A Course in Ring Theory

Donald S. Passman

AMS Chelsea Publishing
American Mathematical Society
Providence, Rhode Island

A Course in Ring Theory

Donald S. Passman

AMS CHELSEA PUBLISHING
American Mathematical Society • Providence, Rhode Island

2000 *Mathematics Subject Classification.* Primary 16–01; Secondary 16–02, 19–02.

For additional information and updates on this book, visit
www.ams.org/bookpages/chel-348

Library of Congress Cataloging-in-Publication Data
Passman, Donald S., 1940–
A course in ring theory / Donald S. Passman.
p. cm.
Originally published: Pacific Grove, Calif. : Wadsworth & Brooks/Cole Advanced Books & Software, c1991.
Includes bibliographical references and index.
ISBN 0-8218-3680-3 (alk. paper)
1. Rings (Algebra) I. Title.

QA247.P28 2004
512′.4—dc22 2004054403

Copying and reprinting. Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy a chapter for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication is permitted only under license from the American Mathematical Society. Requests for such permission should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to `reprint-permission@ams.org`.

© 2004 by Donald S. Passman. All rights reserved.
Printed in the United States of America.

♾ The paper used in this book is acid-free and falls within the guidelines established to ensure permanence and durability.
Visit the AMS home page at `http://www.ams.org/`

10 9 8 7 6 5 4 3 2 1 09 08 07 06 05 04

Preface

These are the somewhat expanded notes from a course in ring theory that I have been giving for about ten years. The nature of the course has evolved over time; I am now relatively happy with the choices made.

In this book, we use the underlying theme of projective and injective modules to touch upon various aspects of commutative and noncommutative ring theory. In particular, we highlight and prove a number of rather major results.

In Part I, "Projective Modules," we begin with basic module theory and a brief study of free and projective modules. We then consider Wedderburn rings and, more general, Artinian rings. Next, come hereditary rings and, in particular, Dedekind domains. With this, we are ready for the key concepts of the projective dimension of a module and of the global dimension of a ring. Finally, we introduce the tensor product of modules and we determine all projective modules of local rings.

In Part II, "Polynomial Rings," we study these rings in a mildly noncommutative setting. We start with skew polynomial rings, determine their global dimension and then compute their Grothendieck and projective Grothendieck groups. In particular, we obtain the Hilbert Syzygy Theorem in the commutative case. Next, we offer an affirmative solution to the Serre Conjecture and, in fact, we determine all the projective modules of these polynomial rings. Finally, we use generic flatness to prove the Hilbert Nullstellensatz for almost commutative algebras.

In Part III, "Injective Modules," we start with injective analogs of projective results, but quickly move on to intrinsically injective properties. In particular, we study the maximal ring of quotients and use it to prove the existence of the classical ring of quotients. We then obtain the

Goldie Theorems, study uniform dimension, and characterize the injective modules of Noetherian rings. We close with basic properties of reduced rank and determine when Artinian quotient rings exist.

This book contains numerous exercises for the student and ends with a list of suggested additional reading.

In closing, I would like to express my thanks to a number of people. First, to my friends Larry Levy, Martin Lorenz, Jim Osterburg, and Lance Small for their input and helpful criticism. Second, to Mike Slattery, who attended the first course I gave on this subject and who offered me a copy of his class notes. I suspect he will be rather surprised at the direction in which this course evolved. Third, to Irving Kaplansky, who introduced noncomputational homological algebra. These notes are written in the spirit of his book "Fields and Rings." Finally, my love and appreciation to my family Marj, Barbara, and Jon for their enthusiastic support of this project. I couldn't have done it without them.

Donald S. Passman

Madison, Wisconsin
November, 1990

Contents

I. Projective Modules

1. Modules and Homomorphisms 3
2. Projective Modules 13
3. Completely Reducible Modules 23
4. Wedderburn Rings 33
5. Artinian Rings 44
6. Hereditary Rings 56
7. Dedekind Domains 64
8. Projective Dimension 74
9. Tensor Products 84
10. Local Rings 95

II. Polynomial Rings

11. Skew Polynomial Rings 105
12. Grothendieck Groups 115
13. Graded Rings and Modules 124
14. Induced Modules 133
15. Syzygy Theorem 142
16. Patching Theorem 152
17. Serre Conjecture 161
18. Big Projectives 171
19. Generic Flatness 180
20. Nullstellensatz 190

III. Injective Modules

21. Injective Modules 203
22. Injective Dimension 213
23. Essential Extensions 223
24. Maximal Ring of Quotients 233
25. Classical Ring of Quotients 242
26. Goldie Rings 252
27. Uniform Dimension 262
28. Uniform Injective Modules 273
29. Reduced Rank 284

Suggested Additional Reading 295

Index 297

A Course in Ring Theory

Part I
Projective Modules

1. Modules and Homomorphisms

In this book we will take a module theoretic stroll through various aspects of commutative and noncommutative ring theory. We assume that the reader has some familiarity with basic ring theoretic concepts such as ideals and homomorphisms. But we make no such assumption regarding modules. Indeed, in this chapter we begin with basic notions and some elementary observations. In particular, we define R-module and R-homomorphism and prove the three fundamental isomorphism theorems.

DEFINITION It will be necessary to use both right and left function notation. To be precise, let X, Y, and Z be sets and suppose $\alpha: X \to Y$ and $\beta: Y \to Z$ are maps. Then *right notation* means that the image of $x \in X$ under α is written as $x\alpha \in Y$ or, in other words, $\alpha: x \mapsto x\alpha$. We then denote the *function composition* first α then β by $\alpha\beta: X \to Z$ so that, by definition,

$$x(\alpha\beta) = (x\alpha)\beta \qquad \text{for all } x \in X$$

Of course, $\alpha\beta$ is the unique function that makes the diagram

$$\begin{array}{ccc} X & \xrightarrow{\alpha} & Y \\ & {\scriptstyle \alpha\beta}\searrow & \downarrow \beta \\ & & Z \end{array}$$

commute.

We note that a diagram of functions and their domains is said to *commute* if all paths from one domain to another yield the same answer. Thus for example

$$\begin{array}{ccc} X & \xrightarrow{\alpha} & Y \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\tau} \\ U & \xrightarrow{\delta} & V \end{array}$$

commutes if and only if $\alpha\tau = \sigma\delta$.

Similarly, *left notation* uses $\alpha: x \mapsto \alpha x$ or perhaps $\alpha: x \mapsto \alpha(x)$ for all $x \in X$. Here the composition first α then β is denoted by $\beta\alpha: X \to Z$ so that, by definition,

$$(\beta\alpha)x = \beta(\alpha x) \qquad \text{for all } x \in X$$

Again $\beta\alpha$ is the unique function that makes the diagram

$$\begin{array}{ccc} X & \xrightarrow{\alpha} & Y \\ & {\scriptstyle\beta\alpha}\searrow & \downarrow{\scriptstyle\beta} \\ & & Z \end{array}$$

commute.

In either case, composition is an associative operation. Thus, for example, if $\gamma: Z \to U$ and if we use right notation, then for all $x \in X$,

$$x\big((\alpha\beta)\gamma\big) = \big(x(\alpha\beta)\big)\gamma = \big((x\alpha)\beta\big)\gamma$$

and, similarly,

$$x\big(\alpha(\beta\gamma)\big) = (x\alpha)(\beta\gamma) = \big((x\alpha)\beta\big)\gamma$$

Thus $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ and both these functions can be described as first α then β then γ.

We will freely use both right and left function notation throughout this book. The particular choice will always be clear from context.

DEFINITION Now let V and W be additive abelian groups. A map $\alpha: V \to W$ is said to be a *homomorphism* if

$$(v_1 + v_2)\alpha = v_1\alpha + v_2\alpha \qquad \text{for all } v_1, v_2 \in V$$

The set of all such homomorphisms is denoted by $\mathrm{Hom}(V, W)$. If $\alpha, \beta \in \mathrm{Hom}(V, W)$, we define their sum $\alpha + \beta: V \to W$ by

$$v(\alpha + \beta) = v\alpha + v\beta \qquad \text{for all } v \in V$$

It follows easily that $\alpha+\beta \in \mathrm{Hom}(V, W)$ and that, in this way, $\mathrm{Hom}(V, W)$ becomes an additive abelian group. Indeed, the zero map is given by $v0 = 0$ for all $v \in V$ and the negative of α satisfies $v(-\alpha) = -(v\alpha)$.

When $W = V$, we call $\alpha: V \to V$ an *endomorphism* of V and write $\mathrm{End}(V) = \mathrm{Hom}(V, V)$. In this case, if $\alpha, \beta \in \mathrm{End}(V)$, then the composite $\alpha\beta: V \to V$ is easily seen to be an endomorphism. Thus $\alpha\beta \in \mathrm{End}(V)$ and, in this way, $\mathrm{End}(V)$ becomes a ring with 1. Here $v1 = v$ for all $v \in V$. Of course, there are also analogous structures determined by left function notation.

DEFINITION Let V be an additive abelian group and let R be a ring with 1. Then V is said to be a *right R-module* if and only if there exists a map $V \times R \to V$, written multiplicatively as $(v, r) \mapsto vr$, such that

i. $(v_1 + v_2)r = v_1r + v_2r$,
ii. $v(r_1 + r_2) = vr_1 + vr_2$,
iii. $v(r_1r_2) = (vr_1)r_2$, and
iv. $v1 = v$

for all $v, v_1, v_2 \in V$ and $r, r_1, r_2 \in R$. We will sometimes write $V = V_R$ to stress the right action of R. Note that if R is a field, then a right R-module is precisely a right R-vector space.

Similarly, V is a *left R-module* if and only if there exists a multiplicative map $R \times V \to V$ satisfying

i′. $r(v_1 + v_2) = rv_1 + rv_2$,
ii′. $(r_1 + r_2)v = r_1v + r_2v$,
iii′. $(r_1r_2)v = r_1(r_2v)$, and
iv′. $1v = v$

for all $v, v_1, v_2 \in V$ and $r, r_1, r_2 \in R$. In this case we write $V = {}_RV$ to indicate the left action of R. The meaning of these sets of axioms will become clear in Lemma 1.1, but first a few comments are in order.

In this book, all rings are assumed to have a 1. Indeed, if R and S are rings, then $R \subseteq S$ means that R is a subring of S with the same 1.

Furthermore, if $\theta: R \to S$ is a ring homomorphism, then we insist that $\theta(1) = 1$. R-modules satisfying (iv) or (iv′) are sometimes said to be *unital*. Here we assume throughout that all modules are unital.

LEMMA 1.1 *If V is a right R-module and $r \in R$, define $\theta(r): V \to V$ by $v\theta(r) = vr$. Then $\theta: R \to \mathrm{End}(V)$ is a ring homomorphism. Conversely, suppose V is an additive abelian group and that $\phi: R \to \mathrm{End}(V)$ is a ring homomorphism. If we define $vr = v\phi(r)$ for all $v \in V$ and $r \in R$, then V becomes an R-module.*

PROOF Assume that V is an R-module. Then (i) says that $\theta(r) \in \mathrm{End}(V)$, whereas (ii), (iii), and (iv) assert that $\theta: R \to \mathrm{End}(V)$ is a ring homomorphism.

Conversely, suppose V is an additive abelian group and that $\phi: R \to \mathrm{End}(V)$ is a ring homomorphism. Since $\phi(r) \in \mathrm{End}(V)$, (i) is satisfied and, since ϕ is a ring homomorphism, (ii), (iii), and (iv) follow. □

In other words, V is an R-module if and only if there is an appropriate ring homomorphism from R to $\mathrm{End}(V)$. This homomorphism is called the *representation* of R associated with V.

DEFINITION Now let V and W be right R-modules. A map $\alpha: V \to W$ is said to be an *R-homomorphism* if α is a homomorphism satisfying

$$\alpha(vr) = (\alpha v)r \qquad \text{for all } v \in V,\ r \in R$$

In other words, first applying r and then α is the same as first α and then r. Thus the latter formula is actually a commutativity condition that translates to an associative law once we write α on the left. The set of all such α is a subset of $\mathrm{Hom}(V, W)$ denoted by $\mathrm{Hom}_R(V, W)$. Indeed, it is easy to see that $\mathrm{Hom}_R(V, W)$ is a subgroup of $\mathrm{Hom}(V, W)$. In case R is a field, $\mathrm{Hom}_R(V, W)$ is clearly the set of R-linear transformations from V to W.

Next, $\alpha: V \to W$ is an *R-isomorphism* if it is an R-homomorphism which is one-to-one and onto. If such an isomorphism exists, we say that V and W are *R-isomorphic* and we write $V \cong W$ or $V_R \cong W_R$. Obviously $\cong$ is an equivalence relation and isomorphic modules are "essentially the same." When $V = W$, an R-homomorphism is said to be an *R-endomorphism* and an R-isomorphism is an *R-automorphism*. The set of all such R-endomorphisms of V is $\mathrm{End}_R(V)$ and this is a subring of $\mathrm{End}(V)$. Furthermore, V is clearly a left $\mathrm{End}_R(V)$-module.

There are, of course, analogous definitions for left R-modules, in which case we write the R-homomorphisms on the right. However, for

the most part we will restrict our attention to right modules and we will not bother to state the obvious left analogs. We now list some additional notation and a few simple observations.

First, if V is an R-module, then $W \subseteq V$ is an *R-submodule* if W is an R-module with the same addition and multiplication. It is clear that W is a submodule if and only if it is a nonempty subset of V closed under $+$ and under multiplication by R. Note that R itself is a right R-module called the *regular module* and the submodules of R_R are precisely the right ideals of R.

Next, if V and W are R-modules, then so is their *external direct sum* $V \oplus W$ once we define $(v \oplus w)r = vr \oplus wr$ for all $v \in V$, $w \in W$ and $r \in R$. In a similar manner, if $\{ V_i \mid i \in \mathcal{I} \}$ is a family of R-modules, then there is a natural R-module structure on the *external weak direct sum* $\oplus \sum_i V_i$. Specifically, the elements of $\oplus \sum_i V_i$ are all the infinite tuples $\oplus_i v_i$ with $v_i \in V_i$ and with only finitely many of the v_i not zero. Furthermore, addition and multiplication by $r \in R$ are defined in a componentwise fashion, so that $(\oplus_i v_i) + (\oplus_i v_i') = \oplus_i (v_i + v_i')$ and $(\oplus_i v_i)r = \oplus_i (v_i r)$. The modifier "weak" is used here to signify that almost all the components in each element $\oplus_i v_i$ are zero. Since our direct sums are almost always of this type, we will usually delete the modifier unless there is a need for emphasis. *Strong direct sums*, where the assumption on components being zero is dropped, will be considered in Chapter 21.

Now if W_1 and W_2 are submodules of V, then so are $W_1 \cap W_2$ and

$$W_1 + W_2 = \{ w_1 + w_2 \mid w_i \in W_i \}$$

Moreover if $W_1 \cap W_2 = 0$, then the map $\theta: W_1 \oplus W_2 \to W_1 + W_2$ given by $w_1 \oplus w_2 \mapsto w_1 + w_2$ is an R-isomorphism. Thus $W_1 + W_2$ is an *internal direct sum*, which we denote by $W_1 \dot{+} W_2$.

Finally, if $\theta: V \to V'$ is an R-homomorphism, then $\mathrm{Im}(\theta) = \theta V$, the *image* of θ, is an R-submodule of V'. Similarly, the *kernel* of θ, $\mathrm{Ker}(\theta) = \{ v \in V \mid \theta v = 0 \}$, is an R-submodule of V. Of course, θ is onto if and only if $\mathrm{Im}(\theta) = V'$ and θ is one-to-one if and only if $\mathrm{Ker}(\theta) = 0$. The following result shows that any submodule of V is the kernel of a homomorphism.

LEMMA 1.2 *Let W be an R-submodule of V. Then V/W has an R-module stucture such that the natural map $\nu: V \to V/W$ is an R-homomorphism onto with* $\mathrm{Ker}(\nu) = W$.

PROOF Since W is an additive subgroup of V, we know that V/W can be given the structure of an additive abelian group. Here, of course, V/W

consists of the distinct cosets $W+v$ with $v \in V$ and the addition in V/W is defined by $(W+v_1)+(W+v_2) = W+(v_1+v_2)$. Furthermore, the natural map $\nu: V \to V/W$ given by $\nu(v) = W+v$ is an epimorphism with kernel W.

Now observe that $(W+v)r = Wr + vr \subseteq W + vr$ for all $v \in V$ and $r \in R$. Thus $(W+v)r$ is contained in a unique coset, namely $W+vr$, and this allows us to define $(W+v)r = W+vr$ unambiguously in V/W. We then have $\nu(v)r = (W+v)r = W+vr = \nu(vr)$ and it follows, by applying ν to the module conditions of V, that V/W is also an R-module and that ν is an R-homomorphism onto with kernel W. □

Note that $V/0 \cong V$. The next result shows that if $\theta: V \to V'$ is an R-homomorphism and if $W \to 0$, then θ *factors through* V/W.

PROPOSITION 1.3 *Let $\theta: V \to V'$ be an R-homomorphism and suppose W is a submodule of V contained in the kernel of θ. Then there exists a unique R-homomorphism $\eta: V/W \to V'$ such that the diagram*

$$\begin{array}{ccc} V & \xrightarrow{\theta} & V' \\ {\scriptstyle \nu}\searrow & & \nearrow{\scriptstyle \eta} \\ & V/W & \end{array}$$

commutes. Thus $\theta = \eta\nu$.

PROOF Since $\theta(W) = 0$, we have $\theta(W+v) = \theta v \in V'$ for all $v \in V$. Thus in V/W, we can define $\eta(W+v) = \theta(W+v) = \theta v$ unambiguously and it follows easily that $\eta: V/W \to V'$ is an R-homomorphism. Furthermore, $\eta\nu(v) = \eta(W+v) = \theta v$, so $\eta\nu = \theta$. □

We can now describe all the homomorphic images of an R-module V and indeed all the homomorphisms emanating from that module.

THEOREM 1.4 (First Isomorphism Theorem) *Let $\theta: V \to V'$ be an R-homomorphism onto. If W is the kernel of θ, then there exists a unique R-isomorphism $\eta: V/W \to V'$ such that the diagram*

$$\begin{array}{ccc} V & \xrightarrow{\theta} & V' \\ {\scriptstyle \nu}\searrow & & \nearrow{\scriptstyle \eta} \\ & V/W & \end{array}$$

commutes. In particular, $V' \cong V/W$ *and* $\eta\nu = \theta$.

PROOF Since $W = \mathrm{Ker}(\theta)$, we have $\theta(W) = 0$ and the previous proposition implies that an appropriate map $\eta: V/W \to V'$ exists. We need only show that η is one-to-one and onto and the latter follows because $\theta = \nu\eta$ is onto. Finally, if $W + v \in \mathrm{Ker}(\eta)$, then $0 = \eta(W + v) = \theta v$, so $v \in \mathrm{Ker}(\theta) = W$. Thus $W + v = W + 0$ is the zero element of V/W, so $\mathrm{Ker}(\eta) = 0$ and η is one-to-one. □

We note that if $\theta: V \to V'$ is an R-homomorphism and if $W \subseteq V$, then $\theta: W \to V'$, the restriction of θ to W, is certainly also an R-homomorphism.

THEOREM 1.5 (Second Isomorphism Theorem) *Let* W *and* X *be* R*-submodules of* V. *Then*

$$(W + X)/W \cong X/(W \cap X)$$

PROOF We assume for convenience that $V = W + X$ and we let $\nu: V \to V/W$ be the natural map. Then $V/W = \nu(W + X) = \nu(X)$, so the restriction $\nu': X \to V/W$ is onto. Furthermore, the kernel of the latter map is the set of those elements of V that both map to 0 and belong to X. Thus $\mathrm{Ker}(\nu') = W \cap X$ and the First Isomorphism Theorem implies that

$$X/(W \cap X) \cong V/W = (W + X)/W$$

as required. □

THEOREM 1.6 (Third Isomorphism Theorem) *Let* $X \subseteq W$ *be* R*-submodules of* V. *Then*

$$\frac{V/X}{W/X} \cong V/W$$

PROOF The natural map $\nu: V \to V/W$ sends X to 0 and therefore, by Proposition 1.3, it can be factored through V/X. In other words, we have an R-epimorphism $\eta: V/X \to V/W$ given by $\eta: X + v \mapsto W + v$. Now clearly $X + v \in \mathrm{Ker}(\eta)$ if and only if $v \in W$ and hence if and only if $X + v \in W/X$. Thus $\mathrm{Ker}(\eta) = W/X$ and the First Isomorphism Theorem again yields the result. □

An R-module V is said to be *cyclic* if it has one generator, that is if $V = v_0R$ for some $v_0 \in V$. Similarly, V is *finitely generated* if it has finitely many generators, that is if $V = v_1R + v_2R + \cdots + v_nR$ for finitely many $v_i \in V$. It is clear that a homomorphic image of a cyclic or finitely generated module is again cyclic or finitely generated. Furthermore, we have:

LEMMA 1.7 *An R-module V is cyclic if and only if $V \cong R/I$ for some right ideal I of R.*

PROOF Clearly R/I is cyclic, being generated by the element $I + 1$. Conversely, if $V = v_0R$, then the map $\theta: R \to V$ given by $r \mapsto v_0r$ is easily seen to be an R-homomorphism onto. If $I = \mathrm{Ker}(\theta) = \{ r \in R \mid v_0r = 0 \}$, then I is a right ideal of R and Theorem 1.4 implies that $V \cong R/I$. □

We close this chapter with two basic properties of the lattice of submodules of an R-module.

LEMMA 1.8 *Let $\theta: V \to V'$ be an R-homomorphism onto and for any submodule W' of V' let*

$$\theta^{-1}(W') = \{ v \in V \mid \theta v \in W' \}$$

Then the maps $\theta: W \mapsto \theta(W)$ and $\theta^{-1}: W' \mapsto \theta^{-1}(W')$ yield a one-to-one inclusion preserving correspondence between those submodules W of V containing $\mathrm{Ker}(\theta)$ and all submodules W' of V'. In particular, these maps respect sums and intersections.

PROOF It is clear that $\theta^{-1}(W')$ is an R-submodule of V containing $\mathrm{Ker}(\theta)$. Moreover, since $\theta: V \to V'$ is onto, we have $\theta\big(\theta^{-1}(W')\big) = W'$.

Conversely if W is a submodule of V containing $\mathrm{Ker}(\theta)$, then $\theta(W)$ is certainly a submodule of V'. Moreover, if $v \in V$ with $\theta v \in \theta(W)$, then $\theta v = \theta w$ for some $w \in W$ and thus $v - w \in \mathrm{Ker}(\theta)$. But $\mathrm{Ker}(\theta) \subseteq W$, so we conclude that $v \in W$ and hence that $\theta^{-1}\big(\theta(W)\big) = W$.

It follows that the maps θ and θ^{-1} do indeed yield a one-to-one correspondence between the appropriate sets of submodules. □

LEMMA 1.9 (Modular Law) *Suppose A, B and C are submodules of V with $A \supseteq B$. Then:*

i. $A \cap (B + C) = B + (A \cap C)$.

ii. If $A + C = B + C$ *and* $A \cap C = B \cap C$, *then* $A = B$.

PROOF (i) It is clear that $A \cap (B + C) \supseteq B + (A \cap C)$. Conversely, let $x \in A \cap (B+C)$, so that $x = a = b+c$ for suitable $a \in A$, $b \in B$ and $c \in C$. Then $c = a-b \in A$, since $B \subseteq A$, so $c \in A \cap C$ and $x = b+c \in B+(A \cap C)$.

(ii) By assumption and (i) we have

$$\begin{aligned} A &= A \cap (A + C) = A \cap (B + C) \\ &= B + (A \cap C) = B + (B \cap C) = B \end{aligned}$$

so the result follows. □

EXERCISES

1. Suppose V is an additive abelian group and that there exists a multiplicative map $V \times R \to V$ satisfying conditions (i), (ii), and (iii) of the definition of an R-module. Prove that $V = V_0 \dot{+} V_1$, where V_0 and V_1 are the additive subgroups given by $V_0 = \{ v \in V \mid v1 = 0 \}$ and $V_1 = \{ v \in V \mid v1 = v \}$. Deduce that $V_0 R = 0$ and that V_1 is a (unital) R-module.
2. Let $\theta: G \to H$ be a homomorphism of groups. Prove that θ sends the identity of G to the identity of H and that it sends inverses to inverses.
3. If V is a right R-module, prove that $v0 = 0 = 0r$ for all $v \in V$ and $r \in R$. Furthermore, show that $(-v)r = -(vr) = v(-r)$.
4. Let W be a subset of V. Prove that W is a submodule if and only if it is nonempty, closed under $+$ and closed under multiplication by R. If X and Y are submodules of V, show that $X \cap Y$ and $X + Y$ are also submodules.
5. Let V and W be additive abelian groups. Verify that $\mathrm{Hom}(V, W)$ is an additive abelian group and that $\mathrm{End}(V)$ is a ring. If V and W are R-modules, verify that $\mathrm{Hom}_R(V, W)$ is a subgroup of $\mathrm{Hom}(V, W)$ and that $\mathrm{End}_R(V)$ is a subring of $\mathrm{End}(V)$.
6. If V and W are vector spaces over the field K, observe that they are K-modules and describe $\mathrm{Hom}_K(V, W)$ and $\mathrm{End}_K(V)$. Be more specific in case $\dim_K V = n < \infty$ and $\dim_K W = m < \infty$.
7. Show that the diagram

$$\begin{array}{ccccc} A & \xrightarrow{\sigma} & B & \xrightarrow{\tau} & C \\ \alpha \downarrow & & \downarrow \beta & & \downarrow \gamma \\ A' & \xrightarrow{\sigma'} & B' & \xrightarrow{\tau'} & C' \end{array}$$

commutes if and only if each of the smaller squares commutes. What is the obvious generalization of this fact?

8. Suppose

$$\begin{array}{ccc} A & \xrightarrow{\sigma} & B \\ \alpha\downarrow & & \downarrow\beta \\ A' & \xrightarrow{\sigma'} & B' \end{array}$$

is a commutative diagram of R-modules and of R-homomorphisms. Prove that $\alpha\colon \mathrm{Ker}(\sigma) \to \mathrm{Ker}(\sigma')$ and furthermore that β induces a map $\tilde{\beta}\colon B/\mathrm{Im}(\sigma) \to B'/\mathrm{Im}(\sigma')$. Here $B/\mathrm{Im}(\sigma)$ is called the *cokernel* of σ.

9. Let V be a nonzero finitely generated R-module.
maximal submodule W.
are no submodules contained properly between W and V. Show by example that this result is false for arbitrary nonzero V.

10. If the collection of subspaces of the K-vector space V satisfies either distributive law $A + (B \cap C) = (A + B) \cap (A + C)$ or $A \cap (B + C) = (A \cap B) + (A \cap C)$, show that $\dim_K V \leq 1$.

2. Projective Modules

As we will see, there are a number of important classes of R-modules with names such as free, projective, flat, injective, completely reducible, and simple. Our goal in this chapter is to introduce the first two. For this, we begin with some notation concerning sequences of homomorphisms.

DEFINITION Let R be a ring. Then the sequence

$$\cdots \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to \cdots$$

of R-modules and R-homomorphisms is said to be a *zero sequence*, or a *complex*, if the composition of adjacent homomorphisms is always the zero map. Thus, for example, the homomorphisms α and β that go into and out of B must satisfy $\beta\alpha = 0$ or, equivalently, $\mathrm{Ker}(\beta) \supseteq \mathrm{Im}(\alpha)$.

Now suppose that the preceding is a zero sequence. If $\mathrm{Ker}(\beta) = \mathrm{Im}(\alpha)$, then the sequence is said to be *exact at* B. Furthermore the sequence is *exact* if it is exact at all such interior modules B. In particular,

$$0 \to A \xrightarrow{\alpha} B$$

is exact if and only if α is one-to-one (an *R-monomorphism*) and

$$B \xrightarrow{\beta} C \to 0$$

is exact if and only if β is onto (an *R-epimorphism*). Thus

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

is a *short exact sequence* if and only if $C = \mathrm{Im}(\beta) \cong B/\mathrm{Ker}(\beta)$ and $\mathrm{Ker}(\beta) = \mathrm{Im}(\alpha) \cong A$. In other words, if W is an R-submodule of V, then the natural map $\nu: V \to V/W$ gives rise to the short exact sequence

$$0 \to W \to V \xrightarrow{\nu} V/W \to 0$$

Now suppose X and Y are R-modules and let $X \oplus Y$ be their external direct sum. Then we have maps

$$\begin{aligned} \pi_X &: X \oplus Y \to X \quad \text{given by} \quad x \oplus y \mapsto x \\ \pi_Y &: X \oplus Y \to Y \quad \text{given by} \quad x \oplus y \mapsto y \end{aligned}$$

which are R-epimorphisms and

$$\begin{aligned} \eta_X &: X \to X \oplus Y \quad \text{given by} \quad x \mapsto x \oplus 0 \\ \eta_Y &: Y \to X \oplus Y \quad \text{given by} \quad y \mapsto 0 \oplus y \end{aligned}$$

which are R-monomorphisms. Clearly $\pi_X \eta_X = 1_X$, the identity map on X, and

$$0 \to X \xrightarrow{\eta_X} X \oplus Y \xrightarrow{\pi_Y} Y \to 0$$

is exact.

Furthermore, the latter sequence has *back maps*, namely the maps π_X and η_Y in the following diagram.

$$0 \to X \underset{\pi_X}{\overset{\eta_X}{\rightleftarrows}} X \oplus Y \underset{\eta_Y}{\overset{\pi_Y}{\rightleftarrows}} Y \to 0$$

Here, of course, $\pi_X \eta_X = 1_X$ and $\pi_Y \eta_Y = 1_Y$. This motivates the following:

DEFINITION The short exact sequence

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

is said to be *split* if either

i. There exists $\gamma: C \to B$ with $\beta\gamma = 1_C$, or

ii. There exists $\delta: B \to A$ with $\delta\alpha = 1_A$.

The R-homomorphism γ or δ is called a *backmap* or a *splitting backmap*. As we will see in Lemma 2.2, conditions (i) and (ii) are, in fact, equivalent.

LEMMA 2.1 *Let X and Y be R-modules.*

i. If there exist R-homomorphisms σ and τ with

$$X \underset{\tau}{\overset{\sigma}{\rightleftarrows}} Y \qquad \text{and} \qquad \sigma\tau = 1_Y$$

then $X = \mathrm{Ker}(\sigma) \dotplus \mathrm{Im}(\tau)$ and $\mathrm{Im}(\tau) \cong Y$. Thus $Y \mid X$; that is, Y is isomorphic to a direct summand of X.

ii. Conversely, if Y is isomorphic to a direct summand of X, then σ and τ exist as before with $\sigma\tau = 1_Y$.

PROOF (i) Let $x' \in \mathrm{Ker}(\sigma) \cap \mathrm{Im}(\tau)$. Then $x' = \tau y'$ for some $y' \in Y$ and $0 = \sigma x' = \sigma\tau y' = y'$. It follows that $x' = \tau 0 = 0$, so $\mathrm{Ker}(\sigma) \cap \mathrm{Im}(\tau) = 0$. Now let $x \in X$ be arbitrary and observe that $x = (x - \tau\sigma x) + \tau\sigma x$. Of course, $\tau\sigma x \in \mathrm{Im}(\tau)$ and we have

$$\sigma(x - \tau\sigma x) = \sigma x - (\sigma\tau)\sigma x = \sigma x - \sigma x = 0$$

so $x - \tau\sigma x \in \mathrm{Ker}(\sigma)$. Thus $x \in \mathrm{Ker}(\sigma) + \mathrm{Im}(\tau)$ and $X = \mathrm{Ker}(\sigma) \dotplus \mathrm{Im}(\tau)$. Finally, since $\sigma\tau = 1_Y$, we see that τ is one-to-one, so $Y \cong \mathrm{Im}(\tau)$ as required.

(ii) Conversely, suppose $X = V \dotplus W$ with $V \cong Y$. If $\alpha: V \to Y$ is the given isomorphism, define $\sigma: X \to Y$ by $\sigma = \alpha\pi_V$ and $\tau: Y \to X$ by $\tau = \eta_V\alpha^{-1}$. Then $\sigma\tau = \alpha(\pi_V\eta_V)\alpha^{-1} = \alpha\alpha^{-1} = 1_Y$ as required. □

As a consequence we have:

LEMMA 2.2 *If*

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

is a split short exact sequence, then $B \cong A \oplus C$. In particular, β has a backmap if and only if α does.

PROOF There are two cases to consider. Suppose first that $\gamma: C \to B$ exists with $\beta\gamma = 1_C$. By the previous lemma, $B = \mathrm{Ker}(\beta) \dotplus \mathrm{Im}(\gamma)$ and $\mathrm{Im}(\gamma) \cong C$. Thus, since $\mathrm{Ker}(\beta) = \mathrm{Im}(\alpha) \cong A$, we conclude that $B \cong A \oplus C$. Furthermore, we obtain a backmap for α by first projecting B into $\mathrm{Im}(\alpha)$ and then following with α_0^{-1}, where α_0 is the isomorphism $\alpha: A \to \mathrm{Im}(\alpha)$.

On the other hand, suppose $\delta: B \to A$ exists with $\delta\alpha = 1_A$. Again the previous lemma yields $\mathrm{Im}(\alpha) \cong A$ and $B = \mathrm{Im}(\alpha) \dotplus \mathrm{Ker}(\delta)$. Furthermore,

$$\mathrm{Ker}(\delta) \cong B/\mathrm{Im}(\alpha) = B/\mathrm{Ker}(\beta) \cong C$$

and therefore $B = \mathrm{Im}(\alpha) \dotplus \mathrm{Ker}(\delta) \cong A \oplus C$. Indeed, the restricted map β_0 given by $\beta: \mathrm{Ker}(\delta) \to C$ is an isomorphism and therefore β_0^{-1} is a backmap for β. □

We now come to the first key:

DEFINITION An R-module F is said to be *free* if it has a *free basis* $\{ f_i \mid i \in \mathcal{I} \}$. By this we mean that every element of F is uniquely writable as a finite sum $\sum_i f_i r_i$ with $r_i \in R$. A familiar example here is, of course, a vector space over a field; vector spaces always have free bases. The following two lemmas are essentially obvious. The first is the module analog of the fact that a vector space of dimension n is isomorphic to the set of n-tuples over the field. The second asserts that homomorphisms from free modules exist and are determined by the images of the basis.

LEMMA 2.3 *Let F be an R-module.*

i. F is free if and only if it is isomorphic to $\oplus \sum_i R_R$, a weak direct sum of copies of the regular module R_R.

ii. If F is free and finitely generated, then every free basis for F is finite.

iii. If F is free and not finitely generated, then all free bases for F have the same infinite size.

PROOF (i) If F has the free basis $\{ f_i \mid i \in \mathcal{I} \}$, then it is easy to see that the map $\oplus \sum_{i \in \mathcal{I}} R_R \to F$ given by $\oplus_i r_i \mapsto \sum_i f_i r_i$ is an R-isomorphism. Conversely, if $F' = \oplus \sum_{j \in \mathcal{J}} R_R$, then F' has the free basis $\{ f'_j \mid j \in \mathcal{J} \}$, with f'_j having a 1 in the jth component and zeros elsewhere.

(ii) Suppose $\{ f_i \mid i \in \mathcal{I} \}$ is a free basis for F and let F be generated by $v_1, v_2, \ldots, v_n$. Since each v_j can be written in terms of finitely many basis elements, we see that all v_j involve only finitely many of the f_i. It follows that the latter collection of f_i's generates F and hence must be the entire basis.

(iii) First, (ii) implies that all bases for F are infinite. Now let $\mathcal{A}$ and $\mathcal{B}$ be two such bases. As before, each $b \in \mathcal{B}$ can be written as an R-linear combination of finitely many members of $\mathcal{A}$. Thus all elements of $\mathcal{B}$ can be written in terms of the members of a subset $\mathcal{A}'$ of $\mathcal{A}$ with $|\mathcal{A}'| \leq \aleph_0 |\mathcal{B}|$. Since $\mathcal{B}$ generates F, it follows that $\mathcal{A}'$ also generates F and then uniqueness of expression implies that $\mathcal{A}' = \mathcal{A}$. We conclude that $|\mathcal{A}| \leq \aleph_0 |\mathcal{B}| = |\mathcal{B}|$, since $\mathcal{B}$ is infinite. By symmetry, $|\mathcal{B}| \leq |\mathcal{A}|$ and the result follows. □

It is clear from (i) that R has free modules with basis of arbitrary

size and that a weak direct sum of free R-modules is again free.

LEMMA 2.4 *Let R be a ring.*

i. Let F have free basis $\{ f_i \mid i \in \mathcal{I} \}$ and let V be an R-module. If $v_i \in V$ are chosen arbitrarily, then there exists a unique R-homomorphism $\theta: F \to V$ with $f_i \mapsto v_i$.

ii. Every module is a homomorphic image of a free module.

iii. Every finitely generated module is a homomorphic image of a finitely generated free module.

PROOF (i) By uniqueness of expression, the map $\theta: F \to V$ given by $\sum_i f_i r_i \mapsto \sum_i v_i r_i$ is well defined and sends each f_i to v_i. Note that the sums here are finite. It is now easy to see that θ is an R-homomorphism.

(ii), (iii) If $\{ v_i \mid i \in \mathcal{I} \}$ is a generating set for V, possibly all of V, choose a free R-module F with basis $\{ f_i \mid i \in \mathcal{I} \}$. The map $\theta: F \to V$ defined by $f_i \mapsto v_i$ is then an R-epimorphism. Of course, if V is finitely generated, then we can take the index set $\mathcal{I}$ to be finite. □

If F is a free R-module with basis $\{ f_i \mid i \in \mathcal{I} \}$, then the *rank* of F, $\operatorname{rank} F$, is defined to be the size of the index set $\mathcal{I}$. It follows from Lemma 2.3(iii) that the rank of F is well defined if it is infinite. On the other hand, unlike the ordinary vector space situation, finite ranks need not be uniquely determined by F. We will briefly consider some aspects of this shortly. As we will see, the problem translates precisely to the question of whether there exist nonsquare invertible matrices over R. To be precise, we say that an $n \times m$ matrix A is *invertible over R* if there exists an $m \times n$ matrix B with entries in R such that $AB = I_n$, the $n \times n$ identity matrix, and $BA = I_m$. If R is a field, then all invertible matrices must be square, but for general rings anomalies do exist. The following is a familiar property of the change of basis matrix.

LEMMA 2.5 *Let F be a free R-module with basis $\{ f_1, f_2, \ldots, f_n \}$ and let $g_1, g_2, \ldots, g_m$ be elements of F. If $a_{i,j} \in R$ with $g_j = \sum_i f_i a_{i,j}$ for all $1 \le j \le m$, then $\{ g_1, g_2, \ldots, g_m \}$ is a free basis for F if and only if the $n \times m$ matrix $A = (a_{i,j})$ is invertible over R.*

PROOF For convenience, we let $\mathcal{F}$ denote the $1 \times n$ row matrix given by $(f_1 \quad f_2 \quad \ldots \quad f_n)$ and similarly we set $\mathcal{G} = (g_1 \quad g_2 \quad \ldots \quad g_m)$. Then, by definition of A, we have $\mathcal{G} = \mathcal{F}A$.

Suppose first that $\{ g_1, g_2, \ldots, g_m \}$ is also a free basis. Then we can write $\mathcal{F} = \mathcal{G}B$ for a unique $m \times n$ matrix B with entries in R. It follows that $\mathcal{F} = \mathcal{G}B = \mathcal{F}(AB)$, so uniqueness of expression yields $AB = I_n$. Similarly, $\mathcal{G} = \mathcal{F}A = \mathcal{G}(BA)$, so $BA = I_m$.

Conversely suppose A is invertible with inverse B. Then we have $\mathcal{G}B = \mathcal{F}(AB) = \mathcal{F}$, since $AB = I_n$, and it follows that $\{ g_1, g_2, \ldots, g_m \}$ is at least a generating set for F. Finally, let $\mathcal{R}$ be any $m \times 1$ column matrix of elements of R with $\mathcal{G}\mathcal{R} = 0$. Then $0 = \mathcal{G}\mathcal{R} = \mathcal{F}(A\mathcal{R})$, so freeness implies that $A\mathcal{R} = 0$. But then $\mathcal{R} = (BA)\mathcal{R} = B0 = 0$ and we conclude that $\{ g_1, g_2, \ldots, g_m \}$ is indeed a free basis. □

DEFINITION The ring R is said to have *invariant basis number*, or *IBN*, if all finitely generated free R-modules have unique rank. In view of the preceding lemma, this occurs if and only if invertible matrices over R are necessarily square. This characterization allows us to easily prove:

LEMMA 2.6 *Let R and S be rings and suppose that S has IBN. If either*

i. There is a homomorphism from R to S, or

ii. R is a subring of S, or

iii. R is commutative,

then R has IBN.

PROOF (i) There is an obvious extension of $\theta\colon R \to S$ to a map from the matrices of R to those of S. Furthermore, this map clearly preserves addition and multiplication when defined and, since $\theta(1) = 1$, it follows that $\theta(I_n) = I_n$. Now suppose that A is an $n \times m$ invertible matrix over R with inverse B. Then by the preceding observations, it is clear that $\theta(A)$ is an invertible matrix over S with inverse $\theta(B)$. But S has IBN, so we conclude that $n = m$ and hence R has IBN.

(ii) This follows immediately from (i), since the identity map is a suitable homomorphism from R to S.

(iii) Since R is commutative, if M is a maximal ideal of R, then R/M is a field. But we know that any field has IBN, so the result again follows from (i). □

Additional facts of this nature as well as some examples of interest are contained in the exercises. We now come to the second key:

DEFINITION An R-module P is *projective* if whenever

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow \alpha & & \\ V & \xrightarrow{\beta} & W & \to & 0 \end{array}$$

is given with the bottom row exact, then there exists an R-homomorphism $\gamma: P \to V$ that makes the diagram commute. That is, given any R-epimorphism $\beta: V \to W$ and any R-homomorphism $\alpha: P \to W$, there exists $\gamma: P \to V$ with $\beta\gamma = \alpha$. As we will see, there is a close relationship between projective and free R-modules.

LEMMA 2.7 *Let P be an R-module and suppose that either*

i. P is free, or

ii. P is isomorphic to a direct summand of a projective module.

Then P is projective.

PROOF Suppose we are given

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow \alpha & & \\ V & \xrightarrow{\beta} & W & \to & 0 \end{array}$$

(i) Let $\{ f_i \mid i \in \mathcal{I} \}$ be a free basis for P. Since $\alpha f_i \in W$ and β is an epimorphism, there exists $v_i \in V$ with $\beta v_i = \alpha f_i$. Now define $\gamma: P \to V$ by $\gamma: f_i \mapsto v_i$.

(ii) Here we suppose that P is isomorphic to a direct summand of the projective module Q. Then by Lemma 2.1(ii) we have

$$P \underset{\tau}{\overset{\sigma}{\rightleftarrows}} Q \qquad \text{with} \qquad \tau\sigma = 1_P$$

Since Q is projective and $\alpha\tau: Q \to W$, it follows that there exists $\gamma: Q \to V$ with $\beta\gamma = \alpha\tau$. But then $\beta(\gamma\sigma) = \alpha(\tau\sigma) = \alpha$, so $\gamma\sigma: P \to V$ is the required map. □

We can now quickly characterize projective modules.

THEOREM 2.8 *Let P be an R-module. The following are equivalent.*

i. P is a projective R-module.

ii. Every short exact sequence $0 \to A \to B \to P \to 0$ splits.

iii. P is isomorphic to a direct summand of a free R-module.

PROOF (i) ⇒(ii) The short exact sequence gives rise to the diagram

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow 1_P & & \\ B & \xrightarrow{\beta} & P & \to & 0 \end{array}$$

where β is the given epimorphism. Hence, since P is projective, there exists a map $\gamma: P \to B$ with $\beta\gamma = 1_P$ and, by definition, the sequence splits.

(ii) $\Rightarrow$(iii) If we choose a free module F that maps onto P, then we obtain a short exact sequence $0 \to A \to F \to P \to 0$. By (ii), this sequence splits and hence, by Lemma 2.2, P is isomorphic to a direct summand of F.

(iii) $\Rightarrow$(i) This follows from both parts of the preceding lemma. □

Notice that the module A in (ii) above is irrelevant. Thus P is projective if and only if for every R-epimorphism $\beta: B \to P$, there exists a back map $\gamma: P \to B$ with $\beta\gamma = 1_P$. We close this chapter with a few simple observations.

