow{\mu} & K_0(\Lambda) \\ \varphi \downarrow & & \downarrow L \otimes_{\Lambda} \cdot \\ \text{Cl}M_n(\Lambda) & \xrightarrow{\mu'} & K_0(M_n(\Lambda)), \end{array}$$

where μ, μ' are monic, and where $\varphi, L \otimes_{\Lambda} \cdot$ are isomorphisms. As a consequence of the above, we have

(38.7) COROLLARY. *Let Λ be an R -order in a separable K -algebra A , where K is an algebraic number field. Let $\Gamma = M_2(\Lambda)$, $B = K\Gamma = M_2(A)$. Let C, \mathcal{S} be as in (38.2). Then whether or not $A = \text{Eichler}/R$, we have*

$$\text{Cl}\Lambda \cong \text{Cl}\Gamma \cong I(C, \mathcal{S})/P_{\Gamma}(C).$$

Proof. Since K is an algebraic number field, it follows that $B = \text{Eichler}/R$ even if $A \neq \text{Eichler}/R$. The ring C and the set \mathcal{S} are the same for Γ as for Λ . The formula for $\text{Cl}\Gamma$ is just the one given by (38.3), with Γ in place of Λ .

All of the material in §37, up to and including (37.22), is valid for arbitrary R -orders (and indeed for R -algebras). The important results (37.23)–(37.25), and the fundamental (37.28), were established in §37 for all R -orders, maximal or not. Of course, Theorems 37.26, 37.27 and 37.32 hold only for the case of maximal orders.

It is possible to salvage (37.34), by introducing the *locally free Picard group* $LFP(\Lambda)$. This is the subgroup of $\text{Picent}\Lambda$ consisting of all $(X) \in \text{Picent}\Lambda$ such

that X is locally free as left Λ -module. (Such X 's are necessarily of rank 1.) By Exercise 38.4, $LFP(\Lambda)$ is indeed a group, and consists of all bimodule isomorphism classes (X) , where X ranges over all two-sided Λ -submodules of A such that $X \vee \Lambda$ as left Λ -modules. (Each such X is necessarily an invertible bimodule, by Exercise 38.4.)

If Λ is a maximal order, then

$$LFP(\Lambda) = \text{Picent } \Lambda$$

by (18.10). This also holds true whenever Λ is commutative, but not necessarily maximal, by virtue of (37.22).

Returning to arbitrary orders, consider the map $\omega: \text{Outcent } \Lambda \rightarrow \text{Picent } \Lambda$. Clearly its image lies in $LFP(\Lambda)$, and hence there is a monomorphism

$$\omega: \text{Outcent } \Lambda \rightarrow LFP(\Lambda),$$

with $\omega(f) = ({}_1\Lambda_f)$. It follows at once from (37.16) that for $(X), (Y) \in LFP(\Lambda)$,

$$(38.8) \quad {}_A X \cong {}_A Y \iff (Y) \in (X) \cdot \text{im } \omega.$$

Furthermore, since $LFP(C) = \text{Picent } C$, we deduce from (37.29) that there is an exact sequence

$$(38.9) \quad 1 \rightarrow LFP(C) \xrightarrow{\epsilon} LFP(\Lambda) \rightarrow \prod_p LFP(\Lambda_p) \rightarrow 1,$$

with $LFP(\Lambda_p) = 1$ a.e. Finally, we have

$$\begin{aligned} LFP(\Lambda_p) &= \{(X) \in \text{Picent } \Lambda_p : X \cong \Lambda_p \text{ as left } \Lambda_p\text{-modules}\} \\ &\cong \text{Outcent } \Lambda_p. \end{aligned}$$

Generalizing (37.34), we prove

(38.10) THEOREM (Fröhlich–Reiner–Ullom [1]). *For any R -order in a separable K -algebra A , there is a homomorphism*

$$\theta: LFP(\Lambda) \rightarrow \text{Cl } \Lambda,$$

given by $\theta(X) = [X]$, $(X) \in LFP(\Lambda)$. Furthermore, suppose that† for left Λ -lattices M, N in the genus of Λ ,

$$(38.11) \quad [M] = [N] \iff M \cong N$$

Then

$$\ker \theta \cong \text{Outcent } \Lambda.$$

Proof. The first half of the proof of (37.34) carries over unchanged, and shows that θ is a well defined homomorphism. Now assume that (38.11) holds true,

† This hypothesis is satisfied whenever K is a global field and $A = \text{Eichler}/R$, by virtue of (38.4). It also holds for arbitrary K when Λ is a commutative order, by virtue of (38.13) below.

and let $(M) \in LFP(\Lambda)$. Then

$$\theta(M) = 1 \iff [M] = [\Lambda] \text{ in } \text{Cl } \Lambda \iff {}_{\Lambda}M \cong {}_{\Lambda}\Lambda.$$

But ${}_{\Lambda}M \cong {}_{\Lambda}\Lambda$ if and only if $(M) \in \text{im } \omega$, by (38.8). This shows that $\ker \theta = \text{im } \omega$, whence $\ker \theta \cong \text{Outcent } \Lambda$ as claimed.

(38.12) COROLLARY. *For any commutative R-order in Λ in a separable K-algebra A, we have*

$$\text{Picent } \Lambda = LFP(\Lambda) \cong \text{Cl } \Lambda.$$

Proof. We shall identify the set of left Λ -modules with the set of (Λ, Λ) -bimodules over Λ ; this can be done since Λ is commutative. We have already remarked that $\text{Picent } \Lambda = LFP(\Lambda)$, by (37.22). Let us now show that θ is an isomorphism. By (38.10), we have $\ker \theta \cong \text{Outcent } \Lambda = 1$, so θ is monic. Further, each element of $\text{Cl } \Lambda$ is of the form $[M]$, for some locally free Λ -lattice M in A . By Exercise 38.4, M is an invertible (Λ, Λ) -bimodule, and hence $(M) \in LFP(\Lambda)$. Clearly $\theta(M) = [M]$, so θ is epic. This completes the proof of the corollary.

In the preceding discussion we made use of the following result, which is of independent interest.

(38.13) THEOREM (Kaplansky). *Let R be any noetherian domain with quotient field K, let Λ be any commutative R-order in a K-algebra A (not necessarily separable over K). By a “ Λ -ideal in A” we mean a finitely generated Λ -submodule M of A such that $KM = A$.*

(i) *Let $M_1, \dots, M_t, N_1, \dots, N_t$ be Λ -ideals in A such that*

$$M_1 \dot{+} \cdots \dot{+} M_t \cong N_1 \dot{+} \cdots \dot{+} N_t \text{ as } \Lambda\text{-modules.}$$

Then

$$M_1 \cdots M_t \cong N_1 \cdots N_t \text{ as } \Lambda\text{-modules,}$$

where these products are computed within A.

(ii) *Two Λ -ideals in A are stably isomorphic if and only if they are isomorphic.*

Proof. (i) The hypotheses imply that for all i, j between 1 and t ,

$$\text{Hom}_A(KM_i, KN_j) \cong K \otimes_K \text{Hom}_{\Lambda}(M_i, N_j).$$

Furthermore, the map

$$\text{Hom}_{\Lambda}(M_i, N_j) \rightarrow \text{Hom}_A(KM_i, KN_j)$$

is monic.

Now let $\varphi: \sum M_i \cong \sum N_j$ be a Λ -isomorphism. Then φ can be extended to an A -isomorphism $\varphi_*: A^{(t)} \cong A^{(t)}$. Hence there exists an invertible matrix $\mu = (\alpha_{ij}) \in M_t(A)$ such that

$$\varphi(m_1, \dots, m_t) = (\alpha_{ij})(m_1, \dots, m_t)^T, \quad m_i \in M_i, \quad 1 \leq i \leq t,$$

where T denotes “transpose”. Therefore

$$(38.14) \quad \alpha_{ij} M_j \subset N_i, \quad 1 \leq i, j \leq t.$$

Set $d = \det \mu$; then $d \in u(A)$ since μ is invertible. Furthermore, d is a sum of products of the form

$$\pm \alpha_{\pi(1), 1} \cdots \alpha_{\pi(t), t},$$

where π is a permutation on $\{1, \dots, t\}$. It follows from (38.14) that

$$d \cdot M_1 \cdots M_t \subset N_1 \cdots N_t.$$

On the other hand, φ^{-1} also extends to an A -isomorphism $(\varphi^{-1})_*: A^{(t)} \cong A^{(t)}$, described by the matrix μ^{-1} of determinant d^{-1} . The above reasoning shows that

$$d^{-1} \cdot N_1 \cdots N_t \subset M_1 \cdots M_t.$$

Therefore $\prod N_i = d \cdot \prod M_i$, whence $\prod N_i \cong \prod M_i$ as claimed.

(ii) Now let M, N be Λ -ideals in A which are stably isomorphic. Then $M + \Lambda^{(r)} \cong N + \Lambda^{(r)}$ for some r , whence $M \cong N$ by (i). This completes the proof of the theorem.

To conclude this section, we give the following generalization of (37.36):

(38.14) THEOREM. Let Λ be an R -order in a separable K -algebra A , where R is a Dedekind domain. Assume† that condition (38.11) holds, that is, stable isomorphism implies isomorphism for locally free left Λ -lattices. Let $n \geq 1$, and set $E = M_n(R)$, $\Gamma = E \otimes_R \Lambda \cong M_n(\Lambda)$, as in (37.36). Then all of the assertions (i)–(iii) in (37.36) remain true, provided that in (37.37) we replace Picent by LFP. Furthermore, (37.40 i) holds true in this case.

Proof. The proofs of (37.37) and (37.40) carry over with only minor modifications. We omit the details.

It is worth pointing out a stronger version of (37.40 ii), namely

(38.15) COROLLARY. Let Λ be a commutative R -order in a separable K -algebra A . Then

$$\text{Outcent } M_n(\Lambda) \cong (\text{Cl } \Lambda)_n$$

for each $n \geq 1$.

† See footnote to (38.10).

Proof. By (38.12) θ is an isomorphism, whence $\text{cok } \theta = 0$. Further, $\text{Outcent } \Lambda = 1$ since Λ is commutative. The desired result now follows from the exactness of the sequence (37.39) asserted in (38.14).

EXERCISES

In the following, Λ is an R -order in a separable K -algebra A , where R is a Dedekind domain.

1. Prove that stably isomorphic left Λ -lattices are in the same genus. [Hint: Let X, Y be Λ -lattices such that

$$X \dot{+} \Lambda^{(r)} \cong Y \dot{+} \Lambda^{(r)}.$$

Complete at an arbitrary P , then show that $X_P \cong Y_P$ by Exercise 6.7.]

2. Prove that every locally free left Λ -lattice is Λ -projective. [Hint: See (3.23).]

3. Let

$$N(\Lambda) = \{x \in u(A) : x\Lambda x^{-1} = \Lambda\},$$

the *normalizer* of Λ in A . Show that

$$N(\Lambda) = \{x \in u(A) : x\Lambda x^{-1} \subset \Lambda\}.$$

[Hint: Let $x \in u(A)$ be such that $x\Lambda = \Lambda x$. By Exercise 10.7,

$$\text{ord}_R \Lambda/x\Lambda = \text{ord}_R \Lambda/\Lambda x.$$

Hence $x\Lambda = \Lambda x$ by (4.17).]

4. Let X be a two-sided Λ -submodule of A . Show that if X is locally free as left Λ -module, then $X \vee \Lambda$ and X is an invertible bimodule whose inverse is also locally free. Deduce from this that $LFP(\Lambda)$ is a subgroup of Picent Λ . [Hint: If $X \vee \Lambda^{(n)}$ then $KX \cong A^{(n)}$, so $n = 1$ and $X \vee \Lambda$. Now put $Y = \{a \in A : Xa \subset \Lambda\}$, another bimodule in A . To prove that X is invertible, we need only show that $XY = YX = \Lambda$. It suffices to verify this after passing to completions. Changing notation, assume that R is complete and that $X = \Lambda u$, where $u \in u(A)$. Then $\Lambda u \cdot \Lambda = \Lambda u$ since X is a bimodule, whence $u\Lambda \subset \Lambda u$. Thus $u\Lambda = \Lambda u$ by Exercise 3, and hence $Y = u^{-1}\Lambda = \Lambda u^{-1}$.]

5. Let R be a principal ideal domain with quotient field K , and let $\Gamma = M_n(R)$, where $n \geq 1$. Show that every invertible matrix $x \in M_n(K)$, such that $x\Gamma x^{-1} = \Gamma$, is of the form $x = \alpha y$ for some nonzero $\alpha \in K$ and some $y \in u(\Gamma)$. [Hint: Take $\Lambda = R$ in (38.15) to deduce that $\text{Outcent } \Gamma = 1$. By (37.25), $\text{Outcent } \Gamma \cong N(\Gamma)/u(\Gamma)u(K)$, where $N(\Gamma)$ is the normalizer of Γ in $K\Gamma$. Hence $N(\Gamma) = u(\Gamma)u(K)$.]

6. Let G be a finite group, R a Dedekind domain with quotient field K , and let $\Lambda = RG$, $A = KA = KG$. Suppose that $|G| \neq 0$ in R , and that no prime divisor of $|G|$ is a unit in R . A fundamental theorem due to Swan asserts that, in this case, every projective left Λ -lattice is locally free. Deduce from this that there is a split exact sequence of additive groups

$$(38.16) \quad 0 \rightarrow \text{Cl } \Lambda \xrightarrow{\mu} K_0(\Lambda) \xrightarrow{\psi} K_0(A),$$

where

$$\mu[M] = [\Lambda] - [M], [M] \in \text{Cl } \Lambda; \quad \psi[X] = [K \otimes_R X], [X] \in K_0(\Lambda).$$

[Hint: Imitate the relevant parts of the proof of Theorem 36.3. The sequence (38.16) splits, since $K_0(A)$ is a free \mathbf{Z} -module by Exercise 36.3.]

9. Hereditary Orders

We shall first present the results of Harada [1–5] and Brumer [1] concerning hereditary orders in separable algebras. The approach used is that of Jacobinski [4]. As we shall see, we can give an explicit description of the structure of hereditary orders. We can also determine the relationship between a hereditary order and the maximal orders which contain it. The local theory in §39 will be applied in §40 to obtain the global theory of hereditary orders. In §41 we consider integral group rings, and prove several theorems which fit in well with the subject matter of this book.

Throughout this chapter, R denotes a Dedekind domain with quotient field K , and Λ is an R -order in a separable K -algebra A . Recall that Λ is (left) *hereditary* if every left ideal of Λ is projective; by (10.7), this occurs if and only if every left Λ -lattice is projective. Now the ring Λ is left and right noetherian, since Λ is finitely generated as R -module. Therefore, as remarked in (2.45 iii), Λ is left hereditary if and only if Λ is right hereditary. A direct proof of this fact is given in Theorem 40.1 below. Hence in our discussion of hereditary orders, we may omit the adjectives “left” and “right”.

39. LOCAL THEORY OF HEREDITARY ORDERS

Throughout this section let R be a complete discrete valuation ring with maximal ideal $P = \pi R$ and residue class field \bar{R} . As we shall see, the key to studying hereditary orders is the investigation of their Jacobson radicals. The first result is due to Auslander–Goldman [1]:

(39.1) **THEOREM.** *An R -order Λ is hereditary if and only if $\text{rad } \Lambda$ is a projective left Λ -module, or equivalently, if and only if $\text{rad } \Lambda$ is an invertible (Λ, Λ) -bimodule.*

Proof. *Step 1.* Let $J = \text{rad } \Lambda$. Surely J is left Λ -projective if Λ is hereditary. Conversely, assume that $\wedge J$ is projective. We shall show that Λ is hereditary by proving that every left ideal L of Λ is projective. Given any L , there is a Λ -exact sequence

$$0 \rightarrow L \rightarrow \Lambda^{(r)} \rightarrow L \rightarrow 0$$

for some r , where L is a left Λ -lattice. We prove below that $\text{Ext}^1(L, L) = 0$, where Ext means Ext_Λ . Once this is known, it follows that the above sequence is Λ -split. Therefore $L|_{\Lambda^{(r)}}$, so L is Λ -projective, whence Λ is hereditary as claimed.

The Λ -exact sequence

$$0 \rightarrow L \xrightarrow{\pi} L \rightarrow L/\pi L \rightarrow 0$$

gives rise to an exact sequence

$$\text{Ext}^1(L, L) \xrightarrow{\pi} \text{Ext}^1(L, L) \rightarrow \text{Ext}^2(L/\pi L, L)$$

by (2.29), where the arrows labelled “ π ” are the maps given by multiplication by π . We set $M = L/\pi L$, and we show below that $\text{Ext}^2(M, L) = 0$. This will imply that

$$\pi \cdot \text{Ext}^1(L, L) = \text{Ext}^1(L, L),$$

whence $\text{Ext}^1(L, L) = 0$ by (2.34) and Nakayama’s Lemma.

The left Λ -module M is artinian, since $\pi M = 0$. We prove by induction on the Λ -composition length of M that $\text{Ext}^2(M, L) = 0$ for every left Λ -module L . Suppose first that M is a simple Λ -module; then M is also a simple left $\bar{\Lambda}$ -module, where $\bar{\Lambda}$ is the semisimple artinian ring Λ/J . Therefore $M|\bar{\Lambda}$, whence $\text{Ext}^2(M, L)$ is a direct summand of $\text{Ext}^2(\bar{\Lambda}, L)$ by (2.28 iv). However, there is a Λ -exact sequence

$$0 \rightarrow J \rightarrow \Lambda \rightarrow \bar{\Lambda} \rightarrow 0,$$

and ${}_J J$ is projective by hypothesis. Hence by (2.27) we obtain $\text{Ext}^2(\bar{\Lambda}, L) = 0$ for all L . Therefore $\text{Ext}^2(M, L) = 0$ for all simple Λ -modules M and all Λ -modules L .

Now suppose that the Λ -module M has composition length at least two, and let S be any simple submodule of M . The Λ -exact sequence

$$0 \rightarrow S \rightarrow M \rightarrow M/S \rightarrow 0$$

gives an exact sequence

$$\text{Ext}^2(M/S, L) \rightarrow \text{Ext}^2(M, L) \rightarrow \text{Ext}^2(S, L).$$

Since the first term vanishes by the induction hypothesis, and since the last term is 0, it follows that $\text{Ext}^2(M, L) = 0$ for all L . This completes the proof that Λ is left hereditary whenever ${}_J J$ is projective. Analogously, Λ is right hereditary whenever J_Λ is projective.

Step 2. We now prove that Λ is hereditary if and only if J is an invertible (Λ, Λ) -bimodule. If J is invertible, then ${}_J J$ is projective by (16.7) or §37, whence Λ is hereditary. For the harder part of the proof, suppose now that

Λ is hereditary, so both ${}_{\Lambda}J$ and J_{Λ} are projective modules. Then $J|\Lambda^{(r)}$ for some r . We shall use this fact in a moment.

Let

$$\Lambda = \sum_{i=1}^t M_i, \quad \{M_i\} \text{ indecomposable left ideals,}$$

with the $\{M_i\}$ numbered so that $\{M_1, \dots, M_u\}$ are a full set of non-isomorphic modules among the $\{M_i\}$. Setting $\bar{M}_i = M_i/JM_i$, it follows from (6.22) that $\{\bar{M}_1, \dots, \bar{M}_u\}$ are a full set of non-isomorphic simple left (Λ/J) -modules.

Since $J|\Lambda^{(r)}$, it follows by Exercise 6.8 that

$$J \cong \sum_{i=1}^u M_i^{(n_i)}$$

for some non-negative integers $\{n_i\}$. Therefore

$$J/J^2 \cong \sum_{i=1}^u \bar{M}_i^{(n_i)} \text{ as left } \Lambda\text{-modules,}$$

and so each $n_i > 0$ by Exercise 6.9. Thus $\Lambda|J^{(s)}$ for some s , whence by (15.2) ${}_{\Lambda}J$ is a progenerator for the category ${}_{\Lambda}\mathcal{M}$. Setting $\Delta = \text{Hom}_{\Lambda}(J, J)$, it follows from (16.9) that the rings Λ, Δ are Morita equivalent, so ${}_{\Lambda}J_{\Delta}$ is an invertible bimodule (see §37) and $\Lambda = \text{Hom}_{\Delta}(J, J)$. Using the identification $\text{Hom}_{\Delta}(J, J) = O_l(J)$, we conclude at once that $\Lambda = O_l(J)$. But then, by symmetry, also $\Lambda = O_r(J)$. Therefore J is an invertible (Λ, Λ) -bimodule, as claimed. This completes the proof of the theorem. (See also Remark following (39.18).)

As preparation for our later discussion, we introduce the following notation:

(39.2) *Definition.* Let Γ be a ring. For each ideal \mathfrak{a} of Γ , let $(\mathfrak{a})^{m \times n}$ denote the set of all $m \times n$ matrices with entries in \mathfrak{a} . If $\{\mathfrak{a}_{ij} : 1 \leq i, j \leq r\}$ is a set of ideals in Γ , we write

$$\Lambda = \left[\begin{array}{cccc} (\mathfrak{a}_{11}) & (\mathfrak{a}_{12}) & \dots & (\mathfrak{a}_{1r}) \\ (\mathfrak{a}_{21}) & (\mathfrak{a}_{22}) & \dots & (\mathfrak{a}_{2r}) \\ \dots & \dots & \dots & \dots \\ (\mathfrak{a}_{r1}) & (\mathfrak{a}_{r2}) & \dots & (\mathfrak{a}_{rr}) \end{array} \right]^{(\mathfrak{a}_{ij})^{n_i \times n_j}}$$

to indicate that Λ is the set of all matrices $[T_{ij}]_{1 \leq i, j \leq r}$, where for each pair (i, j) , the matrix T_{ij} ranges over all elements of $(\mathfrak{a}_{ij})^{n_i \times n_j}$.

Now let V be an n -dimensional right vector space over a skewfield Ω , and set $\text{End}_{\Omega} V = \text{Hom}_{\Omega}(V, V)$. Thus $\text{End}_{\Omega} V$ is the Ω -endomorphism ring of V , and we shall view V as an $(\text{End}_{\Omega} V, \Omega)$ -bimodule. Some of the calculations

which follow are more easily understood by using matrices instead of linear transformations. Once we pick an Ω -basis for V , we may identify V with the space $\Omega^{n \times 1}$ of all $n \times 1$ column vectors over Ω . This gives rise to an identification $\text{End}_\Omega V = M_n(\Omega)$, where the matrices act from the left on the column vectors from V .

A *chain* in V is a strictly decreasing sequence

$$(39.3) \quad E : V = V_0 > V_1 > \cdots > V_r = 0$$

of Ω -subspaces of V . We set

$$n_i = \dim_\Omega V_{i-1}/V_i, \quad 1 \leq i \leq r,$$

and call the ordered r -tuple $\{n_1, \dots, n_r\}$ the *invariants* of the chain E . Now define the *chain ring* $O(E)$ by

$$(39.4) \quad O(E) = \{x \in \text{End}_\Omega V : xV_i \subset V_i, \quad 0 \leq i \leq r\}.$$

We may choose an Ω -basis of V *adapted* to the chain E , that is, the first n_1 basis elements map onto a basis for V_0/V_1 , the next n_2 elements onto a basis for V_1/V_2 , and so on. Clearly $n_1 + \cdots + n_r = n$, and the last $n_i + \cdots + n_r$ basis elements of V form a basis for the subspace V_{i-1} . Relative to this basis, we may identify $O(E)$ with a subring of $M_n(\Omega)$. It is easily seen that $O(E)$ consists of all matrices

$$(39.5) \quad \begin{bmatrix} T_{11} & 0 & 0 & \cdots & 0 \\ T_{21} & T_{22} & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ T_{r1} & T_{r2} & T_{r3} & \cdots & T_{rr} \end{bmatrix},$$

where for $1 \leq j \leq i \leq r$, the matrix T_{ij} ranges over all elements of the additive group $\text{Hom}_\Omega(V_{j-1}/V_j, V_{i-1}/V_i)$. Hence in the notation of (39.2), we may write

$$(39.6) \quad O(E) = \left[\begin{array}{ccccc} (\Omega) & (0) & (0) & \cdots & (0) \\ (\Omega) & (\Omega) & (0) & \cdots & (0) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ (\Omega) & (\Omega) & (\Omega) & \cdots & (\Omega) \end{array} \right]^{(n_1, \dots, n_r)}.$$

We collect some facts about chain rings.

(39.7) THEOREM. *Let the chain E in (39.3) have invariants $\{n_1, \dots, n_r\}$, and let $B = O(E)$ be its chain ring. Then*

(i)

$$\text{rad } B = \{x \in B : xV_i \subset V_{i+1}, \quad 0 \leq i \leq r-1\}.$$

In terms of the identification in (39.6), $\text{rad } B$ is given by

$$(39.8) \quad \text{rad } B = \begin{bmatrix} (0) & (0) & (0) & \dots & (0) \\ (\Omega) & (0) & (0) & \dots & (0) \\ \dots & \dots & \dots & \dots & \dots \\ (\Omega) & (\Omega) & (\Omega) & \dots & (0) \end{bmatrix}^{\{n_1, \dots, n_r\}},$$

that is, $\text{rad } B$ consists of all matrices in (39.5) in which each $T_{ii} = 0$, $1 \leq i \leq r$.

(ii)

$$B/\text{rad } B \cong \sum_{i=1}^r \text{End}_\Omega(V_{i-1}/V_i) \cong \sum_{i=1}^r M_{n_i}(\Omega).$$

The left B -modules $\{V_{i-1}/V_i : 1 \leq i \leq r\}$ are a full set of non-isomorphic simple left B -modules.

(iii) For each t , $0 \leq t \leq r$, we have

$$V_t = (\text{rad } B)^t V, \quad (\text{rad } B)^t = \{x \in B : xV_i \subset V_{i+t}, \quad 0 \leq i \leq r\},$$

where we interpret V_s as 0 when $s \geq r$.

Proof. Let

$$N = \{x \in B : xV_i \subset V_{i+1}, \quad 0 \leq i \leq r-1\}.$$

Then N is a two-sided ideal of B , and $N^r = 0$, whence $N \subset \text{rad } B$. On the other hand, N is the kernel of the ring epimorphism

$$B \rightarrow \sum_{i=1}^r \text{End}_\Omega(V_{i-1}/V_i).$$

Since the direct sum is a semisimple ring, we conclude from Exercise 6.1 that $N \supset \text{rad } B$. This shows that $N = \text{rad } B$, and establishes (i) and the first statement in (ii). The second assertion in (ii) is an immediate consequence of the first.

The easiest way of proving (iii) is by means of matrices. Choosing an Ω -basis for V adapted to the chain E , we have identifications

$$V = \begin{bmatrix} (\Omega)^{n_1 \times 1} \\ \vdots \\ \vdots \\ \vdots \\ (\Omega)^{n_r \times 1} \end{bmatrix}, \quad V_t = \begin{bmatrix} (0) \\ \vdots \\ (0) \\ (\Omega)^{n_{t+1} \times 1} \\ \vdots \\ (\Omega)^{n_r \times 1} \end{bmatrix},$$

for $0 \leq t \leq r$. The assertions in (iii) are then immediate consequences of the matrix expression for $\text{rad } B$ given in part (i). This completes the proof.

By way of illustration, we remark that when the chain E is as fine as possible (that is, each $n_i = 1$), then upon choosing an Ω -basis of V adapted to E , the chain ring $O(E)$ may be identified with the ring of all lower triangular matrices in $M_n(\Omega)$. Its radical consists of all those lower triangular matrices with 0's along the main diagonal. Up to conjugacy, this ring $O(E)$ is the *smallest* chain ring in $M_n(\Omega)$. In this connection, see Exercise 39.5.

Now let B be any subring of $\text{End}_\Omega V$, not necessarily a chain ring. Setting $N = \text{rad } B$, we see that

$$E_B : V > NV > N^2V > \cdots > N^sV = 0$$

is a chain in V . Since $B \subset \text{End}_\Omega V$, it is clear that s is the least integer such that $N^s = 0$. We have

$$(39.9) \quad B \subset O(E_B), \quad \text{and} \quad \text{rad } B = N \subset \text{rad } O(E_B).$$

We are thus led to partially order the set of subrings of $\text{End}_\Omega V$, as follows: given two subrings B, B' of $\text{End}_\Omega V$, we say that B' *radically covers* B (notation: $B' \succ B$) if

$$B' \supset B, \quad \text{and} \quad \text{rad } B' \supset \text{rad } B.$$

Call B an *extremal subring* of $\text{End}_\Omega V$ if $B' \succ B$ implies that $B' = B$.

(39.10) LEMMA. *The extremal subrings of $\text{End}_\Omega V$ are precisely the chain rings.*

Proof. If B is extremal, then $B = O(E_B)$ by (39.9). Conversely, every chain ring $O(E)$ is an extremal subring, by Exercise 39.5.

We now turn to the analogues of these concepts for orders. Let Λ, Λ' denote R -orders in A . We say that Λ' *radically covers* Λ (notation: $\Lambda' \succ \Lambda$) if $\Lambda' \supset \Lambda$ and $\text{rad } \Lambda' \supset \text{rad } \Lambda$. The order Λ is called *extremal* if $\Lambda' \succ \Lambda$ implies that $\Lambda' = \Lambda$. Every maximal order Λ is obviously extremal, since

$$\Lambda' \succ \Lambda \Rightarrow \Lambda' \supset \Lambda \Rightarrow \Lambda' = \Lambda.$$

Our aim is to show that hereditary orders are the same as extremal orders. The problem can be reduced to the central simple case; in this case, we shall show that extremal orders correspond to extremal subrings of full matrix algebras over a skewfield. This correspondence will enable us to determine the structure of hereditary orders in central simple algebras. As a first step in this program, we prove

(39.11) THEOREM. *An R -order Λ in a separable K -algebra A is extremal if and only if $O_\ell(\text{rad } \Lambda) = \Lambda$.*

Proof. Let $J = \text{rad } \Lambda$; since $J \supset P\Lambda$, it is clear that J is a full two-sided Λ -lattice in A . Set

$$\Gamma = O_i(J) = \{x \in A : xJ \subset J\}.$$

Then Γ is an R -order in A , and $J \subset \Lambda \subset \Gamma$. For large n , $J^n \subset P\Lambda \subset P\Gamma$; hence $J \subset \text{rad } \Gamma$ by Exercise 39.1, which shows that $\Gamma > \Lambda$. Hence $\Gamma = \Lambda$ if Λ is an extremal order.

Suppose conversely that $\Gamma = \Lambda$, and let us show that Λ is extremal. Let $\Lambda' > \Lambda$, and set $J' = \text{rad } \Lambda'$, so $J' \supset J$. Since $P^r \Lambda' \subset J$ for some r , it follows that $(J')^s \subset J$ for some s . Obviously $s > 0$, since otherwise $\Lambda' \subset J \subset \Lambda$, which is impossible. If $s \geq 2$ then

$$(J')^{s-1} \cdot J \subset (J')^{s-1} \cdot J' \subset J,$$

so $(J')^{s-1} \subset O_i(J) = \Lambda$. Hence $(J')^{s-1}$ is a two-sided ideal in Λ . But its s th power lies in J , whence also $(J')^{s-1} \subset J$. Continuing in this way, we find eventually that $J' \subset J$. Therefore $J' = J$, and so

$$\Lambda = O_i(J) = O_i(J') \supset \Lambda',$$

whence $\Lambda = \Lambda'$. This completes the proof.

(39.12) COROLLARY. *Hereditary orders are extremal.*

Proof. Let $J = \text{rad } \Lambda$, where Λ is hereditary. The last paragraph of the proof of (39.1) shows that $\Lambda = O_i(J)$. Hence Λ is extremal.

In order to facilitate reduction of the discussion to the central simple case, we now prove the local analogue of (10.5) for extremal orders.

(39.13) THEOREM. *Let $A = \sum_{i=1}^t A_i$ be the decomposition of the separable K -algebra A into simple components $\{A_i\}$, and let R_i be the integral closure of R in the center of A_i . Then every extremal R -order Λ in A is expressible as a direct sum $\Lambda = \sum_{i=1}^t \Lambda_i$, where each Λ_i is an extremal R_i -order in A_i . Conversely, every such direct sum $\sum \Lambda_i$ is an extremal R -order in A .*

Proof. Let $C = \sum_{i=1}^t R_i$, an R -order in the center of A . Then $C\Lambda$ is an R -order in A . Let $J = \text{rad } \Lambda$; then $J^m \subset P\Lambda$ for some m , whence $(CJ)^m \subset P \cdot C\Lambda$. Therefore $CJ \subset \text{rad } C\Lambda$ by Exercise 39.1, and so $C\Lambda > \Lambda$. Since Λ is extremal, this gives $\Lambda = C\Lambda$. But $C\Lambda = \sum_{i=1}^t R_i\Lambda$, and for each i , $R_i\Lambda$ is an extremal R_i -order in A_i . This completes the proof that each extremal order Λ decom-

poses into a direct sum $\sum \Lambda_i$, as claimed. The last assertion in the theorem is obvious, and the result is established.

Since we have shown that every hereditary order is extremal, the above decomposition theorem is valid for all hereditary orders. In (40.7) we shall obtain the global analogue of the above for hereditary orders.

The preceding paragraph shows that the classification of hereditary orders can always be reduced to the central simple case. The basic structure theorem for this case is as follows:

(39.14) **Theorem.** *Let Λ be an R -order in the central simple K -algebra A , where $A \cong M_n(D)$ and D is a skewfield with center K . Let Δ be the unique maximal R -order in D , and set $p = \text{rad } \Delta$, $\bar{\Delta} = \Delta/p$. Then*

(i) Λ is hereditary if and only if Λ is an extremal order.