LEMMA 2.9 *Let R be a ring.*

i. Every R-

module.

ii. Every finitely generated R-module is a homomorphic image of a finitely generated projective R-module.

iii. A weak direct sum of projective R-

PROOF Parts (i) and (ii) follow from Lemma 2.4(ii)(iii) since any free module is projective. Part (iii) follows from the preceding theorem, since a weak direct sum of free R-modules is free. □

EXERCISES

1. It is important to observe that certain properties are *isomorphism invariants*. Prove that a module isomorphic to a free module is free and that a module isomorphic to a projective module is projective.
2. Let

$$\begin{array}{ccccc} A & \to & B & \to & C \\ \alpha\downarrow & & \downarrow\beta & & \downarrow\gamma \\ A' & \to & B' & \to & C' \end{array}$$

be a commutative diagram of modules and homomorphisms with α, β and γ isomorphisms.
the second row is.
3. Suppose the commutative diagram

$$\begin{array}{ccccccccc} A & \to & B & \to & C & \to & D & \to & E \\ \alpha\downarrow & & \beta\downarrow & & \downarrow\gamma & & \downarrow\delta & & \downarrow\epsilon \\ A' & \to & B' & \to & C' & \to & D' & \to & E' \end{array}$$

has exact rows. If α, β, δ and ϵ are isomorphisms, prove that γ is also. This is known as the *Five Lemma.*

4. Prove that R has IBN if either (i) all finitely generated subrings of R have IBN or (ii) R has a subring S with IBN such that R_S is a finitely generated free S-module. In particular, the latter applies when $R = \mathrm{M}_n(S)$.
5. Let R be a ring and let $\mathcal{A}$ be an additive abelian group. An additive homomorphism $\tau\colon R \to \mathcal{A}$ is said to be a *trace map* if $\tau(rs) = \tau(sr)$ for all $r, s \in R$. Show that τ extends naturally to a map from the set of square matrices of R to $\mathcal{A}$ and that this extended map satisfies $\tau(AB) = \tau(BA)$ for all $n \times m$ matrices A and $m \times n$ matrices B. If $\tau(n \cdot 1) \neq 0$ for all integers $n > 0$, prove that R has IBN.
6. Suppose R is the ring of linear transformations on an infinite dimensional K-vector space with basis $\{v_0, v_1, v_2, \ldots\}$. Show that $R_R \cong R_R \oplus R_R$ using shift maps on the basis to construct an appropriate 2×1 invertible R-matrix.
7. Let K be a field and let X be a set of variables. Then the *free K-algebra* $K\langle X\rangle$ is defined just like the polynomial ring $K[X]$ except that the variables do not commute. In particular, $K\langle X\rangle$ has a K-basis consisting of all formally distinct words in the variables and it follows easily that this ring has no zero divisors. Prove that $R = K\langle X\rangle$ has IBN by constructing a homomorphism from R to K. Then show that $|X| \geq 2$ implies that the regular module R_R contains a free submodule of infinite rank.
8. Give a proof, directly from the definition, that a weak direct sum of projective modules is projective. The result is false for strong direct sums, as we will see in Exercise 10. Where does the proof fail?

In the remaining two problems, let $\mathbb{Z}$ be the ring of integers and note that $\mathbb{Z}$-modules are precisely the same as additive abelian groups. If V is such a module, we say that $v \in V$ is *infinitely divisible* if the equation $xn = v$ has solutions $x \in V$ for infinitely many integers n.

9. If F is a free $\mathbb{Z}$-module, show that F has no nonzero infinitely divisible members. In particular, if $\mathbb{Q}$ is the field of rationals, show that $\mathbb{Q}_{\mathbb{Z}} \not\subseteq F$ and deduce that $\mathbb{Q}_{\mathbb{Z}}$ is not projective.

10. Now let $V = \prod_{i=1}^{\infty} \mathbb{Z}_{\mathbb{Z}}$ be the strong direct sum of countably many copies of the regular $\mathbb{Z}$-module and suppose by way of contradiction that V is contained in a free $\mathbb{Z}$-module F with basis $\mathcal{B}$.

i. If W is the submodule of V consisting of all sequences that are eventually 0, observe that $W \cong \oplus \sum_{i=1}^{\infty} \mathbb{Z}_{\mathbb{Z}}$ and hence is countable. Deduce that there is a countable subset $\mathcal{B}'$ of $\mathcal{B}$ such that $W \subseteq F'$, where F' is the free submodule of F generated by $\mathcal{B}'$.

ii. Now note that $F'' = F/F'$ is a free $\mathbb{Z}$-module that contains an isomorphic copy of $V/(V \cap F')$. Furthermore, for each infinite sequence $\epsilon = \{\epsilon_1, \epsilon_2, \dots\}$ of $\pm$ signs, let $v_\epsilon \in V$ be given by $v_\epsilon = \prod_{i=1}^{\infty} \epsilon_i i!$. Show that $v_\epsilon + (V \cap F')$ is an infinitely divisible element of $V/(V \cap F')$ and that some v_ϵ is not contained in $V \cap F'$, since the latter submodule is countable.

iii. Obtain a contradiction from the preceding exercise and deduce that V cannot be contained in F. Conclude that a strong direct sum of projective $\mathbb{Z}$-modules need not be projective.

3. Completely Reducible Modules

If K is a field, then K-modules are vector spaces and hence have bases. Thus all K-modules are free and, in particular, projective. In this chapter we find other rings with this same property and, indeed, we characterize all such rings. To start with, we briefly consider completely reducible modules.

DEFINITION Let R be a ring and let V be an R-module. Then V is said to be *irreducible*, or *simple*, if it is nonzero and has no proper nonzero submodules. More generally, V is *completely reducible* if each of its submodules is a direct summand. This means that if $W \subseteq V$, then there exists $U \subseteq V$ with $V = W \dotplus U$. Obviously, any simple R-module is completely reducible, but the converse is certainly not true.

LEMMA 3.1 *Submodules and homomorphic images of a completely reducible module are completely reducible.*

PROOF Let W be a submodule of the completely reducible module V and let $X \subseteq W$. Then $X \dotplus U = V$ for some $U \subseteq V$ and, since $X \subseteq W$, the Modular Law yields

$$W = W \cap V = W \cap (X \dotplus U) = X + (W \cap U)$$

Furthermore, the latter sum is direct since $W \cap U \subseteq U$. It follows that X is a direct summand of W and hence that W is completely reducible.

Finally we note that $V = W \dotplus Y$, so $V/W \cong Y$. Since Y is completely reducible by the preceding, we conclude that V/W is also. □

Now suppose $\{ V_i \mid i \in \mathcal{I} \}$ is a family of R-submodules of V and let W be the submodule of V that they generate. Then W clearly consists of

all finite sums $\sum_i v_i$ with $v_i \in V_i$ and we write $W = \sum_i V_i$. Furthermore, if $\sum_i V_i$ is naturally isomorphic to $\oplus \sum_i V_i$, then we write $W = \cdot \sum_i V_i$ and we say that W is the *internal direct sum* of the V_i. Of course, the latter occurs if and only if $\sum_i v_i = 0$ with $v_i \in V_i$ implies that all $v_i = 0$.

LEMMA 3.2 *Let V be an R-module and let $\{ V_i \mid i \in \mathcal{I} \}$ be a family of irreducible submodules of V that generate it. If W is a submodule of V, then there exists a subset $\mathcal{J} \subseteq \mathcal{I}$ such that*

$$W \dot{+} \left(\cdot \sum_{j \in \mathcal{J}} V_j \right) = V$$

PROOF Let $\mathbf{S}$ be the set of all subsets $\mathcal{K}$ of $\mathcal{I}$ such that $W \dot{+} (\cdot \sum_{k \in \mathcal{K}} V_k)$ is an internal direct sum. We note that $\mathbf{S}$ is nonempty, since $\emptyset \in \mathbf{S}$. Furthermore, the property of being a direct sum is finitary, so Zorn's Lemma implies that there exists a maximal element $\mathcal{J} \in \mathbf{S}$. By definition, we know that $W' = W \dot{+} (\cdot \sum_{j \in \mathcal{J}} V_j)$ is a direct sum.

Suppose by way of contradiction that $W' \neq V$. Then since V is generated by all V_i, it follows that there exists some V_k with $V_k \not\subseteq W'$. But V_k is irreducible, so this implies that $W' \cap V_k = 0$ and hence that $W' + V_k$ is a direct sum. In particular, if we set $\mathcal{J}' = \mathcal{J} \cup \{ k \}$, then $W \dot{+} (\cdot \sum_{j \in \mathcal{J}'} V_j)$ is also direct and hence $\mathcal{J}' \in \mathbf{S}$. This, of course, contradicts the maximality of $\mathcal{J}$ and thus $W' = V$ as required. □

It is now a simple matter to characterize completely reducible modules.

THEOREM 3.3 *For an R-module V, the following are equivalent.*

i. V is a sum of irreducible submodules.

ii. V is a direct sum of irreducible submodules.

iii. V is completely reducible.

PROOF The implication (i)⇒(ii) follows from the preceding lemma with $W = 0$ and (ii)⇒(iii) follows from the general case of that result. Thus we need only prove that (iii)⇒(i). To this end, let V be completely reducible and let S be the sum of all simple submodules of V. The goal is to show that $S = V$. If this is not the case, fix $v \in V \setminus S$.

By Zorn's Lemma we can choose a submodule M of V maximal with the properties $S \subseteq M$ and $v \notin M$. Now V is completely reducible and clearly $M \neq V$, so $V = M \dot{+} U$ for some nonzero submodule $U \subseteq V$. Furthermore, since $S \subseteq M$, we know that U is not irreducible. In particular, we can let $A \neq 0$ be a proper submodule of U and then, since

U is completely reducible by Lemma 3.1, we have $U = A \dotplus B$ for some $B \neq 0$. It follows that $V = M \dotplus A \dotplus B$ and, by the maximality of M, we see that $v \in M \dotplus A$ and $v \in M \dotplus B$. But then $v \in (M \dotplus A) \cap (M \dotplus B) = M$, a contradiction. Thus $S = V$ and the theorem is proved. □

DEFINITION Let V be an R-module. Then a finite chain

$$0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V$$

of submodules is called a *series* for V. The *factors* of this series are the quotients V_{i+1}/V_i for $i = 0, 1, \ldots, n-1$ and the *length* of this series is n, the number of factors. Two such series are said to be *equivalent* if they have the same length and isomorphic factors in some order.

The series $0 = W_0 \subseteq W_1 \subseteq \cdots \subseteq W_m = V$ is said to be a *refinement* of the preceding if each V_i is some $W_{i'}$.
obtained by adding more submodules to the series.

LEMMA 3.4 (Schreier-Zassenhaus Lemma) *Any two series for the R-module V have equivalent refinements.*

PROOF Suppose we are given the two series

$$0 = X_0 \subseteq X_1 \subseteq \cdots \subseteq X_n = V$$
$$0 = Y_0 \subseteq Y_1 \subseteq \cdots \subseteq Y_m = V$$

We can then refine the X-series by defining the submodules

$$X_{i,}$$

for all $i = 0, 1, \ldots, n-1$ and $j = 0, 1, \ldots, m-1$. Of course this formula also makes sense if $i = n$ or $j = m$. Notice that for fixed i we have

$$X_i = X_{i,0} \subseteq X_{i,1} \subseteq \cdots \subseteq X_{i,m-1} \subseteq X_{i,m} = X_{i+1}$$

It therefore follows that the $X_{i,}$
V on top, is indeed a refinement of the X-series.

Since $X_{i+1,0} = X_{i,m}$,
$X_{i,j+1}/X_{i,j}$ for $i = 0, 1, \ldots, n-1$ and $j = 0, 1, \ldots, m-1$. Furthermore, by the Second Isomorphism Theorem and the Modular Law, we have

$$\frac{X_{i,}}{X_{i,j}} - \frac{}{X_{i,j}} - \frac{}{X_{i,j}}$$
$$\cong \frac{X_{i+1} \cap Y_{j+1}}{(X_{i+1} \cap Y_{j+1}) \cap (X_i + (X_{i+1} \cap Y_j))}$$
$$= \frac{X_{i+1} \cap Y_{j+1}}{(X_i \cap Y_{j+1}) + (X_{i+1} \cap Y_j)}$$

since $X_{i+1} \cap Y_{j+1} \supseteq X_{i+1} \cap Y_j$ and $X_i \cap (X_{i+1} \cap Y_{j+1}) = X_i \cap Y_{j+1}$. But note that the final expression for $X_{i,j+1}/X_{i,j}$ is symmetric in X_i and Y_j. Thus if we define $Y_{i,j}$ similarly by

$$Y_{i,j} = Y_j + (Y_{j+1} \cap X_i)$$

then $X_{i,j+1}/X_{i,j} \cong Y_{i+1,j}/Y_{i,j}$ and therefore the two refinements are equivalent. □

A *composition series* for V is a series

$$0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V$$

such that each factor V_{i+1}/V_i is irreducible. Needless to say, not every module has such a series. As an immediate consequence of the preceding lemma we have:

THEOREM 3.5 (Jordan-Hölder Theorem) *Any two composition series for an R-module V are equivalent, that is they have the same length and isomorphic factors. Furthermore, if V has a composition series, then any series for V with nonzero factors can be refined to a composition series.*

PROOF Let $0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V$ be a composition series for V. Since V_{i+1}/V_i is simple, it follows from the Third Isomorphism Theorem that there are no R-submodules of V contained properly between V_i and V_{i+1}. Thus any refinement of the given composition series merely adds additional copies of the various V_i and therefore has the same nonzero factors as the original. With this observation, the Schreier-Zassenhaus Lemma clearly yields the result. □

If V has a composition series, then the common length of all such series is called the *composition length* of V and is denoted by $\operatorname{len} V$. Similarly, the factors from any such series are called the *composition factors* of V. To be precise, if

$$0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V$$

is any composition series for V, then $\operatorname{len} V = n$ and the composition factors of V are $V_1/V_0, V_2/V_1, \ldots, V_n/V_{n-1}$ counting multiplicities.

LEMMA 3.6 *Let V be an R-module.*

i. Suppose $W \subseteq V$. Then V has a composition series if and only if both W and V/W have composition series. Furthermore, when this

occurs, then $\operatorname{len} V = \operatorname{len} W + \operatorname{len} V/W$ *and the set of composition factors of* V *is the union of those of* W *and of* V/W.

ii. Suppose $V = \cdot$

ducible submodules W_i. *Then* V *has a composition series of length* n *with composition factors* W_1

PROOF (i) We may clearly assume that $W \neq 0, V$.

V has a composition series. Then it follows from the preceding theorem that the series $0 \subseteq W \subseteq V$ can be refined to a composition series, say $0 = V_0 \subseteq V_1$

V_k

$$\frac{V_{i+1}/W}{V_i/W} \cong \frac{V_{i+1}}{V_i}$$

and hence

$$0 = \frac{V_k}{W} \subseteq \frac{V_{k+1}}{W} \subseteq \cdots \subseteq \frac{V_n}{W} = \frac{V}{W}$$

is a composition series for the module V/W.

Conversely, suppose $0 = W_0 \subseteq W_1$

series for W and that $0 = V_0'$

If $\nu: V \to V/W$ denotes the natural map, let

$$V_i = \nu^{-1}$$

be the complete inverse image of V_i'.

submodule of V containing W and $V_i' = \nu(V_i) = V_i/W$. Since

$$\frac{V_{i+1}}{V_i} \cong \frac{V_{i+1}/W}{V_i/W} = \frac{V_{i+1}'}{V_i'}$$

we conclude that

$$0 = W_0 \subseteq W_1 \subseteq \cdots \subseteq W_k = W = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_m = V$$

is a composition series for V.

(ii) Now assume that $V = \cdot \sum_{i=1}^{n}$

let $V_j = \cdot$

$$0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V$$

is a composition series for V. Here $n = \operatorname{len} V$ and the composition factors are precisely $W_1, W_2, \ldots, W_n$. □

DEFINITION Let V be an R-module. Then V satisfies the *minimum condition*, or *min*, if every nonempty collection of submodules of V has a minimal member. By this we mean that if $\mathcal{F}$ is a nonempty family of submodules, then there exists $W \in \mathcal{F}$ such that W contains no other members of $\mathcal{F}$.

In addition, we say that V satisfies the *descending chain condition*, or *d.c.c.*, if every descending chain $V_1 \supseteq V_2 \supseteq \cdots$ of submodules eventually stabilizes. In view of the Jordan-Hölder Theorem, any module with a composition series necessarily satisfies d.c.c.

It is easy to see that these two properties are in fact equivalent. To start with, suppose V satisfies min and let $V_1 \supseteq V_2 \supseteq \cdots$ be a descending chain of submodules. Then the collection $\{ V_1, V_2, \ldots \}$ contains a minimal member, say V_n, and the series stabilizes at n.

Conversely, suppose V satisfies d.c.c. and let $\mathcal{F}$ be a nonempty collection of submodules of V. Choose $V_1 \in \mathcal{F}$. If V_1 is not minimal, then there exists $V_2 \in \mathcal{F}$ with $V_1 \supset V_2$. If V_2 is not minimal, then we can find $V_3 \in \mathcal{F}$ with $V_2 \supset V_3$. Continuing in this manner, we either find a minimal member of $\mathcal{F}$ or we construct an infinite descending chain $V_1 \supset V_2 \supset \cdots$ which does not stabilize.

Modules satisfying min, or equivalently d.c.c., are called *Artinian*.

DEFINITION A ring R is said to be *right Artinian* if the regular module R_R satisfies d.c.c. In addition, R is a *right Wedderburn ring* if it is right Artinian and has no nonzero nilpotent right ideal. Here, of course, a subset X of a ring R is *nilpotent* if $0 = X^n = X \cdot X \cdots X$ for some $n \geq 1$. With either of the preceding ring theoretic properties, we usually delete the modifier "right" unless the side is in doubt; there are of course analogous definitions on the left.

In any ring R, a nonzero right ideal I is said to be *minimal* if I contains no other nonzero right ideal. In particular, I is minimal if and only if I_R is a simple right R-module. If R is Artinian, then the minimum condition guarantees that any nonzero right ideal of R contains a minimal one.

LEMMA 3.7 *Let V be an R-module.*

i. Suppose $W \subseteq V$. Then V is Artinian if and only if both W and V/W are Artinian.

ii. Suppose $\{ W_i \mid i \in \mathcal{I} \}$ is a family of irreducible submodules of V and that $V = \cdot \sum_i W_i$. Then V is Artinian if and only if the index set $\mathcal{I}$ is finite.

iii. Let V be a finitely generated R-module. If R is Artinian, then so is V. Furthermore, if R_R has a composition series, then so does V.

PROOF (i) Suppose first that V is Artinian. Since any descending chain of submodules of W is also a chain of submodules of V, it follows that W inherits d.c.c. from V. Now let $\nu: V \to V/W$ be the natural R-epimorphism and let $V_1' \supseteq V_2' \supseteq \cdots$ be a descending chain of submodules of V/W. If $V_i = \nu^{-1}(V_i')$, then $\nu(V_i) = V_i'$ and V_1
scending chain in V. But the latter chain must stabilize and hence, using $\nu(V_i) = V_i'$, we conclude that the original one does also.

Conversely, suppose W and V/W satisfy d.c.c. and let $V_1 \supseteq V_2$ be a descending chain of submodules of V. Then

$$(V_1 \cap W) \supseteq (V_2$$

is a descending chain of submodules of W and hence this chain must stabilize, say at p. Furthermore,

$$\frac{V_1 + W}{W} \supseteq \frac{V_2 + W}{W} \supseteq \cdots \supseteq \frac{V_i + W}{W} \supseteq \cdots$$

is a descending chain of submodules of V/W and hence this chain must also stabilize, say at q. In particular, if $t \geq p, q$, then $V_{t+1} \cap W = V_t \cap W$ and $V_{t+1} + W = V_t + W$. Thus since $V_t \supseteq V_{t+1}$, the Modular Law implies that $V_t = V_{t+1}$ and we conclude that the original series does indeed stabilize.

(ii) If $\mathcal{I}$ is finite, then V is Artinian by Lemma 3.6(ii). On the other hand, if $\mathcal{I}$ is infinite, then we can construct an infinite strictly descending chain of submodules of V by deleting one summand at a time from the direct sum $V = \cdot \sum_i W_i$.

(iii) Suppose first that R_R is Artinian. Then, by (i) and Lemma 1.7, every cyclic R-module is Artinian. We now proceed by induction on the number of generators. If $V = v_1R + v_2$
can assume that the submodule $W = v_1R + v_2$
But V/W is clearly generated by $W + v_n$ and is therefore cyclic. Thus (i) now yields the result. Finally, if R_R has a composition series, then the same argument, along with Lemma 3.6(i), completes the proof. □

We need one more simple observation.

LEMMA 3.8 *Let I be a right ideal of the ring R.*

i. $I = eR$ for some idempotent $e \in R$ if and only if I is a direct summand of R_R. Furthermore, when this happens, we have $I = eI$.

ii. If I is a minimal right ideal, then either $I^2 = 0$ or $I = eR$ for some idempotent e.

PROOF (i) If $I = eR$, then $R = eR \dot{+} (1-e)R = I \dot{+} (1-e)R$. Conversely, let $R = I \dot{+} J$ and write $1 = e + f$ with $e \in I$ and $f \in J$. If $i \in I$, then

$$i = (e + f)i = ei + fi \in I \dot{+} J$$

and uniqueness of expression yields $ei = i$. It follows that $e^2 = e$, so e is an idempotent, and that $eI = I$. But $eR \subseteq I = eI$ and therefore $I = eR = eI$.

(ii) Assume that $I^2 \neq 0$ and choose $a \in I$ with $aI \neq 0$. Then aI is a right ideal of R and $aI \subseteq I$, so $aI = I$ by the minimality of I. In particular there exists $e \in I$ with $ae = a$. Now let $J = \{ i \in I \mid ai = 0 \}$. Then J is a right ideal of R, $J \subseteq I$, and $J \neq I$. Thus, by the minimality of I again, we have $J = 0$. But $a(e^2 - e) = 0$ and $e^2 - e \in I$, so it follows that $e^2 - e = 0$. In other words, e is an idempotent contained in I and $ae = a \neq 0$ so $e \neq 0$. Thus $0 \neq eR \subseteq I$ and we conclude that $I = eR$. □

With this, we can now prove:

THEOREM 3.9 *If R is a ring, then the following are equivalent.*

i. Every R-module is projective.
ii. Every R-module is completely reducible.
iii. R_R is completely reducible.
iv. R is a Wedderburn ring.

PROOF We first show that (i), (ii), and (iii) are equivalent and then that (iii) is equivalent to (iv).

(i)⇒(ii) If $W \subseteq V$ are R-modules, then V/W is projective by assumption. Thus the short exact sequence $0 \to W \to V \to V/W \to 0$ splits and W is a direct summand of V.

(ii)⇒(iii) This is obvious.

(iii)⇒(i) Since R_R is completely reducible, it is a sum of irreducible submodules. It follows that any free R-module is also a sum of irreducibles and hence is completely reducible. Finally, if V is any R-module, then V is a homomorphic image of some free module F and, since F is completely reducible, this epimorphism must split. Thus V is isomorphic to a direct summand of F and it is therefore projective.

(iii)⇒(iv) Since R_R is completely reducible, we see that $R_R = \cdot \sum_j I_j$ where each I_j is an irreducible R-module and hence a minimal right ideal of R. Say $1 \in I_1 \dot{+} I_2 \dot{+} \cdots \dot{+} I_n$. Then $R = 1R \subseteq I_1 \dot{+} I_2 \dot{+} \cdots \dot{+} I_n$ and equality must occur. Thus R_R satisfies d.c.c. by Lemma 3.7(ii) and R is

an Artinian ring. Furthermore, if I is any right ideal of R, then $R = I \dot{+} J$ by complete reducibility and hence $I = eR$ for some idempotent $e \in I$ by the preceding lemma. In particular, if I is also nilpotent, then clearly $e = 0$ and $I = 0$. Thus R is a Wedderburn ring.

(iv)⇒(iii) Since R is Wedderburn, it follows from Lemma 3.8(ii) that every minimal right ideal of R is generated by an idempotent. Now we show that every right ideal of R is a sum of minimal right ideals. If this is not the case, then since R_R satisfies the minimum condition, there exists a minimal counterexample L. Clearly, $L \neq 0$, so L contains a minimal right ideal $I = eR$. Since $I \dot{+} I' = R$ and $I \subseteq L$, the Modular Law implies that $L = I \dot{+} (I' \cap L)$. In particular, L is properly larger than $I' \cap L$, so the minimal nature of L implies that $I' \cap L$ is a sum of minimal right ideals of R. But then $L = I \dot{+} (I' \cap L)$ is also such a sum, a contradiction. In particular, we conclude that R is a sum of minimal right ideals and hence a sum of irreducible submodules. It follows from Theorem 3.3 that R_R is indeed completely reducible. □

As we will see in Exercise 7, right Artinian rings need not be left Artinian. On the other hand, right Wedderburn rings are necessarily also left Wedderburn.

EXERCISES

1. Let $\{V_i \mid i \in \mathcal{I}\}$ be a family of submodules of V. Show that there exists a natural epimorphism $\theta: \oplus \sum_i V_i \to \sum_i V_i$ and describe $\mathrm{Ker}(\theta)$.
2. Suppose $V_1, V_2, \ldots, V_n$ are finitely many R-submodules of V with $\bigcap_1^n V_i = 0$.
   also. To this end, first observe that V embeds in $\oplus \sum_1^n V/V_i$. Now show by example that the result fails if n is allowed to be infinite. Conclude therefore that a strong direct sum of completely reducible modules is not necessarily completely reducible.
3. Let $I_1, I_2, \ldots, I_n$ be a finite collection of two-sided ideals of R such that $I_i + I_j = R$ for all $i \neq j$.
   prove that there exists $r \in R$ with $r \equiv a_i \bmod I_i$ for all i. Deduce that $R/(\bigcap_1^n I_i) \cong \oplus \sum_1^n R/I_i$. This is the Chinese Remainder Theorem.
4. Let p be a fixed prime number and let A be the multiplicative group of complex p^nth roots of unity for all $n \geq 0$. If we view A additively as a module over the integers, show that A satisfies min but that it does not have a composition series.
5. Let $0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V$ be a series for the R-module V and let $W \subseteq V$. Show that W has a series of length n whose

factors are isomorphic to submodules of the factors of the V-series. Similarly, prove that V/W has a series of length n whose factors are homomorphic images of the factors of the V-series.

6. Let $R \supseteq S$ be rings and assume that R_S is a finitely generated S-module. If S is Artinian, prove that R is also. In particular, if $R = \mathrm{M}_n(S)$ deduce that S is Artinian if and only if R is Artinian.
7. Suppose $K \subseteq F$ are fields with $\dim_K F = \infty$ and let R be the subring

   of $\mathrm{M}_2(F)$

   minimal right ideal of R and then construct a composition series for R_R. Deduce that R is right Artinian and then prove that R is not left Artinian.
8. Show that there is a one-to-one correspondence between idempotents $e \in \mathrm{End}_R(V)$ and direct sum decompositions $V = X \dot{+} Y$.
9. Let I be a two-sided ideal of R. Prove that $I = eR$ for some central idempotent $e \in R$ if and only if $R = I \dot{+} J$ for some two-sided ideal J. When this occurs, show that e and J are uniquely determined by I.
10. Prove that all R-modules are free if and only if R is a division ring. This is quite simple and does not require Theorem 3.9.

4. Wedderburn Rings

The goal now is to obtain a more precise description of Wedderburn rings. We do this by computing the endomorphism ring of certain module direct sums. Since we are dealing with right R-modules, we will of course write all R-homomorphisms on the left. The following lemma is, for the most part, fairly obvious.

LEMMA 4.1 *Let V and W be R-modules.*

i. $\mathrm{Hom}_R(V,W)$ *is a right* $\mathrm{End}_R(V)$*-module and a left* $\mathrm{End}_R(W)$*-module with multiplication given by function composition.*

ii. If $V = \cdot\sum_{i=1}^{n} V_i$ *is a finite direct sum, then* $\mathrm{Hom}_R(V,W)$ *is isomorphic to* $\oplus\sum_{i=1}^{n}\mathrm{Hom}_R(V_i,W)$ *as a left* $\mathrm{End}_R(W)$*-module.*

iii. If $W = \cdot\sum_{j=1}^{m} W_j$ *is a finite direct sum, then* $\mathrm{Hom}_R(V,W)$ *is isomorphic to* $\oplus\sum_{j=1}^{m}\mathrm{Hom}_R(V,W_j)$ *as a right* $\mathrm{End}_R(V)$*-module.*

iv. Let $W = \cdot\sum_j W_j$ *be an arbitrary weak direct sum such that for each j, every nonzero element of* $\mathrm{Hom}_R(V,W_j)$ *is a monomorphism. Then* $\mathrm{Hom}_R(V,W)$ *is* $\mathrm{End}_R(V)$*-isomorphic to* $\oplus\sum_j \mathrm{Hom}_R(V,W_j)$.

PROOF (i) If $\alpha\colon V \to W$ and $\beta\colon V \to V$ are R-homomorphisms, then so is the composite map $\alpha\beta\colon V \to W$. Thus we have a map

$$\mathrm{Hom}_R(V,W) \times \mathrm{End}_R(V) \to \mathrm{Hom}_R(V,W)$$

given by $\alpha \times \beta \mapsto \alpha\beta$ that clearly makes $\mathrm{Hom}_R(V,W)$ into a right $\mathrm{End}_R(V)$-module. The result for W is similar.

(ii) Each element $\alpha \in \mathrm{Hom}_R(V,W)$ determines R-homomorphisms $\alpha_i\colon V_i \to W$ for $i = 1,2,\ldots,n$ by restriction. Furthermore, the map $\alpha \mapsto \alpha_1 \oplus \alpha_2 \oplus \cdots \oplus \alpha_n$ is then easily seen to be an $\mathrm{End}_R(W)$-module isomorphism from $\mathrm{Hom}_R(V,W)$ to $\oplus\sum_i \mathrm{Hom}_R(V_i,W)$.

(iii) Each element $\beta \in \mathrm{Hom}_R(V, W)$ determines R-homomorphisms $\beta_j: V \to W \to W_j$ for $j = 1, 2, \ldots, m$ via composition. It is then easy to see that the map $\beta \mapsto \beta_1 \oplus \beta_2 \oplus \cdots \oplus \beta_m$ is an $\mathrm{End}_R(V)$-module isomorphism from $\mathrm{Hom}_R(V, W)$ to $\oplus \sum_j \mathrm{Hom}_R(V, W_j)$.

(iv) Here the result follows as in (iii), provided that each such β has at most finitely many nonzero β_j. But observe that if $\beta_j \neq 0$, then, by assumption, β_j is a monomorphism. Hence if v is any nonzero element of V, then $\beta_j(v) \neq 0$ and $\beta(v)$ has a nonzero W_j-component. But $\beta(v)$ can have only finitely many nonzero components, so this condition is clearly satisfied. □

The proof of the next lemma is more formal. Parts (i) and (ii) are actually special cases of a more general result that describes $\mathrm{End}_R(V)$ as a suitable *checkered matrix ring* (see Exercise 2).

LEMMA 4.2 *Let $V = V_1 \dotplus V_2 \dotplus \cdots \dotplus V_n$ be a finite direct sum of R-submodules.*

i. If $\mathrm{Hom}_R(V_i, V_j) = 0$ for all $i \neq j$, then $\mathrm{End}_R(V)$ is isomorphic to the ring direct sum $\oplus \sum_{i=1}^n \mathrm{End}_R(V_i)$.

ii. If all V_i are isomorphic to a fixed R-module W, then $\mathrm{End}_R(V)$ is isomorphic to the matrix ring $\mathrm{M}_n(\mathrm{End}_R(W))$.

PROOF For each $i = 1, 2, \ldots, n$, let $\pi_i: V \to V_i$ and $\eta_i: V_i \to V$ be the obvious projection and injection maps. Then $\pi_i \eta_i = 1_i$, the identity on V_i, $\pi_i \eta_j = 0$ for $i \neq j$, and $\sum_{k=1}^n \eta_k \pi_k = 1$, the identity on V. In particular, if $\alpha \in \mathrm{End}_R(V)$, then

$$\alpha = 1\alpha 1 = \sum_{i,j} \eta_i \pi_i \alpha \eta_j \pi_j = \sum_{i,j} \eta_i \alpha_{i,j} \pi_j$$

where $\alpha_{i,j} = \pi_i \alpha \eta_j \in \mathrm{Hom}_R(V_j, V_i)$. We note that if $\beta \in \mathrm{End}_R(V)$, then $(\alpha + \beta)_{i,j} = \alpha_{i,j} + \beta_{i,j}$ and

$$(\alpha\beta)_{i,j} = \pi_i \alpha 1 \beta \eta_j = \sum_{k=1}^n (\pi_i \alpha \eta_k)(\pi_k \beta \eta_j) = \sum_{k=1}^n \alpha_{i,k} \beta_{k,j}$$

(i) By assumption, $\alpha_{i,j} = 0$ for all $i \neq j$. Thus, by the latter formula, the map $\alpha \mapsto \alpha_{i,i}$ is a ring homomorphism and hence so is the map

$$\theta: \mathrm{End}_R(V) \to \oplus \sum_{i=1}^n \mathrm{End}_R(V_i)$$

given by $\alpha \mapsto \alpha_{1,1} \oplus \alpha_{2,2} \oplus \cdots \oplus \alpha_{n,n}$. Note that $1_{i,i} = \pi_i \eta_i = 1_i$. Since $\alpha = \sum_k \eta_k \alpha_{k,k} \pi_k$, it follows that $\mathrm{Ker}(\theta) = 0$ and θ is one-to-one. Finally,

let $\gamma_k \in \mathrm{End}_R(V_k)$
Then

$$\gamma_{i,i} = \pi_i \gamma \eta_i = \sum_{k=1}^{n} \pi_i \eta_k \gamma_k \pi_k \eta_i = \gamma_i$$

and θ is onto.

(ii) Choose isomorphisms $\sigma_i \colon V_i \to W$ and for each $\alpha \in \mathrm{End}_R(V)$, let $\phi(\alpha)_{i,j} = \sigma_i \alpha_{i,j} \sigma_j^{-1} \in \mathrm{End}_R(W)$.
and

$$\begin{aligned}\phi(\alpha\beta)_{i,j} &= \sigma_i \Big(\sum_{k=1}^{n} \alpha_{i,k} \beta_{k,j} \Big) \sigma_j^{-1} \\ &= \sum_{k=1}^{n} \sigma_i \alpha_{i,k} \sigma_k^{-1} \cdot \sigma_k \beta_{k,j} \sigma_j^{-1} = \sum_{k=1}^{n} \phi(\alpha)_{i,k} \phi(\beta)_{k,j}\end{aligned}$$

It follows that the map $\phi \colon \mathrm{End}_R(V) \to \mathrm{M}_n(\mathrm{End}_R(W))$ given explicitly by $\alpha \mapsto (\phi(\alpha)_{i,j})$ is a ring homomorphism. Furthermore, this map is one-to-one, since if $\phi(\alpha) = 0$, then $\alpha_{i,j} = 0$ for all i, j and hence $\alpha = \sum_{i,j} \eta_i \alpha_{i,j} \pi_j = 0$. Finally, let $(\tau_{i,j}) \in \mathrm{M}_n(\mathrm{End}_R(W))$ and set

$$\gamma = \sum_{a,b} \eta_a \sigma_a^{-1} \tau_{a,b} \sigma_b \pi_b \in \mathrm{End}_R(V)$$

Then $\gamma_{i,j} = \pi_i \gamma \eta_j = \sigma_i^{-1} \tau_{i,j} \sigma_j$ and thus $\phi(\gamma)_{i,j} = \sigma_i \gamma_{i,j} \sigma_j^{-1} = \tau_{i,j}$. In other words, $\phi(\gamma) = (\tau_{i,j})$ and we conclude that ϕ is onto. □

In the next two lemmas we consider some concrete computations.

LEMMA 4.3 *Let e and f be idempotents in R.*

i. If V is an R-module, then $\mathrm{Hom}_R(eR, V) \cong Ve$. In particular, $\mathrm{Hom}_R(eR, fR) \cong fRe$.

ii. If $e \neq 0$, then $\mathrm{End}_R(eR)$ is ring isomorphic to eRe acting by left multiplication.

iii. If F is a free R-module of rank n, then $\mathrm{End}_R(F) \cong \mathrm{M}_n(R)$.

PROOF (i) For each $v \in Ve$, let $\theta(v) \in \mathrm{Hom}_R(eR, V)$ be given by $r \mapsto vr$. Then $\theta \colon Ve \to \mathrm{Hom}_R(eR, V)$ is clearly an additive group homomorphism and we show that θ is an isomorphism. Suppose first that $\theta(v) = 0$. Then $0 = \theta(v)e = ve = v$, since $v \in Ve$, and hence θ is one-to-one.
hand, if $\alpha \in \mathrm{Hom}_R(eR, V)$, set $w = \alpha(e)$. Then $w = \alpha(e \cdot e) = \alpha(e)e = we$,

so $w = we \in Ve$. But for any $r \in R$, we have $\alpha(er) = \alpha(e)r = (we)r = w(er)$, so $\alpha = \theta(w)$ and θ is onto.

(ii) Here we need only observe that if $V = eR$, then θ preserves multiplication. For this, let $s, t \in eRe$ and let $r \in eR$. Then $\theta(s)\theta(t)r = \theta(s)tr = str = \theta(st)r$ and this fact is proved.

(iii) It follows from statement (ii), with $e = 1$, that $\mathrm{End}_R(R) \cong R$. Thus, since F is isomorphic to a direct sum of n copies of R, Lemma 4.2(ii) yields the result. □

LEMMA 4.4 (Schur's Lemma) *Let V and W be irreducible R-modules. Then any nonzero element of $\mathrm{Hom}_R(V, W)$ is an isomorphism. In particular, $\mathrm{End}_R(V)$ is a division ring and if $V \ncong W$, then $\mathrm{Hom}_R(V, W) = 0$.*

PROOF Let θ be a nonzero element of $\mathrm{Hom}_R(V, W)$. Then $0 \neq \theta V = \mathrm{Im}(\theta)$ is a submodule of W, so $\mathrm{Im}(\theta) = W$ and θ is onto. Similarly, $\mathrm{Ker}(\theta) \neq V$ is a submodule of V, so $\mathrm{Ker}(\theta) = 0$ and θ is one-to-one. Thus θ is an R-isomorphism and, since θ^{-1}
the result follows. □

DEFINITION Let V be a nonzero R-module. We say that R is *transitive* on V if for all v_1,
easy to see that this occurs if and only if V is simple. Indeed, suppose V is irreducible. Then v_1
and R is transitive. Conversely, suppose R is transitive and let W be a nonzero submodule of V. If $0 \neq v_1 \in W$, then $v_1 R \subseteq W \subseteq V$. But transitivity implies that $v_1 R = V$ and hence $W = V$ as required.

We now come to a fundamental result. Recall that R is defined to be a Wedderburn ring if it is right Artinian and has no nonzero nilpotent right ideal.

THEOREM 4.5 (Artin-Wedderburn Theorem) *R is a Wedderburn ring if and only if $R = \cdot \sum_{k=1}^{m}$*
over division rings. Furthermore, when this occurs, then

i. R has precisely m simple modules $V_1, V_2, \ldots, V_m$, up to isomorphism, and each is a direct summand of R_R.

ii. n_k is the multiplicity of V_k

iii. D_k

Thus the parameters m, n_k, and D_k

PROOF Suppose first that R is a Wedderburn ring. Then by Theorem 3.9, R_R is completely reducible and, by Lemma 3.7(ii), R_R is in fact a finite direct sum of irreducible modules. Let W_1
sentatives of the isomorphism classes of the simple summands of R_R that

occur in this particular direct sum decomposition. Then by suitably permuting all such summands, we can assume that $R_R = U_1 \dot{+} U_2 \dot{+} \cdots \dot{+} U_m$, where each U_k is a direct sum $U_k = W_{k,1} \dot{+} W_{k,2} \dot{+} \cdots \dot{+} W_{k,n_k}$ with all $W_{k,j} \cong W_k$.

Now for $i \neq j$ we have $W_i \ncong W_j$ and hence $\mathrm{Hom}_R(W_i, W_j) = 0$ by Schur's Lemma. It follows that $\mathrm{Hom}_R(U_i, U_j) = 0$ by Lemma 4.1(ii)(iii), so $\mathrm{End}_R(R)$ is ring isomorphic to $\oplus \sum_{k=1}^m \mathrm{End}_R(U_k)$ by Lemma 4.2(i). In addition, the second part of that lemma implies that $\mathrm{End}_R(U_k)$ is isomorphic to the matrix ring $\mathrm{M}_{n_k}(\mathrm{End}_R(W_k))$; observe that $\mathrm{End}_R(W_k)$ is a division ring by Schur's Lemma. Thus, since $\mathrm{End}_R(R) \cong R$, by Lemma 4.3(iii), we conclude that R does indeed have the appropriate structure.

Conversely, assume that $R = \cdot \sum_{k=1}^m \mathrm{M}_{n_k}(D_k)$ is a direct sum of full matrix rings over the division rings D_k. We will show that R is a Wedderburn ring and that (i), (ii), and (iii) are satisfied. To start with, let $\{ e_{i,j}^k \mid i, j \}$ denote the set of matrix units in $\mathrm{M}_{n_k}(D_k)$. Since $W_{k,i} = e_{i,i}^k R = e_{i,i}^k \mathrm{M}_{n_k}(D_k)$ is the ith row of this kth matrix ring, it follows that

$$R = \cdot \sum_{k,i} e_{i,i}^k R = \cdot \sum_{k,i} W_{k,i}$$

is a direct sum of right ideals. Next we claim that each such $W_{k,i}$ is in fact minimal and hence an irreducible R-module. Indeed, let $w = \sum_j e_{i,j}^k d_j$ be a nonzero element of $W_{k,i}$ with all $d_j \in D_k$. If $d_p \neq 0$, then $w \cdot d_p^{-1} e_{p,i}^k = e_{i,i}^k$ and hence $wR = e_{i,i}^k R = W_{k,i}$. In other words, R is transitive on $W_{k,i}$ and we conclude that R_R is the direct sum of the irreducible submodules $W_{k,i}$. Thus R_R is completely reducible and R is a Wedderburn ring by Theorem 3.9.

Now observe that $\mathrm{Hom}_R(W_{k,i}, W_{k',j}) \cong e_{j,j}^{k'} R e_{i,i}^k$ by Lemma 4.3(i) and that the latter expression is clearly zero if $k' \neq k$ and nonzero otherwise. It therefore follows from Schur's Lemma that, for any fixed k, all $W_{k,i}$ are isomorphic to $V_k = W_{k,1}$ and that $V_k \ncong V_{k'}$ when $k \neq k'$. In particular, by Lemma 3.6(ii), n_k is precisely the multiplicity of V_k as a composition factor of R_R. Furthermore, we have

$$\begin{aligned} \mathrm{End}_R(V_k) &= \mathrm{End}_R(e_{1,1}^k R) \cong e_{1,1}^k R e_{1,1}^k \\ &= e_{1,1}^k \mathrm{M}_{n_k}(D_k) e_{1,1}^k = e_{1,1}^k D_k \end{aligned}$$

and the latter ring is clearly isomorphic to D_k. Finally, if V is any irreducible R-module, then, since $\mathrm{Hom}_R(R, V) \neq 0$ by Lemma 4.3(i), it

follows that $\mathrm{Hom}_R(W_{k,i}, V) \neq 0$ for some k, i. Thus $V_k \cong W_{k,i} \cong V$, by Schur's Lemma, and the theorem is proved. □

Since the above matrix characterization of Wedderburn rings is certainly right-left symmetric, we conclude that any right Wedderburn ring is necessarily also left Wedderburn.

For any ring R, we use $I \lhd R$ to indicate that I is a two-sided ideal of R. In particular, R is said to be a *simple ring* if $I \lhd R$ implies that $I = 0$ or $I = R$.

COROLLARY 4.6 *R is a simple Artinian ring if and only if $R = \mathrm{M}_n(D)$ is a full matrix ring over a division ring D.*

PROOF Suppose first that $R = \mathrm{M}_n(D)$. Then by the above we know that R is a Wedderburn ring and, in particular, it is Artinian. Now let I be a nonzero ideal of R and let $r = \sum_{i,j} d_{i,j} e_{i,j}$ be a nonzero element of I. Here, of course, $\{ e_{i,j} \mid i, j \}$ is the set of matrix units of $\mathrm{M}_n(D)$ and each $d_{i,j} \in D$. If $d_{p,q} \neq 0$, then for all subscripts i, j we have $e_{i,j} = e_{i,p} d_{p,q}^{-1} r e_{q,j} \in I$ and hence $I = R$. We conclude that R is simple.

Conversely suppose that R is a simple Artinian ring and let J be a nilpotent right ideal of R with, say, $J^t = 0$. Then $I = RJ \lhd R$ and, using $JR = J$, we have $I^t = 0$.
conclude that $I = 0$ and $J = 0$.
and hence $R = \cdot \sum_{k=1}^{m} \mathrm{M}_{n_k}(D_k)$ by the preceding theorem. But each of these m matrix rings is an ideal of R and thus we must have $m = 1$. □

As we have seen, Lemma 4.2(ii) is a key ingredient in the proof of the Artin-Wedderburn Theorem and hence also of the preceding result. Specifically, the lemma asserts that if $V = \cdot \sum_{i=1}^{n} W_i$ and if $W_i \cong W$ for all i, then $\mathrm{End}_R(V) \cong \mathrm{M}_n(\mathrm{End}_R(W))$. But there is another way to explain the matrix structure of R and this argument applies to more general rings.

DEFINITION If V is an R-module, we say that V is *faithful* if for all $r \in R$, $Vr = 0$ implies that $r = 0$. Equivalently, this means that the natural ring homomorphism $R \to \mathrm{End}(V)$ is one-to-one and therefore that R is essentially a subring of $\mathrm{End}(V)$ acting on the right.

A ring R is said to be *primitive* if it has a faithful irreducible module. For example, suppose R is a simple ring and let M be a maximal right ideal of R. Then $V = R/M$ is an irreducible R-module, by Lemma 1.8, and obviously R must act faithfully on V. Thus any simple ring is necessarily primitive.

Now let R act faithfully on the irreducible module V and set $D = \mathrm{End}_R(V)$. Then D is a division ring, by Schur's Lemma, and as we have observed, V is a left $\mathrm{End}_R(V)$-module. Thus V is a left D-vector space. Furthermore, if $d \in D$, $v \in V$ and $r \in R$, then the associativity condition $d(vr) = (dv)r$ implies that r is a D-endomorphism of V or, equivalently, a D-linear transformation. In other words, we see that $R \subseteq \mathrm{End}_D(V)$. Of course, if $\dim_D V = n < \infty$, then $\mathrm{End}_D(V) \cong \mathrm{M}_n(D)$ and therefore R is at least embedded isomorphically in the matrix ring $\mathrm{M}_n(D)$. More generally, $\mathrm{End}_D(V)$ can be described as the ring of row finite matrices over D and the goal is to show that R is a "large" subset of this endomorphism ring.

DEFINITION Let D be a division ring and let V be a left D-vector space. We say that $R \subseteq \mathrm{End}_D(V)$ is a *dense ring of linear transformations* if for every finite D-linearly independent subset $\{ v_1, v_2, \ldots, v_n \}$ of V and every subset $\{ w_1, w_2, \ldots, w_n \} \subseteq V$, there exists $r \in R$ with $v_i r = w_i$ for all $i = 1, 2, \ldots, n$.

Thus, for example, if $\dim_D V = n < \infty$ and if R is dense, then certainly $R = \mathrm{End}_D(V) \cong \mathrm{M}_n(D)$. On the other hand, suppose $\dim_D V = \infty$ and, for any integer n, choose V_n to be a subspace of V of dimension n. If $R_n = \{ r \in R \mid V_n r \subseteq V_n \}$ then, by density, R_n acts as the full ring of D-linear transformations on V_n. In particular, if $I_n = \{ r \in R \mid V_n r = 0 \}$, then $I_n \lhd R_n$ and $R_n / I_n \cong \mathrm{M}_n(D)$. In other words, if $\dim_D V = \infty$ then, for all $n \geq 1$, the matrix ring $\mathrm{M}_n(D)$ is *involved* in R.

The basic result here is:

THEOREM 4.7 (Chevalley-Jacobson Density Theorem) *Let R be a primitive ring with faithful irreducible right module V and let D denote the division ring $\mathrm{End}_R(V)$. Then R is a dense ring of linear transformations on the left D-vector space ${}_D V$. Furthermore, if R is right Artinian, then $\dim_D V = n < \infty$ and $R \cong \mathrm{M}_n(D)$.*

PROOF If W is a D-subspace of V, then the right annihilator of W in R, $\mathrm{r.ann}_R(W) = \{ r \in R \mid Wr = 0 \}$, is a right ideal of R. We first show that the double annihilator condition holds for finite dimensional subspaces of V. Specifically, we show that if $\dim_D W < \infty$ and if $x \in V$ with $x \cdot \mathrm{r.ann}_R(W) = 0$, then $x \in W$. We proceed by induction on $\dim_D W = m < \infty$, the case $m = 0$ being trivial. Thus suppose that $m \geq 1$ and write $W = W' \dotplus Dw$, where W' is a subspace of dimension $m - 1$. In particular, by induction, if $A' = \mathrm{r.ann}_R(W')$, then $wA' \neq 0$. But A' is a right ideal of R, so wA' is a nonzero R-submodule of V and hence $wA' = V$.

Write $A = \text{r.ann}_R(W)$ and let $x \in V$ with $xA = 0$. The goal is to show that $x \in W$. To this end, recall that $V = wA'$ and let $\delta: V \to V$ be given by $\delta(wa') = xa'$ for all $a' \in A'$. To see that δ is well-defined, it suffices, as usual, to show that if $wa' = 0$, then $xa' = 0$. But if $wa' = 0$, then, since $a' \in A'$ and $W = W' + Dw$, we have $Wa' = 0$. Hence $a' \in A$ and $xa' = 0$ by the choice of x. Thus δ is a well-defined map, which is now easily seen to be an R-endomorphism. In other words, $\delta \in D$. Finally, for all $a' \in A'$, we have $(x - \delta w)a' = 0$, so $x - \delta w$ is contained in the annihilator of A', namely W', and $x \in W' + Dw = W$, as required.

It is a simple matter to complete the proof. Let $\{v_1, v_2, \ldots, v_n\} \subseteq V$ be a D-linearly independent set and let $\{w_1, w_2, \ldots, w_n\}$ be any subset of V. Then for each i, since v_i is not contained in the finite dimensional D-subspace spanned by the remaining v_j's, the double annihilator condition implies that there exists $s_i \in R$ with $v_j s_i = 0$ for $j \neq i$ and $v_i s_i \neq 0$. Furthermore, since R acts transitively on V, there exists $t_i \in R$ with $(vs_i)t_i = w_i$. In particular, if we set $r = \sum_{k=1}^{n} s_k t_k \in R$, then $v_i r = w_i$ for all i and the first part of the theorem is proved.

Finally, suppose $\dim_D V = \infty$ and choose $V_1 \subset V_2 \subset V_3 \subset \cdots$ to be a strictly increasing chain of finite dimensional D-subspaces of V. If $I_i = \text{r.ann}_R(V_i)$, then I_i is a right ideal of R and density implies that $I_1 \supset I_2 \supset I_3 \supset \cdots$ is a strictly decreasing sequence in R. In other words, R is not Artinian. Turning this around, we see that if R is assumed to be Artinian, then $\dim_D V = n < \infty$ and $R \cong \text{M}_n(D)$ by density again. □

Since any simple ring is necessarily primitive, we have therefore obtained an alternate proof of Corollary 4.6. Next, we have an amusing consequence.

LEMMA 4.8 *Let D be a division ring with a central subfield K and let $F \supseteq K$ be a maximal subfield of D. If $\dim_K F < \infty$, then $\dim_K D < \infty$.*

PROOF Since D is a division ring, $V = D$ is a faithful irreducible right D-module. In particular, we can think of D as being embedded in $\text{End}(V)$, acting on the right. Furthermore, since F is a commutative field, there is an embedding $\rho: F \to \text{End}(V)$ given by $\rho(f): v \mapsto fv$ for all $f \in F$ and $v \in V$. Let $F' = \rho(F) \subseteq \text{End}(V)$ and note that F' is not equal to F, in general, since left and right multiplication by $f \in F$ yield distinct endomorphisms of V. On the other hand, since K is central, we do have $K' = \rho(K) = K$.

Let R be the subring of $\text{End}(V)$ generated by D and F'. Since

$$v\big(\rho(f)d\big) = (fv)d = f(vd) = v\big(d\rho(f)\big)$$

for all appropriate v, f, and d, we see that D and F' commute elementwise. Thus $R = F'D$ consists of all finite sums of elements of the form $f'd$ with $f' \in F'$ and $d \in D$. But $\dim_K F' < \infty$, so it follows that R is a finite dimensional right D-vector space. In particular, since any right ideal of R is a D-subspace, we conclude that R is Artinian.

Finally, observe that $R \subseteq \mathrm{End}(V)$ acts faithfully and irreducibly on V. Furthermore, by Lemma 4.3(ii), $\mathrm{End}_R(V) \subseteq \mathrm{End}_D(V) = D$ acting by left multiplication. Since $d \in \mathrm{End}_R(V)$ must also commute with F', we have

$$d(fv) = d\big(v\rho(f)\big) = (dv)\rho(f) = f(dv)$$

for all $f \in F$ and $v \in V$. In other words, $d \in D$ centralizes F. But F is a maximal subfield of D, so this implies that $d \in F$ and it follows that $\mathrm{End}_R(V) = F$. We can now conclude from Theorem 4.7 that $D = V$ is finite dimensional as a left F-vector space. Thus, since $\dim_K F < \infty$ and K is central in D, we have $\dim_K D < \infty$ as a K-vector space on either side. □

We close with an example of interest. Let S be a ring and let G be a multiplicative group. Then the *group ring* $S[G]$ is the set of all formal finite sums $\sum_{x \in G} s_x x$ with $s_x \in S$. Addition in $S[G]$ is defined in a componentwise fashion and multiplication is determined distributively by $(ax) \cdot (by) = (ab)(xy)$ for all $a, b \in S$ and $x, y \in G$. It is easy to verify that $S[G]$ is indeed an associative ring. Furthermore, if $S = K$ is a field, then $K[G]$ is a K-algebra called the *group algebra.*

PROPOSITION 4.9 (Maschke's Theorem) *Let K be a field and let G be a finite group. Then $K[G]$ is an Artinian ring that is Wedderburn if and only if the characteristic of K does not divide $|G|$.*

PROOF Note that $K[G]$ is a finite dimensional K-algebra and that every right or left ideal of $K[G]$ is a K-subspace. Since $K[G]$ satisfies d.c.c. on K-subspaces, it follows that $K[G]$ is Artinian.

Suppose first that the characteristic of K divides $|G|$ so that $|G| = 0$ in K. Define $\gamma = \sum_{g \in G} g \in K[G]$ and observe that $x\gamma = \gamma = \gamma x$ for all $x \in G$. This implies that γ is central in $K[G]$ and that $\gamma^2 = |G| \cdot \gamma = 0$. Thus $\gamma K[G]$ is a nonzero ideal of $K[G]$ of square 0 and hence $K[G]$ is not a Wedderburn ring.

Conversely, assume that $|G| = n$ is not 0 in K and consider the $n \times n$ matrix ring $\mathrm{M}_n(K)$, where we index the rows and columns by the

elements of G. Then the map $\theta: K[G] \to \mathrm{M}_n(K)$ given by $\theta(g) = (\delta_{y,xg})$ is easily seen to determine a K-algebra embedding, since

$$\theta(g)\theta(h) = (\delta_{y,xg})(\delta_{y,xh}) = (\delta_{y,xgh}) = \theta(gh)$$

Here, of course, $g, h, x, y \in G$. Furthermore, $\delta_{x,y} = 1$ when $x = y$ and $\delta_{x,y} = 0$ otherwise.

Next note that the matrix traces satisfy $\operatorname{tr}\theta(1) = n$ and $\operatorname{tr}\theta(g) = 0$ if $1 \neq g \in G$. In particular, if $\alpha = \sum_{g\in G} a_g g \in K[G]$, then $\operatorname{tr}\theta(\alpha) = na_1$. Now, suppose in addition that α is nilpotent. Then so is $\theta(\alpha)$ and hence $\operatorname{tr}\theta(\alpha)$, being the sum of all eigenvalues, must be 0. Thus $na_1 = 0$ and, since $n \neq 0$ in K, we conclude that $a_1 = 0$.

Finally, let I be a nilpotent right ideal of $K[G]$ and let $\sum_{g\in G} b_g g = \beta \in I$. Then, for all $x \in G$, we have $\sum_{g\in G} b_g g x^{-1} = \beta x^{-1} \in I$ and this element, being nilpotent, has its identity coefficient equal to 0. Thus $b_x = 0$ for all x, and therefore $\beta = 0$, as required. □

An alternate proof of this result in a more general context can be found in Exercise 13.7.

EXERCISES

1. Show by example that the addition formulas of Lemma 4.1(ii)(iii) fail for infinite direct sums.
2. Let $V = \cdot\sum_{k=1}^{n} V_k$ be a direct sum of R-modules. Prove that the endomorphism ring $\mathrm{End}_R(V)$ is isomorphic to the checkered matrix ring

$$S = \{(\alpha_{i,j}) \mid \alpha_{i,j} \in \mathrm{Hom}_R(V_j, V_i)\}$$

   Here multiplication of entries is given by function composition.
3. Assume that R does not have IBN. Show that $\mathrm{M}_i(R) \cong \mathrm{M}_j(R)$ for some $i \neq j$. The converse of this is not true. Indeed, let K be a field and define the rings S_n inductively by $S_0 = K$ and $S_{n+1} = \mathrm{M}_2(S_n) \supseteq S_n$ for $n \geq 0$. If $S = \bigcup_{n=0}^{\infty} S_n$, show that $S \cong \mathrm{M}_2(S)$ but that S has IBN.
4. Suppose the ring R has elements $e_{i,j}$ for $i, j = 1, 2, \ldots, n$ that satisfy $e_{i,j}e_{j',k} = 0$ if $j \neq j'$, $e_{i,j}e_{j,k} = e_{i,k}$ and $1 = e_{1,1} + e_{2,2} + \cdots + e_{n,n}$. If S is the centralizer in R of these n^2 elements, prove that $R \cong \mathrm{M}_n(S)$ and that $S \cong e_{1,1}Re_{1,1}$. To start with, define a map $\sigma: \mathrm{M}_n(S) \to R$ by $(s_{i,j}) \mapsto \sum_{i,j} s_{i,j}e_{i,j}$. Then show that σ is a ring isomorphism.

5. Prove that an Artinian ring with no nonzero nilpotent elements and no nontrivial central idempotents is a division ring.
6. Let $R = \mathrm{M}_n(D)$ with D a division ring. Show that R has finitely many right ideals if and only if either $n = 1$ or D is finite.
7. Let K be a field and let $R \subseteq \mathrm{M}_2(K)$ be given by $R = \begin{pmatrix} K & K \\ 0 & K \end{pmatrix}$. If $e = e_{1,1}$, show that $\mathrm{End}_R(eR)$ is a field even though eR is not an irreducible R-module.
8. Write $R = \cdot \sum_{k=1}^{m} \mathrm{M}_{n_k}(D_k)$ as in the Artin-Wedderburn Theorem. If $I \lhd R$, show that I is a direct sum of certain of the $\mathrm{M}_{n_k}(D_k)$. In particular, deduce that the $\mathrm{M}_{n_k}(D_k)$ are the unique minimal two-sided ideals of R and that, if $I \neq R$, then R/I is a Wedderburn ring.
9. If $R = \mathrm{M}_n(S)$, show that all ideals of R are of the form $\mathrm{M}_n(I)$ for $I \lhd S$. Furthermore, prove that $e_{i,i}R \cong e_{j,j}R$ as right R-modules.
10. Let D be a division ring and let R be a ring of D-linear transformations on ${}_DV$. Assume that R is *doubly transitive* on V so that, by definition, if $\{ v_1, v_2 \}$ is a D-linearly independent subset of V and if $\{ w_1, w_2 \} \subseteq V$ is arbitrary, then there exists $r \in R$ with $v_1 r = w_1$ and $v_2 r = w_2$. Show that $\mathrm{End}_R(V) = D$ and conclude that R is a dense ring of linear transformations on V. What happens if we merely assume that R is transitive on V?

5. Artinian Rings

We now move on to consider more general Artinian rings. For this, we must deal with nonzero nilpotent right ideals; there are a number of ways to proceed, which inevitably all turn out to be equivalent. The approach we take uses the nil radical since it can be easily and quickly defined. Later in this chapter we discuss the more important Jacobson radical.

An ideal I of R is said to be *nil* if every element of I is nilpotent. In particular, any nilpotent ideal is nil. Furthermore, as we have observed earlier, if J is a nilpotent right ideal of R, then RJ is a nilpotent, and therefore a nil, two-sided ideal.

LEMMA 5.1 *Let I be a nil ideal of R.*

i. If $x \in R$ is nilpotent, for example if $x \in I$, then $1-x$ is invertible.

ii. If J/I is a nil ideal of R/I, then J is a nil ideal of R.

iii. An arbitrary sum of nil ideals is nil.

PROOF (i) If $x^t = 0$, set $y = 1 + x + \cdots + x^{t-1}$. Then $(1-x)y = y(1-x) = 1 - x^t = 1$ and $y = (1-x)^{-1}$.

(ii) If $r \in J$, then $r+I \in J/I$ is nilpotent. In particular, $(r+I)^m = 0$ for some $m > 0$ and $r^m \in I$. But I is a nil ideal, so r^m is nilpotent and hence so is r.

(iii) Suppose I and J are nil ideals of R. Then $(I+J)/I$ is a nil ideal of R/I, since it is a homomorphic image of J. Thus, by (ii), $I+J$ is nil and it follows by induction that any finite sum of nil ideals is also nil. Finally, any element of the arbitrary sum $\sum_i I_i$ of nil ideals is contained in a finite sum of these ideals and is therefore nilpotent. Thus $\sum_i I_i$ is also nil. □

DEFINITION If R is an arbitrary ring, then its *nil radical* $\mathrm{Nil}(R)$ is the sum of all nil two-sided ideals of R. In view of Lemma 5.1(iii), $\mathrm{Nil}(R)$ is, in fact, the unique largest nil two-sided ideal of R. Furthermore, by (ii) we see that $\mathrm{Nil}\big(R/\mathrm{Nil}(R)\big) = 0$.

LEMMA 5.2 *Let $I \lhd R$.*

i. If W is an R/I-module, then W is naturally an R-module with multiplication given by $wr = w(r+I)$ for all $w \in W$, $r \in R$. Furthermore, the R-submodules of W are precisely the R/I-submodules and any R/I-module homomorphism $W \to W'$ is also an R-homomorphism.

ii. If V is an R-module with $VI = 0$, then V is naturally an R/I-module with multiplication given by $v(r+I) = vr$ for all $v \in V$, $r \in R$. Furthermore, the R/I-submodules of V are precisely the R-submodules and any R-homomorphism $V \to V'$ is also an R/I-homomorphism.

iii. If R is an Artinian ring, then so is R/I.

PROOF We use the module characterization given by Lemma 1.1.

(i) The composite homomorphism $R \to R/I \to \mathrm{End}(W)$ defines W as a right R-module. Since R and R/I have the same image in $\mathrm{End}(W)$, the submodule structure is the same in either case. Finally, the homomorphism result follows from the module multiplication formula $wr = w(r+I)$.

(ii) Since the homomorphism $R \to \mathrm{End}(V)$ sends I to zero, it factors through R/I. Thus we have $R \to R/I \to \mathrm{End}(V)$ and in this way V becomes an R/I-module. Again, R and R/I have the same image in $\mathrm{End}(V)$.

(iii) By assumption R_R is an Artinian module and hence so is $(R/I)_R$ by Lemma 3.7(i). But I annihilates the latter module, so (ii) implies that $(R/I)_{R/I}$ is Artinian and therefore R/I is an Artinian ring. □

We now obtain a key result.

THEOREM 5.3 *Let R be an Artinian ring with $N = \mathrm{Nil}(R)$. Then R/N is a Wedderburn ring and N is the unique largest nilpotent ideal of R.*

PROOF Since $\mathrm{Nil}(R/N) = 0$, we know that R/N has no nonzero nilpotent right ideal. Lemma 5.2(iii) now implies that R/N is a Wedderburn ring. It remains to show that N is nilpotent, since $N = \mathrm{Nil}(R)$ certainly contains all nilpotent ideals of R.

Since R is Artinian, the descending chain $N \supseteq N^2 \supseteq N^3 \supseteq \cdots$ must stabilize. Thus suppose $N^k = N^{k+1}$ and let $I = \{\, r \in R \mid rN^k = 0 \,\}$. Then I is easily seen to be a right ideal of R and the goal is to show that

$I = R$. If this is not the case, then the minimum condition applied to the set of right ideals of R properly larger than I yields a minimal such right ideal J. Clearly $J = I + aR$ for some $a \in J \setminus I$ so $I + JN = I + (aR)N = I + aN$.

If $JN \not\subseteq I$, then the minimality of J implies that $I + JN = J$. Hence, since $a \in J$, we have $a = i + ax$ for some $i \in I$ and $x \in N$. But $1 - x$ is invertible, by Lemma 5.1(i), so $a = i(1-x)^{-1} \in I$, a contradiction. Thus we must have $JN \subseteq I$ and hence $JN^{k+1} = JN \cdot N^k \subseteq IN^k = 0$. But $N^{k+1} = N^k$, so $JN^k = 0$ and by definition of I we have $J \subseteq I$, again a contradiction. Thus $I = R$ and, since $IN^k = 0$, we conclude that $N^k = 0$ as required. □

With this, we can begin to study R-modules.

LEMMA 5.4 *Let R be an arbitrary ring and let N be a nilpotent ideal of R. If $W \subseteq V$ are R-modules with $V = W + VN$, then $V = W$. In particular, if $V = VN$, then $V = 0$.*

PROOF We show by induction on $i \geq 1$ that $V = W + VN^i$. Indeed, if $V = W + VN^i$ is given, then $VN = WN + VN^{i+1}$ and hence $V = W + VN = W + VN^{i+1}$ as required. But N is nilpotent, so $N^k = 0$ for some $k \geq 1$ and we conclude that $V = W + VN^k = W$. □

PROPOSITION 5.5 *Let R be an Artinian ring. Then up to isomorphism, R has $m < \infty$ irreducible modules $V_1, V_2, \ldots, V_m$ and $V_i \cdot \mathrm{Nil}(R) = 0$ for all i. Furthermore, every completely reducible R-module is uniquely a direct sum of copies of these V_i's.*

PROOF Let $N = \mathrm{Nil}(R)$. If W is an irreducible R/N-module, then by Lemma 5.2(i), W is naturally a simple R-module. Conversely, if V is an irreducible R-module, then by the preceding two results, $V \neq VN$. Thus since VN is a submodule of V, we have $VN = 0$ and hence, by Lemma 5.2(ii), V is naturally a simple R/N-module. In view of the homomorphism aspects of Lemma 5.2(i)(ii), it follows that there is a one-to-one correspondence between the isomorphism classes of irreducible R-modules and of irreducible R/N-modules. Thus, since R/N is a Wedderburn ring, there are only finitely many such classes, by Theorem 4.5(i), with representatives $V_1, V_2, \ldots, V_m$, for instance.

Now let U be a completely reducible R-module. Then U is a direct sum of irreducible R-modules, say $U = \cdot\sum_{j \in \mathcal{J}} U_j$, where $U_j \cong V_{f(j)}$. For uniqueness we need to show that, for each i, the cardinality of the set $\mathcal{J}_i = \{ j \in \mathcal{J} \mid f(j) = i \}$ depends only on U and V_i. To this end,

observe that by Schur's Lemma every nonzero member of $\mathrm{Hom}_R(V_i, U_j)$ is an isomorphism. Thus, by Lemma 4.1(iv), $\mathrm{Hom}_R(V_i, U)$ is $\mathrm{End}_R(V_i)$-isomorphic to $\oplus \sum_{j \in \mathcal{J}} \mathrm{Hom}_R(V_i, U_j)$. Thus the cardinality of $\mathcal{J}_i$ is precisely equal to the dimension of $\mathrm{Hom}_R(V_i, U)$ as a vector space over the division ring $\mathrm{End}_R(V_i)$ and hence it is uniquely determined by the modules U and V_i. □

In particular, the preceding result applies to Wedderburn rings and asserts that if R is Wedderburn, then every R-module is uniquely a direct sum of irreducibles.

THEOREM 5.6 (Hopkins-Levitzki Theorem) *If R is an Artinian ring, then any finitely generated R-module has a composition series. In particular, R_R has such a series.*

PROOF Set $N = \mathrm{Nil}(R)$ so that, by Theorem 5.3, $N^k = 0$ for some integer $k \geq 1$. Now let V be a finitely generated R-module. Then V is Artinian, by Lemma 3.7(iii), and hence so are the submodules

$$V \supseteq VN \supseteq VN^2 \supseteq \cdots \supseteq VN^k = 0$$

and the factors $W_i = VN^i/VN^{i+1}$. But $W_iN = 0$, so Lemma 5.2(ii) implies that each W_i is an Artinian R/N-module. Furthermore, since R/N is a Wedderburn ring, each W_i is completely reducible and hence a direct sum of irreducible modules. Thus, by Lemmas 3.7(ii) and 3.6(ii), we conclude that W_i has a composition series as an R/N-module and hence also as an R-module. Lemma 3.6(i) now yields the result. □

Next, we consider the structure of projective R-modules. For this, we need two observations.

LEMMA 5.7 *Let R be an arbitrary ring and let N be a nilpotent ideal of R. If P and Q are projective R-modules, then we have $P \cong Q$ if and only if $P/PN \cong Q/QN$.*

PROOF Suppose first that $\theta: P \to Q$ is an isomorphism. Then $\theta(PN) = \theta(P)N = QN$ and, similarly, $\theta^{-1}(QN) = PN$. Therefore, the kernel of the composite epimorphism $P \to Q \to Q/QN$ is PN and it follows that $P/PN \cong Q/QN$.

Conversely, if $P/PN \cong Q/QN$, then there exists an R-epimorphism

$\alpha: P \to Q/QN$ with kernel PN. This gives rise to the diagram

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow \alpha & & \\ Q & \xrightarrow{\nu} & Q/QN & \to & 0 \end{array}$$

and, since P is projective, there exists a map $\beta: P \to Q$ that makes the diagram commute.

Notice that $\beta(P) + QN$ contains the kernel of ν and maps onto Q/QN since α is an epimorphism. Thus $Q = \beta(P) + QN$, by Lemma 1.8, and then $Q = \beta(P)$, by Lemma 5.4. In other words, $\beta: P \to Q$ is an epimorphism and, since Q is projective, Theorem 2.8 implies that β splits and hence that $P = \mathrm{Ker}(\beta) \dotplus Q'$ for some submodule Q' isomorphic to Q. Finally, since $\nu\beta = \alpha$, it follows that

$$\mathrm{Ker}(\beta) \subseteq \mathrm{Ker}(\alpha) = PN = \mathrm{Ker}(\beta)N \dotplus Q'N$$

Thus $\mathrm{Ker}(\beta) = \mathrm{Ker}(\beta)N$ and Lemma 5.4 yields $\mathrm{Ker}(\beta) = 0$. □

The following result asserts that idempotents can be *lifted* modulo nil ideals.

LEMMA 5.8 *Let N be a nil ideal of R and let $\nu: R \to R/N$ be the natural epimorphism. If $a \in R$ with $\nu(a)$ an idempotent, then there exists $b \in R$ such that $e = aba$ is an idempotent with $\nu(e) = \nu(a)$.*

PROOF If $a \in R$ is as given, then $\nu(a) = \nu(a)^2 = \nu(a^2)$, so $a - a^2 \in N$. Hence, since N is nil, we have $(a - a^2)^k = 0$ for some integer $k \geq 2$. Now observe that $(1 - a)^k = 1 - ad$ for a suitable $d \in R$ with $ad = da$. Furthermore,

$$1 - \nu(ad) = \nu\big((1 - a)^k\big) = \big(1 - \nu(a)\big)^k = 1 - \nu(a)$$

so $\nu(ad) = \nu(a)$ and

$$0 = (a - a^2)^k = a^k(1 - a)^k = a^k(1 - ad)$$

so $a^k = a^k(ad)$. Hence, for any integer $i \geq 1$, we have $a^k = a^k(ad)^i$; in particular, the case $i = k$ yields $a^k = a^k(ad)^k = a^{2k}d^k$, since a and d commute. But then $e = (ad)^k$ is an idempotent and, by the preceding,

$\nu(e) = \nu(ad)^k = \nu(a)^k = \nu(a)$. Finally, since $k \geq 2$, we conclude that $e = (ad)^k = aba$ for some $b \in R$. □

An R-module V is *decomposable* if it is the direct sum $V = V_1 \dot{+} V_2$ of two nonzero submodules. Otherwise, V is *indecomposable*. The following is the key result on projective modules. Its statement implicitly requires Proposition 5.5.

THEOREM 5.9 *Let R be an Artinian ring with nil radical N and suppose $V_1, V_2, \ldots, V_m$ are representatives of the finitely many isomorphism classes of simple R-modules.*

i. For each i, there exists a projective R-module P_i, unique up to isomorphism, with $P_i/P_iN \cong V_i$.

ii. Each P_i is an indecomposable direct summand of R_R with unique maximal submodule P_iN.

iii. Every projective R-module P is uniquely a direct sum of copies of these P_i's. Furthermore, P is finitely generated if and only if the number of summands is finite.

PROOF (i) By Proposition 5.5 and Lemma 5.2(ii), V_i is a simple R/N-module. Hence, since R/N is a Wedderburn ring, Theorem 4.5(i) implies that V_i is isomorphic to a direct summand of R/N. In other words, by Lemma 3.8(i), there exists an idempotent $\bar{e}_i \in R/N$ with $V_i \cong \bar{e}_i(R/N)$. Now N is a nil ideal, so the preceding lemma asserts that $\bar{e}_i$ can be lifted to an idempotent e_i of R and we set $P_i = e_iR$. Thus P_i is a direct summand of R_R and, in particular, it is a projective R-module. Furthermore, if $\bar{}: R \to R/N$ is the natural epimorphism, then

$$P_i/(P_i \cap N) \cong \bar{P}_i = \bar{e}_i\bar{R} \cong V_i$$

Next observe that $P_iN = (e_iR)N = e_iN$ and that

$$e_iN \subseteq P_i \cap N = e_i(P_i \cap N) \subseteq e_iN$$

since e_i acts like a left identity on P_i. Thus $P_i \cap N = e_iN = P_iN$ and $P_i/P_iN \cong V_i$ as required. The uniqueness of P_i follows from Lemma 5.7, since N is nilpotent.

(ii) We already know that P_i is a direct summand of R_R and that P_iN is a maximal submodule, since P_i/P_iN is irreducible. In particular, if W is any submodule of P_i with $W \not\subseteq P_iN$, then $W + P_iN = P_i$. Thus $W = P_i$ by Lemma 5.4 and we conclude that P_iN is the unique maximal submodule of P_i. Furthermore, if $P = W' \dot{+} W''$, then we cannot have

both W' and W'' contained in P_iN. Thus one of these summands must equal P_i and therefore P_i is indecomposable.

(iii) Now let P be an arbitrary projective R-module. Then P/PN is a module for the Wedderburn ring R/N and hence it is completely reducible. Thus P/PN is also completely reducible as an R-module and we can write $P/PN = \cdot\sum_{j\in\mathcal{J}} U_j$ with $U_j \cong V_{f(j)}$. Now define $Q = \oplus\sum_{j\in\mathcal{J}} Q_j$, where $Q_j \cong P_{f(j)}$. Then Q is certainly projective and

$$Q/QN \cong \oplus \sum_{j\in\mathcal{J}} Q_j/Q_jN \cong P/PN$$

since $P_{f(j)}/P_{f(j)}N \cong V_{f(j)}$. Thus, by Lemma 5.7, $P \cong Q$ and P is indeed a direct sum of copies of the P_i's.

Finally, suppose $P = \cdot\sum_{k\in\mathcal{K}} \tilde{P}_k$ with $\tilde{P}_k \cong P_{g(k)}$. Then we have

$$\cdot \sum_{k\in\mathcal{K}} \tilde{P}_k/\tilde{P}_kN = P/PN = \cdot \sum_{j\in\mathcal{J}} U_j$$

and hence the sets $\mathcal{K}_i = \{\, k \in \mathcal{K} \mid g(k) = i \,\}$ and $\mathcal{J}_i = \{\, j \in \mathcal{J} \mid f(j) = i \,\}$ have the same cardinality, by Proposition 5.5. Thus uniqueness is proved and the result follows, since each $P_i = e_iR$ is a cyclic R-module. □

In view of the preceding, $P_1, P_2, \ldots, P_m$ are, up to isomorphism, the only nonzero indecomposable projective R-modules. They are called the *projective indecomposables* or the *principal indecomposables* of R.

DEFINITION If R is an arbitrary ring, then its *Jacobson radical* is given by

$$\mathrm{Rad}(R) = \{\, r \in R \mid Vr = 0 \text{ for all simple } R\text{-modules } V \,\}$$

Thus $\mathrm{Rad}(R)$ is the obstruction to studying R in terms of its irreducible modules. When this obstruction is not present, that is when $\mathrm{Rad}(R) = 0$, we say that R is *semiprimitive*. It is clear that any primitive ring is necessarily semiprimitive.

An ideal I of R is said to be *primitive* if R/I is a primitive ring. In view of Lemma 5.2(i)(ii), I is primitive if and only if there exists an irreducible R-module V with $I = \{\, r \in R \mid Vr = 0 \,\}$. In other words, I is the kernel of the ring homomorphism $R \to \mathrm{End}(V)$.

Finally, the ideal I is *quasi-regular* if $1 - x$ is invertible for all $x \in I$. In particular, by Lemma 5.1(i), every nil ideal is quasi-regular. Basic properties and relations between these concepts are as follows.

LEMMA 5.10 *Let R be an arbitrary ring.*

i. $\mathrm{Rad}(R)$ *is the intersection of all primitive ideals of* R.

ii. $\mathrm{Rad}(R)$ *is the intersection of all maximal right ideals of* R.

iii. $\mathrm{Rad}(R)$ *is the unique largest quasi-regular ideal of* R. *In particular,* $\mathrm{Nil}(R) \subseteq \mathrm{Rad}(R)$.

iv. If $I \lhd R$ *with* $I \subseteq \mathrm{Rad}(R)$, *then* $\mathrm{Rad}(R/I) = \mathrm{Rad}(R)/I$.

PROOF (i) This is essentially obvious. If V is an irreducible R-module, then $\mathrm{r.ann}_R(V) = \{ r \in R \mid Vr = 0 \}$ is a primitive ideal and indeed these are all the primitive ideals of R. Thus, by definition, $\mathrm{Rad}(R) = \bigcap_V \mathrm{r.ann}_R(V)$ is the intersection of all primitive ideals of R.

(ii) If M is a maximal right ideal of R, then R/M is an irreducible R-module, which must therefore be annihilated by $J = \mathrm{Rad}(R)$. In particular, $0 = (1 + M)J = J + M$ and hence $J \subseteq M$. It follows that J is contained in J', the intersection of all maximal right ideals of R.

Conversely, let V be an irreducible R-module and fix any $0 \neq v \in V$. Then $V = vR$, so the map $\theta: R \to V$ given by $r \mapsto vr$ is an R-epimorphism. It follows from Lemma 1.8 that $\mathrm{Ker}(\theta) = \{ r \in R \mid vr = 0 \}$ is a maximal right ideal of R and therefore $\mathrm{Ker}(\theta) \supseteq J'$. Thus $vJ' = 0$ and, since v and V are arbitrary, we obtain the reverse inclusion $J' \subseteq J$.

(iii) Let $I \lhd R$. Suppose first that I is quasi-regular and let M be any maximal right ideal of R. If $I \not\subseteq M$, then $R = I + M$, so $1 = i + m$ for some $i \in I$ and $m \in M$. But then $1 - i = m \in M$ is invertible and this is certainly a contradiction. Thus $I \subseteq M$ for all such M and hence $I \subseteq \bigcap M = \mathrm{Rad}(R)$.

Conversely, suppose $I \subseteq \mathrm{Rad}(R)$ and let $x \in I$. If $(1 - x)R \neq R$ then, by Zorn's Lemma, we have $(1 - x)R \subseteq M$ for some maximal right ideal M. But $I \subseteq \mathrm{Rad}(R) \subseteq M$, so this implies that both x and $1 - x$ are in M, clearly a contradiction. We conclude that $(1 - x)R = R$ for all $x \in I$ and, in particular, that each such $1 - x$ has a right inverse.

Again let $x \in I$ and let $1 - y$ be a right inverse for $1 - x$. Then $1 = (1 - x)(1 - y)$, so $y = xy - x \in I$ and thus $1 - y$ also has a right inverse. But then $1 - y$ has both a left and a right inverse, so it follows that $1 - y$ is invertible with inverse $1 - x$. In other words, $(1 - x)^{-1}$ exists for all $x \in I$ and we conclude that I is quasi-regular.

(iv) Finally, let $\nu: R \to R/I$ be the natural epimorphism. If M' is a maximal right ideal of R/I, then $\nu^{-1}(M')$ is a maximal right ideal of R by Lemma 1.8. Conversely, if M is a maximal right ideal of R, then $M \supseteq \mathrm{Rad}(R) \supseteq I$ and thus $\nu(M)$ is a maximal right ideal of R/I. In this way, we obtain a one-to-one correspondence between the maximal right ideals of these two rings. Since ν^{-1} preserves intersections, by Lemma 1.8,

we conclude from (ii) that $\nu^{-1}\big(\mathrm{Rad}(R/I)\big) = \mathrm{Rad}(R)$. □

In view of (iii), the definition of $\mathrm{Rad}(R)$ is in fact right-left symmetric. In other words, $\mathrm{Rad}(R)$ is also the intersection of the annihilators of all irreducible left R-modules and it is the intersection of all maximal left ideals of R.

LEMMA 5.11 *If R is Artinian, then* $\mathrm{Rad}(R) = \mathrm{Nil}(R)$.

PROOF By Lemma 5.10(iii)(iv), $N = \mathrm{Nil}(R) \subseteq \mathrm{Rad}(R)$ and it suffices to show that R/N is semiprimitive. But R/N is a Wedderburn ring, so the regular module $(R/N)_{R/N}$ is completely reducible and hence a direct sum of irreducible modules. It follows that $\mathrm{Rad}(R/N)$ annihilates the regular module and, in particular, $1 \cdot \mathrm{Rad}(R/N) = 0$. □

We close this chapter by briefly sketching an interesting example. Let K be a field of characteristic $\neq 2$ and let $a_1, a_2, \ldots, a_n$ be fixed elements of K. Then the *Clifford algebra* $C = C(a_1, a_2, \ldots, a_n)$ is the K-algebra generated by noncommuting variables $x_1, x_2, \ldots, x_n$ subject to the relations $x_i x_j = -x_j x_i$ and $x_i^2 = a_i$ for all $i \neq j$. When all the a_i are zero, C is the more familiar *Grassmann algebra*, or *exterior algebra.* On the other hand, $C(-1,-1)$ is the ordinary quaternion algebra over K and therefore $C(a_1, a_2)$ is usually called a *generalized quaternion algebra* when $a_1, a_2 \neq 0$.

The following notation is used in the next proposition. First, if $S = \{i_1, i_2, \ldots, i_s\}$ is a subset of $N = \{1, 2, \ldots, n\}$ with $i_1 < i_2 < \cdots < i_s$, then we write x_S for the monomial $x_{i_1} x_{i_2} \cdots x_{i_s} \in C$. In particular, $x_\emptyset = 1$ and $x_{\{i\}} = x_i$. Next, if S and T are subsets of N, then we denote their *symmetric difference* by $S * T$. Thus, by definition, $S * T = (S \backslash T) \cup (T \backslash S) = (S \cup T) \backslash (S \cap T)$ and, as is well known, $*$ is an associative operation. For convenience, if $i \in N$ we write $S * i$ for $S * \{i\}$ and note that $S * i = S \cup \{i\}$ if $i \notin S$ and $S \backslash \{i\}$ otherwise. Finally, for any such S and i, let $S(i) = \{j \in S \mid j > i\}$.

PROPOSITION 5.12 *The Clifford algebra $C = C(a_1, a_2, \ldots, a_n)$ is a K-algebra with basis $\{x_S \mid S \subseteq N\}$. In particular,* $\dim_K C = 2^n$ *and C is Artinian. Furthermore, C is a Wedderburn ring if and only if* $\prod_1^n a_i \neq 0$.

PROOF C is obviously spanned over K by all monomials in the variables $x_1, x_2, \ldots, x_n$ and, by using the anticommuting relation $x_i x_j = -x_j x_i$, we see that each such monomial is equal to $\pm$ a monomial with the x_i's in the correct order. Furthermore, we can then replace each occurrence of x_i^2 with $a_i \in K$. It follows that every such monomial is a scalar multiple of

some x_S and therefore that C is spanned by $\{ x_S \mid S \subseteq N \}$. In particular, $\dim_K C \leq 2^n$ and C is Artinian.

Now let V be a K-vector space of dimension 2^n having basis elements that correspond to the subsets S of N. Specifically, let $\{ \lceil S \rceil \mid S \subseteq N \}$ be such a basis of V and, for each $i \in N$, let $y_i \colon V \to V$ be the K-linear transformation defined by $\lceil S \rceil y_i = k(S,i) \lceil S*i \rceil$, where $k(S,i) = (-1)^{|S(i)|}$ if $i \notin S$ and $(-1)^{|S(i)|} a_i$ otherwise. Since $S*i*j = S*j*i$ and $S*i*i = S$, it follows easily that $y_i y_j = -y_j y_i$ and $y_i^2 = a_i$ for all $i \neq j$. Thus, by definition of C, there exists a K-algebra homomorphism $C \to \mathrm{End}_K(V)$ with $x_i \mapsto y_i$ and, in this way, V can be viewed as a right C-module. But observe that $\lceil \emptyset \rceil x_S = \lceil S \rceil$; thus, since $\{ \lceil S \rceil \mid S \subseteq N \}$ is linearly independent, it follows that $\{ x_S \mid S \subseteq N \}$ is also linearly independent. In other words, $\dim_K C = 2^n$.

Now suppose that some a_i is zero, say $a_r = 0$. Then the anticommuting relations imply that $x_r C x_r = 0$ and thus $x_r C$ is a nonzero right ideal of C of square 0. In particular, C is not a Wedderburn ring.

For the converse, let $\mathrm{tr} \colon C \to K$ yield the trace of the elements of C viewed as linear transformations on V and note that if $S, T \subseteq N$, then $\lceil T \rceil x_S$ is a scalar multiple of $\lceil T*S \rceil$. Thus, since $T*S \neq T$ when $S \neq \emptyset$, it follows that $\mathrm{tr}\, x_S = 0$ for such S. Furthermore, since $\mathrm{tr}\, x_\emptyset = \dim V = 2^n$, we conclude that $\mathrm{tr}\left(\sum_S a_S x_S\right) = 2^n a_\emptyset$. In particular, if $\alpha = \sum_S a_S x_S$ is a nilpotent element of C, then $\mathrm{tr}\, \alpha = 0$, so $2^n a_\emptyset = 0$ and hence $a_\emptyset = 0$, since the characteristic of K is not 2.

Finally, suppose that all a_i are different from 0. It then follows easily that $x_S x_T$ is a nonzero scalar multiple of x_{S*T} for all $S, T \subseteq N$. Furthermore, note that $S * T = \emptyset$ if and only if $S = T$. Thus if $\beta = \sum_S b_S x_S$ is a nonzero element of C, with, for example, $b_T \neq 0$, then the $x_\emptyset$-coefficient of βx_T is not zero and, in particular, βx_T is not nilpotent. This clearly implies that C has no nonzero nilpotent right ideal and we conclude that C is a Wedderburn ring. □

It can be shown that if C is a Wedderburn ring, then C is a direct sum of at most two simple components.

EXERCISES

An idempotent $e \in R$ is *primitive* if it cannot be written as $e = f + g$, a sum of two nonzero orthogonal idempotents. Here *orthogonal* means that $fg = gf = 0$.

1. If f and g are orthogonal idempotents, show that $e = f + g$ is an idempotent and that $eR = fR + gR$. Conclude that an idempotent

e' of R is primitive if and only if $e'R$ is indecomposable as a right R-module.

2. Let N be a nil ideal of R and let $\{\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_n\}$ be a set of orthogonal idempotents of R/N that sum to 1. If $\nu: R \to R/N$ is the natural epimorphism, prove that there exists a set $\{e_1, e_2, \ldots, e_n\}$ of orthogonal idempotents of R with $\nu(e_i) = \bar{e}_i$ and $e_1 + e_2 + \cdots + e_n = 1$. Furthermore, if $\{f_1, f_2, \ldots, f_n\}$ is a second such lifting, show that $u = e_1 f_1 + e_2 f_2 + \cdots + e_n f_n$ is a unit of R with $u^{-1} e_i u = f_i$ for all i.

A ring R is called *semiprimary* if $N = \mathrm{Nil}(R)$ is a nilpotent ideal with R/N a Wedderburn ring. In particular, by Theorem 5.3, any Artinian ring is necessarily semiprimary. Furthermore, it is easy to see that the results of Proposition 5.5 and Theorem 5.9 apply to these more general rings.

3. Find an example of a semiprimary ring that is not Artinian. A suitable upper triangular 2×2 matrix ring will work.
4. Let I be a nonnilpotent right ideal of the semiprimary ring R. Use Lemma 5.8 to prove that I contains a nonzero idempotent. Furthermore, show that I is minimal with the property of being nonnilpotent if and only if $I = eR$ for some nonzero primitive idempotent $e \in R$. Notice that such right ideals correspond precisely to the projective indecomposables of R.

A ring R is said to be *von Neumann regular* if every cyclic right ideal is generated by an idempotent.