(ii) Given any extremal order Λ in A , there exist positive integers $\{n_1, \dots, n_r\}$ with sum n , and there exists an identification $A = M_n(D)$, such that

$$(39.15) \quad \Lambda = \begin{bmatrix} (\Delta) & (p) & (p) & \dots & (p) \\ (p) & (\Delta) & (p) & \dots & (p) \\ (\Delta) & (\Delta) & (\Delta) & \dots & (p) \\ \dots & \dots & \dots & \dots & \dots \\ (\Delta) & (\Delta) & (\Delta) & \dots & (\Delta) \end{bmatrix}^{\{n_1, \dots, n_r\}}$$

using the notation in (39.2). Conversely, each such order Λ is extremal.

(iii) For the extremal order Λ in (39.15), we have

$$(39.16) \quad \text{rad } \Lambda = \begin{bmatrix} (p) & (p) & (p) & \dots & (p) \\ (p) & (\Delta) & (p) & \dots & (p) \\ (\Delta) & (\Delta) & (p) & \dots & (p) \\ \dots & \dots & \dots & \dots & \dots \\ (\Delta) & (\Delta) & (\Delta) & \dots & (p) \end{bmatrix}^{\{n_1, \dots, n_r\}}$$

and

$$(39.17) \quad \Lambda/\text{rad } \Lambda \cong \sum_{i=1}^r M_{n_i}(\bar{\Delta}).$$

Proof. Every hereditary order is extremal, by (39.12). To prove the converse, let Λ be an extremal order in A , and set $J = \text{rad } \Lambda$. Let $\Lambda \subset \Lambda'$ where Λ' is a maximal order in A with radical J' . Then $\Lambda + J' \succ \Lambda$ by Exercise 39.2, whence $\Lambda + J' = \Lambda$. Therefore $J' \subset J$, so $J' \subset J$ by Exercise 39.3. We set

$$\bar{\Lambda}' = \Lambda'/J', \quad \bar{\Lambda} = \Lambda/J', \quad \bar{J} = J/J'.$$

Then $\bar{\Lambda}$ is a subring of $\bar{\Lambda}'$, and $\bar{J} = \text{rad } \bar{\Lambda}$ by Exercise 39.4.

We now use the results of (17.4) and (17.5). We may find a right Δ -lattice M such that

$$\Lambda' = \text{End}_{\Delta} M \cong M_n(\Delta),$$

where $M \cong \Delta^{(n)}$ is a (Λ', Δ) -bimodule. Then

$$J' = \text{End}_{\Delta} M \mathfrak{p} \cong M_n(\mathfrak{p}), \quad \bar{\Lambda}' \cong \text{End}_{\bar{\Delta}} \bar{M} \cong M_n(\bar{\Delta}),$$

where

$$\bar{M} = M/M\mathfrak{p} = M/J'M \cong \bar{\Delta}^{(n)}.$$

Let ρ be the canonical map

$$\rho: \Lambda' \rightarrow \Lambda'/J' = M_n(\bar{\Delta}),$$

where we have identified Λ'/J' with $M_n(\bar{\Delta})$. Then $\Lambda = \rho(\bar{\Lambda})$, and we shall show that $\bar{\Lambda}$ is an extremal subring of $M_n(\bar{\Delta})$. For suppose that B is any subring of $M_n(\bar{\Delta})$ which radically covers $\bar{\Lambda}$, and let $\Lambda_0 = \rho^{-1}(B)$, $J_0 = \text{rad } \Lambda_0$. Then Λ_0 is an R -order in A such that $J' \subset \Lambda \subset \Lambda_0 \subset \Lambda'$, and so $J' \subset J_0$ by Exercise 39.3. Hence Exercise 39.4 gives

$$J_0/J' = \text{rad } \Lambda_0/J' = \text{rad } B \supset \text{rad } \bar{\Lambda} = J/J',$$

whence $J_0 \supset J$. Therefore $\Lambda_0 \geq \Lambda$, so $\Lambda_0 = \Lambda$ since Λ is an extremal order by hypothesis. This gives $B = \bar{\Lambda}$, and shows that $\bar{\Lambda}$ is an extremal subring of $M_n(\bar{\Delta})$.

We may now use (39.10) to obtain the structure of $\bar{\Lambda}$. We form the chain E in \bar{M} , given by

$$E : \bar{M} > J\bar{M} > J^2\bar{M} > \dots > J^r\bar{M} = 0.$$

Note that $J^i\bar{M} = \bar{J}^i\bar{M}$ for each i , since Λ' and Λ act on \bar{M} via the map ρ . Let $\{n_1, \dots, n_r\}$ be the invariants of the chain E , so by definition

$$n_i = \dim_{\bar{\Delta}} J^{i-1}\bar{M}/J^i\bar{M}, \quad 1 \leq i \leq r.$$

Then (39.6) and (39.8) give

$$\bar{\Lambda} = \begin{bmatrix} (\bar{\Delta}) & (0) & \dots & (0) \\ (\bar{\Delta}) & (\bar{\Delta}) & \dots & (0) \\ \dots & \dots & \dots & \dots \\ (\bar{\Delta}) & (\bar{\Delta}) & \dots & (\bar{\Delta}) \end{bmatrix}^{\{n_1, \dots, n_r\}}, \quad \bar{J} = \begin{bmatrix} (0) & (0) & \dots & (0) \\ (\bar{\Delta}) & (0) & \dots & (0) \\ \dots & \dots & \dots & \dots \\ (\bar{\Delta}) & (\bar{\Delta}) & \dots & (0) \end{bmatrix}^{\{n_1, \dots, n_r\}}.$$

Since the map ρ is precisely ‘‘reduction mod \mathfrak{p} ’’, and since

$$\Lambda = \rho^{-1}(\bar{\Lambda}), \quad J = \rho^{-1}(\bar{J}), \quad \Lambda/J \cong \bar{\Lambda}/\bar{J},$$

we immediately obtain the asserted formulas (39.15)–(39.17).

At this stage we have proved the first two implications in the chain

$$\Lambda \text{ hereditary} \Rightarrow \Lambda \text{ extremal} \Rightarrow \Lambda \text{ satisfies (39.15)} \Rightarrow \Lambda \text{ hereditary.}$$

To complete the proof of the theorem, we need only show that an order Λ given by (39.15) is necessarily hereditary. We set

$$\Lambda' = M_n(\Delta) \supset \Lambda, \quad J' = \text{rad } \Lambda' = M_n(p), \quad \rho: \Lambda' \rightarrow \Lambda'/J',$$

as before. Since ρ is “reduction mod p ”, it is clear from (39.15) that Λ/J is a chain ring in the matrix algebra $M_n(\bar{\Delta})$. But then we know $\text{rad } \Lambda/J$ from (39.8). Since $\text{rad } \Lambda = \rho^{-1}\{\text{rad } \Lambda/J\}$ by Exercise 39.4, we immediately obtain formula (39.16). The remaining formula (39.17) is then obvious.

We are still trying to prove that the order Λ given by (39.15) is hereditary. Let Λ_0 be the order in A defined by taking $n_1 = \dots = n_r = 1$ in (39.15). Since (39.16) gives us $\text{rad } \Lambda_0$, it is easy to check that

$$\text{rad } \Lambda_0 = \Lambda_0 \cdot \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & \pi_p \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{bmatrix},$$

where $p = \pi_D \Delta = \Delta \pi_D$. Hence $\text{rad } \Lambda_0$ is Λ_0 -projective, and thus Λ_0 is hereditary by (39.1). But $\Lambda_0 \subset \Lambda \subset A$, so Λ is also hereditary by (40.4) below. This completes the proof of the theorem.

When Λ is a hereditary order satisfying (39.15)–(39.17), we shall call r the *type* of Λ , and the ordered r -tuple $\{n_1, \dots, n_r\}$ the *invariants* of Λ . It is clear from (39.17) that a given order Λ uniquely determines r and the set of integers $\{n_i\}$. We shall see in (39.24) below that Λ determines the ordered r -tuple $\{n_1, \dots, n_r\}$ uniquely, up to a cyclic permutation. First, however, we shall obtain some consequences of the structure theorem (39.14).

(39.18) COROLLARY. *Let Λ be a hereditary order (in a central simple K -algebra) of type r and invariants $\{n_1, \dots, n_r\}$. Keep the notation of (39.14) and its proof. Then*

- (i) *r is the unique positive integer such that $J^r M = Mp$.*
- (ii) *We have*

$$(39.19) \quad \Lambda = \{x \in A : x \cdot J^i M \subset J^i M \quad \text{for } 0 \leq i \leq r\},$$

$$(39.20) \quad J = \{x \in A : x \cdot J^i M \subset J^{i+1} M \quad \text{for } 0 \leq i \leq r-1\}.$$

- (iii) *$J^{re} = \pi \Lambda$, where e is the ramification index of D over K .*
- (iv) *$\bar{\Lambda}$ is a chain ring in $\bar{\Lambda}'$, corresponding to the chain*

$$(39.21) \quad E : M > J\bar{M} > J^2\bar{M} > \cdots > J^r\bar{M} = 0,$$

with invariants given by

$$n_i = \dim_{\bar{\Delta}} J^{i-1}\bar{M}/J^i\bar{M}, \quad 1 \leq i \leq r.$$

(v) The modules $\{J^{i-1}M/J^iM : 1 \leq i \leq r\}$ are a full set of non-isomorphic simple left Λ -modules.

Proof. Step 1. Let τ be the canonical map

$$\tau : M \rightarrow \bar{M} = M/M\mathfrak{p} = M/J'M,$$

and set

$$\bar{M}_i = J^i\bar{M}, \quad M_i = \tau^{-1}(\bar{M}_i), \quad 0 \leq i \leq r.$$

Since τ is a left Λ -homomorphism, each M_i is a Λ -submodule of M . We claim that

$$(39.22) \quad M_i = J^iM \quad \text{for } 0 \leq i \leq r, \quad J^rM = M\mathfrak{p} = J'M.$$

The easiest way to prove this is by a matrix calculation, as follows: choose a right Δ -basis for M whose images in \bar{M} form a basis adapted to the chain E in (39.21). We may then write

$$M = \Delta^{(n)} = \begin{bmatrix} (\Delta)^{n_1 \times 1} \\ \vdots \\ (\Delta)^{n_r \times 1} \end{bmatrix}, \quad \bar{M} = \bar{\Delta}^{(n)} = \begin{bmatrix} (\bar{\Delta})^{n_1 \times 1} \\ \vdots \\ (\bar{\Delta})^{n_r \times 1} \end{bmatrix}.$$

Therefore for $0 \leq i \leq r$,

$$\bar{M}_i = J^i\bar{M} = \begin{bmatrix} (0)^{n_1 \times 1} \\ \vdots \\ (0)^{n_{i-1} \times 1} \\ (\bar{\Delta})^{n_i \times 1} \\ \vdots \\ (\bar{\Delta})^{n_r \times 1} \end{bmatrix}, \quad M_i = \tau^{-1}(\bar{M}_i) = \begin{bmatrix} (0)^{n_1 \times 1} \\ \vdots \\ (0)^{n_{i-1} \times 1} \\ (\mathfrak{p})^{n_i \times 1} \\ (\Delta)^{n_{i+1} \times 1} \\ \vdots \\ (\Delta)^{n_r \times 1} \end{bmatrix}.$$

Since J is given by (39.16), we have

$$JM = \begin{bmatrix} (\mathfrak{p}) & (\mathfrak{p}) & \dots & (\mathfrak{p}) \\ (\Delta) & (\mathfrak{p}) & \dots & (\mathfrak{p}) \\ \dots & \dots & \dots & \dots \\ (\Delta) & (\Delta) & \dots & (\mathfrak{p}) \end{bmatrix} \begin{bmatrix} (\Delta) \\ (\Delta) \\ \vdots \\ (\Delta) \end{bmatrix} = \begin{bmatrix} (\mathfrak{p}) \\ (\Delta) \\ \vdots \\ (\Delta) \end{bmatrix} = M_1.$$

Continuing in this manner, we easily obtain the formulas in (39.22) by induction on i . This establishes assertions (i) and (iv) of the corollary.

Step 2. For the moment let Λ^* denote the order occurring on the right side of (39.19). Obviously $\Lambda \subset \Lambda^*$ since $\Lambda \cdot J^i = J^i$ for each i . On the other hand, let $x \in \Lambda^*$; then $xM \subset M$, so $x \in \text{End}_\Lambda M = \Lambda'$. Further, for $0 \leq i \leq r$, $xM_i \subset M_i$ implies that $\rho(x)\bar{M}_i \subset \bar{M}_i$. Therefore $\rho(x) \in \bar{\Lambda}$, since $\bar{\Lambda}$ is the chain ring associated with the chain E of (39.21). Hence $x \in \Lambda$, which proves that $\Lambda = \Lambda^*$ and establishes (39.19). A similar argument proves (39.20).

Next, we have seen in the proof of (39.14) that $\Lambda/J \cong \bar{\Lambda}/\bar{J}$, so the simple left Λ -modules are the same as the simple left $\bar{\Lambda}$ -modules, with Λ acting via the map $\rho: \Lambda \rightarrow \bar{\Lambda}$. By (39.7 ii), the modules $\{\bar{M}_{i-1}/\bar{M}_i : 1 \leq i \leq r\}$ are a full set of non-isomorphic simple left $\bar{\Lambda}$ -modules. But τ induces isomorphisms

$$M_{i-1}/M_i \cong \bar{M}_{i-1}/\bar{M}_i, \quad 1 \leq i \leq r,$$

and thus we have proved assertion (v) of the corollary.

Step 3. Now let e be the ramification index of D over K (see §13). Then

$$\mathfrak{p}^e = \pi_D^e \Delta = \Delta \pi_D^e = \pi \Delta.$$

Since $J'M = M\mathfrak{p}$, we obtain

$$J^{re}M = M\mathfrak{p}^e = \pi M.$$

Therefore $T = \pi^{-1} J^{re}$ is a two-sided Λ -ideal in A such that $TM = M$ and $TJ = JT$. Hence

$$TM_i = T \cdot J^i M = J^i \cdot TM = M_i, \quad 0 \leq i \leq r.$$

It follows from (39.19) that $T \subset \Lambda$, and we now show that $T = \Lambda$. Indeed, $(T + J)/J$ is a two-sided ideal of the semisimple artinian ring Λ/J . If it is a proper ideal, it is annihilated by some (nonzero) idempotent ε in Λ/J . By (6.18) ε is the image of some idempotent $a \in \Lambda$, and then obviously $aT \subset J$. Therefore

$$aM_i = aT \cdot J^i M \subset J^{i+1}M = M_{i+1}, \quad 0 \leq i \leq r-1,$$

whence $a \in J$ by (39.20). This is impossible, since $\text{rad } \Lambda$ contains no idempotents of Λ . Therefore $T + J = \Lambda$, whence $T = \Lambda$ by Nakayama's Lemma.

We have thus proved that $\pi^{-1}J^{re} = \Lambda$, whence $J^{re} = \pi\Lambda$ as desired. This completes the proof of the corollary.

Remark. The preceding proof shows that J is an invertible (Λ, Λ) -bimodule, with inverse $\pi^{-1}J^{re-1}$. It should be pointed out that the above argument yields another proof, independent of that given for (39.1), of the implication

$$\Lambda \text{ hereditary} \implies \text{rad } \Lambda \text{ invertible.}$$

From the preceding results, we deduce

(39.23) **Theorem.** *Keeping the hypotheses and notation of (39.18), let*

$$\Gamma_i = \{x \in A : x \cdot J^i M \subset J^i M\}, \quad 0 \leq i \leq r-1.$$

Then $\Gamma_0, \dots, \Gamma_{r-1}$ are precisely the distinct maximal orders of A containing Λ , and

$$\Lambda = \Gamma_0 \cap \Gamma_1 \cap \cdots \cap \Gamma_{r-1}.$$

Furthermore, every indecomposable left Λ -lattice is isomorphic to exactly one of the Λ -lattices $M, JM, \dots, J^{r-1}M$.

Proof. Suppose first that L is any indecomposable left Λ -lattice. The proof of (21.5) shows that KL must be a simple left A -module, and therefore $KL = KM$. Replacing L by an isomorphic copy, we may assume that $L \subset M$. Choose t so that

$$L \subset J^t M, \quad L \not\subset J^{t+1} M.$$

Since J is invertible, it follows that if we set $L_1 = J^{-t}L$, then

$$L_1 \subset M, \quad L_1 \not\subset JM.$$

Thus $(L_1 + JM)/JM$ is a nonzero submodule of the simple Λ -module M/JM , whence $L_1 + JM = M$. Therefore $L_1 = M$, and so $L = J^t M$. Hence the modules $\{J^t M\}$ give all isomorphism classes of indecomposable left Λ -lattices; each is obviously indecomposable, since $K \cdot J^t M$ is a simple A -module.

We show now that $J^s M \cong J^t M$ as left Λ -lattices if and only if $s \equiv t \pmod{r}$. Any such isomorphism extends to an A -isomorphism $KM \cong KM$, hence must be given by right multiplication by some element $d \in D$. Writing $d = u \cdot \pi_D^k$, where $u \in u(\Delta)$ and π_D is a prime element of Δ , it follows that $J^s M \cong J^t M$ if and only if $J^s M = J^t M \cdot \pi_D^k$ for some k . Since $M\pi_D = J^t M$, this occurs if and only if $r|(s-t)$, and the second assertion of the theorem is proved.