5. Prove that R is von Neumann regular if and only if for all $r \in R$ there exists $r' \in R$ with $rr'r = r$. Conclude that the definition of von Neumann regular is right-left symmetric.
6. Show that any Wedderburn ring is von Neumann regular. Conversely, if R is von Neumann regular and Artinian, show that it is a Wedderburn ring. Give an example of a von Neumann regular ring that is not Wedderburn. For this, let X be an infinite set, let D be a division ring and consider the ring of all functions from X to D with pointwise addition and multiplication.
7. Let I be a two-generator right ideal of the von Neumann regular ring R. Show that $I = eR + fR = eR + (1-e)fR = eR + gR$, where e, f and g are idempotents of R with $eg = 0$. Then show that $I = (1-g)eR + gR$ and observe that g and $(1-g)e$ are orthogonal idempotents of R. Conclude that $h = (1-g)e + g$ is an idempotent and that $I = hR$. It follows that every finitely generated right ideal of R is generated by an idempotent and hence is a direct summand of R.

8. If $\theta\colon R \to S$ is a ring epimorphism, prove that $\theta\big(\mathrm{Nil}(R)\big) \subseteq \mathrm{Nil}(S)$ and that $\theta\big(\mathrm{Rad}(R)\big) \subseteq \mathrm{Rad}(S)$. Show by example that these inclusions need not be equalities. What happens if θ is not an epimorphism? Finally, find a commutative integral domain R with $\mathrm{Rad}(R) \neq 0$. Conclude that $\mathrm{Rad}(R)$ can be properly larger than $\mathrm{Nil}(R)$.
9. Let I be a right ideal of R and let $A = \{\, r \in R \mid (R/I)r = 0 \,\}$. Prove that A is the largest two-sided ideal of R contained in I.
10. Let $C = C(a_1, a_2, \ldots, a_n)$ be a Clifford algebra with $a_i \neq 0$ precisely when $i \leq r$. Prove that $\mathrm{Rad}(C)$ is generated by $x_{r+1}, \ldots, x_n$ and that $C/\mathrm{Rad}(C) \cong C(a_1, \ldots, a_r)$.

6. Hereditary Rings

Having completed our study of Wedderburn rings and Artinian rings, we now move on to the corresponding next levels of complication. Thus, in this chapter we consider the very basic properties of hereditary rings and of Noetherian rings. Although it will not become apparent until later on, these are indeed the respective next steps.

Let R be an arbitrary ring. An R-module V_R is said to be *hereditary* if V and all its submodules are projective. Notice that submodules of hereditary modules are necessarily hereditary.

LEMMA 6.1 *Let W be an R-module, let $\mathcal{I}$ be a well-ordered set and suppose $\{W(\alpha) \mid \alpha \in \mathcal{I}\}$ is an increasing chain of submodules of W satisfying $\bigcup_{\alpha\in\mathcal{I}} W(\alpha) = W$. For each α, set $W(\alpha)^- = \bigcup_{\beta<\alpha} W(\beta)$ and assume that $W(\alpha)/W(\alpha)^- = W'_\alpha$ is projective. Then $W \cong \oplus \sum_{\alpha\in\mathcal{I}} W'_\alpha$ and therefore W is projective.*

PROOF Since W'_α is projective, the exact sequence

$$0 \to W(\alpha)^- \to W(\alpha) \to W'_\alpha \to 0$$

splits and thus $W(\alpha) = W(\alpha)^- \dot{+} W_\alpha$ with $W_\alpha \cong W'_\alpha$. We will show that $W = \cdot \sum_\alpha W_\alpha$.

To start with, set $T = \sum_\alpha W_\alpha$. If $W \neq T$, then we can choose $\gamma \in \mathcal{I}$ to be minimal with $W(\gamma) \not\subseteq T$. But then $W(\gamma)^- \subseteq T$ and $W_\gamma \subseteq T$, so $W(\gamma) \subseteq T$, a contradiction. Thus $W = T = \sum_\alpha W_\alpha$.

Finally, suppose $w_{\alpha_1} + w_{\alpha_2} + \cdots + w_{\alpha_n} = 0$ with $w_{\alpha_i} \in W_{\alpha_i}$ and with $\alpha_1 < \alpha_2 < \cdots < \alpha_n$. Then

$$w_{\alpha_n} = -(w_{\alpha_1} + w_{\alpha_2} + \cdots + w_{\alpha_{n-1}}) \in W_{\alpha_n} \cap W(\alpha_n)^- = 0$$

and it follows that the sum $\sum_\alpha W_\alpha$ is direct. Thus

$$W = \cdot \sum_\alpha W_\alpha \cong \oplus \sum_\alpha W'_\alpha$$

and W is projective. □

LEMMA 6.2 *An arbitrary weak direct sum of hereditary R-modules is hereditary. Indeed, let* $\{V_\alpha \mid \alpha \in \mathcal{I}\}$ *be a family of hereditary modules. If* $V = \oplus \sum_{\alpha\in\mathcal{I}} V_\alpha$ *and if* W *is a submodule of* V, *then* $W \cong \oplus \sum_\alpha V'_\alpha$ *with* $V'_\alpha \subseteq V_\alpha$.

PROOF Let $W \subseteq V$ be as given and let $\pi_\alpha: V \to V_\alpha$ be the natural projection. Well-order the set $\mathcal{I}$ and, for each $v \in V$, define $\deg v = \max\{\alpha \mid \pi_\alpha(v) \neq 0\}$. Note that the above set is necessarily finite so the maximum always exists. By definition, $\deg 0 = -\infty < \mathcal{I}$.

Now, for each $\alpha \in \mathcal{I}$, set $W(\alpha) = \{w \in W \mid \deg w \leq \alpha\}$. In this way we obtain an increasing chain of submodules of W whose union is all of W. Furthermore, by restricting π_α to $W(\alpha)$, we have

$$0 \to W(\alpha)^- \to W(\alpha) \xrightarrow{\pi_\alpha} V'_\alpha \to 0$$

where $V'_\alpha = \pi_\alpha\big(W(\alpha)\big) \subseteq V_\alpha$ and

$$W(\alpha)^- = \{w \in W \mid \deg w < \alpha\} = \bigcup_{\beta<\alpha} W(\beta)$$

But $V'_\alpha \subseteq V_\alpha$, so V'_α is projective and the preceding lemma applies. We conclude that $W \cong \oplus \sum_{\alpha\in\mathcal{I}} V'_\alpha$, so W is a projective module and V is therefore hereditary. □

DEFINITION R is said to be a *hereditary ring* if all its right ideals are projective modules. Obviously, this occurs if and only if the regular module R_R is hereditary. In view of Theorem 3.9, all Wedderburn rings are necessarily hereditary.

THEOREM 6.3 *If R is a hereditary ring, then every free R-module is hereditary. Indeed, every submodule of a free R-module, and hence of a projective R-module, is isomorphic to a direct sum of right ideals of R.*

PROOF Let F_R be a free R-module. Then $F = \cdot \sum_\alpha V_\alpha$ with each $V_\alpha \cong R_R$. It follows that F is hereditary by the previous result. Furthermore,

if W is a submodule of F, then $W \cong \oplus \sum_\alpha V'_\alpha$, where $V'_\alpha \subseteq V_\alpha \cong R_R$. In particular, V'_α is isomorphic to a right ideal of R. □

COROLLARY 6.4 *Let R be a commutative principal ideal domain. Then R is hereditary and indeed every submodule of a free R-module is free.*

PROOF If I is a nonzero ideal of R, then $I = dR$ for some $0 \neq d \in R$. Since R is a domain, the map $R \to I$ given by $r \mapsto dr$ is a module isomorphism. Thus $I \cong R_R$ is free, so R is hereditary and the previous theorem yields the result. □

In the following chapter we characterize all hereditary commutative domains. Furthermore, in Chapter 8 we explain why hereditary rings are the natural next step after Wedderburn rings. Here we change topics slightly and introduce the family of Noetherian R-modules.

DEFINITION Let V be an R-module. Then V satisfies the *maximum condition*, or *max*, if every nonempty collection of submodules of V has a maximal member. By this we mean that if $\mathcal{F}$ is a nonempty family of submodules, then there exists $W \in \mathcal{F}$ such that W is contained in no other member of $\mathcal{F}$.

In addition, we say that V satisfies the *ascending chain condition*, or *a.c.c.*, if every ascending chain $V_1 \subseteq V_2 \subseteq \cdots$ of submodules eventually stabilizes. In view of the Jordan-Hölder Theorem, any module with a composition series necessarily satisfies a.c.c.

It is easy to see that these two properties are in fact equivalent. To start with, suppose V satisfies max and let $V_1 \subseteq V_2 \subseteq \cdots$ be an ascending chain of submodules. Then the collection $\{V_1, V_2, \ldots\}$ contains a maximal member, say V_n, and the series stabilizes at n.

Conversely, suppose V satisfies a.c.c. and let $\mathcal{F}$ be a nonempty collection of submodules of V. Choose $V_1 \in \mathcal{F}$. If V_1 is not maximal, then there exists $V_2 \in \mathcal{F}$ with $V_1 \subset V_2$. If V_2 is not maximal, then we can find $V_3 \in \mathcal{F}$ with $V_2 \subset V_3$. Continuing in this manner, we either find a maximal member of $\mathcal{F}$ or we construct an infinite ascending chain $V_1 \subset V_2 \subset \cdots$ that does not stabilize.

Modules satisfying max, or equivalently a.c.c., are also called *Noetherian*. Part (i) of the following lemma contains a key alternate characterization of such modules.

LEMMA 6.5 *Let V be an R-module.*

i. V is Noetherian if and only its submodules are all finitely generated.

ii. Suppose $W \subseteq V$. Then V is Noetherian if and only if both W and V/W are Noetherian.

iii. V has a composition series if and only if it satisfies both a.c.c. and d.c.c.

PROOF (i) Suppose first that all submodules of V are finitely generated and let $V_1 \subseteq V_2 \subseteq \cdots$ be an ascending chain of submodules. If $W = \bigcup_1^\infty V_i$, then W is certainly a submodule of V and hence it is finitely generated. But each generator of W is contained in some V_i and, by taking the largest of these finitely many subscripts, we see that all generators of W are contained in some V_t. Thus $W = V_t$ and we conclude that the series stabilizes at t.

Conversely suppose that V satisfies max and let W be a submodule of V. Since 0 is a finitely generated submodule of W, it follows from max that there exists a submodule W' of W maximal with the property of being finitely generated. But if $w \in W$, then $W' + wR$ is also a finitely generated submodule of W. Thus the maximality of W' implies that $w \in W'$ and therefore that $W' = W$.

(ii) This follows as in Lemma 3.7(i).

(iii) As we have already observed, if V has a composition series, then it satisfies both max and min. Conversely suppose V satisfies both max and min and set $V_0 = 0$. If $V_0 \neq V$, then by min there exists a submodule V_1 of V minimal with the property of properly containing V_0. Again, if $V_1 \neq V$, then there exists V_2 minimal with the property of properly containing V_1. Continuing in this manner, we obtain a strictly increasing sequence $V_0 \subset V_1 \subset V_2 \subset \cdots$ and, since V satisfies max, we conclude that $V = V_n$ for some n. Thus $0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$ is a composition series for V. □

DEFINITION R is said to be a *right Noetherian ring* if the regular module R_R satisfies a.c.c. As usual, we delete the modifier "right" unless the side is in doubt; there is of course an analogous definition on the left. It follows from Lemma 6.5(i) that R is Noetherian if and only if all right ideals of R are finitely generated. Furthermore, by (iii) and the Hopkins-Levitzki Theorem, any Artinian ring is necessarily Noetherian.

LEMMA 6.6 *Let R be a Noetherian ring. If V is a finitely generated R-module, then V is a Noetherian R-module. In particular, all submodules of V are finitely generated.*

PROOF It follows as in Lemma 3.7(iii) that V is Noetherian. Part (i) of the preceding lemma now yields the result. □

DEFINITION A ring R is said to be *prime* if for all nonzero ideals $A, B \lhd R$ we have $AB \neq 0$. In particular, any simple ring is prime.

An ideal P of R is *prime* when R/P is a prime ring. Thus P is prime if and only if for all ideals A, B of R that contain P, the inclusion $AB \subseteq P$ implies $A = P$ or $B = P$. In particular, any maximal ideal of R is prime. Furthermore, it is easy to see that P is prime if and only if for all ideals A, B of R, the inclusion $AB \subseteq P$ implies $A \subseteq P$ or $B \subseteq P$.

In case R is commutative, R being prime is the same as R being an integral domain. Thus P is a prime ideal of R precisely when R/P is an integral domain. As usual, this occurs if and only if $ab \in P$, with $a, b \in R$, implies that $a \in P$ or $b \in P$.

PROPOSITION 6.7 *If R is a Noetherian ring and $A \lhd R$, then there exist not necessarily distinct prime ideals $P_1, P_2, \ldots, P_n$, each containing A, with $P_1 P_2 \cdots P_n \subseteq A$. In particular, 0 is a finite product of prime ideals of R.*

PROOF If false, then the set $\mathcal{C}$ of counterexample ideals is nonempty and hence, by the maximum condition, $\mathcal{C}$ contains a maximal member C. Certainly C is not prime. Thus there exist ideals A and B of R properly containing C with $AB \subseteq C$. Since A and B are not counterexamples, each of these contains a finite product of prime ideals with each prime containing A or B and hence C. Thus AB contains an appropriate finite product of primes and this is a contradiction since $AB \subseteq C$. □

Note that the preceding only requires that R satisfy the maximum condition on its two-sided ideals. We close with two additional results needed for the next chapter.

LEMMA 6.8 *Let A and B be right ideals of R.*

i. If $A + B = R$, then $A \oplus B \cong R \oplus (A \cap B)$ as right R-modules.

ii. In (i), if R is commutative, then $A \cap B = AB$.

iii. If $V_R \cong W_R$, then $VA \cong WA$.

PROOF (i) Let $\pi: A \oplus B \to R$ be the R-homomorphism given by $a \oplus b \mapsto a - b$. Since $A + B = R$, we see that π is onto and, since R is projective, the map splits. Thus $A \oplus B \cong R \oplus J$, where $J = \mathrm{Ker}(\pi)$. But $a \oplus b \in J$ means that $a = b \in A \cap B$, so the map $A \cap B \to J$ given by $c \mapsto c \oplus c$ is an isomorphism and hence $J \cong A \cap B$.

(ii) If R is commutative, then $A \cap B \supseteq AB$. Conversely, since $R = A + B$, we have $A \cap B = (A \cap B)(A + B) \subseteq AB$.

(iii) If $\theta: V \to W$ is the given isomorphism, then $\theta(VA) = \theta(V)A = WA$, so $VA \cong WA$. □

LEMMA 6.9 *Let R be a commutative integral domain with field of fractions F and let $A_1, A_2, \ldots, A_n$ and $B_1, B_2, \ldots, B_m$ be nonzero R-submodules of F. If*

$$A_1 \oplus A_2 \oplus \cdots \oplus A_n \cong B_1 \oplus B_2 \oplus \cdots \oplus B_m$$

then $n = m$ and $\prod_i A_i = q \cdot \prod_j B_j$ for some $0 \neq q \in F$.

PROOF If C is any nonzero R-submodule of F and $0 \neq c \in C$, then $C' = c^{-1}C$ is an R-submodule of F, $1 \in C'$ and $C'_R \cong C_R$. Thus without loss of generality, we can assume that each A_i and B_j contains 1.

Let

$$\theta: A_1 \oplus A_2 \oplus \cdots \oplus A_n \to B_1 \oplus B_2 \oplus \cdots \oplus B_m$$

be the given isomorphism. For each i, write

$$\theta(0 \oplus \cdots \oplus 1_i \oplus \cdots \oplus 0) = b_{i,1} \oplus b_{i,2} \oplus \cdots \oplus b_{i,m}$$

with $b_{i,j} \in B_j$. Here 1_i indicates that 1 occurs in the ith summand. Since R is a commutative ring, it then follows easily that for all $a_i \in A_i$, we have

$$\theta(0 \oplus \cdots \oplus a_i \oplus \cdots \oplus 0) = a_i b_{i,1} \oplus a_i b_{i,2} \oplus \cdots \oplus a_i b_{i,m}$$

and hence $A_i b_{i,j} \subseteq B_j$. Similarly for each j, write

$$\theta^{-1}(0 \oplus \cdots \oplus 1_j \oplus \cdots \oplus 0) = a_{j,1} \oplus a_{j,2} \oplus \cdots \oplus a_{j,n}$$

with $a_{j,i} \in A_i$. Again, this implies that

$$\theta^{-1}(0 \oplus \cdots \oplus b_j \oplus \cdots \oplus 0) = b_j a_{j,1} \oplus b_j a_{j,2} \oplus \cdots \oplus b_j a_{j,n}$$

for all $b_j \in B_j$. Thus $B_j a_{j,i} \subseteq A_i$.

Let $\mathcal{B}$ be the $n \times m$ matrix $\mathcal{B} = (b_{i,j})$ and let $\mathcal{A}$ be the $m \times n$ matrix $\mathcal{A} = (a_{j,i})$. Then by computing the composite maps $\theta^{-1}\theta$ and $\theta\theta^{-1}$, it follows easily that $\mathcal{B}\mathcal{A} = I_n$ and $\mathcal{A}\mathcal{B} = I_m$. In particular, since these are matrices over the field F, we must have $n = m$ and $\mathcal{A} = \mathcal{B}^{-1}$. Finally, $A_i b_{i,j} \subseteq B_j$ implies that $A \cdot \det \mathcal{B} \subseteq B$, where $A = \prod_i A_i$ and $B = \prod_j B_j$. Similarly, $B_j a_{j,i} \subseteq A_i$ yields $B \cdot \det \mathcal{A} \subseteq A$. Thus, since $\det \mathcal{A} \cdot \det \mathcal{B} = 1$, we conclude that $A = B \cdot \det \mathcal{B}$ and the lemma is proved. □

EXERCISES

In the following two problems, let $\mathbb{Z}$ be the ring of integers, $\mathbb{Q}$ the field of rationals, and let R be the subring of $M_2(\mathbb{Q})$ given by $R = \begin{pmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}$. Set $N = \begin{pmatrix} 0 & \mathbb{Q} \\ 0 & 0 \end{pmatrix}$ and let $V = \begin{pmatrix} 0 & 0 \\ 0 & \mathbb{Q} \end{pmatrix}$. We show that R is hereditary but not left hereditary.

1. First prove that N and V are minimal right ideals of R, that V_R is projective and that $N_R \cong V_R$. Next show that any right ideal of R properly containing $N \dotplus V$ has the form $\begin{pmatrix} z\mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}$, where $0 \neq z \in \mathbb{Z}$, and that, as a right R-module, this ideal is isomorphic to R_R. Conclude that R is hereditary. To this end, observe, for example, that if I is a right ideal of R with $I \not\supseteq N$, then $I \cap N = 0$. Thus $I \dotplus N$ is a right ideal containing N and it suffices to show that $I \dotplus N$ is projective.
2. Note that both N and $A = N \dotplus V$ are two-sided ideals of R and that $\bigcap_{n=1}^{\infty} nR = A = AR$. It follows that if F is a free left R-module, then $\bigcap_{n=1}^{\infty} nF = AF$. Now show that ${}_RN$ is not projective. Indeed, if F is a free left R-module with $F = N \dotplus W$, then

$$N = \bigcap_{n=1}^{\infty} nN \subseteq \bigcap_{n=1}^{\infty} nF = AF = AN \dotplus AW = AW$$

Thus R is not left hereditary.

Let R be a ring and let n be a positive integer. Then R is said to be an *n-fir* if all n-generator right ideals of R are free of unique rank.

3. Prove that R is a 1-fir if and only if it is a domain, that is a ring without zero divisors. In one direction, suppose R is a 1-fir, let $0 \neq a \in R$ and consider the short exact sequence $0 \to I \to R \to aR \to 0$, where the epimorphism is left multiplication by a. Since aR is free, $R \cong I \oplus aR$ and hence I is also a 1-generator right ideal of R. The other direction follows easily from Lemma 2.5.

4. Let V be an R-module with a composition series and let $\theta \in \mathrm{End}_R(V)$. Observe that the ascending chain $\{ \mathrm{Ker}(\theta^i) \mid i = 1, 2, \dots \}$ and the descending chain $\{ \mathrm{Im}(\theta^i) \mid i = 1, 2, \dots \}$ must both terminate and choose integer $n \geq 1$ so that $\mathrm{Ker}(\theta^n) = \mathrm{Ker}(\theta^{2n})$ and $\mathrm{Im}(\theta^n) = \mathrm{Im}(\theta^{2n})$. Prove that $V = \mathrm{Ker}(\theta^n) \dotplus \mathrm{Im}(\theta^n)$, that θ is a nilpotent endomorphism on the first summand and that θ is an automorphism of the second. In

particular, if V is indecomposable, conclude that θ is either nilpotent or an automorphism of V. This is Fitting's Lemma.

5. Let S be a ring with the property that every element is either nilpotent or invertible. If $\alpha, \beta, \gamma \in S$ with α and β nilpotent, show that $\alpha\gamma$, $\gamma\alpha$, and $\alpha+\beta$ are nilpotent. For the latter, first observe that $\alpha+\beta$ cannot equal 1. Conclude that $\mathrm{Nil}(S)$ is the set of all nilpotent elements of S. In view of the preceding problem, this applies to $S = \mathrm{End}_R(V)$ if V is an indecomposable R-module with a composition series.

In the next two exercises let V be an R-module with a composition series and write

$$V = V_1 \dotplus V_2 \dotplus \cdots \dotplus V_n = V_1' \dotplus V_2' \dotplus \cdots \dotplus V_m'$$

with all V_i and V_j' indecomposable modules. Let $\pi_i: V \to V_i$, $\eta_i: V_i \to V$, $\pi_j': V \to V_j'$ and $\eta_j': V_j' \to V$ be the natural projections and injections.

6. For each $i = 1, 2, \ldots, n$ define $\alpha_i = \pi_1'\eta_i \in \mathrm{Hom}_R(V_i, V_1')$ and $\beta_i = \pi_i\eta_1' \in \mathrm{Hom}_R(V_1', V_i)$. Then $\alpha_i\beta_i \in \mathrm{End}_R(V_1')$ and note that $1 = \sum_{i=1}^n \alpha_i\beta_i$. Since V_1' is indecomposable, deduce from the preceding problem that some $\alpha_i\beta_i$ is not nilpotent, say $\alpha_1\beta_1$. Now show that $\beta_1\alpha_1$ is a nonnilpotent endomorphism of V_1 and conclude that both $\alpha_1\beta_1$ and $\beta_1\alpha_1$ are automorphisms.
7. Continuing with the preceding notation, show that α_1 is an isomorphism with inverse $(\beta_1\alpha_1)^{-1}\beta_1 = \beta_1(\alpha_1\beta_1)^{-1}$ and conclude that $V_1 \cong V_1'$. Next, prove that $V = V_1 \dotplus V_2' \dotplus \cdots \dotplus V_m'$. To this end, note that α_1 maps $V_1 \cap (V_2' \dotplus \cdots \dotplus V_m')$ to zero and that π_1' maps $V_1 \dotplus V_2' \dotplus \cdots \dotplus V_m'$ onto V_1'. Finally, show by induction on the total number of summands that $n = m$ and that, by suitably relabeling the submodules, we have $V_i \cong V_i'$ for all i. This is the Krull-Schmidt Theorem.

8. Show that any primitive ring is prime. Conversely, if R is a prime ring with a minimal right ideal, prove that R is primitive. Give an example of a prime ring that is not primitive.
9. Prove that a prime Artinian ring is simple. Give an example of a primitive ring that is not simple. For this, let V be an infinite dimensional K-vector space and let R be a suitable subring of $\mathrm{End}_K(V)$.
10. Use the argument of the Hopkins-Levitzki Theorem to show that a ring is Artinian if and only if it is semiprimary and Noetherian.

7. Dedekind Domains

The goal here is to characterize the commutative integral domains that are hereditary. Specifically, we show that these rings are necessarily Dedekind domains and we precisely describe their ideal structure and their projective modules. For convenience, we assume throughout this chapter that R is a commutative integral domain and we let F denote its field of fractions.

DEFINITION If A is an ideal of R, define

$$A^{-1} = \{ q \in F \mid Aq \subseteq R \}$$

It is easy to see that A^{-1} is an R-submodule of F that contains R. Furthermore, $A \subseteq AA^{-1} \subseteq R$ and hence AA^{-1} is an ideal of R. When $AA^{-1} = R$, we say that A is *invertible*. Obviously, this occurs if and only if $1 \in AA^{-1}$ and hence if and only if $1 = \sum_{i=1}^{n} a_i q_i$ for suitable $a_i \in A$ and $q_i \in A^{-1}$.

LEMMA 7.1 *Let A be a nonzero ideal of R.*

i. If either A is invertible or R is Noetherian, then both A and A^{-1} are finitely generated R-modules.

ii. There is an abelian group isomorphism $\theta: A^{-1} \to \mathrm{Hom}_R(A, R)$ given by $\theta(q)a = qa$ for all $q \in A^{-1}$ and $a \in A$.

PROOF (i) Suppose first that A is invertible and let $a_i \in A$ and $q_i \in A^{-1}$ be given with $1 = \sum_{i=1}^{n} a_i q_i$. If $a \in A$, then

$$a = \sum_{i=1}^{n} a_i (q_i a) \in \sum_{i=1}^{n} a_i R$$

and if $q \in A^{-1}$, then

$$q = \sum_{i=1}^{n} (qa_i)q_i \in \sum_{i=1}^{n} Rq_i$$

Thus $A = \sum_i a_i R$ and $A^{-1} = \sum_i q_i R$.

Now let R be Noetherian so that, of course, the ideal A is finitely generated. Furthermore, if $0 \neq a \in A$, then $aA^{-1} \subseteq R$, so $A^{-1} \subseteq a^{-1}R$. But $a^{-1}R$ is a cyclic R-module and A^{-1} is a submodule, so Lemma 6.6 implies that A^{-1} is also finitely generated.

(ii) Since $A^{-1}A \subseteq R$, it follows that $\theta: A^{-1} \to \mathrm{Hom}_R(A, R)$, as described previously, is indeed a homomorphism of abelian groups. Furthermore, θ is one-to-one, since $\theta(q) = 0$ implies that $qA = 0$. Finally, let $\lambda \in \mathrm{Hom}_R(A, R)$ and let $a, b \in A \setminus 0$. Then

$$\lambda(a)b = \lambda(ab) = \lambda(ba) = \lambda(b)a$$

so $\lambda(a)/a = \lambda(b)/b$. Thus $\lambda(a)/a$ is constant for all $0 \neq a \in A$ and we denote this common fraction by $q \in F$. In other words, $\lambda(a) = qa$ for all $a \in A$, including $a = 0$. It follows that $qA = \lambda(A) \subseteq R$, so $q \in A^{-1}$ and, since $\theta(q) = \lambda$, we conclude that θ is onto. □

PROPOSITION 7.2 *Let $0 \neq A \triangleleft R$. Then A_R is projective if and only if A is invertible. In particular, R is a hereditary ring if and only if all its nonzero ideals are invertible.*

PROOF Suppose first that A is invertible and say $1 = \sum_{i=1}^{n} a_i q_i$ for suitable $a_i \in A$ and $q_i \in A^{-1}$. If V is a free R-module of rank n with basis $\{v_1, v_2, \ldots, v_n\}$, then we define $\pi: V \to A$ by $\pi: v_i \mapsto a_i$. Furthermore, we let $\alpha: A \to V$ be given by $\alpha: a \to \sum_{i=1}^{n} v_i(aq_i)$. Then, for all $a \in A$, we have

$$\pi\alpha(a) = \pi\Big(\sum_{i=1}^{n} v_i(aq_i)\Big) = a\sum_{i=1}^{n} a_i q_i = a$$

and thus $\pi\alpha = 1_A$. It follows that A is isomorphic to a direct summand of V and hence that A_R is projective.

Conversely, let A_R be projective and let W be a free R-module with $W = A \dot{+} U$. Suppose W has basis $\{w_j \mid j \in \mathcal{J}\}$ and, for each $a \in A$, let us write $a = \sum_j w_j \lambda_j(a)$, where $\lambda_j(a) \in R$. Obviously, $\lambda_j \in \mathrm{Hom}_R(A, R)$, so the preceding lemma implies that there exists $f_j \in A^{-1}$ with $\lambda_j(a) = f_j a$. In other words, $a = \sum_j w_j(f_j a)$.

Now fix $0 \neq b \in A$. Since b has only finitely many nonzero w_j-components, it follows that $f_j b = 0$ for almost all j and hence that $f_j = 0$ for almost all j. In particular, if $f_1, f_2, \ldots, f_n$ are the finitely many nonzero f_j's, then $b = \sum_{j=1}^{n} w_j(f_j b)$. Finally, if $w_j = b_j \dot{+} u_j \in A \dot{+} U$, then projecting to the A summand yields $b = \sum_{i=1}^{n} b_j(f_j b)$, an equation in $A \subseteq F$. We can therefore cancel the $b \neq 0$ factor here to obtain $1 = \sum_{i=1}^{n} b_j f_j$ and we conclude that A is invertible.

Finally, since the zero ideal is always a projective R-module, the last statement of the proposition is clear. □

DEFINITION Let $S \supseteq R$ be commutative integral domains. An element $s \in S$ is *integral* over R if s is the root of a monic polynomial in $R[x]$. Obviously, this occurs if and only if there exist elements $r_0, r_1, \ldots, r_{n-1} \in R$ with $s^n = r_0 + r_1 s + \cdots + r_{n-1} s^{n-1}$. In particular, every element of R is integral over R and we say that R is *integrally closed* if these are the only elements of the field of fractions F which are integral over R.

Again let R be a commutative integral domain. Then R is a *Dedekind domain* if and only if

1. R is Noetherian,
2. R is integrally closed, and
3. All nonzero prime ideals of R are maximal.

The following lemma yields one direction of the characterization of hereditary domains.

LEMMA 7.3 *If R is a hereditary domain, then R is a Dedekind domain.*

PROOF Note that all nonzero ideals of R are invertible by Proposition 7.2. It is necessary to show that R satisfies conditions (1), (2), and (3) of the preceding definition.

(1) This follows from Lemma 7.1(i).

(2) Let $q \in F$ be integral over R and say $q^n = \sum_{i=0}^{n-1} q^i r_i$ with $r_i \in R$. Set $X = \sum_{i=0}^{n-1} q^i R$ so that X is an R-submodule of F containing q and observe that the formula for q^n implies that $X^2 = X$. Furthermore, by taking a common denominator for the finitely many generators of X, we see that there exists $0 \neq A \lhd R$ with $XA \subseteq R$. Note that $B = XA$ is a nonzero ideal of R and that $B^2 = X^2A^2 = XA^2 = BA$. Thus, since $BB^{-1} = R$, multiplying the latter equation by B^{-1} yields $B = A$. In particular, $A = B = XA$, so multiplying by A^{-1} yields $X = R$ and therefore $q \in R$ as required.

(3) Let P be a nonzero prime ideal of R and let $I \lhd R$ with $P \subset I$. Then $P \subseteq PI^{-1} \subseteq II^{-1} = R$, so $PI^{-1} \lhd R$. Furthermore, $(PI^{-1})I \subseteq P$.

Thus, since P is a prime ideal and $P \subset I$, it follows that $PI^{-1} \subseteq P$ and therefore that $PI^{-1} = P$. Finally, multiplying this equation by IP^{-1} yields $I = R$ and thus P is indeed a maximal ideal. □

We can now complete the characterization.

THEOREM 7.4 *Let R be a commutative integral domain. Then R is a hereditary ring if and only if it is a Dedekind domain. Furthermore, when this occurs, then every nonzero ideal of R is uniquely a finite product of prime ideals.*

PROOF In view of the preceding lemma, it suffices to assume that R is a Dedekind domain. The goal is to show, by Proposition 7.2, that all nonzero ideals of R are invertible and that each is a unique product of primes. We proceed in a series of steps.

STEP 1 *If $P \neq 0$ is a prime ideal of R, then $P^{-1} \supset R$.*

PROOF Let $0 \neq a \in P$. Then, since R is Noetherian, Proposition 6.7 implies that there exist finitely many nonzero prime ideals P_i with $aR \supseteq P_1P_2 \cdots P_n$ and assume that n is minimal with this property. Since $P \supseteq P_1P_2 \cdots P_n$ and P is prime, we must have $P \supseteq P_i$ for some i, say $P \supseteq P_n$, and since P_n is a maximal ideal, it follows that $P = P_n$. Now the minimality of n implies that $P_1P_2 \cdots P_{n-1} \not\subseteq aR$, so there exists b in $P_1P_2 \cdots P_{n-1} \setminus aR$. Notice that $bP \subseteq P_1P_2 \cdots P_n \subseteq aR$ and thus $b/a \in P^{-1}$. On the other hand, $b/a \notin R$, since $b \notin aR$. □

STEP 2 *If P is a nonzero prime ideal of R, then P is invertible.*

PROOF If P is not invertible, then $P \subseteq PP^{-1} \subset R$; hence, since P is maximal, we have $P = PP^{-1}$. It follows that $P(P^{-1})^i = P$ for all $i \geq 0$. Now let $0 \neq a \in P$ and, by Step 1, choose $q \in P^{-1} \setminus R$. Then $aq^i \in P(P^{-1})^i \subseteq R$, so $\sum_{i=0}^{\infty} aq^iR$ is an ideal of R. The Noetherian property now implies that this ideal is finitely generated, say by $aq^0, aq^1, \ldots, aq^{n-1}$. Thus $aq^n = \sum_{i=0}^{n-1} aq^i r_i$ for suitable $r_i \in R$ and, since $a \neq 0$, it follows that q is integral over R. But R is integrally closed, so this implies that $q \in R$, a contradiction. □

STEP 3 *Every nonzero ideal of R is a finite product of prime ideals.*

PROOF Let $0 \neq A \lhd R$. By Proposition 6.7, we know at least that $A \supseteq P_1P_2 \cdots P_n$, a finite product of nonzero prime ideals. Assume n is chosen minimal and proceed by induction on n. If $n = 0$, then $A = R$ is an empty product of primes. Now let $n \geq 1$. Since $A \neq R$, there exists a prime ideal P of R with $P \supseteq A$. Thus $P \supseteq P_1P_2 \cdots P_n$, so P contains

some P_i, say $P \supseteq P_n$. But P_n is maximal, so $P = P_n$ and multiplying by P^{-1} yields

$$R = PP^{-1} \supseteq AP^{-1} \supseteq P_1P_2 \cdots P_{n-1}$$

Thus $AP^{-1} \lhd R$ has parameter smaller than n, so $AP^{-1} = Q_1Q_2 \cdots Q_r$ for suitable prime ideals Q_j and therefore multiplying by P yields a similar formula for A. □

STEP 4 *Completion of the proof.*

PROOF We first show that each nonzero ideal is uniquely a product of primes. To this end, suppose

$$P_1P_2 \cdots P_n = Q_1Q_2 \cdots Q_m$$

are appropriate products and say $n \geq 1$. Then $P_1 \supseteq Q_1Q_2 \cdots Q_m$, so we may suppose $P_1 \supseteq Q_1$. But again, Q_1 is maximal, so $P_1 = Q_1$ and therefore multiplying by $P_1^{-1} = Q_1^{-1}$ yields a shorter relation. Continuing in this manner, we clearly obtain the appropriate uniqueness result.

Finally, if $A = T_1T_2 \cdots T_r$ is written as a product of nonzero primes, set $B = T_r^{-1} \cdots T_2^{-1}T_1^{-1}$. Then $AB = R$, so $B \subseteq A^{-1}$ and $AA^{-1} = R$. In fact, it follows that $B = A^{-1}$, since $AB = R$ now yields $B = A^{-1}(AB) = A^{-1}R = A^{-1}$. □

DEFINITION Let R be a Dedekind domain with field of fractions F. Then any finitely generated R-submodule of F is called a *fractional ideal* of R. In particular, if $0 \neq A \lhd R$, then Lemma 7.1(i) implies that both A and A^{-1} are fractional ideals. It is clear that the set of all fractional ideals of R is closed under multiplication. Furthermore, if A is as before, then the usual exponent laws are satisfied when we define $A^0 = R$ and $A^{-n} = (A^{-1})^n$ for $n \geq 1$. We remark that in this context, ordinary ideals of R are also called *integral ideals*.

COROLLARY 7.5 *Let R be a Dedekind domain. Then the set of nonzero fractional ideals of R is a group under multiplication. Furthermore, every such fractional ideal I is uniquely a finite product $I = P_1^{e_1}P_2^{e_2} \cdots P_n^{e_n}$, with $P_1, P_2, \ldots, P_n$ distinct nonzero prime ideals of R.*

PROOF In view of the preceding remarks, the set $\mathcal{F}$ of nonzero fractional ideals of R is closed under multiplication. Furthermore, if I is such a nonzero ideal, then by taking a common denominator for its finitely many generators, we see that there exists $0 \neq A \lhd R$ with $AI = B \lhd R$. Thus

$I = BA^{-1}$ and I has the multiplicative inverse $I^{-1} = AB^{-1}$. It follows that $\mathcal{F}$ is a group and Theorem 7.4 quickly yields the result. □

If A is a fractional ideal of R and if $0 \neq q \in F$, then qA is also a fractional ideal. Furthermore, as R-modules we have $(qA)_R \cong A_R$. The structure of the projective R-modules is based on:

LEMMA 7.6 *Let R be a Dedekind domain.*

i. If A and B are nonzero fractional ideals of R, then $A \oplus B \cong R \oplus AB$ as R-modules.

ii. If $A_1, A_2, \ldots, A_n$ and $B_1, B_2, \ldots, B_m$ are nonzero fractional ideals of R, then

$$A_1 \oplus A_2 \oplus \cdots \oplus A_n \cong B_1 \oplus B_2 \oplus \cdots \oplus B_m$$

if and only if $n = m$ and $\prod_i A_i = q \cdot \prod_j B_j$ for some $0 \neq q \in F$.

PROOF (i) Let $0 \neq \tilde{a} \in A^{-1}$ and $0 \neq \tilde{b} \in B^{-1}$. Then $\tilde{A} = \tilde{a}A \lhd R$ and $\tilde{B} = \tilde{b}B \lhd R$. Furthermore, $\tilde{A}_R \cong A_R$, $\tilde{B}_R \cong B_R$, and $(\tilde{A}\tilde{B})_R \cong (AB)_R$. Thus, without loss of generality, we can assume that A and B are integral ideals. Observe that if $A + B = R$, then Lemma 6.8(i)(ii) implies that $A \oplus B \cong R \oplus AB$.

We now proceed by induction on the number k of prime factors of A. If $k = 0$, then $A = R$ and $A + B = R$. Next suppose $k = 1$, so that A is a prime ideal of R and hence a maximal ideal. Since $B^{-1}B = R$, there exists $q \in B^{-1}$ with $qB \not\subseteq A$. Thus $qB \lhd R$ and $A + qB = R$, so $A \oplus qB \cong R \oplus qAB$. But $qB \cong B$ and $qAB \cong AB$, so this case is proved.

Finally, let k be arbitrary. Again, if $A + B = R$, we are done, so it suffices to assume that $A + B \subseteq P$ for some prime ideal P. Then $A = A'P$ and $B = B'P$, where $A' = AP^{-1} \lhd R$ and $B' = BP^{-1}$. Since A' has parameter $k - 1$, induction implies that $A' \oplus B' \cong R \oplus A'B'$ and thus Lemma 6.8(iii) yields

$$A \oplus B = (A' \oplus B')P \cong (R \oplus A'B')P = P \oplus AB'$$

But P is prime, so the $k = 1$ case yields

$$P \oplus AB' \cong R \oplus AB'P = R \oplus AB$$

and the result follows.

(ii) Set $A = \prod_i A_i$ and $B = \prod_j B_j$. Then it follows from (i), by induction on n, that

$$A_1 \oplus A_2 \oplus \cdots \oplus A_n \cong R \oplus \cdots \oplus R \oplus A = R^{n-1} \oplus A$$

and similarly

$$B_1 \oplus B_2 \oplus \cdots \oplus B_m \cong R \oplus \cdots \oplus R \oplus B = R^{m-1} \oplus B$$

Thus $n = m$ and $A = qB$ clearly implies that the two direct sums are isomorphic. The converse follows directly from Lemma 6.9. □

It is now a simple matter to prove:

THEOREM 7.7 *Let R be a Dedekind domain and let V be a nonzero projective R-module.*

i. If V is finitely generated, then

$$V \cong R \oplus \cdots \oplus R \oplus A = R^{n-1} \oplus A$$

for some $n \geq 1$ and $0 \neq A \triangleleft R$. Furthermore, n is uniquely determined by V and A is determined up to multiplication by a nonzero constant in the field of fractions of R.

ii. If V is not finitely generated, then V is a free R-module of unique rank.

PROOF Since R is hereditary, it follows from Theorem 6.3 that V is isomorphic to a direct sum of nonzero ideals of R. Suppose first that this sum is finite so that V is finitely generated. Then by Lemma 7.6(i),

$$V \cong R \oplus \cdots \oplus R \oplus A = R^{n-1} \oplus A$$

for some nonzero ideal A of R. Furthermore, Lemma 7.6(ii) implies that n and A are suitably determined by V.

Now suppose the sum is infinite, so that V is clearly not finitely generated. By suitably grouping the summands, we see that it suffices to prove that any countably infinite direct sum of nonzero ideals is free. To this end, let

$$W = A_1 \oplus B_1 \oplus A_2 \oplus B_2 \oplus A_3 \oplus \cdots$$

be such a direct sum. If $C_n = \prod_{i=1}^{n} A_i B_i$ with $C_0 = R$, then $A_n B_n = C_{n-1}^{-1} C_n$, so $A_n \oplus B_n \cong C_{n-1}^{-1} \oplus C_n$ by Lemma 7.6(ii). Thus

$$W \cong C_0^{-1} \oplus C_1 \oplus C_1^{-1} \oplus C_2 \oplus C_2^{-1} \oplus \cdots$$

and, since $C_n \oplus C_n^{-1} \cong R \oplus R$, we conclude that W is indeed free. The uniqueness of the infinite rank of V follows from Lemma 2.3(iii). □

Finally, we remark that the definition of Dedekind domain is sufficiently concrete to yield the following key result. Since the proof of this theorem requires a certain amount of field theory, we merely sketch it here. However, some of the necessary background information is contained in the exercises.

THEOREM 7.8 *Let R be a Dedekind domain with field of fractions F and let K be a finite degree separable field extension of F. If S is the set of elements of K that are integral over R, then S is a Dedekind domain.*

PROOF To start with, we know at least that S is a subring of K, having K as its field of fractions. Indeed, if $\alpha \in K$, then there exists $0 \neq r \in R$ with $r\alpha \in S$. Furthermore, $S \cap F = R$, since R is integrally closed. It remains to verify conditions (1), (2), and (3) of the definition of a Dedekind domain.

(1) In view of the preceding remarks, we can let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be an F-basis for K with each $\alpha_i \in S$. Notice that multiplication by any $\beta \in K$ determines an F-linear transformation of the F-vector space K. We can therefore let $\operatorname{tr}\beta$ denote the trace of this linear transformation. In other words, if $\beta\alpha_i = \sum_{j=1}^{n} f_{i,j}\alpha_j$ with $f_{i,j} \in F$, then $\operatorname{tr}\beta = \sum_{i=1}^{n} f_{i,i}$. Clearly, $\operatorname{tr}: K \to F$ is an F-linear functional and it is not hard to see that if $\beta \in S$, then $\operatorname{tr}\beta \in S \cap F = R$. Furthermore, since F/K is separable, we know that the $n \times n$ matrix $(\operatorname{tr}\alpha_i\alpha_j)$ is nonsingular.

Let $s \in S$ and write $s = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$ with $c_i \in F$. Then for all $j = 1, 2, \ldots, n$ we have

$$\operatorname{tr} s\alpha_j = c_1 \operatorname{tr}\alpha_1\alpha_j + c_2 \operatorname{tr}\alpha_2\alpha_j + \cdots + c_n \operatorname{tr}\alpha_n\alpha_j$$

a system of n linear equations in the n unknowns $c_1, c_2, \ldots, c_n$. Note that $d = \det(\operatorname{tr}\alpha_i\alpha_j) \neq 0$, so this system can be solved by Cramer's Rule. In particular, since the terms $\operatorname{tr} s\alpha_j$ and $\operatorname{tr}\alpha_i\alpha_j$ are all contained in R, we conclude that each $c_i \in d^{-1}R$ and thus that

$$S \subseteq d^{-1}\alpha_1 R + d^{-1}\alpha_2 R + \cdots + d^{-1}\alpha_n R$$

But R is a Noetherian ring and the preceding right-hand side is a finitely generated R-module. Thus Lemma 6.6 implies that S_R is a Noetherian R-module; since any ideal of S is a submodule of S_R, we conclude that S is a Noetherian ring.

(2) Since integrality is transitive, it follows that any $\alpha \in K$ that is integral over S must also be integral over R. Thus $\alpha \in S$ and S is integrally closed.