For each integer t , set $\Gamma_t = \{x \in A : x \cdot J^t M \subset J^t M\}$. Now $J^t M$ is a right Δ -lattice such that $K \cdot J^t M = K \cdot \Delta^{(n)}$, whence $J^t M \cong \Delta^{(n)}$ by Exercise 18.1.

Since $\Gamma_t = \text{End}_\Delta J^t M$ it follows from (17.4) that Γ_t is a maximal order. Clearly $\Gamma_s = \Gamma_t$ whenever $s \equiv t \pmod{r}$. Conversely, if $\Gamma_s = \Gamma_t$ then $J^s M$ and $J^t M$ are a pair of (Γ_r, Δ) -bimodules; hence by (16.14) $J^s M = J^t M \cdot p^k$ for some k , whence $r \mid (s - t)$. This shows that $\Gamma_0, \dots, \Gamma_{r-1}$ are distinct orders containing Λ . Their intersection is Λ , by (39.19). Finally, let Γ be any maximal order of A containing Λ . Every indecomposable left Γ -lattice is also an indecomposable left Λ -lattice, hence may be taken to be one of $\{J^i M : 0 \leq i \leq r-1\}$. Therefore Γ must coincide with one of the orders $\Gamma_0, \dots, \Gamma_{r-1}$, and the theorem is established.

(39.24) COROLLARY. *Keep the above notation and hypotheses. Then Λ uniquely determines the ordered r -tuple $\{n_1, \dots, n_r\}$ of invariants, up to cyclic permutation.*

Proof. Let $\Lambda \subset \Lambda' = \text{End}_\Delta M$, and let us show that the invariants $\{n_1, \dots, n_r\}$ are unaffected by using N in place of M , where N is another Δ -lattice such that $\Lambda' = \text{End}_\Delta N$. By (16.14) we may write $N = Mp^k = M\pi_D^k$ for some integer k . It is then easily verified that the invariants computed using N are the same as those obtained from M .

On the other hand, if Γ_t is one of the maximal orders containing Λ , then we have seen that $\Gamma_t = \text{End}_\Delta J^t M$. Thus we obtain invariants $\{n'_i\}$, where

$$n'_i = \dim_{\overline{\Delta}} J^{i-1} \cdot J^t \overline{M} / J^i \cdot J^t \overline{M} = n_{i+t}, \quad 1 \leq i \leq r,$$

and where the subscript $i + t$ is read mod r . This shows that all cyclic permutations of $\{n_1, \dots, n_r\}$ can arise as invariants, and these are the only possibilities.

Returning to the general case, we have

(39.25) THEOREM. *Let Λ be an R -order in a separable K -algebra. Then Λ is hereditary if and only if Λ is extremal.*

Proof. By (39.12), hereditary orders are extremal. Conversely, any extremal order Λ can be decomposed as $\Lambda = \sum \Lambda_i$ by (39.13). But then each Λ_i is hereditary by (39.14), whence so is Λ .

If we assume merely that R is a discrete valuation ring, not necessarily complete, then the structure theorem (39.14) and its consequences (39.18)–(39.23) remain valid whenever the P -adic completion D_P is a skewfield.

EXERCISES

1. Let L be a left ideal of the R -order Λ . Show that

$$L^m \subset P\Lambda \quad \text{for some } m \iff L \subset \text{rad } \Lambda.$$

[Hint: By (6.15), $(\text{rad } \Lambda)^n \subset P\Lambda \subset \text{rad } \Lambda$ for all sufficiently large n . Hence

$$L \subset \text{rad } \Lambda \implies L^n \subset P\Lambda.$$

Conversely, suppose that $L^m \subset P\Lambda$ for some m . Then $L\Lambda$ is a two-sided ideal of Λ , and

$$(L\Lambda)^m = (L\Lambda)(L\Lambda) \cdots (L\Lambda) \subset L^m\Lambda \subset P\Lambda \subset \text{rad } \Lambda.$$

Hence $L\Lambda \subset \text{rad } \Lambda$ by Exercise 6.3.]

2. Let $\Lambda \subset \Lambda'$ be R -orders in A . Show that $\Lambda + \text{rad } \Lambda'$ is an R -order in A whose radical contains $\text{rad } \Lambda$. [Hint: Let $J = \text{rad } \Lambda$, $J' = \text{rad } \Lambda'$. Clearly $\Lambda + J'$ is an order, and we must show that $J \subset \text{rad } (\Lambda + J')$. For large m ,

$$(J + J')^m \subset J^m + J' \subset P\Lambda + J' \subset P\Lambda' + J',$$

and

$$(P\Lambda' + J')^m \subset P\Lambda' + J'^m \subset P\Lambda'.$$

Thus

$$(J + J')^m \subset P^m\Lambda' \subset P\Lambda \subset P(\Lambda + J')$$

for large m , whence $J + J' \subset \text{rad } (\Lambda + J')$ by Exercise 1.]

3. Let $\Lambda \subset \Lambda'$ be R -orders in A , and suppose that $\text{rad } \Lambda' \subset \Lambda$. Show that $\text{rad } \Lambda' \subset \text{rad } \Lambda$. [Hint: Let $J' = \text{rad } \Lambda'$. As in Exercise 2, we get $J'^r \subset P\Lambda$ for large r . Since J' is an ideal of Λ , it follows from Exercise 1 that $J' \subset \text{rad } \Lambda$.]

4. Let N be a two-sided ideal of the R -order Λ contained in $\text{rad } \Lambda$. Prove that

$$(\text{rad } \Lambda)/N = \text{rad } (\Lambda/N).$$

[Hint: Let $J = \text{rad } \Lambda$, $\bar{J} = J/N$, $\bar{\Lambda} = \Lambda/N$. Then $\bar{\Lambda}/\bar{J} \cong \Lambda/J$, a semisimple ring. Hence $\bar{J} \supset \text{rad } \bar{\Lambda}$ by Exercise 6.1. On the other hand, $\psi: \Lambda \rightarrow \bar{\Lambda}$ is epic, so $\bar{J} = \psi(J) \subset \text{rad } \bar{\Lambda}$ by (6.10).]

5. Let E, E' be a pair of chains in the Ω -space V , and define the chain rings $O(E)$, $O(E')$ as in (39.4). Prove

- (i) $O(E) \supset O(E')$ if and only if E' is a refinement of E .
- (ii) $O(E) > O(E')$ if and only if $E = E'$.
- (iii) $O(E)$ is an extremal subring of $\text{End}_\Omega V$.

[Hint: To prove (i) and (ii), consider the matrix representations (39.6) and (39.8) of the rings $O(E)$, $O(E')$ and their radicals. To prove (iii), let $O(E)$ be given, and consider all subrings B of $M_n(\Omega)$ such that $B > O(E)$. We may choose a maximal element B' relative to this partial ordering. Then B' is an extremal subring of $M_n(\Omega)$, whence $B' = O(E_{B'})$ by (39.10). But then $O(E_{B'}) > O(E)$, so by (ii) we have $B' = O(E_{B'}) = O(E)$.]

In Exercises 6–11, we keep the hypotheses and notation of (39.18) and (39.23) and their proofs.

6. Show that every invertible (Λ, Λ) -bimodule in A is a power of $\text{rad } \Lambda$, and deduce that Picent Λ is cyclic of order re . [Hint: Let T be an invertible bimodule; then $TJT^{-1} = \text{rad } (T\Lambda T^{-1}) = \text{rad } \Lambda = J$, so $TJ = JT$. Let $U = J^kT$ with k chosen so that $U \subset \Lambda$, $U \neq J$. Then $JM < (U + J)M \subset M$, the first inclusion being proper

since otherwise $U \subset J$. Hence $(U + J)M = M$. Now use the argument in Step 3 of the proof of (39.18) to deduce that $U = \Lambda$.]

7. Let Λ be a hereditary order of type r . Prove

(i) There are exactly $2^r - 1$ distinct orders in A containing Λ , namely the intersections of the orders in each non-empty subset of $\{\Gamma_0, \dots, \Gamma_{r-1}\}$.

(ii) The maximal possible length of a chain of orders

$$\Lambda < \Lambda_1 < \dots < \Lambda_s$$

in A is r itself.

(iii) There are precisely r distinct orders Λ_1 with $\Lambda_1 > \Lambda$, such that there is no order properly between Λ_1 and Λ .

8. For the order Λ in (39.15), describe explicitly those maximal orders containing Λ .

9. For $0 \leq t \leq r - 1$, let

$$J_t = \{x \in \Lambda : x \cdot J^t M \subset J^{t+1} M\}.$$

Show that $\{J_0, \dots, J_{r-1}\}$ are the distinct maximal two-sided ideals of Λ , and that $J_t = \text{rad } \Gamma_t$. Prove that

$$\Lambda/J \cong \sum_{t=0}^{r-1} \Gamma_t/J_t.$$

For each t , calculate the conductor $\{x \in A : \Gamma_t \cdot x \subset \Lambda\}$.

10. Prove that $J'\Lambda' = J'$, where Λ' is a maximal order containing Λ , and $J' = \text{rad } \Lambda'$. [Hint: $J'\Lambda'$ is a two-sided ideal of Λ' , hence is a power of J' . Now use (39.22).]

11. Show that the formula

$$J' = J'\Lambda' = L_r \cdot L_{r-1} \cdots L_2 \cdot L_1, \quad \text{where } L_i = J^i \Lambda' J^{-(i-1)},$$

expresses J' as a proper product of r integral ideals L_r, \dots, L_1 . Prove that

$$(39.26) \quad \Lambda = \bigcap_{i=1}^r O_i(L_i),$$

and that the chain (39.21) for Λ is just

$$(39.27) \quad \bar{M} > L_1 \bar{M} > L_2 L_1 \bar{M} > \cdots > (L_r \cdots L_1) \bar{M} = 0.$$

Show conversely that starting with any maximal order Λ' and any proper factorization

$$\text{rad } \Lambda' = L_r \cdot L_{r-1} \cdots L_2 \cdot L_1$$

into integral ideals, the order Λ given by (39.26) is hereditary and corresponds to the chain (39.27).

12. Give an example of two maximal orders Λ_1, Λ_2 in a central simple K -algebra, for which $\Lambda_1 \cap \Lambda_2$ is not hereditary.

13. Let Λ_1, Λ_2 be hereditary R -orders in the central simple K -algebra A . Show that there exists a full R -lattice Y in A such that

$$\Lambda_1 = O_l(Y), \quad \Lambda_2 = O_r(Y),$$

if and only if Λ_1 and Λ_2 are of the same type.

40. GLOBAL THEORY OF HEREDITARY ORDERS

Keeping the notation introduced at the start of this chapter, we assume now that R is any Dedekind domain. Here we shall develop the theory of hereditary R -orders, by using the local results obtained in §39. We prove first

(40.1) **THEOREM.** Λ is left hereditary if and only if Λ is right hereditary.

Proof. Since Λ is both left and right noetherian, the result is a special case of (2.45 iii). We give an independent proof here. Each left Λ -lattice M determines a dual $M^* = \text{Hom}_R(M, R)$, which is a right Λ -lattice, and there is a natural isomorphism $M \cong M^{**}$ (see Exercise 40.2). Furthermore, any exact sequence of left Λ -lattices

$$(40.2) \quad 0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$$

must be R -split, since N is R -projective by (4.13). Hence when we apply $\text{Hom}_R(\cdot, R)$ to (40.2), the resulting sequence

$$(40.3) \quad 0 \rightarrow N^* \rightarrow M^* \rightarrow L^* \rightarrow 0$$

is also R -split, and hence exact. The maps in (40.3) are right Λ -homomorphisms. Conversely, taking duals in (40.3) gives (40.2) again. Hence the sequence (40.2) is Λ -split if and only if (40.3) is Λ -split.

Suppose now that Λ is right hereditary, and let N be any left ideal of Λ . Then we can find a Λ -exact sequence (40.2) in which M is a free left Λ -lattice. Now L^* is a right Λ -lattice, hence is Λ -projective by (10.7). Therefore the sequence (40.3) is Λ -split, whence so is (40.2). This proves that every left ideal of Λ is projective, so Λ is left hereditary. The theorem now follows by an obvious symmetry argument.

(40.4) **THEOREM.** Let $\Lambda \subset \Lambda'$ be R -orders in A . If Λ is hereditary, then so is Λ' .

Proof. Given any left Λ' -lattice L , there is an exact sequence of left Λ' -lattices

$$0 \rightarrow M \rightarrow F \xrightarrow{\varphi} L \rightarrow 0$$

with F Λ' -free. Since L is also a left Λ -lattice, hence Λ -projective, the sequence is Λ -split. Therefore there exists a map $\psi \in \text{Hom}_\Lambda(L, F)$ such that $\varphi\psi = 1$ on L . But Exercise 40.1 shows that ψ is a Λ' -homomorphism, whence the above sequence is Λ' -split. Therefore L is Λ' -projective, which completes the proof that Λ' is hereditary.

It should be pointed out that the preceding theorems and their proofs are valid without the hypothesis that A be a separable K -algebra. For the

remainder of this section, however, we shall keep our hypothesis that A is separable. We intend to investigate R -orders Λ by considering their P -adic completions Λ_P , where P ranges over all maximal ideals of R . As a first step in this direction, we show

(40.5) **THEOREM.** Λ is hereditary if and only if Λ_P is hereditary for all P , or equivalently, if and only if Λ_P is an extremal R_P -order in A_P for all P .

Proof. Note first that since A is K -separable, A_P is K_P -separable for each P , by Exercise 7.13. We showed in (3.24) that Λ is hereditary if and only if each localization $(R - P)^{-1} \Lambda$ is hereditary. The same argument works if we use completions rather than localizations. Alternatively, we saw in §3 that Λ is hereditary if and only if $\dim \Lambda \leq 1$, where “dim” means “left global dimension”. By (3.29) and (3.30),

$$\dim \Lambda = \sup_P \{\dim \Lambda_P\}.$$

This again shows that Λ is hereditary if and only if each Λ_P is hereditary. Finally, for each P we know by (39.25) that Λ_P is hereditary if and only if Λ_P is extremal. This completes the proof.

Let us digress briefly to show that when R contains infinitely many prime ideals, then extremal R -orders are the same as maximal orders.

(40.6) **THEOREM.** For each P , $\text{rad } \Lambda \subset \text{rad } \Lambda_P$. Further,

$$(\text{rad } \Lambda)^n \subset (\text{rad } R) \Lambda, \text{ where } n = (A : K).$$

If R contains infinitely many prime ideals, then $\text{rad } R = 0$ and $\text{rad } \Lambda = 0$; in this case, Λ is extremal if and only if Λ is maximal.

Proof. Given P , let

$$\psi: \Lambda \rightarrow \bar{\Lambda} = \Lambda/P\Lambda \cong \Lambda_P/P\Lambda_P.$$

By (6.10) we have $\psi(\text{rad } \Lambda) \subset \text{rad } \bar{\Lambda}$. The chain

$$\bar{\Lambda} > \text{rad } \bar{\Lambda} > (\text{rad } \bar{\Lambda})^2 > \dots$$

steadily decreases to 0; its length is at most n , since $\bar{\Lambda}$ has dimension n over R/P . Therefore $(\text{rad } \bar{\Lambda})^n = 0$, and so $(\text{rad } \Lambda)^n \subset \ker \psi = P\Lambda$. This implies that

$$\{(\text{rad } \Lambda)_P\}^n \subset P \cdot \Lambda_P \subset \text{rad } \Lambda_P,$$

and therefore

$$\text{rad } \Lambda \subset (\text{rad } \Lambda)_P \subset \text{rad } \Lambda_P,$$

as claimed.

Next we observe that $\text{rad } R = \bigcap_P P$, where P ranges over all maximal ideals of R . Furthermore

$$\bigcap_P P\Lambda = \{\bigcap_P P\} \Lambda = (\text{rad } R)\Lambda,$$

since this holds when $\Lambda = R$, and hence also when Λ is R -projective. Thence

$$(\text{rad } \Lambda)^n \subset \bigcap_P P\Lambda = (\text{rad } R)\Lambda.$$

If R contains infinitely many prime ideals, then $\bigcap_P P = 0$ by §4, whence $(\text{rad } \Lambda)^n = 0$. But then $K \cdot \text{rad } \Lambda$ is a nilpotent two-sided ideal of A , and is therefore 0. Thus $\text{rad } \Lambda = 0$, and the theorem is proved.