(3) Finally, let P be a nonzero prime ideal of S and let s be a nonzero element of P. Then s is integral over R and say $s^j = r_0 + r_1 s + \cdots + r_{j-1}s^{j-1}$ with $r_i \in R$. Furthermore, since S is a domain and $s \neq 0$, we can clearly assume that $r_0 \neq 0$. But $r_0 \in R \cap P$ and therefore $Q = R \cap P \neq 0$. Now R/Q embeds in the integral domain S/P. Thus Q is a prime ideal of R and, since it is nonzero, Q is maximal and R/Q is a field. Moreover, S is a finitely generated R-module, so S/P is a finitely generated module over the field R/Q. Thus since S/P is an integral domain, it follows that S/P is a field and hence that P is a maximal ideal of S. This completes the proof. □

Recall that any principal ideal domain is a hereditary ring and hence a Dedekind domain. Thus, in the Theorem 7.8, we can certainly take R to be the ring of integers or perhaps $R = F_0[t]$, the polynomial ring in one variable over a field F_0.

EXERCISES

1. A ring R is said to be *semihereditary* if every finitely generated right ideal of R is projective. Show that, over such a ring, any finitely generated submodule of a free module is projective.

   In the following three problems, R is a Dedekind domain with field of fractions F. Furthermore, we assume that $A = P_1^{a_1}P_2^{a_2}\cdots P_k^{a_k}$ and $B = P_1^{b_1}P_2^{b_2}\cdots P_k^{b_k}$ are nonzero ideals of R with $P_1, P_2, \ldots, P_k$ distinct primes of R.

2. If V is a finitely generated R-submodule of $F^n = F \oplus F \oplus \cdots \oplus F$, prove that V is projective. Show that F_R is projective if and only if $F = R$.
3. Prove that $A + B = \prod_{i=1}^k P_i^{\min(a_i,b_i)}$ and $A \cap B = \prod_{i=1}^k P_i^{\max(a_i,b_i)}$.
4. Now suppose $A \supsetneq B$ and, for each $i = 1, 2, \ldots, k$, choose an element $\alpha_i \in P_i^{a_i} \setminus P_i^{a_i+1}$. Use the Chinese Remainder Theorem (Exercise 3.3) to find $\alpha \in R$ with $\alpha \equiv \alpha_i \bmod P_i^{a_i+1}$ for all i and then prove that $A = B + \alpha R$. Conclude that if I is any nonzero ideal of R and if $0 \neq \sigma \in I$, then there exists $\tau \in I$ with $I = \sigma R + \tau R$.

   In the next two exercises, $\mathbb{Z}$ denotes the ring of integers and $\mathbb{Q}$ the field of rationals. In addition, $d \in \mathbb{Z}$ is a square free integer.

5. Let R be the ring of all elements of $\mathbb{Q}[\sqrt{d}]$ that are integral over $\mathbb{Z}$. Show that $R = \mathbb{Z}[\sqrt{d}]$ if $d \equiv 2, 3 \bmod 4$ and that $R = \mathbb{Z}[(1 + \sqrt{d})/2]$

if $d \equiv 1 \bmod 4$. If $d \equiv 1 \bmod 4$, find a nonzero, noninvertible ideal in the ring $\mathbb{Z}[\sqrt{d}]$.

6. Now let R be the Dedekind domain $\mathbb{Z}[\sqrt{-5}]$. Show that the norm map $N: R \to \mathbb{Z}$ given by $N(a+b\sqrt{-5}) = a^2+5b^2$ is multiplicative. Use this to prove that the only units in R are ± 1 and that the elements 2, 3, $1 \pm \sqrt{-5}$ are all irreducible, that is they have no proper factorizations. Since $2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$, conclude that R is not a unique factorization domain and hence not a principal ideal domain.

In the remaining problems, let $K \supseteq F$ be a finite extension of fields.

7. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be an F-basis for K. Prove that the $n \times n$ matrix $(\operatorname{tr} \alpha_i \alpha_j)$ is singular if and only if $\operatorname{tr} K = 0$. To this end, observe that if the matrix is singular, then there exist $f_1, f_2, \ldots, f_n \in F$, not all zero, with $\sum_i f_i \cdot \operatorname{tr} \alpha_i \alpha_j = 0$ for all j. In particular, if $\beta = \sum_i f_i \alpha_i$, then $\operatorname{tr} \beta K = 0$. Find an example where $\operatorname{tr} K = 0$. Obviously this can occur only in characteristic $p > 0$.
8. Now suppose that K/F is separable so that, by the Primitive Element Theorem, $K = F[\theta]$. Show that the characteristic polynomial for the F-linear transformation θ is the same as the minimal polynomial for θ over F and observe that this polynomial has distinct roots $\theta_1, \theta_2, \ldots, \theta_n$ in an algebraic closure $\bar{K}$ of K. Conclude that $\operatorname{tr} \theta^i = \theta_1^i + \theta_2^i + \cdots + \theta_n^i$ for all $i \geq 0$ and hence that $\operatorname{tr} \theta^j \neq 0$ for some $j \geq 0$. Thus $\operatorname{tr} K \neq 0$.
9. Let R be a subring of F having F as its field of fractions and let S be the subring of K consisting of those elements that are integral over R. If $\alpha \in K$, show that there exists $0 \neq r \in R$ with $r\alpha \in S$. If $\beta \in S$, show that all roots of its minimal polynomial over F are integral over R. Conclude that $\operatorname{tr} \beta$ is integral over R.
10. In the preceding, let R be a principal ideal domain. Show that S is a free R-module and that any basis $\{s_1, s_2, \ldots, s_n\}$ for S over R is also a basis for K over F. Prove that $\det(\operatorname{tr} s_i s_j)$ is, up to a unit in R, independent of the choice of basis.

8. Projective Dimension

It is finally time to understand the relationship between Wedderburn rings and hereditary rings. For this, it is first necessary to define the projective dimension of a module and the global dimension of a ring. We then show that Wedderburn rings are precisely the rings of global dimension 0 and that those hereditary rings that are not Wedderburn are precisely the rings of global dimension 1. We begin with a key observation.

LEMMA 8.1 (Schanuel's Lemma) *Let R be a ring and let*

$$0 \to B \to P \xrightarrow{\beta} A \to 0$$

$$0 \to B' \to P' \xrightarrow{\beta'} A \to 0$$

be short exact sequences of R-modules with P and P' projective. Then $B \oplus P' \cong B' \oplus P$.

PROOF Let W be the R-submodule of $P \oplus P'$ given by $W = \{ p \oplus p' \mid \beta p = \beta' p' \}$. Then it is easy to see that the projection map $\pi: W \to P$ is onto. Indeed, if $p \in P$, then, since β' is onto, there exists $p' \in P'$ with $\beta' p' = \beta p$. Thus $p \oplus p' \in W$ and $p = \pi(p \oplus p')$. Now P is projective, so the epimorphism $\pi: W \to P$ must split and therefore $W \cong \mathrm{Ker}(\pi) \oplus P$. But

$$\mathrm{Ker}(\pi) = \{ 0 \oplus p' \mid \beta' p' = 0 \} \cong \mathrm{Ker}(\beta') \cong B'$$

and thus $W \cong B' \oplus P$. Similarly, $W \cong B \oplus P'$. □

This motivates the following:

DEFINITION Let A and A' be R-modules. We write $A \sim A'$ if and only if there exist projective R-modules P and P' with $A \oplus P \cong A' \oplus P'$. Obviously $\sim$ is an equivalence relation. Indeed, if $A \sim B$ and $B \sim C$, then $A \oplus P \cong B \oplus P'$ and $B \oplus Q \cong C \oplus Q'$ for suitable projective modules P, P', Q, Q'. Thus

$$\begin{aligned} A \oplus (P \oplus Q) &\cong B \oplus P' \oplus Q \\ &\cong B \oplus Q \oplus P' \cong C \oplus (Q' \oplus P') \end{aligned}$$

and $A \sim C$. We use $[A]$ to denote the equivalence class of A. Since any direct summand of a projective module is projective, it follows that $[0]$ is precisely the set of all projective R-modules.

We need a slight refinement of Schanuel's Lemma.

LEMMA 8.2 *Suppose we are given short exact sequences*

$$0 \to B \to P \to A \to 0$$
$$0 \to B' \to P' \to A' \to 0$$

with P and P' projective. If $A \sim A'$, then $B \sim B'$.

PROOF Since $A \sim A'$, we have $A \oplus Q \cong A' \oplus Q'$ for suitable projective modules Q and Q'. Furthermore, we then have the exact sequences

$$0 \to B \oplus 0 \to P \oplus Q \to A \oplus Q \to 0$$
$$0 \to B' \oplus 0 \to P' \oplus Q' \to A' \oplus Q' \to 0$$

But $A \oplus Q \cong A' \oplus Q'$, so $B \oplus (P' \oplus Q') \cong B' \oplus (P \oplus Q)$ by Lemma 8.1 and hence $B \sim B'$ as required. □

DEFINITION Let A be any R-module. By Lemma 2.9(i), there exists a short exact sequence $0 \to B \to P \to A \to 0$ with P projective and we define the *kernel map* $\mathcal{K}$ by $\mathcal{K}\colon [A] \mapsto [B]$. In view of the preceding lemma, $\mathcal{K}$ is a well-defined map on the $\sim$ equivalence classes of R-modules. That is, $\mathcal{K}$ is independent of the representative of the class and of the particular exact sequence chosen. Since $0 \to 0 \to 0 \to 0 \to 0$ is exact, we have $\mathcal{K}[0] = [0]$.

The *projective dimension* of A, written $\operatorname{pd}_R A = \operatorname{pd} A$, is defined to be the minimal integer n with $\mathcal{K}^n[A] = [0]$. Of course, if no such integer exists, then $\operatorname{pd} A = \infty$. Modules with finite projective dimension are in some sense "close to" the projective modules. For example, $\operatorname{pd} A = 0$ if and only if A is projective.

Suppose $0 \to B \to P \to A \to 0$ is exact and that P is projective. Then $\mathcal{K}^n[A] = \mathcal{K}^{n-1}[B]$ for all $n \geq 1$. Furthermore, if A is projective, then the sequence splits so $B \mid P$ and B is projective. We conclude therefore that

1. $\operatorname{pd} A = \infty$ if and only if $\operatorname{pd} B = \infty$,
2. $\operatorname{pd} A = 0$ implies $\operatorname{pd} B = 0$, and
3. $\operatorname{pd} A = n > 0$ implies $\operatorname{pd} B = n - 1$.

Finally, the (right) *global dimension* of R is defined to be the supremum of the projective dimensions of all right R-modules. Thus $\operatorname{gl\,dim} R$ is either an integer or the symbol ∞. As promised, we now prove:

LEMMA 8.3 *If R is a ring, then*

i. $\operatorname{gl\,dim} R = 0$ *if and only if R is Wedderburn, and*

ii. $\operatorname{gl\,dim} R = 1$ *if and only if R is hereditary but not Wedderburn.*

PROOF (i) By definition, R has global dimension 0 if and only if $\operatorname{pd} A = 0$ for all A_R. This means that all R-modules are projective and hence, by Theorem 3.9, that R is a Wedderburn ring.

(ii) Now suppose that $\operatorname{gl\,dim} R = 1$. If I is a right ideal of R, then the exact sequence $0 \to I \to R \to R/I \to 0$ implies that $\mathcal{K}[R/I] = [I]$. But $\operatorname{pd} R/I \leq \operatorname{gl\,dim} R = 1$, so it follows that $\operatorname{pd} I = 0$. In other words, all right ideals of R are projective and therefore R is a hereditary ring.

Conversely, let R be hereditary. If A is an R-module, map a free module F onto A to obtain $0 \to B \to F \to A \to 0$. But Theorem 6.3 implies that $B \subseteq F$ is projective, so $\mathcal{K}[A] = [B] = [0]$. Thus $\operatorname{pd} A \leq 1$ and, since A is arbitrary, $\operatorname{gl\,dim} R \leq 1$. Part (i) now yields the result. □

In the remainder of this chapter, we obtain some basic properties of projective dimension. To start with, we have:

LEMMA 8.4 *Let $\{A_i \mid i \in \mathcal{I}\}$ be a collection of R-modules and set $A = \oplus \sum_{i \in \mathcal{I}} A_i$. Then* $\operatorname{pd} A = \sup\{\operatorname{pd} A_i \mid i \in \mathcal{I}\}$.

PROOF For each $i \in \mathcal{I}$, let $A_i^0 = A_i$ and then define A_i^j and the projective modules P_i^j inductively so that the sequences

$$0 \to A_i^{j+1} \to P_i^j \to A_i^j \to 0$$

are exact. If $A^j = \oplus \sum_i A_i^j$ and $P^j = \oplus \sum_i P_i^j$, then P^j is a projective R-module and the sequences

$$0 \to A^{j+1} \to P^j \to A^j \to 0$$

are exact. Since $A = A^0$, it follows that $\mathcal{K}^n[A_i] = [A_i^n]$ and $\mathcal{K}^n[A] = [A^n]$.

Finally, fix any integer $n \geq 0$. If $\operatorname{pd} A_i \leq n$ for all i, then each A_i^n is projective. Thus $A^n = \oplus \sum_i A_i^n$ is projective and $\operatorname{pd} A \leq n$. Conversely, if $\operatorname{pd} A \leq n$, then A^n is projective. But $A_i^n \mid A^n$, so each A_i^n is projective and we conclude that $\operatorname{pd} A_i \leq n$ for all $i \in \mathcal{I}$. □

As a consequence, we see that R has infinite global dimension if and only if $\operatorname{pd} A = \infty$ for some R-module A. The next lemma offers a simple way to construct such modules. Let V be an R-module and let $v \in V$. As usual, the *right annihilator* of v in R is given by

$$\operatorname{r.ann}_R(v) = \operatorname{r.ann}(v) = \{ r \in R \mid vr = 0 \}$$

In particular, this applies with $V = R_R$.

LEMMA 8.5 *Suppose* $a, b \in R$ *satisfy* $\operatorname{r.ann}_R(a) = bR$ *and* $\operatorname{r.ann}_R(b) = aR$. *Then either* $\operatorname{pd} aR = \operatorname{pd} bR = \infty$ *or* $aR \oplus bR \cong R$ *and* $\operatorname{pd} aR = \operatorname{pd} bR = 0$.

PROOF The natural map $R \to aR$ given by $r \mapsto ar$ is clearly onto and has kernel $\operatorname{r.ann}(a) = bR$. Thus $0 \to bR \to R \to aR \to 0$ is exact and similarly, so is $0 \to aR \to R \to bR \to 0$. Since R is free, this implies that $\mathcal{K}[aR] = [bR]$ and $\mathcal{K}[bR] = [aR]$. Thus $\mathcal{K}^{2n}[aR] = [aR]$ and $\mathcal{K}^{2n+1}[aR] = [bR]$ for all integers $n \geq 0$. In particular, if $\operatorname{pd} aR < \infty$, then clearly $[aR] = [bR] = [0]$, so aR and bR are both projective. In this case, both exact sequences split, so we conclude that $R \cong aR \oplus bR$. □

For example, let K be a field and set $R = K[x]/(x^2)$ so that $R = K \dotplus K\bar{x}$ with $\bar{x}^2 = 0$. If $a = b = \bar{x}$, then $\operatorname{r.ann}(a) = bR$ and $\operatorname{r.ann}(b) = aR$. Furthermore, $R \ncong \bar{x}R \oplus \bar{x}R$, since $\bar{x}$ annihilates the right-hand module but not the left. Thus $\operatorname{pd} \bar{x}R = \infty$ and hence $\operatorname{gl\,dim} R = \infty$. Similarly, if $\mathbb{Z}$ is the ring of integers, we could take $R' = \mathbb{Z}/(a'b')$ for any $a', b' > 1$.

The following lemma allows us to shift from a given short exact sequence to another one involving modules of smaller projective dimension.

LEMMA 8.6 *Suppose* $0 \to A \to B \to C \to 0$ *is an exact sequence of* R*-modules. Then there exist modules* D, E, *and* P *with* P *projective and short exact sequences*

$$0 \to D \to P \to B \to 0$$
$$0 \to E \to P \to C \to 0$$
$$0 \to D \to E \to A \to 0$$

In particular, $\mathcal{K}[B] = [D]$ *and* $\mathcal{K}[C] = [E]$. *Furthermore, if* R *is Noetherian and* B *is finitely generated, then we can take* D, E, *and* P *to be finitely generated.*

PROOF We can assume that $A \subseteq B$. Map a projective module P onto B to obtain $0 \to D \to P \to B \to 0$. It follows that if E is the preimage of $A \subseteq B$, then $0 \to D \to E \to A \to 0$ is also exact. But the kernel of the combined epimorphism $P \to B \to C$ is clearly equal to E and thus we have $0 \to E \to P \to C \to 0$.

Finally, suppose R is Noetherian and B is finitely generated. Then we can surely take P to be a finitely generated projective R-module. Since $D \subseteq E \subseteq P$, we conclude from Lemma 6.6 that both D and E are also finitely generated. □

The following lemma is crucial.

LEMMA 8.7 *Given the exact sequence* $0 \to A \to B \to C \to 0$. *If any two of these modules have finite projective dimension, then so does the third and*

$$\operatorname{pd} A \leq \max\{\operatorname{pd} B, \operatorname{pd} C\}$$
$$\operatorname{pd} B \leq \max\{1 + \operatorname{pd} A, \operatorname{pd} C\}$$
$$\operatorname{pd} C \leq \max\{1 + \operatorname{pd} A, 1 + \operatorname{pd} B\}$$

Furthermore, if $\operatorname{pd} B = 1$ *and* $\operatorname{pd} C \geq 2$, *then* $\operatorname{pd} C = 1 + \operatorname{pd} A$.

PROOF Set $a = \operatorname{pd} A$, $b = \operatorname{pd} B$ and $c = \operatorname{pd} C$. For the first part, we proceed by induction on the sum of the two given finite dimensions. Suppose first that B is projective, so that $b = 0$ and $\mathcal{K}[C] = [A]$. Then clearly $a \leq c \leq a + 1$ and the result follows in this case. Next, if C is projective, then $c = 0$ and the sequence splits. Thus $B \cong A \oplus C$, so $B \sim A$ and $b = a$. Again, the necessary inequalities are satisfied.

Thus it suffices to assume that neither B nor C is projective. Choose D, E, and P as in the preceding lemma so that

$$0 \to D \to P \to B \to 0$$
$$0 \to E \to P \to C \to 0$$
$$0 \to D \to E \to A \to 0$$

are exact. Since $b, c \neq 0$, we have $d = \operatorname{pd} D = b - 1$ and $e = \operatorname{pd} E = c - 1$. Thus in $0 \to D \to E \to A \to 0$, at least two of the projective dimensions are finite and these have lower sum than in the original sequence. We

therefore conclude by induction that the third projective dimension is also finite. Furthermore,

$$\begin{array}{lll} a \le \max\{1+d, 1+e\} & \Rightarrow & a \le \max\{b, c\} \\ e \le \max\{1+d, a\} & \Rightarrow & c \le \max\{1+b, 1+a\} \\ d \le \max\{e, a\} & \Rightarrow & b \le \max\{1+a, c\} \end{array}$$

so we obtain the required inequalities.

For the second part of the lemma, we now suppose that $b = 1$ and $c \ge 2$. In particular, B and C are not projective, so we obtain, as before, an exact sequence $0 \to D \to E \to A \to 0$ with $d = \operatorname{pd} D = b - 1 = 0$ and $e = \operatorname{pd} E = c - 1 \ge 1$. Note that A cannot be projective here. Otherwise, the latter sequence splits, so $E \cong A \oplus D$ and E is projective, a contradiction. Thus $a \ge 1$ and we can apply the preceding lemma again to obtain the short exact sequence $0 \to F \to G \to D \to 0$ with $f = \operatorname{pd} F = e - 1 = c - 2$ and $g = \operatorname{pd} G = a - 1$. But D is projective, so this sequence splits and $F \sim G$. Thus $f = g$ and therefore $c = a + 1$. □

As we see shortly in a more general context, the inequality for $\operatorname{pd} B$ can actually be sharpened to $\operatorname{pd} B \le \max\{\operatorname{pd} A, \operatorname{pd} C\}$.

LEMMA 8.8 *Let V be an R-module, let $\mathcal{I}$ be a well-ordered set, and let $\{V(\alpha) \mid \alpha \in \mathcal{I}\}$ be an increasing family of submodules of V with $\bigcup_\alpha V(\alpha) = V$. If $V(\alpha)^- = \bigcup_{\beta<\alpha} V(\beta)$, then*

$$\operatorname{pd} V \le \sup\{\operatorname{pd} V(\alpha)/V(\alpha)^- \mid \alpha \in \mathcal{I}\}$$

PROOF If the right-hand side is infinite, there is nothing to prove. Thus we can assume that $\sup\{\operatorname{pd} V(\alpha)/V(\alpha)^- \mid \alpha \in \mathcal{I}\} = n < \infty$ and we proceed by induction on n. If $n = 0$, then each $V(\alpha)/V(\alpha)^- = V'_\alpha$ is projective. It therefore follows from Lemma 6.1 that $V \cong \oplus \sum_\alpha V'_\alpha$ and hence V is projective. Thus $\operatorname{pd} V = 0$ as required.

Now assume that $n \ge 1$. For each α, choose a projective module Q_α and an epimorphism $Q_\alpha \to V(\alpha)$. Define $P = \oplus \sum_\alpha Q_\alpha$ so that P is projective and extend the above maps to an epimorphism

$$\pi: P = \oplus \sum_\alpha Q_\alpha \to \bigcup_\alpha V(\alpha) = V$$

Furthermore, for each $\alpha \in \mathcal{I}$, define $P(\alpha) = \oplus \sum_{\beta \le \alpha} Q_\beta$ so that π maps $P(\alpha)$ onto $V(\alpha)$. Thus, if

$$P(\alpha)^- = \bigcup_{\beta<\alpha} P(\beta) = \oplus \sum_{\beta<\alpha} Q_\beta$$

then π clearly maps $P(\alpha)^-$ onto $V(\alpha)^-$. Notice that $P(\alpha)/P(\alpha)^- \cong Q_\alpha$ is projective.

Set $W = \mathrm{Ker}(\pi)$ and, for each $\alpha \in \mathcal{I}$, define $W(\alpha) = W \cap P(\alpha)$. In this way, we obtain an increasing sequence of submodules of W with

$$\bigcup_\alpha W(\alpha) = W \cap \Big(\bigcup_\alpha P(\alpha)\Big) = W \cap P = W$$

Moreover, if $W(\alpha)^- = \bigcup_{\beta<\alpha} W(\beta)$, then we have

$$\begin{aligned} W(\alpha)^- &= \bigcup_{\beta<\alpha} W \cap P(\beta) \\ &= W \cap \Big(\bigcup_{\beta<\alpha} P(\beta)\Big) = W \cap P(\alpha)^- \end{aligned}$$

Now π_α, the restriction of π to $P(\alpha)$, maps $P(\alpha)$ onto $V(\alpha)$ and we consider the combined epimorphism

$$P(\alpha) \xrightarrow{\pi_\alpha} V(\alpha) \to V(\alpha)/V(\alpha)^-$$

Since $P(\alpha)^- \to 0$, this yields an epimorphism

$$P(\alpha)/P(\alpha)^- \xrightarrow{\phi_\alpha} V(\alpha)/V(\alpha)^- \to 0$$

and we compute the kernel of this map. To start with, $\mathrm{Ker}(\phi_\alpha) = L_\alpha/P(\alpha)^-$, where $L_\alpha = \pi_\alpha^{-1}\big(V(\alpha)^-\big)$. But note that $W(\alpha) + P(\alpha)^-$ contains $\mathrm{Ker}(\pi_\alpha)$ and maps onto $V(\alpha)^-$. Thus, by Lemma 1.8, $L = W(\alpha) + P(\alpha)^-$, so

$$\begin{aligned} \mathrm{Ker}(\phi_\alpha) &= \frac{W(\alpha) + P(\alpha)^-}{P(\alpha)^-} \cong \frac{W(\alpha)}{W(\alpha) \cap P(\alpha)^-} \\ &= \frac{W(\alpha)}{W \cap P(\alpha)^-} = \frac{W(\alpha)}{W(\alpha)^-} \end{aligned}$$

In particular, for each α, we have the short exact sequence

$$0 \to \frac{W(\alpha)}{W(\alpha)^-} \to \frac{P(\alpha)}{P(\alpha)^-} \xrightarrow{\phi_\alpha} \frac{V(\alpha)}{V(\alpha)^-} \to 0$$

Notice that $n \geq 1$, $\mathrm{pd}\, V(\alpha)/V(\alpha)^- \leq n$, and $P(\alpha)/P(\alpha)^- \cong Q_\alpha$ is projective. Thus $\mathrm{pd}\, W(\alpha)/W(\alpha)^- \leq n-1$ for all $\alpha \in \mathcal{I}$, and hence

induction implies that $\operatorname{pd} W \leq n-1$. But $0 \to W \to P \to V \to 0$ is exact and P is projective, so $\operatorname{pd} V \leq n$ as required. □

For convenience, let us record a special case of the preceding.

LEMMA 8.9 *If $0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_m = V$ is a finite series for the R-module V, then*

$$\operatorname{pd} V \leq \max\{\operatorname{pd} V_i/V_{i-1} \mid i = 1, 2, \ldots, m\}$$

We close with an interesting consequence of Lemma 8.8.

THEOREM 8.10 *The global dimension of any ring R is equal to the supremum of the projective dimensions of all cyclic R-modules. Furthermore, if R is Artinian, then $\operatorname{gl\,dim} R$ is equal to the largest of the projective dimensions of the finitely many irreducible R-modules.*

PROOF Since $\operatorname{gl\,dim} R \geq \operatorname{pd} W$ for all R-modules W, it suffices to bound $\operatorname{gl\,dim} R$ suitably. To this end, let V be any R-module and suppose V is generated by $\{v_\alpha \mid \alpha \in \mathcal{I}\}$. If we well-order $\mathcal{I}$ and define $V(\alpha) = \sum_{\beta \leq \alpha} v_\beta R$, then we obtain an increasing sequence of submodules whose union is all of V. Furthermore, for each α we have $V(\alpha) = v_\alpha R + V(\alpha)^-$, so $V(\alpha)/V(\alpha)^-$ is cyclic, generated by the image of v_α. But

$$\operatorname{pd} V \leq \sup\{\operatorname{pd} V(\alpha)/V(\alpha)^- \mid \alpha \in \mathcal{I}\}$$

by Lemma 8.8, and thus $\operatorname{pd} V$ is bounded above by the supremum of the projective dimensions of all cyclic R-modules. Since V is arbitrary, the same is true of $\operatorname{gl\,dim} R$.

Finally suppose R is Artinian. Then, by Theorem 5.6, any cyclic R-module V has a composition series. The result now follows from the preceding lemma since, by Proposition 5.5, R has only finitely many irreducible modules. □

We remark that it is possible for all cyclic R-modules to have finite projective dimension even though $\operatorname{gl\,dim} R = \infty$.

EXERCISES

1. If R is not a Wedderburn ring, prove that $\operatorname{gl\,dim} R = 1 + \sup\{\operatorname{pd}_R I\}$, where I runs through all right ideals of R. For this, first observe that every cyclic R-module is of the form R/I.

2. If N is a nilpotent ideal of R, show that $\operatorname{gl\,dim} R = \sup\{\operatorname{pd}_R V \mid VN = 0\}$.
3. Let D be a division ring, let R be the ring of upper triangular $n \times n$ matrices over D and let N be the set of strictly upper triangular matrices. First show that R is an Artinian ring with $N = \operatorname{Rad}(R)$ and that R has precisely n irreducible modules, namely $V_i \cong e_i R/e_i N$ for $i = 1, 2, \ldots, n$, where $e_i = e_{i,i}$. Furthermore, prove that $e_i N \cong e_{i+1} R$ as right R-modules for $i < n$ and conclude that $\operatorname{gl\,dim} R \leq 1$.
4. Let $R \supseteq S$ be rings with R_S a projective S-module. If V is an R-module, prove that $\operatorname{pd}_R V \geq \operatorname{pd}_S V$. If in addition $R = S \dotplus I$ with $I \lhd R$, prove that $\operatorname{gl\,dim} R \geq \operatorname{gl\,dim} S$. For the latter, observe that any S-module is an R-module by way of the homomorphism $R \to R/I \cong S$ and that this R-module restricts properly to S.

Let A be an R-module. A *projective resolution* for A is a long exact sequence

$$\cdots \to P_2 \xrightarrow{\alpha_2} P_1 \xrightarrow{\alpha_1} P_0 \xrightarrow{\alpha_0} A \to 0$$

with each P_i a projective R-module. If all P_i are free, then this sequence is a *free resolution* for A.

5. If

$$\cdots \to Q_2 \xrightarrow{\beta_2} Q_1 \xrightarrow{\beta_1} Q_0 \xrightarrow{\beta_0} A \to 0$$

is a second projective resolution for A, prove that

$$\begin{aligned}\operatorname{Ker}(\alpha_n) \oplus Q_n \oplus P_{n-1} \oplus Q_{n-2} \oplus P_{n-3} \oplus \cdots \\ \cong \operatorname{Ker}(\beta_n) \oplus P_n \oplus Q_{n-1} \oplus P_{n-2} \oplus Q_{n-3} \oplus \cdots\end{aligned}$$

for all $n \geq 0$. In particular, observe that $\operatorname{Ker}(\alpha_n) \sim \operatorname{Ker}(\beta_n)$. This is, of course, a generalization of Schanuel's Lemma.
6. Prove that A has a projective resolution and that if R is Noetherian and A is finitely generated, then A has such a resolution with all P_i finitely generated. Show that $\mathcal{K}^n[A] = [\operatorname{Ker}(\alpha_{n-1})]$ for all $n \geq 1$ and then characterize $\operatorname{pd} A$ in terms of the projective resolutions of A.
7. Let

$$\cdots \to C_2 \xrightarrow{\gamma_2} C_1 \xrightarrow{\gamma_1} C_0 \xrightarrow{\gamma_0} C \to 0$$

be a complex of R-modules and R-homomorphisms. Suppose that there exist abelian group homomorphisms $\sigma: C \to C_0$ and $\sigma_i: C_i \to C_{i+1}$ such that $\gamma_0\sigma = 1_C$, $\sigma\gamma_0 + \gamma_1\sigma_0 = 1_{C_0}$ and $\sigma_{n-1}\gamma_n + \gamma_{n+1}\sigma_n = 1_{C_n}$ for all $n \geq 1$. Prove that this sequence is exact.

8. Now assume that the preceding C-sequence is exact and that $f: A \to C$ is an R-module homomorphism. Prove that there exist homomorphisms $f_i: P_i \to C_i$ such that the diagram

$$\begin{array}{ccccccccc} \to & P_2 & \xrightarrow{\alpha_2} & P_1 & \xrightarrow{\alpha_1} & P_0 & \xrightarrow{\alpha_0} & A & \to 0 \\ & \downarrow f_2 & & \downarrow f_1 & & \downarrow f_0 & & \downarrow f & \\ \to & C_2 & \xrightarrow{\gamma_2} & C_1 & \xrightarrow{\gamma_1} & C_0 & \xrightarrow{\gamma_0} & C & \to 0 \end{array}$$

commutes.

Let S be a ring and let Γ be a multiplicative semigroup. Then the *semigroup ring* $R = S[\Gamma]$ is the set of all formal finite sums $\sum_{x\in\Gamma} s_x x$ with $s_x \in S$. Addition in $S[\Gamma]$ is componentwise and multiplication is determined distributively by $ax \cdot by = (ab)(xy)$ for all $a, b \in S$ and $x, y \in \Gamma$. For example, the polynomial ring $R = S[x_1, x_2, \ldots, x_n]$ is a semigroup ring with $\Gamma = \langle x_1, x_2, \ldots, x_n \rangle$. Furthermore, if $\Gamma = G$ is a multiplicative group, then $S[G]$ is, of course, the group ring.

9. If $R = S[\Gamma]$, use Problem 4 to prove that $\operatorname{gl\,dim} R \geq \operatorname{gl\,dim} S$.
10. Suppose $R = S[G]$ with G a multiplicative group and, for each $n \geq 0$, let F_n be the free right S-module with basis consisting of all $(n+1)$-tuples $[g_0, g_1, \ldots, g_n]$ with $g_i \in G$. If $x \in G$, define $[g_0, g_1, \ldots, g_n]x = [g_0x, g_1x, \ldots, g_nx]$ and, for all $n \geq 1$, let the map $\alpha_n: F_n \to F_{n-1}$ be determined by

$$[g_0, g_1, \ldots, g_n]s \mapsto \sum_{k=0}^{n} (-)^k [g_0, \ldots, \hat{g}_k, \ldots, g_n]s$$

where $\hat{g}_k$ indicates that g_k is omitted. If $\alpha_0: F_0 \to S$ is given by $[g_0]s \mapsto s$, show that

$$\cdots \to F_2 \xrightarrow{\alpha_2} F_1 \xrightarrow{\alpha_1} F_0 \xrightarrow{\alpha_0} S \to 0$$

is a free resolution for the R-module S_R. For exactness, observe that the maps $\sigma: S \to F_0$ and $\sigma_n: F_n \to F_{n+1}$ given by $\sigma: s \mapsto [1]s$ and

$$\sigma_n: [g_0, g_1, \ldots, g_n]s \mapsto [1, g_0, g_1, \ldots, g_n]s$$

satisfy the assumptions of Problem 7.

9. Tensor Products

Let R be a ring and suppose that A and B are both right R-modules or both left R-modules. Then $\mathrm{Hom}_R(A, B)$ is an abelian group determined by the pair (A, B). As we will see shortly, the tensor product is another abelian group determined by a pair of modules. But here the similarity ends. First, the tensor product $A \otimes B$ requires that we deal simultaneously with both right and left R-modules. Indeed, A_R is right and ${}_RB$ is left. Second, the tensor product is more than just an abelian group. It comes endowed with a canonical map $A \times B \to A \otimes B$. Finally, $A \otimes B$ is defined in terms of its properties rather than as a union of its elements. Thus, it is incumbent upon us to show that the appropriate structure exists.

DEFINITION Let A_R and ${}_RB$ be right and left R-modules respectively. If U is any additive abelian group, then $\varphi: A \times B \to U$ is said to be a *balanced map* provided that

1. $\varphi(a_1 + a_2, b) = \varphi(a_1, b) + \varphi(a_2, b)$,
2. $\varphi(a, b_1 + b_2) = \varphi(a, b_1) + \varphi(a, b_2)$, and
3. $\varphi(ar, b) = \varphi(a, rb)$

for all $a, a_1, a_2 \in A$, $b, b_1, b_2 \in B$ and $r \in R$. In particular, conditions (1) and (2) assert that φ is bilinear, whereas (3) is an associative law of sorts. Notice that if $\eta: U \to U'$ is a group homomorphism, then the composite map $\eta\varphi: A \times B \to U'$ is also balanced. This observation is the basis for the following *universal definition* of tensor product.

Let A_R and ${}_RB$ be given. Then a *tensor product* (X, θ) of A and B over R is an additive abelian group X and a balanced map $\theta: A \times B \to X$ such that any balanced map from $A \times B$ factors uniquely through X. More precisely, if $\varphi: A \times B \to U$ is balanced, then there exists a unique

group homomorphism $\eta\colon X \to U$ such that the diagram

$$\begin{array}{ccc} A \times B & \xrightarrow{\theta} & X \\ & \searrow \varphi & \downarrow \eta \\ & & U \end{array}$$

commutes. In other words, $\varphi = \eta\theta$. As we will see shortly, tensor products exist and are essentially unique. We begin with the construction.

If A_R and ${}_RB$ are any R-modules, then we define $S = \mathcal{S}(A, B)$ to be the free abelian group whose free generators are the elements of the Cartesian product $A \times B$. In other words, every element of S is uniquely a finite sum of the form

$$\sum_{(a,b)\in A\times B} z_{a,b}\,(a, b)$$

with $z_{a,b} \in \mathbb{Z}$, the ring of integers. Furthermore, we let $S_0 = \mathcal{S}_0(A, B)$ be the subgroup of S generated by all elements of the form

$$\begin{aligned} &(a_1 + a_2, b) - (a_1, b) - (a_2, b) \\ &(a, b_1 + b_2) - (a, b_1) - (a, b_2) \\ &(ar, b) - (a, rb) \end{aligned}$$

with $a, a_1, a_2 \in A$, $b, b_1, b_2 \in B$ and $r \in R$. Now define $A \otimes B = A \otimes_R B$ to be the additive abelian group S/S_0. Notice that $A \times B$ is a $\mathbb{Z}$-basis for S and thus the restriction of the natural epimorphism $S \to S/S_0$ to $A \times B$ yields a map $\theta\colon A \times B \to A \otimes B$. We denote the image of (a, b) under θ by $a \otimes b$. Since any element of S_0 maps to zero in S/S_0, it follows from the definition of S_0 that

$$\begin{aligned} (a_1 + a_2) \otimes b &= a_1 \otimes b + a_2 \otimes b \\ a \otimes (b_1 + b_2) &= a \otimes b_1 + a \otimes b_2 \\ ar \otimes b &= a \otimes rb \end{aligned}$$

for all appropriate elements in A, B and R. In particular, θ is a balanced map.

PROPOSITION 9.1 *Let A_R and ${}_RB$ be R-modules. Then $(A \otimes_R B, \theta)$ as just given is a tensor product of A and B over R. Furthermore, if (X, θ') is*

any other tensor product, then there exists an abelian group isomorphism $\sigma: A \otimes B \to X$ *with* $\theta' = \sigma\theta$.

PROOF As we have observed, $A \otimes B$ is an abelian group and $\theta: A \times B \to A \otimes B$ is a balanced map. Now let $\varphi: A \times B \to U$ be any balanced map. Since the elements (a, b) form a $\mathbb{Z}$-basis for $S = \mathcal{S}(A, B)$, we can clearly define an abelian group homomorphism $\eta': S \to U$ by

$$\eta': \sum_{(a,b)\in A\times B} z_{a,b}\,(a,b) \mapsto \sum_{(a,b)\in A\times B} z_{a,b}\,\varphi(a,b)$$

Furthermore, since φ is balanced, it follows easily that η' maps the generators of S_0 to 0. Thus S_0 is contained in the kernel of η' and therefore η' factors through $S/S_0 = A \otimes B$. In other words, there exists a homomorphism $\eta: A \otimes B \to U$ with $\eta(a \otimes b) = \varphi(a, b)$. Furthermore, η is uniquely determined, since the elements $a \otimes b$ clearly generate $A \otimes B$. Thus $(A \otimes B, \theta)$ is indeed a tensor product for A and B over R.

Finally, let (X, θ') be any other such tensor product. Since the map $\theta': A \times B \to X$ is balanced, there exists $\sigma: A \otimes B \to X$ with $\theta' = \sigma\theta$. Similarly, since $\theta: A \times B \to A \otimes B$ is balanced, there exists $\tau: X \to A \otimes B$ with $\theta = \tau\theta'$. Thus $\theta' = \sigma\tau\theta'$ and $\theta = \tau\sigma\theta$, so uniqueness implies that $\sigma\tau$ and $\tau\sigma$ are both identity maps on the appropriate groups. In particular, σ is an isomorphism and the result follows. □

With slight abuse of notation we now call $A \otimes_R B$ the tensor product of A and B over R. We do this with the understanding that the corresponding balanced map is given by $(a, b) \mapsto a \otimes b$. Notice that bilinearity implies

$$(a \otimes b)z = az \otimes b = a \otimes zb$$

for all $a \in A$, $b \in B$ and $z \in \mathbb{Z}$. In particular, $0 \otimes b = a \otimes 0 = 0$.

We compute an example. Set $R = \mathbb{Z}$, $A = \mathbb{Z}/(m)$ and $B = \mathbb{Z}/(n)$ for any $m, n \geq 1$. Since A is the cyclic $\mathbb{Z}$-module generated by $a_0 = 1 + (m)$ and since B is generated by $b_0 = 1 + (n)$, it follows from the preceding that $A \otimes_{\mathbb{Z}} B$ is the cyclic group generated by $a_0 \otimes b_0$. Furthermore,

$$(a_0 \otimes b_0)m = a_0 m \otimes b_0 = 0 \otimes b_0 = 0$$
$$(a_0 \otimes b_0)n = a_0 \otimes nb_0 = a_0 \otimes 0 = 0$$

so $(a_0 \otimes b_0)d = 0$ where $d = \gcd(m, n)$. In particular, $A \otimes B$ is a homomorphic image of $\mathbb{Z}/(d)$ and hence has order at most d. On the other hand, observe that the map $\varphi: A \times B \to \mathbb{Z}/(d)$ given by

$$\varphi: \big(i + (m), j + (n)\big) \mapsto ij + (d)$$

is balanced. Thus there exists a homomorphism $\sigma: A \otimes B \to \mathbb{Z}/(d)$ with $\sigma(a \otimes b) = \varphi(a, b)$. But $\sigma(a_0 \otimes b_0) = \varphi(a_0, b_0) = 1 + (d)$, so σ is onto. By order considerations, σ is an isomorphism and hence $\mathbb{Z}/(m) \otimes_{\mathbb{Z}} \mathbb{Z}/(n) \cong \mathbb{Z}/(d)$.

The following is a key property of tensor products.

LEMMA 9.2 *Let A, A', A'' be right R-modules and let B, B', B'' be left R-modules. If $\alpha: A \to A'$ and $\beta: B \to B'$ are R-homomorphisms, then there exists a natural abelian group homomorphism $\alpha \otimes \beta: A \otimes B \to A' \otimes B'$ with*

$$\alpha \otimes \beta: a \otimes b \mapsto \alpha a \otimes b\beta$$

for all $a \in A, b \in B$. Furthermore, if $\alpha': A' \to A''$ and $\beta': B' \to B''$ are also homomorphisms, then

$$(\alpha' \otimes \beta')(\alpha \otimes \beta) = (\alpha'\alpha) \otimes (\beta\beta')$$

In particular, if α and β are isomorphisms, then so is $\alpha \otimes \beta$.

PROOF The map $A \times B \to A' \otimes B'$ given by $(a, b) \mapsto \alpha a \otimes b\beta$ is easily seen to be balanced and hence gives rise to the abelian group homomorphism $\alpha \otimes \beta: A \otimes B \to A' \otimes B'$ with $\alpha \otimes \beta: a \otimes b \mapsto \alpha a \otimes b\beta$. The remaining facts now follow easily by evaluating the appropriate maps on the generating set $\{ a \otimes b \mid a \in A, b \in B \}$. □

Since the tensor product is defined in a right-left symmetric manner, it is clear that its properties will also exhibit this symmetry. Thus to avoid unnecessary repetition, we usually just state one-sided versions of each result.

DEFINITION Let V be an additive abelian group and let R and S be rings. Then V is said to be an (R, S)-*bimodule*, written $V = {}_R V_S$, if V is a left R-module and a right S-module and if the module structures are related by the formula

$$(rv)s = r(vs) \qquad \text{for all } r \in R, s \in S, v \in V$$

In particular, multiplication by $s \in S$ is an R-endomorphism of V and multiplication by $r \in R$ is an S-endomorphism. If V and V' are both (R, S)-bimodules, then the map $\theta: V \to V'$ is a *bimodule homomorphism* if it is both an R-module and an S-module homomorphism.

LEMMA 9.3 *Let R, S, T be rings and let ${}_TA_R$ and ${}_RB_S$ be given. Then the tensor product $A \otimes_R B$ is a (T,S)-bimodule with $t(a \otimes b)s = (ta) \otimes (bs)$. Furthermore, if $\alpha: A \to A'$ and $\beta: B \to B'$ are appropriate bimodule homomorphisms, then $\alpha \otimes \beta: A \otimes_R B \to A' \otimes_R B'$ is a (T,S)-bimodule homomorphism.*

PROOF Let $s \in S$ and let 1_A denote the identity automorphism of A. Then by the previous lemma, $1_A \otimes s: A \otimes B \to A \otimes B$ given by $1_A \otimes s: a \otimes b \mapsto a \otimes bs$ is an endomorphism of the abelian group $A \otimes_R B$. Furthermore, the map $S \to \mathrm{End}(A \otimes B)$ given by $s \mapsto 1_A \otimes s$ is easily seen to be a ring homomorphism. Thus, by Lemma 1.1, $A \otimes B$ is a right S-module. Similarly, it is a left T-module and the remainder is clear. □

In view of the preceding, any tensor product result will usually have a bimodule version. For the sake of simplicity, we do not bother to offer these more complicated formulations. The next result is the *associativity of tensor products.*

LEMMA 9.4 *Let R and S be rings and let A_R, ${}_RB_S$ and ${}_SC$ be appropriate modules. Then $A \otimes_R (B \otimes_S C) \cong (A \otimes_R B) \otimes_S C$ via the map $a \otimes (b \otimes c) \mapsto (a \otimes b) \otimes c$.*

PROOF For each $a \in A$, the map $B \times C \to (A \otimes B) \otimes C$ defined by $(b, c) \mapsto (a \otimes b) \otimes c$ is easily seen to be balanced and therefore yields $\theta_a: B \otimes C \to (A \otimes B) \otimes C$. Furthermore, the map $A \times (B \otimes C) \to (A \otimes B) \otimes C$ given by $(a, d) \mapsto \theta_a(d)$ is now also balanced and hence we have $\varphi: A \otimes_R (B \otimes_S C) \to (A \otimes_R B) \otimes_S C$ with $a \otimes (b \otimes c) \mapsto (a \otimes b) \otimes c$. Since the reverse map also exists, φ is an isomorphism. □

Part (i) of the next lemma asserts that the tensor product "commutes with" direct sums. Part (ii) says that it is *right exact.*

LEMMA 9.5 *Let R be a ring and B a left R-module.*

i. If $A = \cdot \sum_{i \in \mathcal{I}} A_i$, then

$$A \otimes_R B = \cdot \sum_{i \in \mathcal{I}} A_i \otimes B$$

ii. If $A' \xrightarrow{\alpha'} A \xrightarrow{\alpha''} A'' \to 0$ is exact, then so is

$$A' \otimes B \xrightarrow{\alpha' \otimes 1_B} A \otimes B \xrightarrow{\alpha'' \otimes 1_B} A'' \otimes B \to 0$$

PROOF (i) This follows from Lemma 9.2, since direct sums can be characterized by homomorphisms. Specifically, let $\pi_i: A \to A_i$ and $\eta_i: A_i \to A$ be the corresponding projection and injection maps associated with the direct sum $A = \cdot\sum_{i\in\mathcal{I}} A_i$. Then $\pi_i\eta_i = 1_{A_i}$, $\pi_i\eta_j = 0$ for $i \neq j$, and $\sum_i \eta_i\pi_i = 1_A$ with the understanding that for any $a \in A$ almost all $\pi_i(a)$ are zero. By Lemma 9.2, we obtain maps $\tilde{\pi}_i = \pi_i \otimes 1_B: A \otimes B \to A_i \otimes B$ and $\tilde{\eta}_i = \eta_i \otimes 1_B: A_i \otimes B \to A \otimes B$ which satisfy the analogous relations. Thus the result is proved.