We are now ready to prove that the decomposition theorem (10.5) holds equally well for hereditary orders. We have

(40.7) THEOREM. *Let A be a separable K -algebra with simple components $\{A_i\}$, and let R_i be the integral closure of R in K_i . Then*

- (i) *For each hereditary R -order Λ in A , we have $\Lambda = \sum^* \Lambda e_i$, where the $\{e_i\}$ are the central idempotents of A such that $A_i = Ae_i$. Further, for each i , Λe_i is a hereditary R -order in A_i .*
- (ii) *If each Λ_i is a hereditary R -order in A_i , then $\sum^* \Lambda_i$ is a hereditary R -order in A .*
- (iii) *An R -order Λ_i in A_i is a hereditary R -order if and only if Λ_i is a hereditary R_i -order.*

Proof. As in the proof of (10.5) and (39.13), we need only show that $\Lambda = C\Lambda$, where $C = \sum^* R_i$. For each P , $(C\Lambda)_P$ is an R_P -order in A_P such that $(C\Lambda)_P \succ \Lambda_P$. Since Λ_P is extremal, it follows that $(C\Lambda)_P = \Lambda_P$ for all P . Therefore $\Lambda = C\Lambda$, and the rest of the argument is straightforward.

We have now shown that, just as in the local case, the study of hereditary orders can be reduced to the situation where A is a central simple K -algebra. Let us now examine this case in some detail. Let Λ be a hereditary R -order in a central simple K -algebra A of local capacity κ_p , local index m_p , at each prime P . This means that $A_P \cong M_{\kappa_p}(S_p)$ for some skewfield S_p of index m_p . Let r_p denote the type of the hereditary R_p -order Λ_p , that is, $\Lambda_p/\text{rad } \Lambda_p$ is a direct sum of r_p simple components. Call r_p the *local type* of Λ at P ; clearly $r_p = 1$ if and only if Λ_p is a maximal order, by (39.23). Thus $r_p = 1$ a.e., and we have previously shown that $m_p = 1$ a.e. Whether or not $r_p = 1$ or $m_p = 1$, we know the structure of Λ_p from §39, and we can recover the order Λ by using the formula

$$\Lambda = A \cap \left\{ \bigcap_P \Lambda_P \right\}.$$

If Λ' is a bigger R -order in A , then $\Lambda_p \subset (\Lambda')_P$ for all P , with equality a.e.

Conversely, suppose that for each P we are given an R_P -order $X(P)$ in A_P , with $X(P) \supset \Lambda_P$ for all P , and $X(P) = \Lambda_P$ a.e. Then by (5.3),

$$X = A \cap \left\{ \bigcap_P X(P) \right\}$$

is an R -order in A containing Λ , and $X_P = X(P)$ for all P . Hence we may determine all possible orders Λ' containing Λ by determining all possible sets of $X(P)$'s. Our main result is as follows:

(40.8) THEOREM. *Let Λ be a hereditary R -order in the central simple K -algebra A , and let $S = \{P_1, \dots, P_m\}$ be the (finite) set of prime ideals P of R at which Λ_P is not a maximal order. Let r_i denote the type of the hereditary R_{P_i} -order Λ_{P_i} , $1 \leq i \leq m$.*

- (i) *There are precisely $\prod_{i=1}^m r_i$ distinct maximal R -orders in A containing Λ .*
- (ii) *There are precisely $\prod_{i=1}^m (2^{r_i} - 1)$ distinct R -orders in A containing Λ .*
- (iii) *There are $\sum_{i=1}^m r_i$ orders in A which minimally contain† Λ .*

Proof. All three assertions are immediate consequences of (39.23) and Exercise 39.7. It is of interest to list the orders mentioned in (i) and (iii). For convenience of notation, we set

$$\tilde{\Lambda} = A \cap \left\{ \bigcap_{P \notin S} \Lambda_P \right\}.$$

We may remark that $\tilde{\Lambda}$ is a maximal \tilde{R} -order in A , where \tilde{R} is the ring of elements of K which are integral at each $P \notin S$.

For each $P_i \in S$, let $\{\Gamma_{ij} : 1 \leq j \leq r_i\}$ be the distinct maximal orders in A_{P_i} containing Λ_{P_i} . Let

$$\mathfrak{M} = \{(a_1, \dots, a_m) : a_i \in \mathbf{Z}, 1 \leq a_i \leq r_i \text{ for } 1 \leq i \leq m\}.$$

For each $m = (a_1, \dots, a_m) \in \mathfrak{M}$, define

$$\Gamma^m = \tilde{\Lambda} \cap \Gamma_{1, a_1} \cap \cdots \cap \Gamma_{m, a_m}.$$

Then

$$(\Gamma^m)_{P_i} = \Gamma_{i, a_i}, \quad 1 \leq i \leq m.$$

Hence as m ranges over the $\prod_{i=1}^m r_i$ m -tuples in \mathfrak{M} , the R -order Γ^m ranges over

† The order Λ' *minimally contains* Λ if $\Lambda' > \Lambda$, but there is no order Λ'' such that $\Lambda' > \Lambda'' > \Lambda$.

all maximal orders in A containing Λ , and different m 's give different Γ^m 's.

Now put

$$\Sigma_{is} = \bigcap_{\substack{1 \leq j \leq r_i, \\ j \neq s}} \Gamma_{ij}, \quad 1 \leq s \leq r_i, \quad 1 \leq i \leq m.$$

Set

$$\Omega_{is} = \tilde{\Lambda} \cap \Sigma_{is} \cap \left\{ \bigcap_{\substack{P \in S \\ P \neq P_i}} \Lambda_P \right\}, \quad 1 \leq s \leq r_i, 1 \leq i \leq m.$$

Then the $\sum_1^m r_i$ distinct orders $\{\Omega_{is}\}$ are precisely the orders in A which minimally contain Λ .

To complete our discussion, we observe that every R -order in A containing Λ is expressible as an intersection of a non-empty set of Γ^m 's. This follows at once from Exercise 39.7, which asserts that for $1 \leq i \leq m$, every order in A_{P_i} containing Λ_{P_i} is an intersection of some of the orders $\{\Gamma_{ij}: 1 \leq j \leq r_i\}$. It should be pointed out, however, that different sets of Γ^m 's may yield the same R -order in A . For instance, suppose that $S = \{P_1, P_2\}$, $r_1 = r_2 = 2$; then

$$\Gamma^{(a, b)} = \tilde{\Lambda} \cap \Gamma_{1, a} \cap \Gamma_{2, b}, \quad 1 \leq a, b \leq 2.$$

We have

$$\Gamma^{(1, 1)} \cap \Gamma^{(1, 2)} \cap \Gamma^{(2, 1)} = \Lambda = \Gamma^{(1, 1)} \cap \Gamma^{(2, 2)}.$$

Analogously, for $1 \leq i \leq m$, every order in A_{P_i} containing Λ_{P_i} is a sum of orders from $\{\Sigma_{is}: 1 \leq s \leq r_i\}$. It follows readily that every order Λ' properly containing Λ is expressible as a sum of orders chosen from the set $\{\Omega_{is}: 1 \leq s \leq r_i, 1 \leq i \leq m\}$. We leave as an exercise for the reader the proof that each Λ' is uniquely so expressible. Finally, we caution that not every sum of Ω 's is an order.

By the same type of reasoning, we have

(40.9) THEOREM. *Keep the notation of (40.8). For each P , let*

$$X(P) = \Lambda \cap \text{rad } \Lambda_P.$$

Then

(i) *For each P , $X(P)$ is a two-sided ideal in Λ such that*

$$\{X(P)\}_Q = \begin{cases} \text{rad } \Lambda_P, & Q = P, \\ \Lambda_Q, & Q \neq P, \end{cases}$$

where Q ranges over all prime ideals of R .

(ii) Let $I(\Lambda)$ be the group of invertible two-sided Λ -ideals in A (see §37). Then $I(\Lambda)$ is the free abelian group with generators $\{X(P): P \text{ arbitrary}\}$.

(iii) There is an exact sequence

$$1 \rightarrow \text{Cl } R \rightarrow \text{Picent } \Lambda \rightarrow \prod_P \mathbf{Z}/e_p r_p \mathbf{Z} \rightarrow 1,$$

where for each P , r_p is the local type of Λ at P , and e_p is the ramification index of the skewfield part of A_P .

Proof. Assertion (i) is clear from the discussion preceding (40.8), and implies (ii) by virtue of Exercise 39.6. Furthermore, (iii) follows from (37.29) and Exercise 39.6. Note that $e_p r_p = 1$ a.e.

Next we shall prove the global version of Exercise 39.11:

(40.10) THEOREM. (Jacobinski [3]). Let $\{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$ be any set of distinct prime ideals of the maximal R -order Λ' in a central simple K -algebra A . Let

$$(40.11) \quad \mathfrak{P}_1 \cdots \mathfrak{P}_r = L_s \cdots L_1$$

be any factorization of $\prod \mathfrak{P}_i$ into a proper product of integral ideals $\{L_j\}$. Set

$$(40.12) \quad \Lambda = \bigcap_{j=1}^s O_i(L_j).$$

Then Λ is a hereditary R -order contained in Λ' . Conversely, every hereditary order arises in this way.

Proof. Starting with Λ' and (40.11), let Λ be given by (40.12). All of the formulas behave properly when we pass to completions, and for each prime ideal P of R , we have

$$\prod (\mathfrak{P}_i)_P = \begin{cases} \text{rad } \Lambda'_P & \text{if some } \mathfrak{P}_i \supset P, \\ \Lambda' & \text{otherwise.} \end{cases}$$

Hence for each P , Λ_P is hereditary by Exercise 39.11. Therefore Λ is hereditary by virtue of (40.5).

Conversely, let Λ be a given hereditary order in A , and choose $\Lambda' \supset \Lambda$, Λ' maximal. Suppose that Λ_P is maximal except at $\{P_1, \dots, P_r\}$, and let \mathfrak{P}_i be the prime ideal of Λ' containing P_i . By Exercise 39.11, there is a factorization (for each i)

$$\text{rad } \Lambda'_{P_i} = L_s^{(i)} \cdots L_1^{(i)}$$

into a proper product of integral ideals, such that (40.12) holds locally at P_i . We may assume that the number of factors s is independent of i , by inserting (if need be) additional factors L which are maximal orders. Now choose integral ideals L_s, \dots, L_1 in A by setting

$$L_j = \Lambda' \cap L_j^{(1)} \cap \cdots \cap L_j^{(r)}, \quad 1 \leq j \leq s.$$

It is then an easy exercise, left to the reader, to verify that (40.11) and (40.12) hold true.

Turning now from abstract properties of hereditary orders, we shall give a concrete example of a hereditary order which arises naturally in representation theory. Let L/K be a finite galois extension (of fields), with galois group G . Let R be a Dedekind domain with quotient field K , and let S be the integral closure of R in L . We shall assume that for each prime ideal P_1 of S , the residue class field S/P_1 is separable over $R/(R \cap P_1)$. Call S/R tamely ramified if for each P_1 , the ramification index $e(P_1, L/K)$ is not zero in $R/(R \cap P_1)$. Then (see references listed in §4) S/R is tamely ramified if and only if there exists an $s_0 \in S$ such that $\sum_{\sigma \in G} \sigma(s_0) = 1$.

Now let $A = (L/K, 1) = \sum_{\sigma \in G} Lu_\sigma$ be the trivial crossed-product algebra given in Exercise 29.14. We set $\Lambda = \sum_{\sigma \in G} Su_\sigma$, an R -order in the central simple K -algebra A . Sometimes Λ is called a *twisted group ring*, and is denoted by $S \circ G$.

(40.13) THEOREM (Rosen). *The twisted group ring $S \circ G$ is a hereditary R -order if and only if S/R is tamely ramified.*

Proof. Let $\Lambda = S \circ G$; we may regard S as embedded in Λ via $s \mapsto s \cdot u_1$, $s \in S$, and then every left Λ -module is also a left S -module. Suppose that S/R is tamely ramified, and let $s_0 \in S$ be such that $\sum_{\sigma \in G} \sigma(s_0) = 1$. Given any left ideal X of Λ , there is an exact sequence of left Λ -lattices

$$0 \rightarrow X' \rightarrow F \xrightarrow{\varphi} X \rightarrow 0,$$

with F Λ -free. Since X is also a left S -lattice, and hence S -projective, the sequence is S -split. Thus there exists a map $\psi \in \text{Hom}_S(X, F)$ such that $\varphi\psi = 1$ on X . Now set

$$\psi' = \sum_{\sigma \in G} u_\sigma \cdot s_0 \psi \cdot u_\sigma^{-1}.$$

It is easily verified that $\psi' \in \text{Hom}_\Lambda(X, F)$, and for $x \in X$ we have

$$\begin{aligned} \varphi\psi'(x) &= \sum_{\sigma} \varphi u_\sigma \cdot s_0 \psi \cdot u_\sigma^{-1} x = \sum_{\sigma} u_\sigma s_0 \cdot \varphi \psi \cdot u_\sigma^{-1} x \\ &= \sum_{\sigma} u_\sigma s_0 u_\sigma^{-1} x = \{\sum_{\sigma} \sigma^{-1}(s_0)\} x = x. \end{aligned}$$

Thus the sequence is Λ -split, whence X is Λ -projective. This proves that if S/R is tamely ramified, then Λ is hereditary.

Conversely, suppose that Λ is hereditary, and set $x = \sum_{\sigma \in G} u_\sigma \in \Lambda$. Then the epimorphism

$$\varphi: \Lambda \rightarrow \Lambda x, \text{ given by } \varphi(\lambda) = \lambda x, \lambda \in \Lambda,$$

must be split. Hence there exists a map $\psi \in \text{Hom}_\Lambda(\Lambda x, \Lambda)$ such that $\varphi\psi = 1$. Let us write

$$\psi(x) = \sum_{\sigma \in G} a_\sigma u_\sigma, \quad a_\sigma \in S.$$

Since $u_\tau \cdot x = x$ for each $\tau \in G$, we find readily that $a_\sigma = \sigma(a_1)$, $\sigma \in G$. But then

$$x = \varphi\psi(x) = (\sum_{\sigma} a_\sigma)x = (\sum_{\sigma} \sigma(a_1))x.$$

Therefore $\sum_{\sigma} \sigma(a_1) = 1$, whence S/R is tamely ramified. This completes the proof. The reader should compare this with the proofs of (7.20) and Exercise 7.9.

Keeping the above terminology and notation, let us prove

(40.14) THEOREM (Auslander–Goldman–Rim). *The twisted group ring $S \circ G$ is a maximal R -order if and only if S/R is unramified, that is, if and only if the discriminant ideal $d(S/R)$ equals R .*

Proof. It suffices to establish the result for the case where R is a discrete valuation ring, with maximal ideal P . Let $\Lambda = S \circ G$, $A = L \circ G = \sum L u_\sigma$ as above, and set $(L:K) = n$, so $A \cong M_n(K)$. Suppose that Λ is a maximal order in A ; it follows from (17.5) and (18.3) that

$$\text{rad } \Lambda = P\Lambda = \sum_{\sigma} PSu_\sigma,$$

and that $\text{rad } \Lambda$ is the unique maximal two-sided ideal of Λ . If $d(S/R) \neq R$, then we may write $PS = \prod P_i^{e_i}$, where the $\{P_i\}$ are distinct prime ideals of S , and where each $e_i > 1$. Setting $\mathfrak{a} = \prod P_i$, it is clear that

$$\text{rad } \Lambda < \sum_{\sigma} \mathfrak{a} u_\sigma < \Lambda,$$

and that $\sum \mathfrak{a} u_\sigma$ is a two-sided ideal of Λ . This gives a contradiction, and shows that S/R must be unramified whenever Λ is a maximal order.

Suppose conversely that S/R is unramified, so the inverse different $\mathfrak{D}^{-1}(S/R)$ equals S by (4.37). Let Γ be any R -order in A containing Λ , and let

$$\gamma = \sum_{\sigma} a_\sigma u_\sigma \in \Gamma, \quad a_\sigma \in L.$$

Fix $\tau \in G$, and let s range over all elements of S . Then $s\gamma u_{\tau^{-1}} \in \Gamma$, whence

$$\text{tr}_{A/K} s\gamma u_{\tau^{-1}} \in R \text{ for all } s \in S.$$

By Exercise 40.4, this gives

$$T_{L/K}(sa_\tau) \in R \text{ for all } s \in S.$$

Therefore $a_\tau \in \mathfrak{D}^{-1}(S/R) = S$ for each $\tau \in G$, whence $\Gamma = \Lambda$. This completes the proof of the theorem.

Also of interest is the following generalization of (40.13):

(40.15) THEOREM (Williamson, Harada). *Keep the notation and hypotheses introduced before (40.13), and let $f: G \times G \rightarrow u(S)$ be a factor set. Let*

$$B = (L/K, f) = \sum_{\sigma \in G} Lv_\sigma, \quad \Gamma = \sum_{\sigma \in G} Sv_\sigma,$$

so Γ is an R -order in the central simple K -algebra B . Then Γ is a hereditary order if and only if S/R is tamely ramified.

Proof. See Williamson [1] and Harada [7].

The remainder of this section gives Reiner's simplified version [2] of some results of Jacobinski [4]. First of all, we show that when Λ is hereditary, the calculation of the locally free class group $\text{Cl } \Lambda$ (defined in §38) can be reduced to the case of maximal orders.

(40.16) THEOREM. *Let Λ be a hereditary R -order in a separable K -algebra A , and let Λ' be any R -order in A containing Λ . Then there is an isomorphism*

$$\beta: \text{Cl } \Lambda \cong \text{Cl } \Lambda',$$

given by $\beta[X] = [\Lambda' \otimes_\Lambda X]$, $[X] \in \text{Cl } \Lambda$.

Proof. Denote \otimes_Λ by \otimes throughout this proof. It is easily checked that the stable isomorphism class of $\Lambda' \otimes X$ depends only on that of X , and that $(\Lambda' \otimes X) v \Lambda'$ whenever $X v \Lambda$. Thus β is well defined, and it follows readily from the definition of the additive structure of the class groups that β is a homomorphism.

We now show that β is epic. Given any $[X'] \in \text{Cl } \Lambda'$, where X' is a locally free left Λ' -lattice in A , we may write (for each P)

$$X_P = \Lambda'_P x_P, \quad x_P \in u(A_P),$$

with $x_P = 1$ a.e. Set

$$X = A \cap \left\{ \bigcap_P \Lambda_P x_P \right\}.$$

Then X is a locally free left Λ -lattice in A such that $\Lambda' X = X'$. Since $\Lambda' \otimes X \cong \Lambda' X$, it follows that $\beta[X] = [X']$, whence β is epic.

Now let $\mathcal{S} = \{P_1, \dots, P_n\}$ be the set of all P 's in R such that $\Lambda_P \neq \Lambda'_P$. Given any $[X] \in \text{Cl } \Lambda$, we imitate the proof of (37.34). By (27.1) there exists a Λ -exact sequence

$$(40.17) \quad 0 \rightarrow X \rightarrow \Lambda \rightarrow T \rightarrow 0,$$

where $T_P = 0$ for all $P \in \mathcal{S}$. Since Λ' is projective as right Λ -module, applying $\Lambda' \otimes \cdot$ to (40.17) yields a Λ' -exact sequence

$$(40.18) \quad 0 \rightarrow \Lambda' \otimes X \rightarrow \Lambda' \rightarrow \Lambda' \otimes T \rightarrow 0.$$

Now we claim that $\Lambda' \otimes T \cong T$ as left Λ -modules. Indeed, both are R -torsion modules, and for each P we have

$$\Lambda'_P \otimes T_P = T_P.$$

(This is clear when $P \notin \mathcal{S}$, while for $P \in \mathcal{S}$ it holds since then $\Lambda'_P = \Lambda_P$.) Thus (40.18) yields a Λ -exact sequence

$$(40.19) \quad 0 \rightarrow \Lambda' \otimes X \rightarrow \Lambda' \rightarrow T \rightarrow 0.$$

Comparing this with (40.17) and using Schanuel's Lemma, we obtain

$$(40.20) \quad X \dot{+} \Lambda' = \Lambda \dot{+} \Lambda' \otimes X \quad \text{as left } \Lambda\text{-modules.}$$

Suppose now that $[X] \in \ker \beta$; then $\Lambda' \otimes X$ is stably isomorphic to Λ' , so there exists a free left Λ' -lattice F' with

$$\Lambda' \dot{+} F' \cong \Lambda' \otimes X \dot{+} F'.$$

Then (40.20) gives

$$X \dot{+} (\Lambda' \dot{+} F') \cong \Lambda \dot{+} (\Lambda' \dot{+} F').$$

But $\Lambda' \dot{+} F'$ is a projective Λ -lattice, whence $\Lambda' \dot{+} F' \dot{+} L$ is Λ -free for some Λ -lattice L . Adding L to both sides of the preceding equation, we deduce that X is stably isomorphic to Λ as Λ -lattices. Thus $[X] = 0$ in $\text{Cl } \Lambda$, which shows that β is monic, and completes the proof of the theorem.

The preceding result shows, in particular, that $\text{Cl } \Lambda \cong \text{Cl } \Lambda'$ for every maximal order Λ' containing Λ . Keeping the notation of (40.7), let us write $\Lambda' = \Sigma \Lambda'_i$, where Λ'_i is a maximal R_i -order in A_i . Then

$$\text{Cl } \Lambda \cong \text{Cl } \Lambda' \cong \sum \text{Cl } \Lambda'_i.$$

If K is an algebraic number field, or if K is a function field and $A_i = \text{Eichler}/R_i$ for each i , then by (35.14) we have

$$\text{Cl } \Lambda'_i \cong \text{Cl}_{A_i} R_i \quad \text{for each } i.$$

Thus, in these cases the class group $\text{Cl } \Lambda$ is known explicitly as a ray class group of the center of Λ .

Generalizing Exercise 21.1, we prove next

(40.21) THEOREM. Let M be any nonzero left Λ -lattice, where Λ is a hereditary R -order. Then $\text{End}_\Lambda M$ is a hereditary R -order in $\text{End}_\Lambda KM$.

Proof. Choose a left Λ -lattice M' such that $M \dot{+} M' = \Lambda^{(n)}$ for some n , and let $\Gamma = \text{End}_\Lambda \Lambda^{(n)}$. Then Γ is Morita equivalent to Λ , whence Γ is also hereditary by Exercise 15.4. Let $e: \Lambda^{(n)} \rightarrow M$ be the projection associated with the direct sum decomposition $\Lambda^{(n)} = M \dot{+} M'$. Then

$$\text{End}_\Lambda M \cong e\Gamma e,$$

and so $\text{End}_\Lambda M$ is hereditary by Exercise 40.3.

Using this, we now show

(40.22) THEOREM. Let Λ be a hereditary R -order in the separable K -algebra A , where K is a global field. Let M, N be a pair of left Λ -lattices such that $M \vee N$ and $\Lambda'M \cong \Lambda'N$ for some order Λ' containing Λ . If the K -algebra $\text{End}_A KM$ satisfies the Eichler condition relative to R (see (38.1)), then $M \cong N$.

Proof. Let us set

$$\Gamma = \text{End}_\Lambda M, \quad \Gamma' = \text{End}_{\Lambda'} \Lambda' M, \quad B = \text{End}_A KM.$$

Then by (40.21), Γ is a hereditary R -order in the separable K -algebra B . Replacing N by αN for some nonzero $\alpha \in R$, we may assume that $N \subset M$. View M as a bimodule ${}_\Lambda M_\Gamma$, and set

$$J = \text{Hom}_\Lambda(M, N).$$

Then J is a left ideal in Γ ; we claim that $J \vee \Gamma$ and that $N = MJ$.

For each P , there is an isomorphism $M_P \cong N_P$, so we may write

$$N_P = M_P u_P, \quad u_P \in u(B_P).$$

Therefore

$$J_P = \text{Hom}_{\Lambda_P}(M_P, N_P) = \Gamma_P u_P.$$

This shows that $J \vee \Gamma$. It also establishes that $N = MJ$, since the equality holds locally at all P . Therefore $[J]$ is an element of the locally free class group $\text{Cl}\Gamma$.

Now we have

$$\Gamma' J = \text{Hom}_{\Lambda'}(\Lambda' M, \Lambda' N),$$

since the equality holds locally at each P . On the other hand, $\Lambda' N = \Lambda' M \cdot y$ for some $y \in u(B)$, since $\Lambda' M \cong \Lambda' N$ by hypothesis. Therefore $\Gamma' J = \Gamma' y$, so that $[J]$ maps onto zero under the homomorphism $\text{Cl}\Gamma \rightarrow \text{Cl}\Gamma'$ defined

as in (40.16). Hence by (40.16) it follows that $[J] = [\Gamma]$. Therefore $J \cong \Gamma$ by (38.4), so $J = \Gamma z$ for some $z \in u(B)$. Hence $N = MJ = Mz \cong M$, which completes the proof of the theorem.

EXERCISES

1. Let $\Lambda \subset \Lambda'$ be R -orders in a K -algebra A , and let X, Y be left Λ' -modules such that Y is R -torsionfree. Prove that

$$\text{Hom}_{\Lambda'}(X, Y) = \text{Hom}_{\Lambda}(X, Y).$$

[Hint: The left hand expression is clearly included in the right hand expression. Now let $f \in \text{Hom}_{\Lambda}(X, Y)$. Given $\lambda' \in \Lambda'$, choose a nonzero $r \in R$ such that $r\lambda' \in \Lambda$. Then

$$r \cdot f(\lambda'x) = f(r\lambda' \cdot x) = r\lambda' f(x), \quad x \in X,$$

whence $f(\lambda'x) = \lambda'f(x)$ for all λ', x since Y is R -torsionfree.]

2. Let Λ be an R -order, M and N left Λ -modules.

- (i) Let $M^* = \text{Hom}_R(M, R)$, the *dual* of M . Show that M^* is a right Λ -module. Prove that each $f \in \text{Hom}_{\Lambda}(M, N)$ induces an $f^* \in \text{Hom}_{\Lambda}(N^*, M^*)$.
- (ii) Show that analogous results hold when “left” and “right” are interchanged.
- (iii) Let $\varphi_M: M \rightarrow M^{**}$ be the *evaluation map* defined by

$$\{\varphi_M(m)\}f = f(m), \quad f \in M^*, \quad m \in M.$$

Show that φ_M is a left Λ -homomorphism.

- (iv) Show that if M is a Λ -lattice, then so are M^* and M^{**} . Prove that $\varphi_M: M \cong M^{**}$, and show that the isomorphism $M \cong M^{**}$ is natural, that is, for each homomorphism $f: M \rightarrow N$ of left Λ -lattices, there is a commutative diagram

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \varphi_M \downarrow & & \downarrow \varphi_N \\ M^{**} & \xrightarrow{f^{**}} & N^{**}, \end{array}$$

where f induces f^{**} . [Hint: Use (4.24).]

3. Let $e \in \Gamma$ be idempotent, where Γ is a hereditary R -order. Show that $e\Gamma e$ is also a hereditary R -order. [Hint: Let L be any left ideal of $e\Gamma e$; there exists a left $e\Gamma e$ -epimorphism

$$\varphi: (e\Gamma e)^{(r)} \rightarrow L, \quad \varphi(\alpha_1, \dots, \alpha_r) = \sum_{i=1}^r \alpha_i l_i \quad (\text{say}), \quad \alpha_i \in e\Gamma e.$$

Extend φ to a left Γ -epimorphism

$$\varphi': \Gamma^{(r)} \rightarrow \Gamma L, \quad \varphi'(\gamma_1, \dots, \gamma_r) = \sum_{i=1}^r \gamma_i l_i, \quad \gamma_i \in \Gamma,$$

where ΓL is a left ideal in Γ . Since Γ is hereditary, there exists a left Γ -map $\psi': \Gamma L \rightarrow \Gamma^{(r)}$ splitting φ' . Let

$$\psi'(y) = (\psi_1(y), \dots, \psi_r(y)), \quad y \in \Gamma L.$$

Then each $\psi_i \in \text{Hom}_\Gamma(\Gamma L, \Gamma)$, and $\psi_i(x) = e\psi_i(x)$, $x \in L$. Define $\psi: L \rightarrow (e\Gamma e)^{(r)}$ by

$$\psi(x) = (\psi_1(x)e, \dots, \psi_r(x)e), \quad x \in L.$$

Then ψ is an $e\Gamma e$ -homomorphism, and

$$\varphi\psi(x) = \sum_{i=1}^r \psi_i(x)el_i = \sum_{i=1}^r \psi_i(x)l_i = \varphi'\psi'(x) = x, \quad x \in L.$$

Thus L is $e\Gamma e$ -projective.]

4. Let $A = (L/K, 1) = \sum_{\sigma \in G} Lu_\sigma$ be a trivial crossed-product algebra with $u_1 = 1$.

Prove that for each $a \in L$ and each $\sigma \in G$,

$$\text{tr}_{A/K} au_\sigma = \begin{cases} T_{L/K} a, & \sigma = 1, \\ 0, & \sigma \neq 1. \end{cases}$$

41. GROUP RINGS

We shall collect here some miscellaneous results on integral group rings, concerned mostly with their relations with maximal orders. Throughout this section, let G denote a finite group of order n , and let $A = KG$ be the group algebra of G over K . We assume once and for all that $\text{char } K \nmid n$, so A is a separable K -algebra by Exercise 7.8. The *integral group ring* RG is the R -order in A consisting of all formal sums $\sum_{x \in G} \alpha_x x$, where the coefficients $\{\alpha_x\}$ lie in R . We set $\Lambda = RG$ throughout. Since the study of integral representations of G reduces to the investigation of Λ -modules, it is desirable to know as much as possible about the R -order Λ .

(41.1) THEOREM. *Let Γ be any R -order in A containing Λ . Then*

$$\Lambda \subset \Gamma \subset n^{-1}\Lambda.$$

Furthermore,

$$\Lambda \text{ is maximal} \iff \Lambda \text{ is hereditary} \iff n \in u(R).$$

Proof: Let $T = T_{A/K}$ be the ordinary trace map. For $x \in G$, let $x_i: a \rightarrow xa$, $a \in A$, be left multiplication by x . Relative to the K -basis of A consisting of the elements of G , x_i is represented by an $n \times n$ permutation matrix. If $x \neq 1$, then all of the main diagonal entries of this matrix are 0. This gives

$$(41.2) \quad T_{A/K} x = \begin{cases} n, & x = 1, \\ 0, & x \in G, x \neq 1. \end{cases}$$

Now let $\gamma = \sum \alpha_x x \in \Gamma$, where each $\alpha_x \in K$. Since Γ contains all elements of G , we have $\gamma y^{-1} \in \Gamma$ for all $y \in G$. But $T(\gamma y^{-1}) \in R$ by Exercise 1.1, and thus

$$T(\gamma y^{-1}) = \sum_x \alpha_x T(xy^{-1}) = n\alpha_y \in R.$$

Therefore $\alpha_y \in n^{-1}R$ for all $y \in G$, whence $\gamma \in n^{-1} \cdot RG$. This proves that $\Gamma \subset n^{-1}\Lambda$, as claimed.

If $n \in u(R)$, the above shows that every order Γ containing Λ must coincide with Λ ; thus Λ is maximal, and also hereditary. Conversely, suppose Λ is hereditary. Then by (40.7), Λ contains the central idempotent $n^{-1} \cdot \sum_{x \in G} x$ of A . Therefore $n^{-1} \in R$, whence $n \in u(R)$. This completes the proof of the theorem.

For the rest of this section, let Γ denote a maximal order in A containing Λ . We have just shown that $n\Gamma \subset \Lambda$. Jacobinski's refinement of this result, to be given below, is based on using reduced traces rather than ordinary traces. Departing slightly from his terminology, we set

$$(\Gamma : \Lambda)_l = \{x \in A : x\Gamma \subset \Lambda\} = \text{left conductor of } \Gamma \text{ into } \Lambda,$$

$$(\Gamma : \Lambda)_r = \{x \in A : \Gamma x \subset \Lambda\} = \text{right conductor of } \Gamma \text{ into } \Lambda.$$

We shall use the following notation hereafter:

$$A = \sum_{i=1}^t A_i \quad (\text{simple components}).$$

$$K_i = \text{center of } A_i, (A_i : K_i) = n_i^2, \quad R_i = \text{integral closure of } R \text{ in } K_i.$$

$$\Gamma = \sum_{i=1}^t \Gamma_i, \quad \Gamma_i = \text{maximal } R_i\text{-order in } A_i.$$

$$\text{tr}_i = \text{tr}_{A_i/K} = \text{reduced trace from } A_i \text{ to } K.$$

$$\mathfrak{D}_i = \mathfrak{D}(\Gamma_i/R) = \text{different of } \Gamma_i \text{ with respect to } R.$$

Let us recall from §25 that the inverse different \mathfrak{D}_i^{-1} is the complementary ideal of Γ_i with respect to tr_i , that is,

$$\mathfrak{D}_i^{-1} = \{x \in A_i : \text{tr}_i(x\Gamma_i) \subset R\}.$$

We note that the right conductor $(\Gamma : \Lambda)_r$ is a (Γ, Λ) -bimodule, and is the largest left Γ -submodule of Λ .

(41.3) **Theorem** (Jacobinski [1]). *We have*

$$(\Gamma : \Lambda)_l = (\Gamma : \Lambda)_r = \sum_{i=1}^t (n/n_i) \mathfrak{D}_i^{-1}.$$

Proof. Let $\tau: A \times A \rightarrow K$ be the bilinear trace form defined by $\tau(x, y) = T(xy)$, $x, y \in A$, where $T = T_{A/K}$ as above. Let $G = \{x_1, \dots, x_n\}$, $x_1 = 1$, so that $\{x_1, \dots, x_n\}$ is a K -basis for A . From (41.2) we obtain

$$(41.4) \quad \tau(x_i, n^{-1}x_j^{-1}) = \delta_{ij} \quad (\text{Kronecker delta}), \quad 1 \leq i, j \leq n.$$

Thus $\{n^{-1}x_1^{-1}, \dots, n^{-1}x_n^{-1}\}$ is a dual basis to $\{x_1, \dots, x_n\}$ relative to τ , and so the form τ is nondegenerate.