(ii) It is clear that

$$A' \otimes B \xrightarrow{\alpha'\otimes 1_B} A \otimes B \xrightarrow{\alpha''\otimes 1_B} A'' \otimes B \to 0$$

is a zero sequence and that $\alpha'' \otimes 1_B$ is an epimorphism. Thus we must show that the sequence is exact at $A \otimes B$. To this end, let $C = \mathrm{Im}(\alpha' \otimes 1_B)$ and observe that the map $A'' \times B \to (A \otimes B)/C$ given by $(a'', b) \mapsto (a \otimes b) + C$, where $\alpha''(a) = a''$, is well defined and balanced. Thus we obtain a map $\theta: A'' \otimes B \to (A \otimes B)/C$ such that $\theta\big((\alpha'' \otimes 1_B)(x)\big) = x + C \in (A \otimes B)/C$ for all $x \in A \otimes B$. In particular, if $x \in \mathrm{Ker}(\alpha'' \otimes 1_B)$, then $x \in C$ as required. □

DEFINITION We say that the left R-module ${}_RB$ is *flat* if, for all short exact sequences $0 \to A' \to A \to A'' \to 0$ of right R-modules, the sequence

$$0 \to A' \otimes B \to A \otimes B \to A'' \otimes B \to 0$$

is also exact. In view of the preceding lemma, ${}_RB$ is flat if and only if, for all monomorphisms $\alpha': A' \to A$, the map $\alpha' \otimes 1_B: A' \otimes B \to A \otimes B$ is also a monomorphism. Equivalently, this means that if $A' \subseteq A$, then $A' \otimes B$ embeds naturally in $A \otimes B$. There is, of course, an analogous definition for flatness of right R-modules.

An example of the failure of flatness is as follows. Let $R = \mathbb{Z}$ and let $\mathbb{Z}/(n)$ be embedded in $\mathbb{Z}/(n^2)$ as all multiples of $n \geq 2$. Then the image of the map

$$\mathbb{Z}/(n) \cong \mathbb{Z}/(n) \otimes \mathbb{Z}/(n) \to \mathbb{Z}/(n^2) \otimes \mathbb{Z}/(n) \cong \mathbb{Z}/(n)$$

is zero, since any $x \otimes y$ maps to $x'n \otimes y = x' \otimes ny = x' \otimes 0 = 0$. In particular, $\mathbb{Z}/(n)$ is not a flat $\mathbb{Z}$-module. Other examples come from:

LEMMA 9.6 *Let I be a left ideal of R. If A_R is a right R-module, then $A \otimes_R (R/I)$ is isomorphic to A/AI via the map $a \otimes (r + I) \mapsto ar + AI$. Furthermore, if $0 \to A \to B \to C \to 0$ is exact with $A \subseteq B$, then*

$$0 \to A \otimes (R/I) \to B \otimes (R/I) \to C \otimes (R/I) \to 0$$

is exact if and only if $A \cap BI = AI$.

PROOF Let $^-: R \to \bar{R} = R/I$ be the natural module epimorphism. Then for all $a \in A$ and $\bar{r} \in \bar{R}$, we have $a \otimes \bar{r} = a \otimes r\bar{1} = ar \otimes \bar{1}$. It therefore follows that every element of $A \otimes \bar{R}$ is of the form $a \otimes \bar{1}$ for some $a \in A$.

Next note that the map $A \times \bar{R} \to A/AI$ given by $(a, r+I) \mapsto ar + AI$ is well defined and balanced. Thus we obtain a map $\theta: A \otimes \bar{R} \to A/AI$, which is clearly onto. It suffices to show that θ is one-to-one. To this end, let $a \otimes \bar{1} \in \mathrm{Ker}(\theta)$. Then $0 = \theta(a \otimes \bar{1}) = a + AI$, so $a \in AI$. In other words, we can write $a = \sum_i a_i r_i$ with $r_i \in I$. But then

$$a \otimes \bar{1} = \sum_i a_i r_i \otimes \bar{1} = \sum_i a_i \otimes r_i \bar{1} = \sum_i a_i \otimes \bar{0} = 0$$

and we conclude that $\mathrm{Ker}(\theta) = 0$.

Finally, if $A \subseteq B$ then we have the commutative diagram

$$\begin{array}{ccc} A \otimes \bar{R} & \xrightarrow{\mu \otimes 1} & B \otimes \bar{R} \\ \downarrow & & \downarrow \\ A/AI & \xrightarrow{\bar{\mu}} & B/BI \end{array}$$

where $\mu: A \to B$ is the natural embedding and $\bar{\mu}: a + AI \mapsto a + BI$. Since the vertical maps are the isomorphisms described previously, it follows that $\mu \otimes 1$ is a monomorphism if and only if $\bar{\mu}$ is. But the kernel of $\bar{\mu}$ is clearly $(A \cap BI)/AI$, so the result follows. □

Note that if $I \lhd R$, then R/I is an $(R, R/I)$-bimodule and the preceding maps are all R/I-homomorphisms.

LEMMA 9.7 *If* ${}_R B$ *is a free left* R*-module with basis* $\{ b_i \mid i \in \mathcal{I} \}$*, then every element of* $A \otimes_R B$ *is uniquely a finite sum of the form* $\sum_i a_i \otimes b_i$ *with* $a_i \in A$.

PROOF Since $B = \cdot \sum_{i \in \mathcal{I}} Rb_i$, it follows from Lemma 9.3(i) that $A \otimes B = \cdot \sum_{i \in \mathcal{I}} A \otimes Rb_i$. Thus it suffices to show that each element of $A \otimes Rb_i$ is uniquely of the form $a_i \otimes b_i$ with $a_i \in A$. For this, first observe that $a \otimes rb_i = ar \otimes b_i$, so every element is indeed of this form. Furthermore, $Rb_i \cong R$, so $A \otimes Rb_i \cong A \otimes R \cong A$ by the previous lemma with $I = 0$. Since the isomorphism $A \otimes Rb_i \to A$ is given by $a \otimes b_i \mapsto a$, the A-term is unique. □

We can actually better understand flatness by going back to Proposition 9.1. Thus suppose $A' \subseteq A$ are right R-modules and that B is a left R-module. Then certainly $\mathcal{S}(A', B) \subseteq \mathcal{S}(A, B)$ and $\mathcal{S}_0(A', B) \subseteq \mathcal{S}_0(A, B)$. Furthermore, if $\mu\colon A' \to A$ is the inclusion map, then $\mu \otimes 1_B$ is the homomorphism

$$\frac{\mathcal{S}(A', B)}{\mathcal{S}_0(A', B)} \longrightarrow \frac{\mathcal{S}(A, B)}{\mathcal{S}_0(A, B)}$$

determined by the inclusion $\mathcal{S}(A', B) \subseteq \mathcal{S}(A, B)$. Thus, by the Second Isomorphism Theorem, $\mu \otimes 1_B$ is one-to-one if and only if

$$\mathcal{S}_0(A', B) = \mathcal{S}(A', B) \cap \mathcal{S}_0(A, B)$$

As we will see shortly, this implies that the monomorphism condition is local.

Let $\mathcal{M}$ be a family of submodules of B. Then $\mathcal{M}$ is a *local system* for B if every finitely generated submodule of B is contained in some $M \in \mathcal{M}$.

LEMMA 9.8 *Let ${}_RB$ and $A'_R \subseteq A_R$ be given and let $\mathcal{M}$ be a local system for B. Furthermore, let $\mathcal{L}$ be a local system for A whose members all contain A'. If $A' \otimes M \to L \otimes M$ is a monomorphism for all $L \in \mathcal{L}$ and $M \in \mathcal{M}$, then $A' \otimes B \to A \otimes B$ is also a monomorphism.*

PROOF Let $x \in \mathcal{S}(A', B) \cap \mathcal{S}_0(A, B)$. Then the presentation of x in $\mathcal{S}(A', B)$ involves only finitely many elements of B and similarly the presentation of x in $\mathcal{S}_0(A, B)$ as a sum of generators involves only finitely many elements of A and B. Thus, since $\mathcal{L}$ and $\mathcal{M}$ are local systems, it follows that there exists $L \in \mathcal{L}$ and $M \in \mathcal{M}$ with $x \in \mathcal{S}(A', M) \cap \mathcal{S}_0(L, M)$. But $A' \otimes M \to L \otimes M$ is given to be a monomorphism, so $x \in \mathcal{S}_0(A', M) \subseteq \mathcal{S}_0(A', B)$. In other words, $\mathcal{S}_0(A', B) = \mathcal{S}(A', B) \cap \mathcal{S}_0(A, B)$ and we conclude that $A' \otimes B \to A \otimes B$ is indeed a monomorphism. □

As a consequence we have:

LEMMA 9.9 *Let R be a ring.*

i. If ${}_RB$ has a local system of flat submodules, then ${}_RB$ is flat.

ii. An arbitrary direct sum of flat modules is flat. A direct summand of a flat module is flat.

iii. Any projective R-module is flat.

PROOF (i) This follows from the preceding lemma by taking $\mathcal{L} = \{A\}$ and $\mathcal{M}$ the given local system of flat submodules.

(ii) This follows from the definition of flatness and the fact that the tensor product commutes with direct sums.

(iii) In view of (ii), it suffices to verify that ${}_RR$ is flat, which follows from Lemma 9.6 with $I = 0$. □

LEMMA 9.10 *If R is a commutative principal ideal domain, then the R-module ${}_RB$ is flat if and only if it is torsion free.*

PROOF Suppose first that B is torsion free. If M is a finitely generated submodule of B, then, since R is a principal ideal domain, M is free and hence flat. By Lemma 9.9(i), B is also flat.

Conversely, suppose B is flat and let $0 \neq r \in R$. Since R is a domain, multiplication by r is a monomorphism from R to R. Hence $r \otimes 1_B : R \otimes B \to R \otimes B$ must also be a monomorphism. In particular, if $0 \neq b \in B$, then $1 \otimes b \neq 0$ by Lemma 9.6 with $I = 0$ and hence

$$0 \neq (r \otimes 1_B)(1 \otimes b) = r \otimes b = 1 \otimes rb$$

Thus $rb \neq 0$ and B is torsion free. □

Now suppose $\phi : R \to S$ is a ring homomorphism. Then S is a left R-module via $r \cdot s = \phi(r)s$ and S is a right S-module by way of the regular representation. It then follows from the associative law that S is in fact an (R, S)-bimodule. In particular, if A_R is any right R-module, then $A \otimes_R S$ is a right S-module, the S-module *induced* by A. For example, if $I \lhd R$ and $S = R/I$, then $A \otimes_R S = A \otimes_R (R/I)$ is the module considered in Lemma 9.6. Basic properties are as follows.

LEMMA 9.11 *Let $\phi : R \to S$ be a ring homomorphism.*

i. If A_R is a projective or free or finitely generated R-module, then $A \otimes S$ has the corresponding property as an S-module.

ii. Suppose $R \subseteq S$ and that ϕ is the natural inclusion. If ${}_RS$ is free with basis $\{ s_i \mid i \in \mathcal{I} \}$, then every element of $A \otimes S$ is uniquely a finite sum of the form $\sum_{i \in \mathcal{I}} a_i \otimes s_i = \sum_{i \in \mathcal{I}} (a_i \otimes 1) s_i$ with $a_i \in A$.

PROOF (i) By Lemma 9.6 with $I = 0$, it follows that $(R \otimes_R S)_S \cong S_S$. Thus, since tensor product commutes with direct sums, we see that if A_R is free or projective, then so is $(A \otimes S)_S$. Now let $A = \sum_{i=1}^{n} a_i R$ be finitely generated. Then every element of $A \otimes S$ is a finite sum of the form

$$\begin{aligned} \sum_{i,j} a_i r_{i,j} \otimes s_{i,j} &= \sum_{i=1}^{n} a_i \otimes \Big(\sum_j \phi(r_{i,j}) s_{i,j} \Big) \\ &= \sum_{i=1}^{n} (a_i \otimes 1) \Big(\sum_j \phi(r_{i,j}) s_{i,j} \Big) \end{aligned}$$

with $r_{i,j} \in R$ and $s_{i,j} \in S$. Thus $A \otimes S$ is generated over S by the elements $a_i \otimes 1$ for $i = 1, 2, \ldots, n$.

(ii) It follows from Lemma 9.7 that every element of $A \otimes S$ is uniquely a finite sum of the form $\sum_{i \in \mathcal{I}} a_i \otimes s_i$ with $a_i \in A$. Since $a_i \otimes s_i = (a_i \otimes 1)s_i$, the lemma is proved. □

Finally we prove *transitivity of induction.*

LEMMA 9.12 *Let $\phi: R \to S$ and $\psi: S \to T$ be ring homomorphisms. Then $\psi\phi: R \to T$ is a ring homomorphism and, for all right R-modules A, we have*

$$(A \otimes_R S) \otimes_S T \cong A \otimes_R T$$

as right T-modules.

PROOF By Lemma 9.6 with $I = 0$, we have $S \otimes_S T \cong T$ via the map $s \otimes t \mapsto s \cdot t = \psi(s)t$ for all $s \in S$, $t \in T$. Thus by the associativity of tensor product,

$$(A \otimes_R S) \otimes_S T \cong A \otimes_R (S \otimes_S T) \cong A \otimes_R T$$

and the result follows. □

EXERCISES

1. Suppose $I \lhd R$ and that A_R and ${}_RB$ are R-modules with $AI = 0 = IB$. Prove that $A \otimes_{(R/I)} B$ is naturally isomorphic to $A \otimes_R B$.
2. Let I be a left ideal of R and J a right ideal. If ${}_RI$ is flat, prove that $J \otimes I \cong JI$. If ${}_R(R/I)$ is flat, show that $J \cap I = JI$.
3. If all R-modules are flat, prove that R is von Neumann regular. Conversely if R is von Neumann regular, show at least that all submodules of free R-modules are flat. For the first part, choose $r \in R$ and apply the preceding exercise with $I = Rr$ and $J = rR$. For the converse, use the fact that R is semihereditary.
4. Let R be the polynomial ring $K[x, y]$ and let $I = Rx + Ry$. Show that ${}_RI$ is not flat. For this, first observe that if I is flat, then $I^2 \cong I \otimes I$ as (R, R)-bimodules. Next note that I^2/I^3 is the largest homomorphic image of I^2 that is annihilated on both sides by I and that $\dim_K I^2/I^3 = 3$. On the other hand, show that $I \otimes I$ maps onto $(I/I^2) \otimes_R (I/I^2)$ and that this has dimension 4.

A flat module ${}_RB$ is *faithfully flat* if for all nonzero modules A_R we have $A \otimes B \neq 0$.

5. Show that the direct sum of a flat module and a faithfully flat module is faithfully flat. Conclude, therefore, that any nonzero free module is faithfully flat. Find an example of a flat $\mathbb{Z}$-module that is not faithfully flat.
6. Show that ${}_RB$ is faithfully flat if and only if, for all maps $\alpha: A \to A'$, either α or $\alpha \otimes 1_B$ being a monomorphism implies that the other is also. This is a key alternate characterization of faithfully flat modules.
7. A family $\mathcal{M}$ of submodules of B is said to be *directed* if its members generate B and if every two members are contained in a third. If $\mathcal{M}$ is such a directed family, show that $B = \bigcup_{M \in \mathcal{M}} M$ and that $\mathcal{M}$ is a local system.
8. Let $A'_R \subseteq A_R$ and ${}_RB$ be given. Show that there exists a submodule L of A containing A' that is maximal with respect to $A' \otimes B \to L \otimes B$ being a monomorphism. Similarly, show that there exists a submodule M of B maximal with respect to $A' \otimes M \to A \otimes M$ being a monomorphism.
9. Let K be a field and let R and S be K-algebras. We consider the tensor product $R \otimes_K S$. To start with, define a multiplication in $\mathcal{S}(R, S)$ distributively by $(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2)$. Then show that, in this way, $\mathcal{S}(R, S)$ is an associative ring and that $\mathcal{S}_0(R, S)$ is a two-sided ideal. Conclude that $R \otimes_K S$ is an associative K-algebra with multiplication given by $(r_1 \otimes s_1) \cdot (r_2 \otimes s_2) = (r_1 r_2) \otimes (s_1 s_2)$.
10. If R is any K-algebra, prove that $R \otimes_K \mathrm{M}_n(K) \cong \mathrm{M}_n(R)$ and that $R \otimes_K K[x] \cong R[x]$.

10. Local Rings

We close Part I by considering an important class of rings, the local rings. Our goal here is to show that every projective module over such a ring is free of unique rank. We begin with Nakayama's Lemma, a simple result with powerful applications. It quickly yields our goal in the finitely generated case.

As usual, let $\mathrm{Rad}(R)$ denote the Jacobson radical of R. Then $\mathrm{Rad}(R)$ is the largest quasi-regular two-sided ideal of R and, in particular, its definition is right-left symmetric. Furthermore Lemma 5.10(ii) asserts that $\mathrm{Rad}(R)$ is the intersection of all maximal right ideals of R and hence also the intersection of all maximal left ideals.

LEMMA 10.1 (Nakayama's Lemma) *Let V be a finitely generated right R-module and let W be a submodule of V.*

i. If $W \subset V$, then there exists a maximal submodule M of V with $W \subseteq M \subset V$.

ii. If $J = \mathrm{Rad}(R)$ and $V = W + VJ$, then $V = W$. In particular, $V = VJ$ implies $V = 0$.

PROOF (i) Since V is finitely generated and $W \subset V$, it follows by adding one generator at a time that there exists a submodule W' of V with $W \subseteq W' \subset V$ and V/W' cyclic. But then $V/W' \cong R/I$ for some proper right ideal I of R and, of course, I is contained in a maximal right ideal N of R. In particular, if M is the complete inverse image of N in V, then M is a maximal submodule of V containing W' and hence W.

(ii) If $W \neq V$, choose M as above. Since V/M is an irreducible R-module, we have $(V/M)J = 0$ and hence $W + VJ \subseteq M$, a contradiction. For the final remark, take $W = 0$. □

As a consequence, we obtain the following analog of Lemma 5.7.

LEMMA 10.2 *Let P be a finitely generated projective R-module and write $J = \mathrm{Rad}(R)$.*

(i) Suppose V is a finitely generated R-module and $\mu: V \to P$ is an R-homomorphism. If $\bar{\mu}: V/VJ \to P/PJ$ is an isomorphism, then μ is also an isomorphism.

(ii) If P/PJ is a free R/J-module, then P is a free R-module.

PROOF (i) Note that $\bar{\mu}$ is defined by $\bar{\mu}: v + VJ \mapsto \mu(v) + PJ$. Thus, since $\bar{\mu}$ is onto, we have $P = \mu(V) + PJ$ and therefore $P = \mu(V)$ by Nakayama's Lemma. Now μ is an epimorphism and P is projective, so we know that μ must split. In particular, $V = W \dotplus P'$, where $W = \mathrm{Ker}(\mu)$ and $P' \cong P$. Since $\mu(W) = 0$, we have $(W + VJ)/VJ \subseteq \mathrm{Ker}(\bar{\mu}) = 0$. Hence $W \subseteq VJ = WJ \dotplus P'J$ and therefore $W = WJ$. But $W \cong V/P'$ is finitely generated, so Nakayama's Lemma implies that $W = 0$ and μ is one-to-one.

(ii) Since P/PJ is finitely generated and free, $P/PJ \cong \oplus \sum_1^n R/J$. In particular, if we set $F = \oplus \sum_1^n R$, then $F/FJ \cong P/PJ$ and there is an epimorphism α with

$$\begin{array}{ccccc} & & F & & \\ & & \downarrow \alpha & & \\ P & \to & P/PJ & \to & 0 \end{array}$$

and $\mathrm{Ker}(\alpha) = FJ$. But F is free and hence projective, so there exists a map $\mu: F \to P$ that makes this diagram commute. Thus $\bar{\mu}: F/FJ \to P/PJ$ is the isomorphism α and part (i) therefore implies that μ is also an isomorphism. □

A ring R is said to be *local* if $R/\mathrm{Rad}(R)$ is a division ring. As we will see, the preceding result is particularly useful in this context. We start by listing some additional characterizations of such rings.

LEMMA 10.3 *The following are equivalent.*

i. R is a local ring.

ii. $\mathrm{Rad}(R)$ *is a maximal right (or left) ideal of R.*

iii. Every element of R not contained in $\mathrm{Rad}(R)$ *is a unit.*

PROOF (i)⇒(ii) This is clear, since $R/\mathrm{Rad}(R)$ is a division ring and hence has no nontrivial one-sided ideals.

(ii)⇒(iii) Since $\mathrm{Rad}(R)$ is the intersection of all maximal right ideals, by Lemma 5.10(ii), it must be the unique maximal right ideal of R. Now let $x \in R \setminus \mathrm{Rad}(R)$. If xR were a proper right ideal of R, then it would be contained in a maximal right ideal and hence $x \in \mathrm{Rad}(R)$, a contradiction. Thus $xR = R$ and there exists $y \in R$ with $xy = 1$. Clearly $y \notin \mathrm{Rad}(R)$ so the same argument implies that there exists $z \in R$ with $yz = 1$. In other words, y has a right and left inverse, so y is invertible. We conclude that $y^{-1} = x = z$ and therefore x is invertible with inverse y.

(iii)⇒(i) Since units map to units, it follows that all nonzero elements of $R/\mathrm{Rad}(R)$ are invertible. Thus $R/\mathrm{Rad}(R)$ is a division ring. □

Suppose that R is a commutative integral domain and that T is a *multiplicatively closed subset* of R. By this we mean that $1 \in T$, $0 \notin T$, and if $a, b \in T$, then so is ab. It is then a simple matter to form the ring of fractions RT^{-1}. This is the set of all formal fractions rt^{-1} with $r \in R$, $t \in T$ and with equality given by $r_1 t_1^{-1} = r_2 t_2^{-1}$ if and only if $r_1 t_2 = r_2 t_1$. With the usual addition and multiplication, RT^{-1} is clearly a commutative ring and R embeds in this ring via the map $r \mapsto r1^{-1}$. Notice that the elements of T are now invertible in RT^{-1}. When $T = R \setminus 0$, then RT^{-1} is the field of fractions of R and, by abuse of notation, we sometimes write this as RR^{-1}.

If Q is a prime ideal of R, then $T = R \setminus Q$ is multiplicatively closed and $QT^{-1} = \{ qt^{-1} \mid q \in Q, t \in T \}$ is a proper ideal of RT^{-1}, since $1 \notin QT^{-1}$. Furthermore, every element of RT^{-1} not contained in QT^{-1} is clearly invertible. It follows that RT^{-1} is a local ring with Jacobson radical QT^{-1}. This procedure is known as *localization*.

Part (ii) of the following result generalizes the implication (i)⇒(iii) of Lemma 10.3 and can be obtained fairly directly from it (see Exercise 3). Here we offer a module theoretic proof.

THEOREM 10.4 *Let R be a local ring.*

i. All finitely generated projective R-modules are free.

ii. Let $(c_{i,j}) \in \mathrm{M}_n(R)$. If $c_{i,i} \notin \mathrm{Rad}(R)$ for all i and $c_{i,j} \in \mathrm{Rad}(R)$ for all $i \neq j$, then the matrix $(c_{i,j})$ is invertible.

PROOF For convenience, write $J = \mathrm{Rad}(R)$ and let $^- : R \to R/J$ be the natural homomorphism.

(i) Let P be a finitely generated projective R-module and observe that P/PJ is an R/J-module. But R/J is a division ring, so all its modules are free. Thus P/PJ is free and hence, by the preceding lemma, so is P.

(ii) Let F be a free R-module of rank n and note, by Lemma 4.3(iii), that $(c_{i,j})$ corresponds to an endomorphism μ of F. Moreover, the matrix $(\bar{c}_{i,j}) \in \mathrm{M}_n(R/J)$ corresponds to the endomorphism $\bar{\mu}\colon F/FJ \to F/FJ$. Note that $\bar{c}_{i,j} = 0$ for $i \neq j$ and that $\bar{c}_{i,i} \neq 0$. Thus, since R/J is a division ring, we see that $(\bar{c}_{i,j})$ is invertible, so $\bar{\mu}$ is an isomorphism. By Lemma 10.2(i), μ is also an isomorphism and thus $(c_{i,j})$ is invertible. □

We now move on to infinitely generated projective modules. Here the proof is considerably more complicated, but it is made tractable by the following reduction, which applies to all rings.

THEOREM 10.5 *Let V be a direct sum of countably generated R-modules. If $P \mid V$, then P is also a direct sum of countably generated modules. In particular, any projective R-module is a direct sum of countably generated projectives.*

PROOF Write $V = \cdot\sum_{i\in\mathcal{I}} V_i$ with each V_i countably generated. Furthermore, write $V = P \dot{+} Q$ and let $\pi_P\colon V \to P$ and $\pi_Q\colon V \to Q$ be the natural projections. A submodule W of V is said to satisfy $(*)$ if $\pi_P(W) \subseteq W$, $\pi_Q(W) \subseteq W$, and $W = \cdot\sum_{i\in\mathcal{A}} V_i$ for some $\mathcal{A} \subseteq \mathcal{I}$. Obviously, if W satisfies $(*)$, then $W \mid V$ and $W = \pi_P(W) \dot{+} \pi_Q(W)$.

CLAIM *Given any V_k, there exists a countable subset $\mathcal{B}$ of $\mathcal{I}$ such that $k \in \mathcal{B}$ and $S = \cdot\sum_{i\in\mathcal{B}} V_i$ satisfies $(*)$.*

PROOF Define the countable subsets $\mathcal{B}_n$ of $\mathcal{I}$ and the modules $S_n = \cdot\sum_{i\in\mathcal{B}_n} V_i$ inductively as follows. First let $\mathcal{B}_0 = \{k\}$. Now if $\mathcal{B}_n$ is a countable subset of $\mathcal{I}$, then S_n is a countably generated submodule of V and hence so are $\pi_P(S_n)$ and $\pi_Q(S_n)$. Thus there exists a countable subset $\mathcal{B}_{n+1}$ of $\mathcal{I}$ containing $\mathcal{B}_n$ with $\pi_P(S_n)$ and $\pi_Q(S_n)$ both contained in S_{n+1}.

Finally, let $B = \bigcup_{n=0}^{\infty} \mathcal{B}_n$ and $S = \cdot\sum_{i\in\mathcal{B}} V_i$. Then $\mathcal{B}$ is countable and S satisfies $(*)$, since any $i \in \mathcal{B}$ is contained in some $\mathcal{B}_n$ and then $\pi_P(V_i)$ and $\pi_Q(V_i)$ are contained in $S_{n+1} \subseteq S$. □

Now we say that a submodule W of V satisfies $(**)$ if it satisfies $(*)$ and if $\pi_P(W)$ is a direct sum of countably generated modules. Note that $W = 0$ satisfies $(**)$. The goal is to find a submodule of V maximal with this property and for this it is necessary to keep track of the precise decomposition of $\pi_P(W)$. Thus we use Ξ to denote the particular collection of countably generated submodules that direct sum to $\pi_P(W)$. Of course, Ξ is not uniquely determined by W; therefore we study the pair (W, Ξ).

Write $(W_1, \Xi_1) \leq (W_2, \Xi_2)$ if and only if $W_1 \subseteq W_2$ and $\Xi_1 \subseteq \Xi_2$. If $\{(W_j, \Xi_j) \mid j \in \mathcal{J}\}$ is a chain of such pairs, then it follows easily that $(\bigcup_j W_j, \bigcup_j \Xi_j)$ also satisfies $(**)$. We can now conclude from Zorn's Lemma that a maximal pair (W, Ξ) exists.

If $W \neq V$, then there exist $V_k \not\subseteq W$ and we can let S be the countably generated $(*)$-submodule of V given by the claim. Then $W' = W + S \supset W$ and certainly W' satisfies $(*)$. Next observe that $\pi_P(W) \mid W$ and $W \mid V$, so $\pi_P(W) \mid V$. Furthermore, $\pi_P(W) \subseteq \pi_P(W')$, so the Modular Law implies that $\pi_P(W') = \pi_P(W) \dotplus \tilde{P}$. Similarly, we have $\pi_Q(W') = \pi_Q(W) \dotplus \tilde{Q}$. Now notice that $W'/W = (W + S)/W \cong S/(S \cap W)$ is countably generated. Since

$$W' = \pi_P(W') \dotplus \pi_Q(W') = W \dotplus \tilde{P} \dotplus \tilde{Q}$$

we have $W'/W \cong \tilde{P} \dotplus \tilde{Q}$ and thus $\tilde{P}$, being a homomorphic image of W'/W, is also countably generated. But then $(W, \Xi) < (W', \Xi')$, where $\Xi' = \Xi \cup \{\tilde{P}\}$, and this contradicts the maximality of (W, Ξ). We conclude therefore that $W = V$. In other words, V satisfies $(**)$ and hence $P = \pi_P(V)$ is a direct sum of countably generated submodules.

Finally, if P' is any projective R-module, then $P' \dotplus Q' = F'$, where F' is free. But then F' is a direct sum of copies of the cyclic R-module R_R, so the preceding implies that P' is a direct sum of countably generated R-modules. The result now follows because any direct summand of a projective module is projective. □

With this result in hand, it now clearly suffices to consider countably generated projective modules. The next two lemmas contain the necessary work.

LEMMA 10.6 *Let V be a countably generated R-module. Assume that for every $W \mid V$ and $x \in W$, we have $W = F \dotplus Q$, where F is free and $x \in F$. Then V is a free R-module.*

PROOF Let $x_1, x_2, x_3, \ldots$ generate V. We construct free submodules F_i inductively so that

$$V = F_1 \dotplus F_2 \dotplus \cdots \dotplus F_n \dotplus Q_n$$

and $x_1, x_2, \ldots, x_n \in F_1 \dotplus F_2 \dotplus \cdots \dotplus F_n$. For convenience, set $F_0 = 0$ and $Q_0 = V$.

Given $n \geq 0$, write $x_{n+1} = f_n + q_n$, where $f_n \in F_1 \dotplus F_2 \dotplus \cdots \dotplus F_n$ and $q_n \in Q_n$. Since $Q_n \mid V$, the hypothesis implies that $Q_n = F_{n+1} \dotplus Q_{n+1}$ with F_{n+1} free and $q_n \in F_{n+1}$. Thus

$$V = F_1 \dotplus F_2 \dotplus \cdots \dotplus F_n \dotplus F_{n+1} \dotplus Q_{n+1}$$

and $x_{n+1} \in F_1 \dot{+} F_2 \dot{+} \cdots \dot{+} F_n \dot{+} F_{n+1}$. This proves the induction step and we conclude that $V = \cdot \sum_{i=1}^{\infty} F_i$ is free. □

Next we show that the preceding hypothesis holds when R is local.

LEMMA 10.7 *Let R be a local ring, let P be a projective R-module and let $x \in P$. Then $P = Y \dot{+} T$ with Y a free R-submodule containing x.*

PROOF Write $P \dot{+} Q = F$, where F is free, and choose a basis $\{ f_i \mid i \in \mathcal{I} \}$ of F so that x is written in terms of the minimal number, say n, of basis elements. By relabeling the subscripts, we can assume that $x = \sum_{i=1}^{n} f_i r_i$ with $r_i \in R$. Let F' denote the free submodule of F spanned by the remaining basis elements f_k with $k > n$.

We first note that no r_j is a left R-linear combination of the other r_i's. Indeed, if $r_n = \sum_{i=1}^{n-1} b_i r_i$ with $b_i \in R$, then

$$\{ f_1 + f_n b_1, f_2 + f_n b_2, \ldots, f_{n-1} + f_n b_{n-1}, f_n, f_{n+1}, \ldots \}$$

is another free basis for F and $x = \sum_{i=1}^{n-1} (f_i + f_n b_i) r_i$ involves fewer terms, a contradiction.

Let $\pi_P : F \to P$ be the natural projection and set $\pi_P(f_i) = y_i$ for $i = 1, 2, \ldots, n$. Since $\pi_P(x) = x$, we have

$$\sum_{i=1}^{n} f_i r_i = x = \pi_P(x) = \sum_{i=1}^{n} y_i r_i$$

Furthermore, $y_i \in F$, so we can write

$$y_i \equiv \sum_{j=1}^{n} f_j c_{j,i} \mod F'$$

for suitable $c_{j,i} \in R$. Thus

$$\sum_{i=1}^{n} f_i r_i = \sum_{i=1}^{n} y_i r_i \equiv \sum_{i,j=1}^{n} f_j c_{j,i} r_i \mod F'$$

and hence $r_j = \sum_{i=1}^{n} c_{j,i} r_i$ for all $j = 1, 2, \ldots, n$.

We study the latter system of equations. To start with, if $c_{j,i} \notin \mathrm{Rad}(R)$ for some $j \neq i$, then $c_{j,i}$ is invertible and hence r_i is a left R-linear combination of the remaining r_k's, a contradiction. Thus $c_{j,i} \in \mathrm{Rad}(R)$ for all $j \neq i$. Similarly, $1 - c_{j,j} \in \mathrm{Rad}(R)$ for all j, so $c_{j,j} \notin \mathrm{Rad}(R)$. It

now follows from Theorem 10.5(ii) that the $n \times n$ matrix $(c_{j,i})$ is invertible in $M_n(R)$. Hence Lemma 2.5 implies that $\{y_1, y_2, \ldots, y_n\}$ is also a free basis for F modulo F'. In other words, if $Y = \sum_{i=1}^{n} y_i R$, then Y is a free submodule of P and $Y \dotplus F' = F$. Thus $P = Y \dotplus (F' \cap P)$ and the result follows because $x \in Y$. □

We can now quickly prove:

THEOREM 10.8 (Kaplansky's Theorem) *If R is a local ring, then all projective R-modules are free of unique rank.*

PROOF We first show that projectives are free and, in view of Theorem 10.5, it suffices to consider countably generated projective modules. Let P be such a module and suppose that W is a direct summand of P. Then W is projective and, for any $x \in W$, the preceding lemma implies that $W = F \dotplus Q$ with F free and $x \in F$. Lemma 10.6 now implies that P is free. Finally, the uniqueness of rank follows from Lemmas 2.3 and 2.6, since $R/\mathrm{Rad}(R)$ is a division ring. □

EXERCISES

1. Prove Lemma 10.1(ii) directly from the quasi-regular property of $J = \mathrm{Rad}(R)$. To this end, suppose $\{v_1, v_2, \ldots, v_n\} \subseteq V$ is a minimal generating set for V modulo W and write $v_n \in W + VJ = W + \sum_i v_i J$. Now solve for the generator v_n.
2. Let Γ be the semigroup consisting of all symbols x^q, where q is a nonnegative rational number, and let the multiplication in Γ be given by $x^a \cdot x^b = x^{a+b}$. Form the semigroup algebra $R = K[\Gamma]$ and let $\bar{R} = R/x^1R$. Show that $\bar{R}$ is a local ring with $\bar{J} = \mathrm{Rad}(\bar{R})$ a nil, but not nilpotent, ideal. Furthermore, show that $\bar{J}^2 = \bar{J} \neq 0$, so that Nakayama's Lemma can indeed fail for infinitely generated modules.
3. Now let R be a local ring and suppose $C = (c_{i,j}) \in M_n(R)$ with $c_{i,i} \notin \mathrm{Rad}(R)$ and $c_{i,j} \in \mathrm{Rad}(R)$ for all $i \neq j$. Show that C is both row and column equivalent to the identity matrix. Conclude from this that C is invertible.
4. Suppose T is a multiplicatively closed subset of the commutative domain R. If $\tilde{T}$ is the set of divisors of elements of T, prove that $\tilde{T}$ is multiplicatively closed and that $RT^{-1} = R\tilde{T}^{-1}$. In particular, if R is a unique factorization domain, show that the rings RT^{-1} correspond in a one-to-one manner to the sets of prime elements of R.

If V is an R-module, then $\mathrm{Rad}(V)$ is defined to be the intersection

of all maximal submodules of V. In particular, $\mathrm{Rad}(R_R)$ is the usual Jacobson radical of R.

5. Let $W \subseteq V$. If M is a maximal submodule of V, show that either $M \supseteq W$ or that $W \cap M$ is a maximal submodule of W. Conclude that $\mathrm{Rad}(W) \subseteq W \cap \mathrm{Rad}(V)$ with equality if $W \mid V$. Find an example of $\mathbb{Z}$-modules where equality fails.
6. Show that $\mathrm{Rad}(V) \supseteq V \cdot \mathrm{Rad}(R)$ with equality if V is free and then if V is projective. Show that equality fails when $R = \mathbb{Z}$ and $V = \mathbb{Q}_{\mathbb{Z}}$.

An R-module V has a *projective cover* $P \xrightarrow{\alpha} V \to 0$ if P is projective and if no proper submodule of P maps onto V.

7. If $P \xrightarrow{\alpha} V \to 0$ and $Q \xrightarrow{\beta} V \to 0$ are projective covers for V, prove that $P \cong Q$. Furthermore, if R is Artinian, use the argument of Theorem 5.9(iii) to show that every R-module has a projective cover.
8. If $P \xrightarrow{\alpha} V \to 0$ is a projective cover, show that $\mathrm{Ker}(\alpha) \subseteq \mathrm{Rad}(P)$. Conclude from Exercise 6 that if $\mathrm{Rad}(R) = 0$, then α must be an isomorphism. In particular, if $\mathrm{Rad}(R) = 0$, then only projective R-modules have projective covers.
9. If P is a cyclic projective R-module, show that $P \cong eR$ for some idempotent $e \in R$. Conclude that if R has no idempotents other than 0 or 1 and if V is an irreducible R-module with a projective cover, then R is a local ring. Conversely, if R is a local ring, show that all finitely generated R-modules have projective covers.
10. Let $F \xrightarrow{\alpha} V \to 0$ be a projective cover for V with F a free R-module. Since $F \neq F \cdot \mathrm{Rad}(R)$, conclude that $V \neq V \cdot \mathrm{Rad}(R)$. Now use Exercise 2 to show that not every module over a local ring has a projective cover.

Part II
Polynomial Rings

11. Skew Polynomial Rings

Skew polynomial rings are polynomial rings in a noncommutative setting. Their study allows us to discuss and develop important concepts while working in a concrete, reasonably familiar environment.

DEFINITION Let R be a ring and let σ be an automorphism of R. We define the *skew polynomial ring* $R[x;\sigma]$ to consist of all *polynomials* $\sum_i r_i x^i$ with $r_i \in R$ and with at most finitely many of these coefficients nonzero. The addition in $R[x;\sigma]$ is as usual, but multiplication is given by

$$ax^i \cdot bx^j = ab^{\sigma^{-i}} x^{i+j}$$

for all $a, b \in R$ and integers $i, j \geq 0$. This multiplication is, of course, analogous to the semidirect product construction in groups. To check associativity, let $a, b, c \in R$. Then

$$\begin{aligned}(ax^i \cdot bx^j) \cdot cx^k &= ab^{\sigma^{-i}} x^{i+j} \cdot cx^k \\ &= ab^{\sigma^{-i}} c^{\sigma^{-i-j}} x^{i+j+k}\end{aligned}$$

and

$$\begin{aligned}ax^i \cdot (bx^j \cdot cx^k) &= ax^i \cdot bc^{\sigma^{-j}} x^{j+k} \\ &= a(bc^{\sigma^{-j}})^{\sigma^{-i}} x^{i+j+k} \\ &= ab^{\sigma^{-i}} c^{\sigma^{-i-j}} x^{i+j+k}\end{aligned}$$

as required.

We now identify $r \in R$ with rx^0, so $R \subseteq R[x;\sigma]$, and we identify x with $1x^1$. It is then clear that $R[x;\sigma]$ is the associative ring freely generated by R and x subject to the relations $rx = xr^\sigma$ for all $r \in R$. Furthermore, it follows that $R[x;\sigma]$ is symmetrically defined so that every element is also uniquely a polynomial of the form $\sum_i x^i s_i$ with $s_i \in R$. If $\sigma = 1$, then $R[x;\sigma] = R[x]$ is the ordinary polynomial ring over R.

In the course of this chapter we will be concerned with the nature of the finitely generated $R[x;\sigma]$-modules. For this, it is appropriate to work in the context of Noetherian rings. We therefore start with a noncommutative version of the classical Hilbert Basis Theorem using the same proof.

THEOREM 11.1 (Hilbert Basis Theorem) *If R is a right Noetherian ring, then so is $R[x;\sigma]$.*

PROOF We show that each right ideal of $R[x;\sigma]$ is finitely generated. Let $I \subseteq R[x;\sigma]$ be a right ideal and for each integer $n \geq 0$ define

$$I_n = \{ r \in R \mid r_0 + r_1 x + \cdots + r_n x^n \in I \text{ and } r = r_n \}$$

Since

$$(r_0 + r_1 x + \cdots + r_n x^n) s^{\sigma^n} = r_0 s^{\sigma^n} + r_1 s^{\sigma^{n-1}} x + \cdots + r_n s x^n$$

we see that I_n is a right ideal of R. In addition,

$$(r_0 + r_1 x + \cdots + r_n x^n) x = r_0 x + r_1 x^2 + \cdots + r_n x^{n+1}$$

so $I_n \subseteq I_{n+1}$.

Since R is Noetherian, the ascending chain $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ must stabilize, say at t. Furthermore, each I_i is finitely generated, so for $0 \leq i \leq t$ we can choose finite sets $\{ r_{i,j} \}$ that generate I_i. By definition, there exist $f_{i,j} \in I$ with

$$f_{i,j} = r_{i,j} x^i + \text{lower degree terms}$$

We claim that I is generated as a right ideal of $R[x;\sigma]$ by the finitely many elements $f_{i,j} \in I$.

If $f \in I$, we show by induction on its degree that $f \in \sum_{i,j} f_{i,j} R[x;\sigma]$. Since 0 is contained in the right-hand side, we can assume that $n = \deg f \geq 0$. Write $f = r_0 + r_1 x + \cdots + r_n x^n$ so that $r_n \in I_n$. If $n \leq t$, then $r_n = \sum_j r_{n,j} u_j$ for suitable $u_j \in R$; thus

$$g = f - \sum_j f_{n,j} u_j^{\sigma^n}$$

is a polynomial of lower degree contained in I. Hence $g \in \sum_{i,j} f_{i,j}R[x;\sigma]$ by induction and so f is also contained in this sum. On the other hand, if $n > t$, then $r_n \in I_n = I_t$ and there exist suitable $v_j \in R$ with

$$h = f - \sum_j f_{t,j} v_j^{\sigma^t} x^{n-t}$$

a polynomial in I with $\deg h < n$. Again, h is in the sum $\sum_{i,j} f_{i,j}R[x;\sigma]$ and hence so is f. Thus I is generated by the finitely many $f_{i,j}$ and the result follows. □

The remainder of this chapter is concerned with global dimension. Our goal is to compute $\operatorname{gl\,dim} R[x;\sigma]$ as a function of $\operatorname{gl\,dim} R$. To start with, we need

DEFINITION Let A be an R-module and let τ be an automorphism of R. Then the *conjugate module* A^τ is just an isomorphic copy of the abelian group A and we write this isomorphism as $a \mapsto a^\tau$. Furthermore, the action of R on A^τ is given by

$$a^\tau r^\tau = (ar)^\tau \quad \text{for all } a \in A,\ r \in R$$

It is easy to verify that A^τ is an R-module. Indeed, if the R-module structure of A is determined by the homomorphism $\rho\colon R \to \operatorname{End}(A)$, then the structure of A^τ is given by the composite map

$$R \xrightarrow{\tau^{-1}} R \xrightarrow{\rho} \operatorname{End}(A)$$

once A and A^τ are suitably identified.

We now obtain the first key inequality.