Every full R -lattice M in A determines a *dual* lattice \tilde{M} (see Exercise 4.12), defined by

$$\tilde{M} = \{a \in A : \tau(a, M) \subset R\}.$$

As shown in Exercise 4.12, the correspondence $M \mapsto \tilde{M}$ is one-to-one inclusion-reversing, and $\tilde{\tilde{M}} = M$. If M is a *right* Γ -lattice in A , then \tilde{M} is a *left* Γ -lattice in A . If M is R -free with basis $\{m_i\}$, then $\tilde{M} = \sum Rm'_j$, where $\tau(m_i, m'_j) = \delta_{ij}$, $1 \leq i, j \leq n$. From (41.4) we conclude at once that

$$(41.5) \quad \tilde{\Lambda} = \sum_{j=1}^n Rn^{-1}x_j^{-1} = n^{-1}\Lambda.$$

Now take $M = (\Gamma:\Lambda)_r$, the largest left Γ -module in Λ . Then \tilde{M} is the *smallest* right Γ -module containing $\tilde{\Lambda}$, that is,

$$\tilde{M} = \tilde{\Lambda}\Gamma = n^{-1}\Lambda \cdot \Gamma = n^{-1}\Gamma.$$

Therefore $M = \tilde{M} = n\tilde{\Gamma}$, where

$$\tilde{\Gamma} = \{x \in A : T(x\Gamma) \subset R\}.$$

Each $x \in A$ may be written as $x = \sum x_i$, $x_i \in A_i$. By (9.22) we know that

$$T(x) = \sum_{i=1}^t n_i \text{tr}_i x_i.$$

This gives at once

$$\begin{aligned} \tilde{\Gamma} &= \{x \in A : n_i \text{tr}_i (x_i \Gamma_i) \subset R \quad \text{for } 1 \leq i \leq t\} \\ &= \sum_{i=1}^t n_i^{-1} \mathfrak{D}_i^{-1}. \end{aligned}$$

Therefore

$$(\Gamma:\Lambda)_r = n\tilde{\Gamma} = \sum (n/n_i) \mathfrak{D}_i^{-1},$$

as desired. The same argument works equally well for $(\Gamma:\Lambda)_l$, and the theorem is proved.

From the preceding we obtain

$$n\Gamma \subset n\tilde{\Gamma} = (\Gamma:\Lambda)_r \subset \Lambda,$$

so we recover part of (41.1). From the proof of (41.3), we may also show directly that if Λ is hereditary, then Λ is maximal. If Λ is hereditary, then Γ is projective as right Λ -lattice. Hence by (16.7) we obtain

$$\Gamma \otimes_{\Lambda} \text{Hom}_{\Lambda}(\Gamma, \Lambda) \cong \text{End}_{\Lambda} \Gamma.$$

After making some obvious identifications, we may rewrite this as

$$\Gamma \cdot (\Gamma : \Lambda) = \Gamma.$$

But $(\Gamma : \Lambda)_i$ is a left Γ -lattice, since it equals $(\Gamma : \Lambda)_r$ by (41.3). Therefore $(\Gamma : \Lambda)_i = \Gamma$, which implies that $\Gamma = \Lambda$.

Turning next to questions of ramification, let us first generalize the definitions given in §§4,32.

(41.6) *Definition.* Let B be a separable K -algebra, and let P be any prime of K . We say that B is *unramified at P* if the P -adic completion B_P is expressible as

$$B_P \cong \sum M_{n_j}(E_j),$$

where for each j , E_j is a field which is unramified over the P -adic field K_P . (When P is an infinite prime, this latter condition is taken to mean that $E_j = K_P$.)

(41.7) *THEOREM.* *Let P be a maximal ideal of R , where $R = \text{alg. int. } \{K\}$ and K is an algebraic number field. Then KG is unramified at P whenever $P \nmid nR$.*

Proof. Replacing R by its localization $(R - P)^{-1}R$ and changing notation, we may assume that R is the P -adic valuation ring in K , and that $n \in u(R)$. Keep the notation introduced before (41.3). By Exercise 41.4, it suffices to show that each A_i is unramified at P . Keep i fixed; since $n_i | n$ by Exercise 41.1, we have $n/n_i \in u(R)$. But $n/n_i \in \mathfrak{D}_i$ by (41.3), whence $\mathfrak{D}_i = \Gamma_i$. Therefore

$$\Gamma_i = \mathfrak{D}(\Gamma_i / R_i) \cdot \mathfrak{D}(R_i / R)$$

by Exercise 25.1, that is,

$$(41.8) \quad \mathfrak{D}(\Gamma_i / R_i) = \Gamma_i, \quad \mathfrak{D}(R_i / R) = R_i.$$

Let p range over the primes of R_i dividing P . By (25.7) and the first equality in (41.8), we may conclude that A_i has local index 1 at each p . Therefore A_i is unramified at each p . On the other hand, from (4.37) and the second equality in (41.8), it follows that each p is unramified in the extension K_i / K . Hence by §5c, each $(K_i)_p$ is unramified over K_p . Therefore A_i is unramified at P , by Exercise 41.6, and the theorem is established.

The converse of (41.7) is false, as we shall see below. It may well happen that A is unramified at a prime P dividing n . We shall find examples where this occurs by using the next theorem, which is of importance in its own right.

(41.9) **Theorem** (Schilling). *Let G be a group of order p^r , where p is prime, and let K be a field of characteristic 0.*

(i) *If p is odd, then each simple component of KG is a full matrix algebra over a field.*

(ii) *If $p = 2$, then each simple component of KG is of the form $M_k(D)$, where D is either a field or a skewfield of index 2.*

Proof. First let $M_k(D)$ be a simple component of $\mathbf{Q}G$, where D is a skewfield with center L . Let ω be a primitive p^r -th root of 1. By Curtis-Reiner [1, (70.8)], L is a subfield of $\mathbf{Q}(\omega)$. Since p is completely ramified in the extension $\mathbf{Q}(\omega)/\mathbf{Q}$, there is a unique prime P_0 of L dividing p (see references listed in §4). Hence by (41.7), P_0 is the only finite prime of L at which $M_k(D)$ can possibly ramify. Thus D has local Hasse invariant 0 at every finite prime of L except possibly at P_0 .

Suppose now that p is odd. Then D has odd index, since this index divides p^r by Exercise 41.1. Therefore no infinite prime of L ramifies in D by Exercise 32.2. It follows from Exercise 32.1 that $D = L$, which proves (i) for the case $K = \mathbf{Q}$.

Now let $p = 2$, and let D have index m . Some real primes of L may ramify in D ; at each such prime, the local Hasse invariant of D is 1/2. But by (32.13a), the sum of all of the local invariants of D is 0. This shows that $m = 1$ or 2, and establishes (ii) when $K = \mathbf{Q}$.

Now let K be arbitrary, and let $\{B_i\}$ range over the simple components of $\mathbf{Q}G$. As in the proof of Exercise 41.1, we have

$$KG \cong \sum_{i,j} F_{ij} \otimes_{K_i} B_i,$$

where K_i is the center of B_i . We have just shown that B_i is of the form $M_k(D)$, where D is a skewfield of index 1 or 2. Then each $F_{ij} \otimes_{K_i} B_i$ is also of the form $M_s(D')$, where D' is a skewfield of index 1 or 2. This completes the proof.

This theorem was rediscovered, with different proofs, by Witt and Roquette; see also Feit [1, (14.5)].

EXERCISES

In Exercises 1–3, we keep the notation of (41.3) and its proof.

1. Show that $n_i|n$ when $\text{char } K = 0$. [Hint: First take $K = \mathbf{Q}$, $R = \mathbf{Z}$ in (41.3). For each i , we have $(n/n_i)\mathfrak{D}_i^{-1} \subset \Gamma_i$, and so $n/n_i \in \mathfrak{D}_i \subset \Gamma_i$. Hence n/n_i is integral over \mathbf{Z} , whence $n_i|n$. Now let E be any field of characteristic 0. Then $E \supset \mathbf{Q}$, and

$$EG \cong E \otimes_{\mathbf{Q}} \mathbf{Q}G \cong \sum_{i=1}^t (E \otimes_{\mathbf{Q}} K_i) \otimes_{K_i} A_i.$$

Fix i , and let $E \otimes_{\mathbf{Q}} K_i \cong \sum F_{ij}$ be a direct sum of fields $\{F_{ij}\}$. Then

$$(E \otimes_{\mathbf{Q}} K_i) \otimes_{K_i} A_i \cong \sum_j F_{ij} \otimes_{K_i} A_i,$$

and each summand $F_{ij} \otimes A_i$ is a simple algebra of dimension n_i^2 over its center $F_{ij}.$]

2. Let K be an algebraic number field. Prove that for each $i,$

$$R_i \cap (n/n_i) \mathfrak{D}_i^{-1} = (n/n_i) \mathfrak{D}^{-1}(R_i/R).$$

Deduce that

$$\{x \in R : x\Gamma \subset \Lambda\} = \bigcap_{i=1}^t (n/n_i)(K \cap \mathfrak{D}^{-1}(R_i/R)).$$

[Hint (Jacobinski [1]): By Exercise 25.1, $\mathfrak{D}_i = \mathfrak{A}\mathfrak{B}$ where

$$\mathfrak{A} = \mathfrak{D}(\Gamma_i/R_i), \quad \mathfrak{B} = \mathfrak{D}(R_i/R).$$

For $x \in R_i,$

$$x \in (n/n_i)\mathfrak{A}^{-1}\mathfrak{B}^{-1} \Leftrightarrow x\mathfrak{B} \subset (n/n_i)\mathfrak{A}^{-1} \Leftrightarrow x\mathfrak{B} \subset (n/n_i)(K_i \cap \mathfrak{A}^{-1}).$$

Write $K_i \cap \mathfrak{A}^{-1} = \mathfrak{a}^{-1}$, where \mathfrak{a} is an ideal of $R_i.$ If $\mathfrak{a} \neq R_i,$ choose a prime ideal P of R_i dividing $\mathfrak{a},$ and let \mathfrak{P} be the prime ideal of Γ_i corresponding to $P.$ If $P\Gamma_i = \mathfrak{P}^e,$ then the power of \mathfrak{P} in \mathfrak{A} is precisely $\mathfrak{P}^{e-1}.$ But then

$$P \supset \mathfrak{a} \Rightarrow P^{-1} \subset \mathfrak{a}^{-1} \Rightarrow P^{-1} \subset \mathfrak{A}^{-1} \Rightarrow P\Gamma_i | \mathfrak{A},$$

a contradiction. Hence $K_i \cap \mathfrak{A}^{-1} = R_i$ so for $x \in R_i$ we have

$$x \in (n/n_i) \mathfrak{D}_i^{-1} \Leftrightarrow x\mathfrak{B} \subset (n/n_i)R_i \Leftrightarrow x \in (n/n_i)\mathfrak{B}^{-1}.$$

But $(n/n_i)\mathfrak{B}^{-1} \subset R_i,$ since $(n/n_i)\mathfrak{B}^{-1} \subset (n/n_i)\mathfrak{D}_i^{-1} \subset \Lambda,$ so each element of $(n/n_i)\mathfrak{B}^{-1}$ is integral over $R.$ This proves the first assertion, and the second is an easy consequence of the first.]

3. Let e be a central idempotent in $A,$ and let M be a left Λ -lattice such that $eM = M.$ Let

$$f_e = \bigcap_i (n/n_i)(K \cap \mathfrak{D}^{-1}(R_i/R)),$$

where i ranges over all indices such that e_i occurs in $e.$ Prove that

$$f_e \cdot \text{Ext}_{\Lambda}^1(M, X) = 0, \quad f_e \cdot \text{Ext}_{\Lambda}^1(X, M) = 0$$

for all left Λ -lattices $X.$ [Hint (Jacobinski [1]): First reduce the problem to the case where $eX = X.$ Changing notation, we may then assume that $e = 1.$ Each $r \in f_e$ is an element of R such that $r\Gamma \subset \Lambda.$ Using the fact that Γ is hereditary, deduce that r annihilates $\text{Ext}_{\Lambda}^1(M, \cdot)$ and $\text{Ext}_{\Lambda}^1(\cdot, M).$]

(For generalizations of the above, see T. V. Fossum [1, 2], Roggenkamp, Huber-Dyson [1].)

4. Let $B = \sum_i B_i$ (simple components) be a separable K -algebra, and let P be a prime of $K.$ Show that B is unramified at P if and only if each B_i is unramified at $P.$

5. Let B be a central simple L -algebra, and let \mathfrak{p} be a prime of $L.$ Show that B is unramified at \mathfrak{p} if and only if $B_{\mathfrak{p}}$ is a full matrix algebra over $L_{\mathfrak{p}},$ that is, if and only if the local index of B at \mathfrak{p} equals 1.

6. Let B be a central simple L -algebra, and let K be a subfield of L such that $(L:K)$ is finite. Let P be a prime of K , and let \mathfrak{p} range over the primes of L dividing P . Prove that

$$(i) \quad B_P \cong \sum_{\mathfrak{p}} B_{\mathfrak{p}}, \text{ where } B_{\mathfrak{p}} = L_{\mathfrak{p}} \otimes_L B \text{ is a central simple } L_{\mathfrak{p}}\text{-algebra.}$$

(ii) Let P be a finite prime. Then B is unramified at P if and only if for each \mathfrak{p} , $L_{\mathfrak{p}}$ is unramified over $K_{\mathfrak{p}}$ and $B_{\mathfrak{p}}$ is a full matrix algebra over $L_{\mathfrak{p}}$.

(iii) Let P be an infinite prime. Then B is unramified at P if and only if for each \mathfrak{p} , $L_{\mathfrak{p}} = K_{\mathfrak{p}}$ and $B_{\mathfrak{p}}$ is a full matrix algebra over $L_{\mathfrak{p}}$.

[Hint: Write

$$B_P \cong (K_P \otimes_K L) \otimes_L B, \quad K_P \otimes_K L \cong \sum_{\mathfrak{p}} L_{\mathfrak{p}},$$

where \mathfrak{p} ranges over the distinct primes of L dividing P .]

References

ALBERT, A. A.

1. "Structure of Algebras." Amer. Math. Soc., New York, 1939; revised, 1961.

AMITSUR, S.

1. On central division algebras. *Israel J. Math.* **12** (1972), 408–420.

ARTIN, E.

1. "Questions de Base Minimale dans la Théorie des Nombres Algébriques." Centre Nat. Rech. Sci. XXIV, Colloq. Int., Paris (1950), 19–20. Reprinted in Collected Papers, ed. S. Lang and J. Tate, Addison-Wesley 1965, pp. 229–231.

ARTIN, E., NESBITT, C. J., THRALL, R. M.

1. "Rings with Minimum Condition." Univ. of Michigan Press, Ann Arbor, 1948.

ARTIN, E., TATE, J. T.

1. "Class Field Theory." Benjamin, New York, 1967.

ASANO, K.

1. Arithmetische Idealtheorie in nichtkommutativen Ringen. *Japan. J. Math.* **16** (1936), 1–36.
2. Arithmetik in Schiefringen I. *Osaka Math. J.* **1** (1949), 98–134.

AUSLANDER, M., GOLDMAN, O.

1. Maximal orders. *Trans. Amer. Math. Soc.* **97** (1960), 1–24.
2. The Brauer group of a commutative ring. *ibid.*, 367–409.

AZUMAYA, G.

1. On maximally central algebras. *Nagoya Math. J.* **2** (1951), 119–150.

BABAKHANIAN, A.

1. "Cohomological Methods in Group Theory." Dekker, New York, 1972.

BASS, H.

1. "Algebraic K-theory," Math. Lecture Notes. Benjamin, New York, 1968.

BERGER, T. R., REINER, I.

1. The normal basis theorem. *Amer. Math. Monthly* (1975), to appear.

BOURBAKI, N.

1. "Algèbre: Modules et Anneaux Semi-simples" (Ch. 8). Hermann, Paris, 1958.
2. "Algèbre Commutative: Modules Plats, Localisation" (Ch. 1, 2). Hermann, Paris, 1961.
3. "Algèbre: "Graduations, . . ." (Ch. 3, 4). Hermann, Paris, 1961.
4. "Algèbre: Entiers, valuations" (Ch. 5, 6). Hermann, Paris. 1964.
5. "Algèbre: Diviseurs" (Ch. 7). Hermann, Paris. 1965.

BRUMER, A.

1. "Structure of Hereditary Orders." Thesis, Princeton Univ. 1963; *Bull. Amer. Math. Soc.* **69** (1963), 721–724; addendum, *ibid.* **70** (1964), 185.

CARTAN, H., EILENBERG, S.

1. "Homological Algebra." Princeton Univ. Press, Princeton, 1956.