THEOREM 11.2 *For any ring R,*

$$\operatorname{gl\,dim} R[x;\sigma] \leq 1 + \operatorname{gl\,dim} R$$

PROOF We can assume that $\operatorname{gl\,dim} R = n < \infty$ and for convenience we write $S = R[x;\sigma]$. There are two cases to consider.

CASE 1 *Induced S-modules have projective dimension at most n.*

PROOF Let A be an R-module. Define the R-modules $A_0, A_1, \ldots, A_n$ and the projective R-modules $P_1, P_2, \ldots, P_n$ inductively so that $A_0 = A$ and

$$0 \to A_i \to P_i \to A_{i-1} \to 0$$

is exact for all $i = 1, 2, \ldots, n$. Since $\operatorname{gl\,dim} R = n$, it follows that A_n is also projective. Now ${}_RS$ is free and hence flat by Lemma 9.9(iii), so

$$0 \to A_i \otimes S \to P_i \otimes S \to A_{i-1} \otimes S \to 0$$

is an exact sequence of right S-modules for all $i = 1, 2, \ldots, n$. Furthermore, $P_i \otimes S$ and $A_n \otimes S$ are projective by Lemma 9.11(i), so we conclude that the induced S-module $A \otimes S = A_0 \otimes S$ has projective dimension at most n.

We remark that $A \otimes S = \cdot \sum_j A \otimes x^j$, since $\{ x^j \mid j = 0, 1, 2, \ldots \}$ is a basis for S as a left R-module. Thus every element of $A \otimes S$ can be written uniquely as a "polynomial" $\sum_j a_j \otimes x^j$ with "coefficients" $a_j \in A$ almost all zero. In particular, it makes sense to speak about the "degree" of such an element. □

CASE 2 *Arbitrary S-modules have projective dimension at most $n + 1$.*

PROOF If B is an S-module, then by restriction B becomes an R-module B_R and we can form the induced S-module $B_R \otimes S$. Since the map $B_R \times S \to B$ given by $b \times s \mapsto bs$ is clearly balanced, there exists a homomorphism $\xi\colon B_R \otimes S \to B$ given by $b \otimes s \mapsto bs$. It is clear that ξ is an S-module epimorphism. Let $L = \operatorname{Ker}(\xi)$.

Since $\sigma \in \operatorname{Aut}(R)$, we can also consider the conjugate R-module B_R^σ and the induced S-module $B_R^\sigma \otimes S$. Observe that the map $B_R^\sigma \times S \to B_R \otimes S$ given by

$$b^\sigma \times s \mapsto b \otimes xs - bx \otimes s$$

is balanced. Indeed, it is certainly bilinear and if $r \in R$, then $b^\sigma r^\sigma \times s = (br)^\sigma \times s$ maps to

$$\begin{aligned} br \otimes xs - brx \otimes s &= b \otimes rxs - brx \otimes s \\ &= b \otimes xr^\sigma s - bxr^\sigma \otimes s \\ &= b \otimes xr^\sigma s - bx \otimes r^\sigma s \end{aligned}$$

and this is the image of $b^\sigma \times r^\sigma s$. Thus we obtain an additive map $\eta\colon B_R^\sigma \otimes S \to B_R \otimes S$ given by

$$b^\sigma \otimes s \mapsto b \otimes xs - bx \otimes s$$

and this is clearly a right S-module homomorphism. Furthermore, since

$$\xi(b \otimes xs - bx \otimes s) = bxs - bxs = 0$$

we see that the image of η is contained in $L = \mathrm{Ker}(\xi)$.

We claim that $\eta\colon B_R^\sigma \otimes S \to L$ is in fact an isomorphism. First, let $0 \neq v \in B_R^\sigma \otimes S$ and write v as

$$v = b^\sigma \otimes x^k + \text{lower degree terms}$$

with $0 \neq b \in B$. Then

$$\eta(v) = b \otimes x^{k+1} + \text{lower degree terms}$$

so $\eta(v) \neq 0$, by the final remarks of Case 1, and hence η is one-to-one. Second, we show by induction on the degree of $\ell \in L$ that $\ell \in \mathrm{Im}(\eta)$. If $\ell \neq 0$, then clearly $\deg \ell = k + 1 \geq 1$ and we have

$$\ell = b \otimes x^{k+1} + \text{lower degree terms}$$

Thus if we set $u = b^\sigma \otimes x^k \in B_R^\sigma \otimes S$, then $\ell - \eta(u) \in L$ and has degree at most k. By induction, $\ell - \eta(u) \in \mathrm{Im}(\eta)$ and hence $\ell \in \mathrm{Im}(\eta)$, as required.

We have therefore obtained the short exact sequence

$$0 \to B_R^\sigma \otimes S \xrightarrow{\eta} B_R \otimes S \xrightarrow{\xi} B \to 0$$

of S-modules. Furthermore, by Case 1, $B_R^\sigma \otimes S$ and $B_R \otimes S$ both have projective dimension at most n. Thus by Lemma 8.7, $\mathrm{pd}_S B \leq n+1$ and, since B is arbitrary, we conclude that $\mathrm{gl\,dim}\, S \leq n + 1$. □

We will show, in fact, that $\mathrm{gl\,dim}\, R[x;\sigma] = 1 + \mathrm{gl\,dim}\, R$. For this, we need to consider ring homomorphisms.

Let $I \lhd R$ and set $\bar{R} = R/I$. If W is an $\bar{R}$-module, then via the composite homomorphism $R \to \bar{R} \to \mathrm{End}(W)$, we see that W is also an R-module. It is clear that this procedure respects submodules, unions, intersections, and direct sums. It certainly need not respect the properties of being free or projective.

Conversely, let V be an R-module. Then $\bar{V} = V \otimes_R \bar{R} = V/VI$ is an $\bar{R}$-module by Lemma 9.6. Here the procedure does not respect submodules, but we know from Lemma 9.11(i) that if V is a projective or free R-module, then $\bar{V}$ is a projective or free $\bar{R}$-module.

DEFINITION An element $\zeta \in R$ is said to be *normal* if $\zeta R = R\zeta$. When this occurs, then clearly $I = \zeta R \lhd R$. Furthermore, if V is an R-module, then $VI = V(R\zeta) = V\zeta$ and $\bar{V} = V/VI = V/V\zeta$. Obviously, 0 and the units of R are normal elements of R.

THEOREM 11.3 *Let ζ be a normal element of R that is neither a zero divisor nor a unit. If $\operatorname{gl\,dim} R/\zeta R < \infty$, then*

$$\operatorname{gl\,dim} R \geq 1 + \operatorname{gl\,dim} R/\zeta R$$

PROOF Set $\bar{R} = R/\zeta R$ and observe that $\bar{R} \neq 0$, since ζ is not a unit of R. We proceed in a series of steps.

STEP 1 *If $\bar{Q}$ is a nonzero projective $\bar{R}$-module, then $\operatorname{pd}_R \bar{Q} = 1$.*

PROOF First consider the short exact sequence

$$0 \to \zeta R \to R \to \bar{R} \to 0$$

of R-modules. Since ζ is not a zero divisor, $\zeta R \cong R$ is free and hence $\operatorname{pd}_R \bar{R} \leq 1$. Furthermore, by Lemma 8.4, the projective dimension of a direct sum is the supremum of the dimensions of the summands. It follows first that every free $\bar{R}$-module has projective dimension at most 1 as an R-module and then that the same is true for projective $\bar{R}$-modules. Thus $\operatorname{pd}_R \bar{Q} \leq 1$.

Finally, if $\operatorname{pd}_R \bar{Q} = 0$, then $\bar{Q}$ is a projective R-module and hence embeds in a free R-module. But ζ annihilates no nonzero element of a free R-module and $\bar{Q}\zeta = 0$, so we conclude that $\bar{Q} = 0$. □

STEP 2 *Let $\bar{A}$ be an $\bar{R}$-module. If $\operatorname{pd}_{\bar{R}} \bar{A} \leq 1$ and $\operatorname{pd}_R \bar{A} \leq 1$, then $\bar{A}$ is a projective $\bar{R}$-module.*

PROOF Map a free R-module F onto $\bar{A}$ to obtain the exact sequence

$$0 \to B \to F \to \bar{A} \to 0$$

Since $\operatorname{pd}_R \bar{A} \leq 1$, we know that B is a projective R-module. Notice that $B \supseteq F\zeta$, so we also get

$$0 \to B/F\zeta \to F/F\zeta \to \bar{A} \to 0$$

which we can view as an exact sequence of $\bar{R}$-modules. Since $F/F\zeta = \bar{F}$ is a free $\bar{R}$-module and $\operatorname{pd}_{\bar{R}} \bar{A} \leq 1$, we see that $B/F\zeta$ is a projective $\bar{R}$-module.

Now $B \supseteq F\zeta \supseteq B\zeta$, so the Third Isomorphism Theorem yields

$$0 \to F\zeta/B\zeta \to B/B\zeta \to B/F\zeta \to 0$$

an exact sequence of R-modules and of $\bar{R}$-modules. But $B/F\zeta$ is a projective $\bar{R}$-module, so the sequence splits and we have

$$B/B\zeta \cong F\zeta/B\zeta \oplus B/F\zeta$$

Furthermore, B is a projective R-module, so $\bar{B} = B/B\zeta$ is a projective $\bar{R}$-module and hence so is $F\zeta/B\zeta$.

Now note that $F\zeta \supseteq B\zeta \supseteq F\zeta^2$, so the Third Isomorphism Theorem yields

$$0 \to B\zeta/F\zeta^2 \to F\zeta/F\zeta^2 \to F\zeta/B\zeta \to 0$$

and this splits as $\bar{R}$-modules, since $F\zeta/B\zeta$ is projective. Thus we have

$$F\zeta/F\zeta^2 = B\zeta/F\zeta^2 \dot{+} D/F\zeta^2$$

where D is an R-module with $F\zeta^2 \subseteq D \subseteq F\zeta$. In particular, if we let $C = \{ f \in F \mid f\zeta \in D \}$, then $D = C\zeta$ and $C \supseteq F\zeta$. Furthermore, C is an R-submodule of F. Indeed, if $f \in C$ and $r \in R$, then for some $r' \in R$ we have $fr\zeta = f\zeta r' \in D$ and hence $fr \in C$.

Finally, ζ annihilates no nonzero element of F, so $F\zeta = B\zeta + C\zeta$ yields $F = B + C$ and $B\zeta \cap C\zeta = F\zeta^2$ yields $B \cap C = F\zeta$. Thus $F/F\zeta = B/F\zeta \dot{+} C/F\zeta$ and $C/F\zeta$ is a projective $\bar{R}$-module. But $C/F\zeta \cong F/B \cong \bar{A}$, so we conclude that $\bar{A}$ is a projective $\bar{R}$-module. □

STEP 3 *If $\bar{A}$ is a nonzero $\bar{R}$-module with $\operatorname{pd}_{\bar{R}} \bar{A} = k < \infty$, then $\operatorname{pd}_R \bar{A} \geq k + 1$.*

PROOF We proceed by induction on k, the case $k = 0$ following from Step 1. Now let $k \geq 1$ and map a projective $\bar{R}$-module $\bar{P}$ onto $\bar{A}$ to obtain

$$0 \to \bar{B} \to \bar{P} \to \bar{A} \to 0$$

As $\bar{R}$-modules we have $\operatorname{pd}_{\bar{R}} \bar{A} = k$, $\operatorname{pd}_{\bar{R}} \bar{P} = 0$, and hence $\operatorname{pd}_{\bar{R}} \bar{B} = k - 1$. As R-modules we have $\operatorname{pd}_R \bar{A} = a$, $\operatorname{pd}_R \bar{B} = b$, and $\operatorname{pd}_R \bar{P} = 1$ by Step 1. Furthermore, by induction, $b \geq (k-1) + 1 = k$.

If $a \geq 2$, then Lemma 8.7 implies that $a = 1 + b \geq 1 + k$ as required. On the other hand, if $a \leq 1$, then the same lemma yields $b \leq \max\{1, a\} = 1$, so $k \leq 1$. In other words, $\operatorname{pd}_R \bar{A} = a \leq 1$ and $\operatorname{pd}_{\bar{R}} \bar{A} = k \leq 1$, so Step 2 yields $k = 0$, a contradiction. Thus Step 3 is proved.

Finally, if $\operatorname{gl\,dim} \bar{R} = n < \infty$, then there exists a nonzero $\bar{R}$-module $\bar{A}$ with $\operatorname{pd}_{\bar{R}} \bar{A} = n$. We conclude that $\operatorname{gl\,dim} R \geq \operatorname{pd}_R \bar{A} \geq n + 1$ and the result follows. □

The hypothesis $\operatorname{gl\,dim} R/\zeta R < \infty$ of the preceding theorem is actually necessary. For example, let $R = \mathbb{Z}$ be the ring of integers and let $\zeta = 4$. Then ζ is a normal element of $\mathbb{Z}$ and $\operatorname{gl\,dim} \mathbb{Z} = 1$. On the other hand, by the remarks following Lemma 8.5, the global dimension of $R/\zeta R = \mathbb{Z}/4\mathbb{Z}$ is infinite.

We can now quickly prove the main result of this chapter.

COROLLARY 11.4 *If R is a ring and $\sigma \in \operatorname{Aut}(R)$, then*

$$\operatorname{gl\,dim} R[x; \sigma] = 1 + \operatorname{gl\,dim} R$$

PROOF If $S = R[x; \sigma]$, then we know from Theorem 11.2 that $\operatorname{gl\,dim} S \leq 1 + \operatorname{gl\,dim} R$. Thus the result follows if $\operatorname{gl\,dim} S = \infty$ and it suffices to assume that $\operatorname{gl\,dim} S = n < \infty$.

Since S is a free right R-module, it follows that any free S-module is a free R-module and then that any projective S-module is a projective R-module by restriction. Now let A be an arbitrary S-module and let the S-modules $A_0, A_1, \ldots, A_n$ and the projective S-modules $P_1, P_2, \ldots, P_n$ be defined inductively so that $A_0 = A$ and

$$0 \to A_i \to P_i \to A_{i-1} \to 0$$

is exact for all $i = 1, 2, \ldots, n$. Since $\operatorname{gl\,dim} S = n$, we have A_n projective. By restriction, the preceding become exact sequences of R-modules with the restrictions of all P_i and of A_n projective. Thus, clearly, $\operatorname{pd}_R A \leq n$. In particular, if B is any R-module, then the induced S-module $B \otimes S$ satisfies $\operatorname{pd}_R B \otimes S \leq n$. But $B \otimes S = \cdot \sum_i B \otimes x^i$ is a direct sum of R-submodules with $B \cong B \otimes 1$ via the map $b \mapsto b \otimes 1$. Thus B is an R-direct summand of $(B \otimes S)_R$ and hence $\operatorname{pd}_R B \leq \operatorname{pd}_R B \otimes S \leq n$. We conclude at least that $\operatorname{gl\,dim} R \leq n < \infty$.

Finally, notice that x is a normal element of S that is neither a unit nor a zero divisor. Moreover, $\bar{S} = S/xS \cong R$. Thus, since $\operatorname{gl\,dim} R < \infty$, the preceding theorem yields

$$n = \operatorname{gl\,dim} S \geq 1 + \operatorname{gl\,dim} \bar{S} = 1 + \operatorname{gl\,dim} R$$

and the reverse inequality is proved. □

COROLLARY 11.5 *Let K be a field and let $K[x_1, x_2, \ldots, x_n]$ be the ordinary polynomial ring in n variables over K. Then*

$$\operatorname{gl\,dim} K[x_1, x_2, \ldots, x_n] = n$$

PROOF This follows by induction on n, since $\operatorname{gl\,dim} K = 0$. □

The preceding is one aspect of the Hilbert Syzygy Theorem, which we consider in complete detail in Chapter 15.

EXERCISES

1. Verify that $R[x;\sigma]$ is freely generated by R and x subject to the relations $rx = xr^{\sigma}$ for all $r \in R$. Then show that R is a right $R[x;\sigma]$-module with R acting as right multiplication and with x acting like the automorphism σ. What are the $R[x;\sigma]$-submodules of R?
2. Let A be an R-module and let $\tau \in \operatorname{Aut}(R)$. Prove that A^{τ} is an R-module and verify that the action of R is determined by the composite map

$$R \xrightarrow{\tau^{-1}} R \xrightarrow{\rho} \operatorname{End}(A)$$

A *derivation* $\delta: R \to R$ is a map satisfying $\delta(a+b) = \delta(a) + \delta(b)$ and $\delta(ab) = a\delta(b) + \delta(a)b$ for all $a, b \in R$.

3. If $y \in R$, prove that the map $\operatorname{ad}_y: R \to R$ given by $\operatorname{ad}_y: r \mapsto [r, y] = ry - yr$ is a derivation of R. Such derivations are said to be *inner*.
4. Let δ be a derivation of R. Prove that $\delta(1) = 0$ and that δ extends to a derivation δ' of the ordinary polynomial ring $R[t]$ by defining $\delta'(rt^n) = \delta(r)t^n + nrt^{n-1}$ for all $n \geq 0$.

If δ is a derivation of R, then the *Ore extension* $R[x;\delta]$ is the ring freely generated by R and x subject to the relations $rx - xr = \delta(r)$ for all $r \in R$. In particular, δ is now the restriction of ad_x to R. We use this notation in the remaining exercises.

5. Show that the ordinary polynomial ring $R[X]$ is a right $R[x;\delta]$-module with R acting as right multiplication and with x acting by $X^i r \cdot x = X^{i+1}r + X^i\delta(r)$. Conclude that $1 \cdot x^j = X^j 1$ for all $j \geq 0$.
6. First show that every element of $R[x;\delta]$ can be written as a polynomial $\sum_i x^i r_i$ with $r_i \in R$. Then use the preceding module to prove that

the coefficients r_i are uniquely determined. Conclude similarly that every element of $R[x;\delta]$ is uniquely a polynomial of the form $\sum_i s_i x^i$.

7. Let R be right Noetherian and let S be any ring generated by R and some element y such that $R + Ry = R + yR$. Prove that S is right Noetherian. In particular, observe that this applies with $S = R[x;\delta]$.
8. Use the arguments of Theorem 11.2 to prove that $\operatorname{gl\,dim} R[x;\delta] \leq 1 + \operatorname{gl\,dim} R$. Here conjugate modules are not needed, but one must still verify that the map $B_R \times S \to B_R \otimes S$ given by $b \times s \mapsto b \otimes xs - bx \otimes s$ is balanced.
9. If R is a Wedderburn ring, show that $\operatorname{gl\,dim} R[x;\delta] = 1$.
10. Let K be a field of characteristic 2 and consider the matrix ring $S = \mathrm{M}_2(K[t]) = \mathrm{M}_2(K)[t]$. Let $x, y \in S$ be given by

$$x = \begin{pmatrix} 0 & t \\ 1 & 0 \end{pmatrix} \qquad y = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

If R is the subring of S generated by K and y, show that $S = R[x;\delta]$ for a suitable derivation δ. Since $\operatorname{gl\,dim} R = \infty$ and $\operatorname{gl\,dim} S = 1$, we see that $\operatorname{gl\,dim} R$ is not bounded by $\operatorname{gl\,dim} R[x;\delta]$ in this example.

In general, if $\operatorname{gl\,dim} R < \infty$, then

$$\operatorname{gl\,dim} R \leq \operatorname{gl\,dim} R[x;\delta] \leq 1 + \operatorname{gl\,dim} R$$

and either equality can occur.

12. Grothendieck Groups

The Grothendieck group of a ring R is an additive abelian group that is determined by all the finitely generated R-modules. It is important because it is simple enough to be computed, yet subtle enough to contain at least some global information on the modules. As usual, when we study such modules, it is appropriate to work in the context of Noetherian rings. Thus we will assume throughout this chapter that R is right Noetherian and we freely use the fact that submodules of finitely generated R-modules are finitely generated (Lemma 6.6).

DEFINITION Let R be a right Noetherian ring and let $\mathcal{F}$ be the free additive abelian group whose free generators are the isomorphism classes of the finitely generated R-modules. Notice that every such finitely generated module is a homomorphic image of some free R-module R^n of finite rank n. Because of this, the collection of isomorphism classes of finitely generated R-modules is a set and we can choose representatives for the individual classes from among modules of the form R^n/N, with N a submodule of R^n. In other words, the construction of $\mathcal{F}$ involves no set theoretic difficulties.

If A is a finitely generated R-module, let $\tilde{A}$ denote the generator of $\mathcal{F}$ that is its isomorphism class. Then the subgroup $\mathcal{R}$ of *relations* of $\mathcal{F}$ is defined to be the span of all expressions of the form $\tilde{B} - \tilde{A} - \tilde{C}$ whenever there exists a short exact sequence $0 \to A \to B \to C \to 0$. The abelian group $\mathcal{F}/\mathcal{R}$ is the *Grothendieck group* of R and is denoted by $\mathbf{G_0}(R)$. Furthermore, we denote the image of $\tilde{A}$ in $\mathbf{G_0}(R)$ by $[A]$. Thus $\mathbf{G_0}(R)$ is the abelian group generated by the symbols $[A]$ for all finitely generated R-modules A subject to the relations $[B] = [A] + [C]$ whenever $0 \to A \to B \to C \to 0$ is exact. Notice that $[0] = 0$, since

$0 \to 0 \to 0 \to 0 \to 0$ is exact.

LEMMA 12.1 *Let $A_1, A_2, \ldots, A_n$ be finitely generated R-modules.*

i. If

$$0 \to A_1 \to A_2 \to \cdots \to A_n \to 0$$

is exact, then $\sum_{i=1}^{n}(-)^i[A_i] = 0$ in $\mathbf{G_0}(R)$.

ii. If

$$0 = A_0 \subseteq A_1 \subseteq \cdots \subseteq A_n = A$$

then $[A] = \sum_{i=1}^{n}[A_i/A_{i-1}]$.

PROOF (i) We proceed by induction on n, the cases $n \leq 3$ being clear. If $n > 3$ and C is the image of the map $A_{n-2} \to A_{n-1}$, then the original sequence separates into the two exact sequences

$$0 \to A_1 \to A_2 \to \cdots \to A_{n-2} \to C \to 0$$

and $0 \to C \to A_{n-1} \to A_n \to 0$. Thus

$$\sum_{i=1}^{n-2}(-)^i[A_i] + (-)^{n-1}[C] = 0$$

by induction and, since $[C] - [A_{n-1}] + [A_n] = 0$, the result follows.

(ii) This part is clear, since $[A_i/A_{i-1}] = [A_i] - [A_{i-1}]$ and since $[A_0] = [0] = 0$. □

Now let us compute some examples. Part (i) of Lemma 12.2 is a key observation. We paraphrase its hypothesis by saying that θ' *respects short exact sequences.* The statement of part (ii) implicitly uses Proposition 5.5.

LEMMA 12.2 *Let R be a ring.*

i. Let $\mathcal{A}$ be an additive abelian group and let θ' be a map from the collection of all finitely generated R-modules to $\mathcal{A}$. Suppose $\theta'(B) = \theta'(A) + \theta'(C)$ whenever $0 \to A \to B \to C \to 0$ is exact. Then θ' determines a homomorphism $\theta\colon \mathbf{G_0}(R) \to \mathcal{A}$ given by $\theta([A]) = \theta'(A)$.

ii. Assume that R is right Artinian and let $V_1, V_2, \ldots, V_k$ be representatives of the finitely many isomorphism classes of simple R-modules. Then $\mathbf{G_0}(R)$ is the free abelian group on the generators $[V_1], [V_2], \ldots, [V_k]$.

Furthermore, the composition length of a module determines a group homomorphism $\rho: \mathbf{G_0}(R) \to \mathbb{Z}$.

PROOF (i) From the exact sequence $0 \to 0 \to 0 \to 0 \to 0$, we see that $\theta'(0) = \theta'(0) + \theta'(0)$ and hence that $\theta'(0) = 0 \in \mathcal{A}$. Next from $0 \to 0 \to B \to C \to 0$, we see that $B \cong C$ implies that $\theta'(B) = \theta'(C)$. Since $\mathcal{F}$ is free abelian, we can now define $\theta: \mathcal{F} \to \mathcal{A}$ by $\theta(\tilde{A}) = \theta'(A)$. Furthermore, since $\theta(\mathcal{R}) = 0$, this map factors through $\mathbf{G_0}(R) = \mathcal{F}/\mathcal{R}$.

(ii) Now let R be Artinian. Since every finitely generated R-module has a composition series by the Hopkins-Levitzki Theorem, it follows from Lemma 12.1(ii) that $\mathbf{G_0}(R)$ is spanned by $[V_1], [V_2], \ldots, [V_k]$. For independence, let $\mathcal{A}$ be the free abelian group on the generators $v_1, v_2, \ldots, v_k$ and for each finitely generated R-module A, define $\theta'(A) = \sum_j m_j v_j \in \mathcal{A}$, where m_j is the multiplicity of V_j as a composition factor of A. Then $\theta'(A)$ is well defined, by the Jordan-Hölder Theorem, and it respects short exact sequences. Thus by (i), θ' determines a homomorphism $\theta: \mathbf{G_0}(R) \to \mathcal{A}$. But $\theta([V_i]) = \theta'(V_i) = v_i$ and hence it follows that $[V_1], [V_2], \ldots, [V_k]$ are also independent. Finally for the result concerning ρ, we need only observe that the composition length of A is a well-defined integer that respects short exact sequences. □

Next we consider the behavior of $\mathbf{G_0}$ under a change of rings. Recall that if $\phi: R \to S$ is a ring homomorphism with $\phi(1) = 1$, then S becomes an (R, S)-bimodule with $r \cdot s = \phi(r)s$ for all $r \in R$ and $s \in S$. Furthermore, if A is a right R-module, then $A \otimes_R S$ is the right S-module induced from A.

LEMMA 12.3 *Let R and S be Noetherian rings and let $\phi: R \to S$ be a ring homomorphism. If ${}_RS$ is flat, then the induced module map $A \mapsto A \otimes S$ determines a homomorphism $\theta: \mathbf{G_0}(R) \to \mathbf{G_0}(S)$ given by $[A] \mapsto [A \otimes S]$.*

PROOF If $A = \sum_1^n a_i R$ is a finitely generated R-module, then $A \otimes S$ is a finitely generated S-module with generators $a_i \otimes 1$ for $i = 1, 2, \ldots, n$. Thus $\theta': A \mapsto [A \otimes S]$ is a well-defined map from the finitely generated R-modules to $\mathbf{G_0}(S)$. Furthermore, since ${}_RS$ is flat, if $0 \to A \to B \to C \to 0$ is exact, then so is

$$0 \to A \otimes S \to B \otimes S \to C \otimes S \to 0$$

Thus

$$\begin{aligned} \theta'(B) &= [B \otimes S] = [A \otimes S] + [C \otimes S] \\ &= \theta'(A) + \theta'(C) \end{aligned}$$

and θ' respects short exact sequences. By Lemma 12.2(i), θ' determines the appropriate map $\theta\colon \mathbf{G_0}(R) \to \mathbf{G_0}(S)$. □

As an application, we compute the Grothendieck group of $\mathbb{Z}$.

LEMMA 12.4 *If $\mathbb{Z}$ is the ring of integers, then $\mathbf{G_0}(\mathbb{Z})$ is the infinite cyclic group generated by $[\mathbb{Z}]$.*

PROOF Let n be a positive integer. Then $n\mathbb{Z} \cong \mathbb{Z}$ as $\mathbb{Z}$-modules, so $[n\mathbb{Z}] = [\mathbb{Z}]$ in $\mathbf{G_0}(\mathbb{Z})$ and hence $[\mathbb{Z}/n\mathbb{Z}] = [\mathbb{Z}] - [n\mathbb{Z}] = 0$. Now every finitely generated $\mathbb{Z}$-module is a finite direct sum of copies of $\mathbb{Z}$ and of $\mathbb{Z}/n\mathbb{Z}$ for various n. Thus we conclude from the preceding and Lemma 12.1(ii) that $\mathbf{G_0}(\mathbb{Z})$ is generated by the single element $[\mathbb{Z}]$. It remains to show that $[\mathbb{Z}]$ has infinite order. To this end, let $\mathbb{Q}$ be the field of rational numbers, let $\phi\colon \mathbb{Z} \to \mathbb{Q}$ be the usual embedding, and note that ${}_{\mathbb{Z}}\mathbb{Q}$ is flat by Lemma 9.10. Thus the preceding result implies that the induced module map yields a homomorphism $\theta\colon \mathbf{G_0}(\mathbb{Z}) \to \mathbf{G_0}(\mathbb{Q})$. Furthermore, by Lemma 12.2(ii), $\mathbf{G_0}(\mathbb{Q})$ is the infinite cyclic group generated by $[\mathbb{Q}]$. Since $\mathbb{Z} \otimes \mathbb{Q} \cong \mathbb{Q}$, we have $\theta([\mathbb{Z}]) = [\mathbb{Q}]$ and $[\mathbb{Z}]$ does indeed have infinite order. □

There are, in fact, more exotic maps between the Grothendieck groups of rings. For example, let $S = R[x;\sigma]$ and note that x is a normal element of S. Thus if A is an S-module, then A/Ax is an S-module and hence an R-module, since $R \subseteq S$. Next, $xS = Sx$ implies that $\mathrm{l.ann}_A(x) = \{\, a \in A \mid ax = 0 \,\}$ is an S-submodule of A and hence also an R-submodule. Since $\sigma \in \mathrm{Aut}(R)$, it therefore makes sense to consider the conjugate R-module $\mathrm{l.ann}_A(x)^\sigma$.

LEMMA 12.5 *Let $S = R[x;\sigma]$ and let $0 \to A \to B \to C \to 0$ be an exact sequence of right S-modules. Then there exists a long exact sequence*

$$0 \to \mathrm{l.ann}_A(x)^\sigma \to \mathrm{l.ann}_B(x)^\sigma \to \mathrm{l.ann}_C(x)^\sigma \to A/Ax \to B/Bx \to C/Cx \to 0$$

of R-modules.

PROOF We may suppose that $A \subseteq B$ and let $\bar{}\colon B \to C$ denote the given epimorphism. Since $A + Bx$ is the complete inverse image of Cx in B, it follows that

$$0 \to (A + Bx)/Bx \to B/Bx \to C/Cx \to 0$$

is exact. Furthermore, $(A + Bx)/Bx \cong A/(A \cap Bx)$ and

$$0 \to (A \cap Bx)/Ax \to A/Ax \to A/(A \cap Bx) \to 0$$

is exact by the Third Isomorphism Theorem. The maps here are, of course, all S-homomorphisms and hence R-homomorphiisms. It therefore suffices to construct an exact sequence

$$0 \to \text{l.ann}_A(x)^\sigma \to \text{l.ann}_B(x)^\sigma \to \text{l.ann}_C(x)^\sigma \to (A \cap Bx)/Ax \to 0$$

To this end, let $c \in \text{l.ann}_C(x)$ and say $c = \bar{b}$ with $b \in B$. Then $0 = cx = \bar{b}x$, so $bx \in A \cap Bx$. Furthermore, b is unique up to a summand in A, so bx is uniquely determined by c up to a summand in Ax. Thus we have a well-defined map

$$\delta\colon \text{l.ann}_C(x)^\sigma \to (A \cap Bx)/Ax$$

given by $c^\sigma \mapsto bx + Ax$ if $c = \bar{b}$. Observe that if $r \in R$ and if b and c are as before, then $cr = \overline{br}$, so

$$\begin{aligned}\delta(c^\sigma r^\sigma) &= \delta\big((cr)^\sigma\big) = brx + Ax \\ &= bxr^\sigma + Ax = \delta(c^\sigma)r^\sigma\end{aligned}$$

and δ is indeed an R-homomorphism. Moreover, δ is onto, since $bx \in A \cap Bx$ implies that $0 = \overline{bx} = \bar{b}x$, so $\bar{b} \in \text{l.ann}_C(x)$ and $\delta(\bar{b}^\sigma) = bx + Ax$.

Finally, suppose $\delta(\bar{b}^\sigma) = 0$. Then $bx \in Ax$, so $bx = ax$ for some $a \in A$ and $(b - a)x = 0$. Also $\overline{b - a} = \bar{b}$. Thus we see that $\text{Ker}(\delta)$ is the image of $\text{l.ann}_B(x)^\sigma$ under the R-homomorphism given by $b^\sigma \mapsto (\bar{b})^\sigma$. But the kernel of $\bar{}\colon \text{l.ann}_B(x) \to \text{l.ann}_C(x)$ is $A \cap \text{l.ann}_B(x) = \text{l.ann}_A(x)$, so the lemma is proved. □

As a consequence we have:

PROPOSITION 12.6 *Let R be a right Noetherian ring and let $S = R[x;\sigma]$. Then there is a group homomorphism $\theta\colon \mathbf{G_0}(S) \to \mathbf{G_0}(R)$ given by*

$$[A] \mapsto [A/Ax] - [\text{l.ann}_A(x)^\sigma]$$

for all finitely generated S-modules A.

PROOF Since R is Noetherian, so is S. If A is a finitely generated S-module, then both A/Ax and $\text{l.ann}_A(x)$ are finitely generated S-modules. But $S = R + xS$ and xS acts trivially on each of these modules, so we

conclude that both A/Ax and $\mathrm{l.ann}_A(x)$ are finitely generated R-modules. Hence so is $\mathrm{l.ann}_A(x)^\sigma$ and it makes sense to define

$$\theta'(A) = [A/Ax] - [\mathrm{l.ann}_A(x)^\sigma] \in \mathbf{G_0}(R)$$

Now suppose $0 \to A \to B \to C \to 0$ is an exact sequence of S-modules. Then by the preceding lemma we have

$$0 \to \mathrm{l.ann}_A(x)^\sigma \to \mathrm{l.ann}_B(x)^\sigma \to \mathrm{l.ann}_C(x)^\sigma \to A/Ax \to B/Bx \to C/Cx \to 0$$

an exact sequence of finitely generated R-modules. By Lemma 12.1(i), this yields

$$[\mathrm{l.ann}_A(x)^\sigma] - [\mathrm{l.ann}_B(x)^\sigma] + [\mathrm{l.ann}_C(x)^\sigma] - [A/Ax] + [B/Bx] - [C/Cx] = 0$$

in $\mathbf{G_0}(R)$ and hence $\theta'(B) - \theta'(A) - \theta'(C) = 0$. Lemma 12.2(i) now implies that θ' determines a group homomorphism $\theta\colon \mathbf{G_0}(S) \to \mathbf{G_0}(R)$. □

In case R has finite global dimension, the finitely generated projective R-modules determine $\mathbf{G_0}(R)$. We will make this statement more precise in Chapter 15. For now we prove:

LEMMA 12.7 *Assume that all finitely generated R-modules have finite projective dimension and let $\mathcal{P}$ denote the collection of finitely generated projective R-modules.*

i. $\mathbf{G_0}(R)$ is spanned by the elements $[P]$ for all $P \in \mathcal{P}$.

ii. Let $\mathcal{A}$ be an additive abelian group and assume that for each $P \in \mathcal{P}$, we have $\theta'(P) \in \mathcal{A}$. Furthermore, suppose $\theta'(P_3) = \theta'(P_1) + \theta'(P_2)$ whenever $P_3 \cong P_1 \oplus P_2$. Then θ' determines a group homomorphism $\theta\colon \mathbf{G_0}(R) \to \mathcal{A}$ satisfying $\theta([P]) = \theta'(P)$ for all $P \in \mathcal{P}$.

PROOF As usual, we freely use the fact that submodules of finitely generated R-modules are finitely generated.

(i) Let A be a finitely generated R-module. We show by induction on $k = \mathrm{pd}\, A$ that $[A]$ is in the span of $[P]$ for all $P \in \mathcal{P}$. This is clear, by definition, when $k = 0$. If $k > 0$, choose $P' \in \mathcal{P}$ with $0 \to B \to P' \to A \to 0$ exact. Then $[A] = [P'] - [B]$ and $\mathrm{pd}\, B = k - 1$. By induction $[B]$ is in the appropriate span and hence so is $[A]$.

(ii) Now we show by induction on $k = \mathrm{pd}\, A$ that $\theta'(A) \in \mathcal{A}$ can be defined so that

a. If $0 \to B \to P \to A \to 0$ is exact and $P \in \mathcal{P}$, then $\theta'(A)+\theta'(B) = \theta'(P)$.

b. If $C \cong A \oplus P_1$ with $P_1 \in \mathcal{P}$, then $\theta'(C) = \theta'(A) + \theta'(P_1)$.

First we verify the case $k = 0$. Here A is projective, so the sequence in (a) splits and $P \cong A \oplus B$. Then B is also projective and $\theta'(A)+\theta'(B) = \theta'(P)$ follows by hypothesis. Similarly, in (b) the module C must be projective, so this again follows by hypothesis.

Now suppose $k > 0$ and that the result holds for $k-1$. If the sequences $0 \to B \to P \to A \to 0$ and $0 \to B_1 \to P_1 \to A \to 0$ are both exact and $P, P_1 \in \mathcal{P}$, then by Schanuel's Lemma (Lemma 8.1) we have $B \oplus P_1 \cong B_1 \oplus P$. Furthermore, $\operatorname{pd} B = \operatorname{pd} B_1 = k-1$. Thus statement (b) for $k-1$ yields

$$\begin{aligned}\theta'(B) + \theta'(P_1) &= \theta'(B \oplus P_1) \\ &= \theta'(B_1 \oplus P) = \theta'(B_1) + \theta'(P)\end{aligned}$$

and hence $\theta'(P) - \theta'(B) = \theta'(P_1) - \theta'(B_1)$. We can now define $\theta'(A)$ unambiguously by $\theta'(A) = \theta'(P) - \theta'(B)$ and, with this, (a) follows. For (b), observe that if $0 \to B \to P \to A \to 0$ is exact and $C \cong A \oplus P_1$, then $0 \to B \to P \oplus P_1 \to C \to 0$ is also exact. Furthermore, $\operatorname{pd} C = \operatorname{pd} A = k$, so this yields

$$\begin{aligned}\theta'(C) &= \theta'(P \oplus P_1) - \theta'(B) \\ &= \theta'(P) + \theta'(P_1) - \theta'(B) = \theta'(A) + \theta'(P_1)\end{aligned}$$

as required. Thus, by induction, (a) and (b) are true in general.

It remains to show that θ' respects short exact sequences. To this end, suppose $0 \to A \to B \to C \to 0$ is exact. The goal is to show that $\theta'(B) = \theta'(A) + \theta'(C)$ and we proceed by induction on the sum of the three projective dimensions. If $\operatorname{pd} C = 0$, then $C \in \mathcal{P}$ and the sequence splits. Thus $B \cong A \oplus C$ and $\theta'(B) = \theta'(A) + \theta'(C)$ by (b). On the other hand, if $\operatorname{pd} B = 0$, then $B \in \mathcal{P}$, so $\theta'(B) = \theta'(A) + \theta'(C)$ by (a).

Finally, suppose that $\operatorname{pd} B$, $\operatorname{pd} C > 0$. Then by Lemma 8.6, there exist finitely generated modules D, E, and $P \in \mathcal{P}$ with

$$\begin{aligned}&0 \to D \to P \to B \to 0 \\ &0 \to E \to P \to C \to 0 \\ &0 \to D \to E \to A \to 0\end{aligned}$$

all exact. In particular, $\operatorname{pd} D = \operatorname{pd} B - 1$ and $\operatorname{pd} E = \operatorname{pd} C - 1$, so (a) and induction yield $\theta'(B) = \theta'(P) - \theta'(D)$, $\theta'(C) = \theta'(P) - \theta'(E)$ and $\theta'(E) = \theta'(A) + \theta'(D)$. Thus

$$\theta'(B) - \theta'(C) = \theta'(E) - \theta'(D) = \theta'(A)$$

and θ' does indeed respect short exact sequences. By Lemma 12.2(i), θ' determines a homomorphism $\theta\colon \mathbf{G_0}(R) \to \mathcal{A}$ satisfying $\theta([P]) = \theta'(P)$ for all $P \in \mathcal{P}$. □

EXERCISES

Let R be a ring and let e be a nonzero idempotent of R; assume that $R = ReR$ so that $1 = \sum_1^n r_i e r_i'$ for suitable $r_i, r_i' \in R$. If A is a right module for the ring eRe, then, since eR is an (eRe, R)-bimodule, we can define the right R-module $\alpha(A)$ by $\alpha(A) = A \otimes_{eRe} eR$. Conversely, if B is an R-module, define the right eRe-module $\beta(B)$ by $\beta(B) = Be$. The following six problems are aspects of the classical *Morita correspondence*. We use all the preceding notation.

1. Show that α and β are inverse maps and thus yield a one-to-one correspondence between the isomorphism classes of right eRe-modules and of right R-modules. To prove that $\alpha\beta(B) \cong B$, first observe that there is an R-module homomorphism $\eta\colon Be \otimes_{eRe} eR \to B$ given by $be \otimes er \mapsto ber$. Then note that η is onto and that $\mathrm{Ker}(\eta)\, e = 0$.
2. Use the maps $\sigma\colon (eRe)^n \to Re$ and $\tau\colon Re \to (eRe)^n$ defined by

$$\sigma\colon (s_1, s_2, \ldots, s_n) \mapsto \sum_1^n r_i s_i$$

$$\tau\colon re \mapsto (er_1're, er_2're, \ldots, er_n're)$$

to prove that Re is a finitely generated projective right eRe-module. In the same way, eR is a finitely generated projective left eRe-module.
3. Show that A is finitely generated or projective if and only if $\alpha(A)$ is finitely generated or projective.
4. Prove that α and β are exact functors. In other words, show that if

$$0 \to A_1 \xrightarrow{\epsilon} A_2 \xrightarrow{\delta} A_3 \to 0$$

is an exact sequence of eRe-modules, then

$$0 \to \alpha(A_1) \xrightarrow{\epsilon \otimes 1} \alpha(A_2) \xrightarrow{\delta \otimes 1} \alpha(A_3) \to 0$$

is an exact sequence of R-modules. Furthermore, show that if

$$0 \to B_1 \xrightarrow{\epsilon'} B_2 \xrightarrow{\delta'} B_3 \to 0$$

is an exact sequence of R-modules, then

$$0 \to \beta(B_1) \xrightarrow{\epsilon'} \beta(B_2) \xrightarrow{\delta'} \beta(B_3) \to 0$$

is an exact sequence of eRe-modules using the same homomorphisms restricted to the subsets $\beta(B) = Be \subseteq B$.

5. Prove that $\mathrm{pd}_{eRe} A = \mathrm{pd}_R \alpha(A)$. Furthermore, if R is right Noetherian, show that eRe is also right Noetherian and deduce that $\mathbf{G_0}(R)$ and $\mathbf{G_0}(eRe)$ are isomorphic via maps determined by α and β.
6. What does all this say about the matrix ring $R = \mathrm{M}_m(S)$?

The remaining exercises use the following notation. Let R be a ring and let $R[x]$ be the ordinary polynomial ring over R. If I is an ideal of R, define $R(I)$ to be the subring of $R[x]$ given by

$$R(I) = R + Ix + I^2x^2 + \cdots$$

If V is an R-module, then

$$V \otimes R[x] = V \otimes 1 \dotplus V \otimes x \dotplus V \otimes x^2 \dotplus \cdots$$

is an $R[x]$-module and we define $V(I) \subseteq V \otimes R[x]$ by

$$V(I) = V \otimes 1 \dotplus VI \otimes x \dotplus VI^2 \otimes x^2 \dotplus \cdots$$

7. If R is right Noetherian and if I is generated by finitely many central elements of R, prove that $R(I)$ is right Noetherian. This, of course, always holds when R is commutative.
8. If V is a finitely generated R-module, show that $V(I)$ is a finitely generated $R(I)$-module.
9. Let W be a submodule of V. Show that

$$\widetilde{W} = W \otimes 1 \dotplus (W \cap VI) \otimes x \dotplus (W \cap VI^2) \otimes x^2 \dotplus \cdots$$

is an $R(I)$-submodule of $V(I)$. If $\widetilde{W}$ is finitely generated as an $R(I)$-module, prove that $W \cap VI^n \subseteq WI$ for some integer $n \geq 0$.
10. Suppose R is right Noetherian and that I is generated by finitely many central elements. If V is a finitely generated R-module and $W \subseteq V$, prove that $W \cap VI^n \subseteq WI$ for some integer $n \geq 0$. This is the (weak) Artin-Rees Lemma.

13. Graded Rings and Modules

The ultimate goal of these few chapters is to prove that $\mathbf{G_0}(R)$ is isomorphic to $\mathbf{G_0}(R[x;\sigma])$ via the induced module map. To do this, it is necessary to take a brief detour through graded rings and modules.

DEFINITION A ring S is said to be *graded* if it is the direct sum

$$S = S_0 \dot{+} S_1 \dot{+} \cdots \dot{+} S_n \dot{+} \cdots$$

of the additive abelian subgroups S_n and if multiplication satisfies

$$S_i S_j \subseteq S_{i+j} \qquad \text{for all } i, j \geq 0$$

The nonzero elements of the component S_n are called *homogeneous* of degree n. Of course, $S = R[x;\sigma]$ is graded with $S_n = Rx^n$.