- CASSELS, J. W. S., FRÖHLICH, A.
1. "Algebraic Number Theory." Academic Press, London and Thompson Publ. Co., Washington, D.C., 1967.
- COHN, H.
1. "A Second Course in Number Theory." Wiley, New York, 1962.
- COHN, P. M.
1. "Morita Equivalence and Duality." Queen Mary Coll. Math. Notes, 1966.
- COXETER, H. S. M.
1. The binary polyhedral groups and other generalizations of the quaternion group. *Duke Math. J.* **7** (1940), 367–379.
- COXETER, H. S. M., MOSER, W. O. J.
1. "Generators and Relations for Discrete Groups." Springer, Berlin, 1957.
- CURTIS, C. W., REINER, I.
1. "Representation Theory of Finite Groups and Associative Algebras." Wiley (Interscience), New York, 1962.
- DEURING, M.
1. "Algebren." Springer, Berlin, 1935 (revised, 1968).
- EICHLER, M.
1. Über die Idealklassenzahl total definiter Quaternionalgebren. *Math. Zeit.* **43** (1938), 102–109.
 2. Über die Idealklassenzahl hyperkomplexer Zahlen. *Math. Zeit.* **43** (1938), 481–494.
- FADDEEV, D. K.
1. An introduction to the multiplicative theory of integral representations. *Proc. Steklov Inst. Math.* **80** (1965), A.M.S. translation (1968).
- FAITH, C.
1. "Algebra: Rings, modules and categories I." Springer, Berlin–New York, 1973.
- FOSSUM, R.
1. The Noetherian different of projective orders. *J. reine angew. Math.* **224** (1966), 207–218.
 2. Maximal orders over Krull domains. *J. Algebra* **10** (1968), 321–332.
 3. Injective modules over Krull orders. *Math. Scand.* **28** (1971), 233–246.
 4. The divisor class group of a Krull domain. *Ergeb. Math.*, Springer, Berlin, 1973.
- FOSSUM, T. V.
1. On symmetric orders and separable algebras. *Trans. Amer. Math. Soc.* (1975), to appear.
- FRÖHLICH, A.
1. The Picard group of non-commutative rings, in particular of orders. *Trans. Amer. Math. Soc.* **180** (1973), 1–46.
 2. Locally free modules over arithmetic orders. *J. reine angew. Math.* (1975), to appear.
- FRÖHLICH, A., REINER, I., ULLOM, S.
1. Class groups and Picard groups of orders. *Proc. London Math. Soc.* **29** (1974), 405–434.
- GRUENBERG, K. W.
1. "Cohomological Topics in Group Theory," Springer Lecture notes No. 143. Springer, Berlin, 1970.
- HARADA, M.
1. Hereditary orders. *Trans. Amer. Math. Soc.* **107** (1963), 273–290.
 2. Structure of hereditary orders. *J. Math. Osaka City Univ.* **14** (1963), 1–22.

3. Hereditary orders in generalized quaternions. *ibid.*, 71–81.
4. Multiplicative ideal theory in hereditary orders. *ibid.*, 83–106.
5. Hereditary orders which are dual. *ibid.*, 107–115.
6. On generalization of Asano's maximal orders in a ring. *Osaka J. Math.* **1** (1964), 61–68.
7. Some criteria for hereditarity of crossed products. *ibid.*, 69–80.

HASSE, H.

1. Über p-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme. *Math. Ann.* **104** (1931), 495–534.

HERSTEIN, I. N.

1. "Noncommutative Rings," Carus Monograph 15. Math. Assoc. America, 1968.

HILTON, P. J., STAMMBACH, U.

1. "A Course in Homological Algebra." Springer, Berlin–New York, 1971.

JACOBSON, N.

1. "The Theory of Rings." Amer. Math. Soc., New York, 1943.
2. "Structure of Rings." Amer. Math. Soc., New York, 1956.

JACOBINSKI, H.

1. On extensions of lattices. *Michigan Math. J.* **13** (1966), 471–475.
2. Über die Geschlechter von Gittern über Ordnungen. *J. reine angew. Math.* **230** (1968), 29–39.
3. Genera and decomposition of lattices over orders. *Acta Math.* **121** (1968), 1–29.
4. Two remarks about hereditary orders. *Proc. Amer. Math. Soc.* **28** (1971), 1–8.

JANS, J. P.

1. "Rings and Homology". Holt Rinehart Winston, New York, 1964.

JANUSZ, G. J.

1. "Algebraic Number Theory." Academic Press, New York, 1973.

KAPLANSKY, I.

1. "Commutative Rings." Allyn and Bacon, Boston, 1970.

KNEBUSCH, M.

1. Elementarteilertheorie über Maximalordnungen. *J. reine angew. Math.* **226** (1967), 175–183.

MACLANE, S.

1. "Homology". Springer, Berlin–New York, 1963.

MATSUMURA, H.

1. "Commutative Algebra." Benjamin, New York, 1970.

MICHLER, G. O.

1. Asano orders. *Proc. London Math. Soc.* (3) **19** (1969), 421–443.

NEUKIRCH, J.

1. "Klassenkörpertheorie." Bibliog. Inst., Mannheim, 1969.
2. Eine Bemerkung zum Existenzsatz von Grunwald-Hasse-Wang. *J. reine angew. Math.* **268/269** (1974), 315–317.

NORTHCOTT, D. G.

1. "An Introduction to Homological Algebra." Cambridge Univ. Press, Cambridge, 1960.

O'MEARA, O. T.

1. "Introduction to Quadratic Forms." Springer, Berlin–New York, 1963.

REINER, I.

1. A survey of integral representation theory. *Bull. Amer. Math. Soc.* **76** (1970), 159–227.

2. Hereditary orders. *Rend. Sem. Mat. Univ. Padova* (1975), to appear.
- RIBENBOIM, P.
1. L'arithmétique des Corps," Hermann, Paris, 1972.
- ROBSON, J. C.
1. Non-commutative Dedekind rings. *J. Algebra* **9** (1968), 249–265.
 2. Idealizers and hereditary noetherian prime rings. *J. Algebra* **22** (1972), 45–81.
- ROGGENKAMP, K. W.
1. "Lattices over Orders II," Springer Lecture notes No. 142. Springer, Berlin, 1970.
 2. Projective homomorphisms and extensions of lattices. *J. reine angew. Math.* **246** (1971), 41–45.
- ROGGENKAMP, K. W., HUBER-DYSON, V.
1. "Lattices over Orders I," Springer Lecture notes No. 115. Springer, Berlin, 1970.
- ROSENBERG, A., ZELINSKY, D.
1. Automorphisms of separable algebras. *Pacific J. Math.* **11** (1961), 1109–1117.
- ROTMAN, J. J.
1. "Notes on Homological Algebra." van Nostrand Reinhold, New York, 1970.
- SAMUEL, P.
1. "Théorie Algébrique des Nombres." Hermann, Paris, 1967.
- SCHACHER, M. M., SMALL, L.
1. Noncrossed products in characteristic p . *J. Algebra* **24** (1973), 100–103.
- SCHILLING, O. F. G.
1. "The theory of valuations." Amer. Math. Soc., New York, 1950.
- SERRE, J.-P.
1. "Corps Locaux." Hermann, Paris, 1962.
- SWAN, R. G.
1. Projective modules over group rings and maximal orders. *Ann. of Math.* (2) **76** (1962), 55–61.
 2. "Algebraic K -theory," Springer Lecture notes No. 76. Springer, Berlin, 1968.
- SWAN, R. G., EVANS, E. G.
1. " K -theory of Finite Groups and Orders," Springer Lecture notes 149. Springer, Berlin, 1970.
- WANG, S.
1. On Grunwald's theorem. *Ann. of Math.* (2) **51** (1950), 471–484.
- WEIL, A.
1. "Basic Number Theory." Springer, Berlin–New York, 1967.
- WEISS, E.
1. "Algebraic Number Theory." McGraw Hill, New York, 1963.
 2. "Cohomology of Groups." Academic Press, New York, 1969.
- WILLIAMSON, S.
1. Crossed products and hereditary orders. *Nagoya Math. J.* **23** (1963), 103–120.
- WILSON, S. M. J.
1. Reduced norms in the K -theory of orders. *J. Algebra* (1976), to appear.
- ZARISKI, O., SAMUEL, P.
1. "Commutative algebra," Vol. I. van Nostrand, Princeton, 1958.

Subject Index

A

A.C.C., 13
additive functor 14
a.e. (almost everywhere)
algebra
 Azumaya, 338
 central separable, 338
 central simple, 92
 over a commutative ring, 1
 separable, 99, 106
algebraic number field, 46
alg. int., 46
annihilator, 44, 77
archimedean valuation, 52, 71
artinian, 13
Asano order, 207
associative bilinear form, 116
augmentation map, 258
Autcent, 328
Azumaya algebra, 338

B

bimodule, 9
bimodule over R , 319
Brandt groupoid, 201
Brauer group, 238

C

capacity, 179, 213, 222
centralizer, 95
central simple, 92
chain in a vector space, 354
chain ring, 354
Change of Rings Theorem, 26
characteristic polynomial, 2
characteristic polynomial (reduced), 113,
 119, 121

Chinese remainder theorem, 47
class group, 306, 308, 343
cohomology group, 242, 257
cok (cokernel), 8
commutative diagram, 9
complementary ideal, 60, 217, 223
complementary lattice, 60
complete (in N -adic topology), 85
complete discrete valuation ring, 135
complete field, 67
completely primary, 82
complex prime, 64
completely ramified, 73
conductor, 366, 380
conjugate, 146, 285
conjugate orders, 232
contravariant (functor), 9, 14
counting norm, 59, 216
covariant (functor), 9, 14
cyclic algebra, 259
cyclic module, 50
crossed-product algebra, 242

D

D.C.C., 13
Dedekind domain, 45
deleted projective resolution, 20
dense, 68
decomposition group, 274
derived Morita context, 162
different, 60, 150, 184, 217
dimension shifting, 23
direct product of rings, 90
direct sum of rings, 90
discrete valuation, 51
discrete valuation ring, 52, 135
discriminant (ideal), 61, 66, 126, 218
discriminant (of element), 67
division ring, 91

double centralizer property, 93
dual of lattice, 367, 381

E

Eichler condition, 294, 343
Eichler/ R , 294, 343
Eichler's Theorem, 297, 298
Eisenstein extension, 74
Eisenstein polynomial, 73
enveloping algebra, 101
epimorphism (of rings), 77
equivalence
 of categories, 155
 of embeddings, 74
 of extensions, 19
 of factor sets, 243
 of valuations, 51
evaluation map, 55, 378
exact (right, left), 14
exact functor, 14
exact sequence, 8
 $\exp[A]$, 253
exponential valuation, 53
extension of modules, 19
extremal order, 356
extremal subring, 356

F

factor set, 242
faithful functor, 155
faithful module, 93
faithfully flat, 17
faithfully projective, 158
fibre product, 11
finite prime, 63, 64
finitely presented, 24
flat, 16
free basis, 15
free module, 15
fractional ideal, 47, 143
free resolution, 20
Frobenius automorphism, 73
full functor, 155
full lattice, 44, 108, 192
full matrix algebra, 91
function field, 63
functor, 14

G

Gauss' Lemma, 5
generator (of category), 155
genus, 232
global dimension, 41
global field, 63
global problem, 36
greatest common divisor, 47
Grothendieck group, 314
ground ideal, 222
group algebra, 108
group ring, 256, 373, 379
groupoid, 201
Grunwald-Wang Theorem, 279

H

Hasse-Brauer-Noether-Albert
Theorem, 276
Hasse invariant, 148, 266, 274
Hasse Norm Theorem, 275
Hasse-Schilling-Maass Theorem, 289
Hensel's Lemma, 71
hereditary ring, 27, 130
homological dimension, 20, 40

I

ideal
 class, 48, 224, 307, 343
 class group, 48, 306, 308
 class number, 224, 226
 fractional, 47, 143
 integral, 47, 182, 193
 invertible, 327
 maximal, 35
 maximal integral, 182, 195
 normal, 181, 193
 prime, 35, 190
 proper, 35
idempotent, 80
im (image), 8
indecomposable element, 230
indecomposable ideal, 182
indecomposable module, 88
index $[A]$, 253
index (of skewfield), 143, 238

Index Reduction Theorem, 255
 inertia field, 72, 145
 inertial degree, 140, 212
 infinite prime, 63
 inflation, 249
 injective module, 16
 inner automorphism, 103, 322
 integral closure, 5
 integral element, 3
 integral group ring, 256, 379
 integral ideal, 47, 182, 193
 integrally closed, 5, 6
 $\text{inv}[\mathcal{A}]$, 266
 Invariant Factor Theorem, 49
 invariant (Hasse), 148, 266, 274
 invariants of chain, 354
 invariants of hereditary order, 360
 inverse different, 60, 150, 184, 217
 invertible action, 33
 invertible bimodule, 319–320
 invertible ideal, 327
 irreducible, 78
 isomorphism of categories, 155
 isomorphism of K -algebras, 1

J

Jacobson radical, 78
 Jordan–Zassenhaus condition, 224
 Jordan–Zassenhaus Theorem, 228

K

K -isomorphism of K -algebras, 1
 \ker (kernel), 8
 Krasner's Lemma, 285
 Krull ring, 56
 Krull–Schmidt Theorem, 88

L

Ladder Theorem, 23
 lattice, 44, 108, 129
 least common multiple, 47
 left exact, 14
 left hereditary, 27
 left order, 109

lifting idempotents, 85, 86
 LFP, 345
 local ring, 82
 local capacity, 222
 local degree (of field extension), 275
 local field, 135
 local index, 222
 local problem, 36
 localization, 36
 locally free class group, 343
 locally free module, 343
 locally free Picard group, 345

M

maximal ideal, 35
 maximal integral ideal, 182, 195
 maximal order, 110
 minimal left ideal, 90
 minimal prime, 56
 minimally contains, 370
 minimum polynomial, 2
 module of quotients, 32
 monic, 1
 Morita context, 162
 Morita context, derived, 162
 Morita equivalence, 162
 morphism, 14
 multiplicative subset, 30

N

N -adic topology, 85
 Nakayama's Lemma, 81
 natural equivalence, 154
 natural transformation, 154
 nilpotent, 80
 noetherian, 13
 non-archimedean valuation, 51
 nondegenerate form, 46
 non- R primes, 294
 norm (counting), 59, 216
 norm (of element), 3
 norm (of ideal), 59, 150, 185, 210
 norm (reduced), 116, 119, 121
 norm (reduced, of ideal), 214
 normal basis theorem, 258
 normal ideal, 181, 193

normalized factor set, 243
 normalized valuation, 64, 139
 normalizer of an order, 328

O

opposite ring, 91, 101
 order, 108
 order ideal, 49
 order, left, 109
 order, maximal, 110
 order, right, 109
 orthogonal idempotents, 84, 85
 Outcent, 328
 outer automorphism group, 322

P

P-adic field, 68
P-adic topology, 83
 Picard group, 320
 Picent, 320
 preserves direct sums, 157
 primary component, 201
 primary ring, 177
 prime element, 53, 139
 prime ideal, 35, 190
 primitive idempotent, 85, 90
 principal factor set, 242
 product formula, 64
 progenerator, 158
 projective module, 15
 projective object, 155
 projective resolution, 20
 proper ideal, 35
 proper product, 183, 196
 pullback (diagram), 11
 pure, 45
 pushout (diagram), 10

Q

quaternion skewfield, 114, 244, 271

R

radical, 78

radically cover, 356
 ramification (at P), 272
 ramification index, 57, 71, 139
 ramified prime, 272
 rank, 44
 ray class group, 309
 ray group, 309
 real prime, 64
 reduced characteristic polynomial, 113, 119, 121
 reduced norm, 116, 119, 121
 reduced norm of ideal, 214
 reduced trace, 116, 119, 121
 reflexive, 55
 relative norm, 59
 relatively prime (ideals), 47, 217, 234
 residue class degree, 57, 71
 restriction map, 248
 right exact, 14
 right order, 109
 ring of quotients, 31

S

saturated, 35
 Schanuel's Lemma, 30
 Schilling's Theorem, 383
 Schur's Lemma, 105
 self-centralizing maximal subfield, 240
 semisimple (ring), 78, 90
 separable algebra, 99, 106
 short exact sequence, 8
 similar algebras, 237
 similar ideals, 199
 similar orders, 181
 simple components, 91
 simple (module), 78
 simple ring, 90
 skewfield, 82, 91
 skewfield over K , 92
 skewfield part, 237
 Skolem–Noether Theorem, 103
 Snake Lemma, 30
 split (sequence), 8
 splitting field, 96
 stable isomorphism, 307, 314
 Steinitz's Theorem, 49
 Strong Approximation Theorem, 48

T

tamely ramified, 373
totally definite quaternion algebra, 293
torsion element, 31, 32, 44
torsion submodule, 32, 44
torsionfree, 17, 44
trace, 3
trace form, 46
trace ideal, 156
trace (reduced), 116, 119, 121
trivial factor set, 242
trivial valuation, 51
trivial ZG -module, 256
twisted group ring, 373
type (of hereditary order), 360

U

unit, 79, 224

unital, 1
unramified, 57, 382

V

valuation, 51
valuation (exponential), 53
valuation (J -adic) 216
valuation ring, 51, 137
value group (of valuation), 51, 135
Very Strong Approximation Theorem,
64

W

Weak Approximation Theorem, 291
Wedderburn Structure Theorem, 91
Wedderburn Theorem on finite skew-
fields, 104