Now let $S_+ = S_1 \dot{+} S_2 \dot{+} \cdots$, so that S_+ is clearly a two-sided ideal of S. Note that if $1 = s_0 + s'$ with $s_0 \in S_0$ and $s' \in S_+$, then for all $s \in S_n$ we have $s = 1s = s_0 s + s's$ and matching terms of degree n yields $s = s_0 s$. Similarly $s = s s_0$, so s_0 acts like the identity on all homogeneous elements of S and thus clearly on all elements of S. In other words, $1 = s_0 \in S_0$. Since $(S_0)^2 \subseteq S_0$, it now follows that S_0 is a subring of S with the same 1. Moreover, the projection map $\pi: S \to S_0$, which sends an element to its zeroth component, is a ring epimorphism with kernel S_+.

An S-module V is said to be *graded* if

$$V = V_0 \dot{+} V_1 \dot{+} \cdots \dot{+} V_n \dot{+} \cdots$$

is a direct sum of the additive abelian subgroups V_n and if

$$V_i S_j \subseteq V_{i+j} \qquad \text{for all } i, j \geq 0$$

In particular, each V_n is an S_0-submodule of V and, as above, the nonzero elements of V_n are called *homogeneous* of degree n. Obviously, S is graded as a right S-module.

Now let W and V be graded S-modules. Then $\alpha: W \to V$ is a *graded homomorphism* if it is an S-module homomorphism with $\alpha(W_n) \subseteq V_n$ for all n. In particular, W is a *graded submodule* of V if $W \subseteq V$ and $W_n = W \cap V_n \subseteq V_n$ for all n.

Some basic properties are as follows.

LEMMA 13.1 *Let U, V and W be graded S-modules with $W \subseteq V$.*

i. W is a graded submodule of V if and only if it is generated by homogeneous elements of V.

ii. If $\alpha: V \to U$ is a graded homomorphism, then $\mathrm{Ker}(\alpha)$ *is a graded submodule of V.*

iii. If W is a graded submodule of V, then $V/W = \cdot\sum_i V_i/W_i$ is a graded S-module and the natural map $V \to V/W$ is a graded homomorphism.

iv. Let W be a graded submodule of V and suppose that $V = W \dot{+} X$ for some submodule X of V. Then there exists a graded submodule Y of V with $V = W \dot{+} Y$.

PROOF (i) If W is a graded submodule of V, then $W = \cdot\sum_i W_i = \cdot\sum_i (W \cap V_i)$ is generated by the homogeneous elements $W \cap V_n$ of V for all n. Conversely, suppose W is generated by homogeneous elements of V. Then $\sum_i (W \cap V_i)$ is a direct sum that is easily seen to be a graded submodule of V contained in W. But, by hypothesis, this sum contains all the generators of W. Thus $W = \cdot\sum_i (W \cap V_i)$ as required.

(ii), (iii) These are obvious.

(iv) For each n, define $W'_n = \cdot\sum_{i \neq n} W_i$ and set $Y_n = (W'_n + X) \cap V_n$. Since $V = W_n \dot{+} W'_n \dot{+} X$ and $W_n \subseteq V_n$, the Modular Law yields

$$\begin{aligned} V_n = V \cap V_n &= (W_n \dot{+} W'_n \dot{+} X) \cap V_n \\ &= W_n \dot{+} \big((W'_n + X) \cap V_n\big) = W_n \dot{+} Y_n \end{aligned}$$

In particular, if $Y = \cdot\sum_i Y_i$, then $V = W \dot{+} Y$. Finally, note that $W'_n S_k \subseteq W'_{n+k}$, so $Y_n S_k \subseteq Y_{n+k}$ and we conclude that Y is an appropriate graded complement for W in V. □

DEFINITION We say that F is a *graded-free* S-module if it is a free S-module with a homogeneous basis. Suppose, for example, that $\{ f_i \}$ is such a basis and that $\deg f_i = d_i$. Let U be any graded S-module and let $\{ u_i \}$

be any set of homogeneous elements of U with $\deg u_i = d_i$. Then there exists an S-homomorphism $F \to U$ determined by $f_i \mapsto u_i$ for all i and this map is clearly a graded homomorphism.

Now let P be a graded S-module. We say that P is *graded-projective* if and only if whenever we are given

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow \beta & & \\ V & \xrightarrow{\alpha} & W & \to & 0 \end{array}$$

with V and W graded modules and with α and β graded maps, then there exists a graded homomorphism $\gamma: P \to V$ satisfying $\alpha\gamma = \beta$.

As with ordinary modules, we can easily show:

LEMMA 13.2 *Let S be a graded ring.*

i. Every graded S-module U is a homomorphic image of a graded-free module F. Furthermore, if U is finitely generated, then we may take F to be finitely generated.

ii. P is graded-projective if and only if $P \dotplus Q = F$, where P and Q are graded submodules of the graded-free module F.

PROOF (i) If U is a graded S-module, then U has homogeneous generators. Furthermore, if U is finitely generated, then, by taking the components of each generator, we see that U is generated by finitely many homogeneous elements. Now apply the comments contained in the preceding definition.

(ii) This follows as in Lemma 2.7 and Theorem 2.8. □

Graded modules that happen to be free are not necessarily graded-free. For example, suppose $S = S_0$ is commutative and let $e \neq 0, 1$ be an idempotent of the ring. Then $V = V_0 \dotplus V_1$ with $V_0 = eS$ and $V_1 = (1-e)S$ is clearly free but not graded-free. On the other hand, we have:

LEMMA 13.3 *Let P be a graded S-module. Then P is graded-projective if and only if it is projective.*

PROOF If P is graded-projective, then, by the previous lemma, $P \dotplus Q = F$ for some graded-free module F. But F is free and therefore P is projective. Conversely, let P be graded and projective and let $\alpha: F \to P$ be a graded epimorphism with F graded-free. Since P is projective, the sequence splits, but the back map need not be graded. In any case, if

$W = \mathrm{Ker}(\alpha)$, then W is a graded submodule of F, $F/W \cong P$, and $F = W \dotplus X$ for some submodule X. Lemma 13.1(iv) now implies that there exists a graded submodule Y of F with $F = W \dotplus Y$. But Y is graded isomorphic to $F/W \cong P$ and thus P is graded-projective by Lemma 13.2(ii). □

We now state the graded version of Nakayama's Lemma. It is a trivial observation but surprisingly powerful. Indeed, it is the main reason for this graded excursion.

LEMMA 13.4 (Graded Nakayama's Lemma) *Let S be a graded ring and let V be a graded S-module.*

i. If $VS_+ = V$, then $V = 0$.

ii. If W is a graded submodule of V and $V = W + VS_+$, then $V = W$.

PROOF (i) For all $n \geq 0$, we have $V = V(S_+)^n$, so V contains no homogeneous elements of degree less than n. Since V is generated by homogeneous elements, we conclude that $V = 0$.

(ii) If $^- : V \to V/W$ is the natural graded homomorphism, then $V = W + VS_+$ yields $\bar{V} = \bar{V}S_+$. Thus $\bar{V} = 0$ and $V = W$. □

As is to be expected, there is a graded analog of the Grothendieck group $\mathbf{G_0}$. The definition of this group is slightly complicated because we must consider both graded homomorphisms and abstract (that is, not necessarily graded) isomorphisms. Again, it is appropriate to work in the context of Noetherian rings.

DEFINITION Let $S = S_0 \dotplus S_1 \dotplus \cdots$ be a right Noetherian graded ring and let $\mathcal{F}$ be the free additive abelian group whose free generators are the isomorphism classes of finitely generated graded S-modules. If A is such a graded S-module, then we let $\tilde{A}$ denote the generator of $\mathcal{F}$ that is its isomorphism class. In other words, if A and B are graded S-modules that are abstractly isomorphic, then $\tilde{A} = \tilde{B}$ even though A and B need not be graded isomorphic. Thus, for example, if A is graded in two different ways, then these two modules are abstractly isomorphic and hence yield the same generator $\tilde{A}$.

Now we define the subgroup $\mathcal{R}$ of *relations* of $\mathcal{F}$ to be generated by all expressions of the form $\tilde{B} - \tilde{A} - \tilde{C}$ whenever there exists a short exact sequence $0 \to A \to B \to C \to 0$ with graded homomorphisms. The abelian group $\mathcal{F}/\mathcal{R}$ is called the *graded Grothendieck group* of S and is denoted by $\mathbf{gr}\,\mathbf{G_0}(S)$. Furthermore, we denote the image of $\tilde{A}$ in $\mathbf{gr}\,\mathbf{G_0}(S)$ by $[A]$. Thus $\mathbf{gr}\,\mathbf{G_0}(S)$ is the abelian group generated by the symbols $[A]$

for all finitely generated graded S-modules A subject to the relations $[A] = [B]$ if $A \cong B$ and $[B] = [A] + [C]$ whenever $0 \to A \to B \to C \to 0$ is graded exact. Notice that $[0] = 0$.

The following lemma indicates how these two types of relations can be combined into one. Again, we paraphrase its hypothesis by saying that θ' *respects graded short exact sequences.* Note, however, that β is not assumed to be a graded map.

LEMMA 13.5 *Let S be a graded ring, let $\mathcal{A}$ be an additive abelian group and let θ' be a map from the collection of finitely generated graded S-modules to $\mathcal{A}$. If $\theta'(B) = \theta'(A) + \theta'(C)$ whenever*

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

is exact with α a graded homomorphism, then θ' determines a group homomorphism θ: $\mathbf{gr}\,\mathbf{G_0}(S) \to \mathcal{A}$ given by $\theta([A]) = \theta'(A)$.

PROOF From the exact sequence $0 \to 0 \to 0 \to 0 \to 0$ we see that $\theta'(0) = \theta'(0) + \theta'(0)$ and hence that $\theta'(0) = 0 \in \mathcal{A}$. Next from $0 \to 0 \to B \to C \to 0$ we see that $B \cong C$ implies that $\theta'(B) = \theta'(C)$. Of course, the inclusion map $0 \to B$ is a graded homomorphism here. Since $\mathcal{F}$ is free abelian, we can now define $\theta: \mathcal{F} \to \mathcal{A}$ by $\theta(\tilde{A}) = \theta'(A)$. Furthermore, since $\theta(\mathcal{R}) = 0$, this map factors through $\mathbf{gr}\,\mathbf{G_0}(S) = \mathcal{F}/\mathcal{R}$. □

Again, let $S = \cdot \sum_{i=0}^{\infty} S_i$ be graded and form the ordinary polynomial ring $S[y]$. Then $S[y]$ is graded by *total degree* if we define

$$\deg S_i y^j = i + j \qquad \text{for all } i, j$$

In particular, $S[y]_0 = S_0$. The following is a key result. Notice that the ring homomorphism that occurs here "cuts across the grade."

PROPOSITION 13.6 *Let $S = \cdot \sum_{i=0}^{\infty} S_i$ be a right Noetherian graded ring and let the polynomial ring $S[y]$ be graded by total degree. Then the ring homomorphism $S[y] \to S$ given by $y \mapsto 1$ determines a group epimorphism $\mathbf{gr}\,\mathbf{G_0}(S[y]) \to \mathbf{G_0}(S)$.*

PROOF Note that $S[y]$ is right Noetherian and that the kernel of the homomorphism ϕ: $S[y] \to S$ is the principal ideal $I = (y-1)S[y]$ generated by the central element $y - 1$. Since $y - 1$ is a normal element of $S[y]$, Lemmas 9.6 and 9.11(i) imply that ϕ determines a map from the finitely generated $S[y]$-modules to the finitely generated S-modules given by

$$A \mapsto A \otimes_{S[y]} S \cong A/AI = A/A(y-1)$$

In particular, we get a map θ' from the finitely generated graded $S[y]$-modules to $\mathbf{G_0}(S)$ by defining $\theta'(A) = [A/A(y-1)] \in \mathbf{G_0}(S)$. This, in turn, yields a group homomorphism from $\mathbf{gr}\,\mathbf{G_0}(S[y])$ to $\mathbf{G_0}(S)$, provided we show that θ' respects graded short exact sequences.

To this end, let

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

be a short exact sequence of graded modules with α a graded homomorphism. We may, of course, suppose that A is a submodule of B; then, since α is graded, A is in fact a graded submodule of B. The goal is to show that there exists an exact sequence

$$0 \to A/A(y-1) \to B/B(y-1) \to C/C(y-1) \to 0$$

of S-modules and, in view of Lemma 9.6, it merely suffices to show that $A \cap BI = AI$ or, equivalently, that $A \cap B(y-1) = A(y-1)$. Certainly we have $A \cap B(y-1) \supseteq A(y-1)$.

For the converse, suppose $\sum_i a_i \in A$ and $\sum_i b_i \in B$ are elements written in terms of their homogeneous components with

$$\sum_i a_i = \Big(\sum_i b_i\Big)(y-1) \in A \cap B(y-1)$$

Then by comparing homogenous components we have $a_0 = -b_0$ and $a_n = b_{n-1}y - b_n$ for all integers $n \geq 1$. Thus $b_0 = -a_0 \in A$ and, by induction, $b_n = b_{n-1}y - a_n \in A$ for all n. In other words, $\big(\sum_i b_i\big)(y-1) \in A(y-1)$ and we conclude that $A \cap B(y-1) = A(y-1)$ as required. It follows that

$$0 \to A/A(y-1) \to B/B(y-1) \to C/C(y-1) \to 0$$

is exact and thus $\theta'(B) = \theta'(A) + \theta'(C)$ in $\mathbf{G_0}(S)$. By the previous lemma, θ' determines a group homomorphism $\theta\colon \mathbf{gr}\,\mathbf{G_0}(S[y]) \to \mathbf{G_0}(S)$.

It remains to show that θ is an epimorphism. To this end, let V' be a finitely generated S-module. Then, for some integer n, we can map the free S-module $F' = \cdot \sum_1^n f_i' S$ onto V' with kernel U'. Let $F = \cdot \sum_1^n f_i S[y]$ be a free $S[y]$-module on the generators $f_1, f_2, \ldots, f_n$, graded so that each f_i is homogeneous of degree 0. Now each $u' \in U'$ can be written uniquely as $u' = \sum_i f_i' s_i = \sum_{i,j} f_i' s_{i,j}$, where $s_i = \sum_j s_{i,j}$ is the decomposition of s_i into its homogeneous components with $s_{i,j} \in S_j$. If m is the largest such j that occurs with $s_{i,j} \neq 0$, we define $\eta(u') \in F$ by

$$\eta(u') = \sum_{i,j} f_i s_{i,j} y^{m-j}$$

Then $\eta(u')$ is a homogeneous element of F of degree m and we let U be the $S[y]$-submodule of F generated by all $\eta(u')$ for $u' \in U'$. By Lemma 13.1(i), U is a graded submodule of F and it is finitely generated, since $S[y]$ is right Noetherian. Furthermore, if $V = F/U$, then V is a finitely generated graded $S[y]$-module with $0 \to U \to F \to V \to 0$ graded exact. By the results of the preceding paragraph, we know that $U \cap F(y-1) = U(y-1)$ and that

$$0 \to U/U(y-1) \to F/F(y-1) \to V/V(y-1) \to 0$$

is an exact sequence of S-modules.

Consider the additive group epimorphism $F \to F'$ given by $f_i s y^j \mapsto f_i' s$ for all i, j and all $s \in S$. The kernel of this map is clearly $F(y-1)$ and hence we obtain an S-isomorphism $F/F(y-1) \to F'$. Under this map, the image of $\eta(u') + F(y-1)$ is precisely u' and therefore $U/U(y-1) = U/\big(U \cap F(y-1)\big)$ maps onto U'. Thus $V' \cong F'/U' \cong V/V(y-1)$, so $[V'] = \theta([V])$ and θ is indeed an epimorphism. □

It is apparent that the second half of the preceding proof is an analog of the classical trick of adding a new variable to introduce homogeneous coordinates.

EXERCISES

1. The graded ring $S = S_0 \dot{+} S_1 \dot{+} \cdots$ is said to be *graded Noetherian* if the set of graded right ideals of S satisfies the ascending chain condition. Prove that S is Noetherian if and only if it is graded Noetherian. Note that if I is any right ideal of S and if I_n denotes the set of degree n components of elements of $I \cap (S_0 \dot{+} S_1 \dot{+} \cdots \dot{+} S_n)$, then $I_0 \dot{+} I_1 \dot{+} \cdots$ is a graded right ideal of S. With this, one can proceed as in the proof of the Hilbert Basis Theorem.
2. Show that S_0 Noetherian does not imply S Noetherian in general.
3. Let $S = S_0 \dot{+} S_1 \dot{+} \cdots$ be a graded ring and assume that every projective S_0-module is free. Prove that every graded-projective S-module $P = P_0 \dot{+} P_1 \dot{+} \cdots$ is graded-free. To this end, observe that $PS_+ = N$ is a graded submodule of P and that $P/PS_+ = P/N = \cdot \sum_i P_i/N_i$ is a projective S_0-module by Lemma 9.11(i). Thus each P_i/N_i is a projective and hence free S_0-module. Now use the argument of Lemma 10.2 along with the Graded Nakayama's Lemma.
4. Find all finitely generated graded $K[x]$-modules up to abstract isomorphism. Remember, $K[x]$ is a principal ideal domain.

Let R be a ring and let G be a multiplicative group. Assume that G acts as automorphisms on R, so we have a group homomorphism $G \to \mathrm{Aut}(R)$. As usual, the *fixed ring* R^G of R is defined by

$$R^G = \{ r \in R \mid r^g = r \text{ for all } g \in G \}$$

where the map $r \mapsto r^g$ is the automorphism corresponding to $g \in G$. Furthermore, we define the *skew group ring* $R*G$ to be the set of all formal finite sums $\sum_{g \in G} r_g g$ with coefficients $r_g \in R$. Addition in $R*G$ is componentwise and multiplication is determined distributively by the formula

$$ag \cdot bh = ab^{g^{-1}}(gh)$$

for all $a, b \in R$ and $g, h \in G$. As with ordinary group rings, we identify r with $r1$ and g with $1g$ so $R, G \subseteq R*G$. In Problems 6 and 7 we assume that $|G| = n < \infty$.

5. Verify that R^G is a subring of R and that $R*G$ is an associative ring with 1.
6. If $1/n \in R$, show that $e = (1/n) \sum_{g \in G} g$ is an idempotent of $R*G$ with $e(R*G)e = eR^G \cong R^G$.
7. Let $W \subseteq V$ be $R*G$-modules and assume that $V_R = W_R \dot{+} X_R$ for some R-submodule X of V. If $1/n \in R$, show that $V = W \dot{+} Y$ for some $R*G$-submodule Y of V. To this end, let $\pi: V \to W$ be the R-module projection map determined by $V = W \dot{+} X$ and define $\pi': V \to W$ by $\pi'(v) = (1/n) \sum_{g \in G} \pi(vg^{-1})g$. Prove that π' is an $R*G$-module projection map from V to W. Explain why this generalizes Maschke's Theorem (Proposition 4.9).

Again let G be a multiplicative group. A ring S is said to be *G-graded* if $S = \dot{\sum}_{g \in G} S_g$ is a direct sum of the additive subgroups S_g and if $S_g S_h \subseteq S_{gh}$ for all $g, h \in G$. Furthermore, S is *strongly G-graded* if $S_g S_h = S_{gh}$ for all $g, h \in G$. Observe that $S = R*G$ is strongly G-graded with $S_g = Rg$.

8. Let S be a G-graded ring with 1. Show that $1 \in S_1$ and that S is strongly G-graded if and only if $1 \in S_g S_{g^{-1}}$ for all $g \in G$. Furthermore, if $u \in S_g$ is a unit of S, prove that $u^{-1} \in S_{g^{-1}}$.
9. Let $S = \mathrm{M}_3(K)$ and let $G = \{1, g\}$ be a group of order 2. Define

$$S_1 = \begin{pmatrix} K & K & 0 \\ K & K & 0 \\ 0 & 0 & K \end{pmatrix} \quad \text{and} \quad S_g = \begin{pmatrix} 0 & 0 & K \\ 0 & 0 & K \\ K & K & 0 \end{pmatrix}$$

Show that this makes S a strongly G-graded ring but that S is not a skew group ring.

10. If $|G| = n$, let $\mathrm{M}_G(R)$ be the ring of $n \times n$ matrices over R with rows and columns indexed by the elements of G. Show that $S = \mathrm{M}_G(R)$ becomes G-graded by assigning a grade of $g^{-1}h$ to the entries in the (g, h)-position. Thus $\mathrm{M}_n(R)$ is a G-graded ring for any group G of order n.

14. Induced Modules

We are finally ready to compute the Grothendieck group of a skew polynomial ring. We start by fixing certain notation, which will remain in force until Theorem 14.7 is proved.

Let R be a right Noetherian ring and let $S = R[x;\sigma]$ be a skew polynomial ring over R. Then S becomes a graded ring by defining $S_n = Rx^n$ for all n. Next, we let $T = S[y]$ be the ordinary polynomial ring over S in the variable y and we grade T by total degree. Thus, by definition,

$$T_n = \cdot \sum_{i+j=n} S_i y^j = \cdot \sum_{i+j=n} Rx^i y^j$$

It is convenient to think of T as a skew polynomial ring over R in the two variables x and y with the additional proviso that $xy = yx$. Of course, y is actually a central element of T.

Let I denote the ideal T_+ of T. Then, since x and y are normal elements of T, we have

$$I = T_+ = xT + yT = Tx + Ty$$

In particular, if A is a right T-module, then $AI = A(Tx+Ty) = Ax+Ay$. Furthermore, $T/I = T/T_+ \cong T_0 = R$ and, in this way, R becomes a left and a right T-module.

Let A_T and ${}_TB$ be T-modules. In homological algebra there is an interesting and important sequence of abelian groups constructed from A and B. These are denoted by $\mathrm{Tor}_n(A,B)$ for $n = 0,1,2,\ldots$ and they start with $\mathrm{Tor}_0(A,B) = A \otimes B$. They are used to compensate for the fact that the tensor product is not an exact functor. Although we will

not need much of this Tor machinery in the following arguments, we will nevertheless be using certain elementary aspects that, in our case, can be proved directly. We also properly label the following assumptions as Tor conditions, even though we do not formally define Tor.

DEFINITION Let A be a right T-module. We say that $\mathrm{Tor}_1(A,R)=0$ if and only if, for all $a_1,a_2\in A$, $a_1x=a_2y$ implies that $a_1=ay$ and $a_2=ax$ for some $a\in A$. Furthermore, we say $\mathrm{Tor}_2(A,R)=0$ if and only if, for all $a\in A$, $ax=0=ay$ implies $a=0$. In particular, $\mathrm{Tor}_2(A,R)=0$ is equivalent to $\mathrm{l.ann}_A(x)\cap\mathrm{l.ann}_A(y)=0$.

The following two lemmas contain all the Tor machinery we require.

LEMMA 14.1 *Let $0\to A\to B\to C\to 0$ be an exact sequence of T-modules with $A\subseteq B$.*

i. If $\mathrm{Tor}_1(C,R)=0$, then $A\cap BI=AI$.

ii. If $A\cap BI=AI$ and $\mathrm{Tor}_1(B,R)=0$, then $\mathrm{Tor}_1(C,R)=0$.

PROOF Let $\bar{}: B\to C$ be the given map and recall that $BI=Bx+By$.

(i) Suppose that $b_1x-b_2y\in A\cap BI$. Then $\bar{b}_1x=\bar{b}_2y$ and, since $\mathrm{Tor}_1(C,R)=0$, we have $\bar{b}_1=\bar{b}y$ and $\bar{b}_2=\bar{b}x$ for some $b\in B$. Thus there exist $a_1,a_2\in A$ with $b_1=by+a_1$ and $b_2=bx+a_2$. Since $xy=yx$, this yields

$$\begin{aligned} b_1x-b_2y&=(by+a_1)x-(bx+a_2)y\\ &=a_1x-a_2y\in AI \end{aligned}$$

and hence $A\cap BI\subseteq AI$ as required.

(ii) Let $c_1=\bar{b}_1$ and $c_2=\bar{b}_2$ be elements of C with $c_1x=c_2y$. Then $\bar{b}_1x=\bar{b}_2y$, so $b_1x-b_2y\in A\cap BI=AI$, by assumption. Thus there exist $a_1,a_2\in A$ with $b_1x-b_2y=a_1x-a_2y$, so $(b_1-a_1)x=(b_2-a_2)y$. Since $\mathrm{Tor}_1(B,R)=0$, there exists $b\in B$ with $b_1-a_1=by$ and $b_2-a_2=bx$. But $\overline{b_1-a_1}=\bar{b}_1=c_1$ and $\overline{b_2-a_2}=\bar{b}_2=c_2$, so we conclude that $c_1=\bar{b}y$, $c_2=\bar{b}x$ and $\mathrm{Tor}_1(C,R)=0$. □

LEMMA 14.2 *Let $0\to A\to B\to C\to 0$ be exact and suppose $A\subseteq B$.*

i. If $\mathrm{Tor}_1(B,R)=0$ and $\mathrm{Tor}_2(C,R)=0$, then $\mathrm{Tor}_1(A,R)=0$.

ii. If $\mathrm{Tor}_2(B,R)=0$, then $\mathrm{Tor}_2(A,R)=0$.

PROOF (i) Again let $\bar{}: B\to C$ denote the given map and suppose $a_1,a_2\in A$ satisfy $a_1x=a_2y$. Since $A\subseteq B$ and $\mathrm{Tor}_1(B,R)=0$, there exists $b\in B$ with $a_1=by$ and $a_2=bx$. But then $\bar{b}y=\bar{b}x=0$, so $\mathrm{Tor}_2(C,R)=0$ implies that $\bar{b}=0$. In other words, $b\in A$ and we conclude that $\mathrm{Tor}_1(A,R)=0$.

(ii) This is clear since $A \subseteq B$. □

If D is a finitely generated R-module, then, by Lemma 9.11(ii), the induced module

$$A = D \otimes T = \cdot \sum_{i,j \geq 0} D \otimes x^i y^j$$

is a graded T-module once we define

$$A_n = \cdot \sum_{i+j=n} D \otimes x^i y^j$$

Furthermore, A is finitely generated by the elements $d \otimes 1$ as d runs through the generators of D. Notice that $T_T \cong R \otimes T$; therefore, since $\otimes$ commutes with direct sums, every free T-module is abstractly isomorphic to an induced module.

LEMMA 14.3 *The induced module map determines a group homomorphism* $\mathbf{G_0}(R) \to \mathbf{gr}\,\mathbf{G_0}(T)$. *Furthermore if A is an induced T-module, then we have* $\mathrm{Tor}_1(A, R) = 0$ *and* $\mathrm{Tor}_2(A, R) = 0$.

PROOF The map $\theta' : D \mapsto [D \otimes T]$ sends finitely generated R-modules to elements of the abelian group $\mathbf{gr}\,\mathbf{G_0}(T)$. Furthermore, if

$$0 \to D_1 \xrightarrow{\alpha} D_2 \xrightarrow{\beta} D_3 \to 0$$

is exact, then

$$0 \to D_1 \otimes T \xrightarrow{\alpha \otimes 1} D_2 \otimes T \xrightarrow{\beta \otimes 1} D_3 \otimes T \to 0$$

is an exact sequence of graded T-modules, since ${}_RT$ is free and hence flat. Since $\alpha \otimes 1$ and $\beta \otimes 1$ are clearly graded homomorphisms, it follows that

$$0 = [D_2 \otimes T] - [D_1 \otimes T] - [D_3 \otimes T]$$

in $\mathbf{gr}\,\mathbf{G_0}(T)$ and hence that $\theta'(D_2) = \theta'(D_1) + \theta'(D_3)$. Lemma 12.2(i) now implies that θ' determines a group homomorphism θ: $\mathbf{G_0}(R) \to \mathbf{gr}\,\mathbf{G_0}(T)$.

Finally let $A = D \otimes T$, so that every element of A is uniquely of the form $a = \sum_{i,j} d_{i,j} \otimes x^i y^j$ with $d_{i,j} \in D$. In particular, we have $\mathrm{l.ann}_A(x) = \mathrm{l.ann}_A(y) = 0$; hence $\mathrm{Tor}_2(A, R) = 0$. Furthermore, suppose a_1 and a_2 are elements of A with $a_1 x = a_2 y$. Then it is clear that a_1 has

no nonzero summands of the form $d \otimes x^i y^0$ and that a_2 has no summands of the form $d \otimes x^0 y^j$. Thus $a_1 = a_1' y$ and $a_2 = a_2' x$ for some $a_1', a_2' \in A$. But then $(a_1' - a_2')xy = a_1 x - a_2 y = 0$ and it follows that $a_1' = a_2'$, as required. □

We say that a graded T-module is *induced* if it is abstractly isomorphic to some $D \otimes T$. In particular, our previous observation implies that every graded-free T-module is induced.

LEMMA 14.4 *Let $C = \cdot \sum_{i=0}^{\infty} C_i$ be a graded T-module and assume that $C = C_k T$ for some k. If $\operatorname{Tor}_1(C, R) = 0$, then $C \cong C_k \otimes T$ and hence C is an induced module. Furthermore, if C is a finitely generated T-module, then C_k is a finitely generated R-module.*

PROOF Note that C_k is a module for $T_0 = R$ and thus $C_k \otimes T$ is a T-module. We now define a shifted grading on $C_k \otimes T$ so that $c_k \otimes x^i y^j$ has degree $i + j + k$. Since the map $C_k \times T \to C$ given by $(c_k, t) \mapsto c_k t$ is balanced, there is a T-module homomorphism $\xi: C_k \otimes T \to C$ given by $c_k \otimes t \mapsto c_k t$. By definition of the grading, it is clear that ξ is a graded homomorphism and, since $C = C_k T$, we see that ξ is onto. The goal is to show that ξ is one-to-one.

To start with, let $a \in \operatorname{Ker}(\xi)$ and write $a = \sum_{i,j} d_{i,j} \otimes x^i y^j$ with $d_{i,j} \in C_k$. Then

$$0 = \xi(a) = \sum_{i,j} d_{i,j} x^i y^j$$

and, since $d_{i,j} x^i y^j$ has degree $i + j + k$, we conclude that $d_{0,0} = 0$. Thus $a \in (C_k \otimes T)I$ and hence $\operatorname{Ker}(\xi) \subseteq (C_k \otimes T)I$.

Next consider the short exact sequence

$$0 \to \operatorname{Ker}(\xi) \to C_k \otimes T \xrightarrow{\xi} C \to 0$$

Since $\operatorname{Tor}_1(C, R) = 0$, Lemma 14.1(i) implies that $\operatorname{Ker}(\xi) \cap (C_k \otimes T)I = \operatorname{Ker}(\xi)I$. But $\operatorname{Ker}(\xi) \subseteq (C_k \otimes T)I$, by the preceding, so $\operatorname{Ker}(\xi) = \operatorname{Ker}(\xi)I$. The Graded Nakayama's Lemma now yields $\operatorname{Ker}(\xi) = 0$ and thus C is graded isomorphic to $C_k \otimes T$ with the shifted grading. In particular, C is abstractly isomorphic to $C_k \otimes T$, with the usual grading, and hence C is an induced module.

Finally, since $C = C_k T$, we have $C = C_k \dot{+} C_{k+1} \dot{+} \cdots$. Thus if $C' = C_{k+1} \dot{+} C_{k+2} \dot{+} \cdots$, then C' is a T-submodule of C with $C/C' \cong C_k$

as modules for the ring $T/I \cong R$. In particular, if C is a finitely generated T-module, then $C_k \cong C/C'$ is a finitely generated R-module. □

We will also need the following simple observation.

LEMMA 14.5 *Let $B = \cdot\sum_{i=0}^{\infty} B_i$ be a graded T-module and let $k \geq 0$ be an integer. If $A = \sum_{i<k} B_i T$, then A is a graded submodule of B with $A = \sum_{i<k} A_i T$ and $A \cap BI = AI$.*

PROOF Note that A is generated by homogenous elements of B, so A is a graded submodule of B. Also, if $i < k$, then $A_i = B_i$ and hence $A = \sum_{i<k} A_i T$.

Now clearly $A \cap BI \supseteq AI$. For the converse, first observe that

$$A = \sum_{i<k} A_i(R + I) = C + AI$$

where we set $C = \cdot\sum_{i<k} A_i$. Thus since $AI \subseteq BI$, we have

$$A \cap BI = (C + AI) \cap BI = (C \cap BI) + AI$$

and it suffices to show that

$$\Big(\sum_{i<k} A_i\Big) \cap BI = C \cap BI \subseteq AI$$

To this end, let b belong to the latter intersection. Since $b \in BI$, we can write $b = \sum_j b_j t_j$ with $b_j \in B$, $t_j \in I$ and all these elements homogeneous. Furthermore, since $b \in C$, we have $\deg b < k$, so we can assume that each summand satisfies $\deg b_j + \deg t_j < k$. But then $b_j \in A$, so $b_j t_j \in AI$ and hence $b \in AI$ as required. □

We can now prove:

THEOREM 14.6 *Let R be a right Noetherian ring, let $S = R[x;\sigma]$ be a skew polynomial ring over R and set $T = S[y]$. If T is graded by total degree, then the induced module map determines an epimorphism $\theta\colon \mathbf{G_0}(R) \to \mathbf{gr}\,\mathbf{G_0}(T)$.*

PROOF Lemma 14.3 asserts that the induced module map $\theta\colon \mathbf{G_0}(R) \to \mathbf{gr}\,\mathbf{G_0}(T)$ exists. If $B = \cdot\sum_{i=0}^{\infty} B_i$ is a finitely generated graded T-module, we show that $[B] \in \mathrm{Im}(\theta)$ by considering several cases.

CASE 1 $\mathrm{Tor}_1(B, R) = 0$.

PROOF Since B is finitely generated, we have $B = \sum_{i=0}^{k} B_i T$ for some k and we proceed by induction on k. Set

$$A = \sum_{i<k} B_i T = \sum_{i<k} A_i T$$

so that, by the previous lemma, A is a graded submodule of B with $AI = A \cap BI$. Let $C = B/A$. Then Lemma 14.1(ii) and the graded exact sequence $0 \to A \to B \to C \to 0$ imply that $\mathrm{Tor}_1(C, R) = 0$. Furthermore, by definition of A, it is clear that $C = C_k T$. Thus, by Lemma 14.4, $C \cong C_k \otimes T$ is an induced module with C_k a finitely generated R-module. It follows that $[C] \in \mathrm{Im}(\theta)$ and then, by Lemma 14.3, that $\mathrm{Tor}_2(C, R) = 0$. But then Lemma 14.2(i) yields $\mathrm{Tor}_1(A, R) = 0$, so, by induction, we have $[A] \in \mathrm{Im}(\theta)$ and therefore $[B] = [A] + [C]$ is also contained in $\mathrm{Im}(\theta)$. □

CASE 2 $\mathrm{Tor}_2(B, R) = 0$.

PROOF Let F be a finitely generated graded-free T-module with $0 \to A \to F \to B \to 0$ graded exact. Since F is induced, we have $[F] \in \mathrm{Im}(\theta)$; also, $\mathrm{Tor}_1(F, R) = 0$ by Lemma 14.3. Since $\mathrm{Tor}_2(B, R) = 0$, Lemma 14.2(i) implies that $\mathrm{Tor}_1(A, R) = 0$. Thus $[A] \in \mathrm{Im}(\theta)$, by Case 1, and therefore $[B] = [F] - [A] \in \mathrm{Im}(\theta)$. □

CASE 3 *B arbitrary.*

PROOF As before, let $0 \to A \to F \to B \to 0$ be graded exact with F a finitely generated graded-free T-module. Then F is induced, so $[F] \in \mathrm{Im}(\theta)$ and $\mathrm{Tor}_2(F, R) = 0$. Hence $\mathrm{Tor}_2(A, R) = 0$, by Lemma 14.2(ii), and we conclude from Case 2 that $[A] \in \mathrm{Im}(\theta)$. Thus $[B] = [F] - [A] \in \mathrm{Im}(\theta)$ and the theorem is proved. □

It is now a simple matter to put all the ingredients together. Notice that the following conclusion asserts that θ is an isomorphism.

THEOREM 14.7 (Grothendieck-Quillen Theorem) *Let R be a right Noetherian ring and let $S = R[x; \sigma]$ be a skew polynomial ring over R. Then the induced module map determines an isomorphism $\theta: \mathbf{G_0}(R) \to \mathbf{G_0}(S)$. Specifically, $\theta: [A] \mapsto [A \otimes S]$ and $\theta^{-1}: [B] \mapsto [B/Bx] - [\mathrm{l.ann}_B(x)^\sigma]$.*

PROOF Form the ordinary polynomial ring $T = S[y]$ and observe that both S and T are right Noetherian by the Hilbert Basis Theorem. If we grade S so that $S_n = Rx^n$ and if we grade T by total degree, then Theorem 14.6 asserts that there exists an epimorphism $\theta_1: \mathbf{G_0}(R) \to \mathbf{gr}\,\mathbf{G_0}(T)$ given by $\theta_1: [A] \mapsto [A \otimes_R T]$. Next, Proposition 13.6 implies that the

ring epimorphism ϕ from $T = S[y]$ to S given by $y \mapsto 1$ determines a group epimorphism $\theta_2: \mathbf{gr}\,\mathbf{G_0}(T) \to \mathbf{G_0}(S)$. Here $\theta_2: [C] \mapsto [C \otimes_T S] = [C/C(y-1)]$.

It follows that the composite map

$$\theta: \mathbf{G_0}(R) \xrightarrow{\theta_1} \mathbf{gr}\,\mathbf{G_0}(T) \xrightarrow{\theta_2} \mathbf{G_0}(S)$$

is also an epimorphism. Furthermore, by transitivity of induction, we have $\theta: [A] \mapsto [A \otimes_R S]$, where S is viewed as a left R-module via the combined map $R \to T \xrightarrow{\phi} S$. But the latter map is just the usual embedding of R into S, so θ is precisely the homomorphism corresponding to the induced module map.

We now know that θ is onto. It remains to show that it is one-to-one. To this end, note that, by Proposition 12.6, there is a group homomorphism $\theta_3: \mathbf{G_0}(S) \to \mathbf{G_0}(R)$ given by $[B] \mapsto [B/Bx] - [\mathrm{l.ann}_B(x)^\sigma]$. We consider the composite map

$$\mathbf{G_0}(R) \xrightarrow{\theta} \mathbf{G_0}(S) \xrightarrow{\theta_3} \mathbf{G_0}(R)$$

If A is a finitely generated R-module, then, by Lemma 9.11(ii),

$$B = A \otimes_R S = A \otimes_R R[x;\sigma] = \cdot \sum_{i=0}^{\infty} A \otimes x^i$$

It follows that $B/Bx \cong A$ as R-modules and that $\mathrm{l.ann}_B(x) = 0$. Thus $\theta_3\theta([A]) = \theta_3([B]) = [A]$ and $\theta_3\theta$ is the identity on $\mathbf{G_0}(R)$. We conclude first that θ is one-to-one and then that $\theta^{-1} = \theta_3$. □

We remark that Grothendieck proved the above result for ordinary polynomial rings over commutative rings. On the other hand, Quillen's result is far more general than what we quote here. It applies to a fairly large class of graded rings S with $S_0 = R$ and its proof requires the full Tor machinery.

COROLLARY 14.8 *Let $S = R[x_1, x_2, \ldots, x_n]$ be an ordinary polynomial ring in n variables over the right Noetherian ring R. Then the induced module map determines an isomorphism $\mathbf{G_0}(R) \to \mathbf{G_0}(S)$.*

PROOF This follows easily by induction on n and the transitivity of the induced module map (Lemma 9.12). □

EXERCISES

Let R be an arbitrary ring, let A_R and ${}_RB$ be R-modules and let

$$\cdots \to P_2 \xrightarrow{\beta_2} P_1 \xrightarrow{\beta_1} P_0 \to B \to 0$$
$$\cdots \to P_2' \xrightarrow{\alpha_2} P_1' \xrightarrow{\alpha_1} P_0' \to A \to 0$$

be projective resolutions. If we tensor these sequences with A and B, respectively, and then delete the $A \otimes B$ term, we obtain the complexes

$$\cdots \to A \otimes P_2 \xrightarrow{1\otimes\beta_2} A \otimes P_1 \xrightarrow{1\otimes\beta_1} A \otimes P_0 \xrightarrow{1\otimes\beta_0} 0$$
$$\cdots \to P_2' \otimes B \xrightarrow{\alpha_2\otimes 1} P_1' \otimes B \xrightarrow{\alpha_1\otimes 1} P_0' \otimes B \xrightarrow{\alpha_0\otimes 1} 0$$

where, for convenience, we let $1\otimes\beta_0$ and $\alpha_0 \otimes 1$ denote the appropriate zero maps. The abelian groups $\operatorname{Tor}_n^R(A, B)$ are now defined by

$$\operatorname{Tor}_n^R(A, B) = \operatorname{Tor}_n(A, B) = \operatorname{Ker}(1 \otimes \beta_n)/\operatorname{Im}(1 \otimes \beta_{n+1})$$

for $n = 0, 1, 2, \ldots$. It can be shown that $\operatorname{Tor}_n(A, B)$ depends only on A and B and not on the particular projective resolution chosen for B. Furthermore, the definition is symmetric in that

$$\operatorname{Tor}_n^R(A, B) = \operatorname{Tor}_n(A, B) = \operatorname{Ker}(\alpha_n \otimes 1)/\operatorname{Im}(\alpha_{n+1} \otimes 1)$$

1. Prove that $\operatorname{Tor}_0(A, B) \cong A \otimes B$ and that

$$\operatorname{Tor}_n(A, B \oplus C) \cong \operatorname{Tor}_n(A, B) \oplus \operatorname{Tor}_n(A, C)$$

2. Suppose $\gamma\colon B \to C$ is a left R-module homomorphism. Show that γ determines a group homomorphism $\operatorname{Tor}_n(\gamma)\colon \operatorname{Tor}_n(A, B) \to \operatorname{Tor}_n(A, C)$, which enjoys properties similar to those of $1 \otimes \gamma$. In particular, if B is an (R, S)-bimodule, conclude that $\operatorname{Tor}_n(A, B)$ is a right S-module.
3. If A or B is flat, prove that $\operatorname{Tor}_n(A, B) = 0$ for all $n \geq 1$.
4. If $\operatorname{pd} A = k$ or $\operatorname{pd} B = k$, show that $\operatorname{Tor}_n(A, B) = 0$ for all $n \geq k + 1$.
5. Suppose $0 \to C \to P \to B \to 0$ is an exact sequence of left R-modules with P projective. Prove that $\operatorname{Tor}_n(A, C) \cong \operatorname{Tor}_{n+1}(A, B)$ for all $n \geq 1$. Furthermore, show that

$$0 \to \operatorname{Tor}_1(A, B) \to A \otimes C \to A \otimes P \to A \otimes B \to 0$$

is exact.

6. Let $R \subseteq S$ be rings with ${}_RS$ flat. Let A be a right R-module and let B be a left S-module. Note that B is a left R-module by restriction. Prove that

$$\operatorname{Tor}_n^S(A \otimes_R S, B) \cong \operatorname{Tor}_n^R(A, {}_RB)$$

To this end, start with a projective resolution for A and tensor it with the flat module ${}_RS$ to obtain a projective resolution for $A \otimes_R S$. Then use these sequences to compute the appropriate Tor groups.

Now let R be a right Noetherian ring and use all the notation of this chapter. In particular, let $S = R[x; \sigma]$ be graded with $S_n = Rx^n$ and let $T = S[y]$ be graded by total degree. Furthermore, view R as the left S-module $R \cong S/Sx$ and as the left T-module $R \cong T/I = T/(Tx + Ty)$.

7. If A is a right S-module, compute $\operatorname{Tor}_n^S(A, R)$ from the short exact sequence $0 \to Sx \to S \to R \to 0$.
8. Prove that the induced module map determines a group isomorphism $\theta\colon \mathbf{G_0}(R) \to \mathbf{gr}\,\mathbf{G_0}(S)$. To this end, define $\operatorname{Tor}_1(A, R) = 0$ to mean that $\operatorname{l.ann}_A(x) = 0$ and follow the proof of Theorem 14.6. The necessary Tor machinery is all contained in Lemma 12.5.
9. Show that the map θ of Theorem 14.6 is an isomorphism.
10. Prove that the sequence of left T-modules

$$0 \to T \xrightarrow{\xi} T \oplus T \xrightarrow{\eta} T \to R \to 0$$

with $\xi\colon t \mapsto (ty, tx)$ and $\eta\colon (t_1, t_2) \mapsto t_1x - t_2y$ is exact. If A is a right T-module, use this sequence to compute $\operatorname{Tor}_n^T(A, R)$. In particular, justify the definitions given at the beginning of this chapter.

15. Syzygy Theorem

We now return to the study of finitely generated projective R-modules and again we assume throughout that R is right Noetherian. The goal is to obtain a projective analog of the isomorphism $\mathbf{G_0}(R) \cong \mathbf{G_0}(R[x;\sigma])$ and for this we need a projective version of the Grothendieck group.

DEFINITION Let R be a right Noetherian ring and let $\mathcal{F}$ be the free abelian group whose free generators are the isomorphism classes of the finitely generated projective R-modules. As usual, if P is such a module, then we let $\tilde{P}$ denote the generator of $\mathcal{F}$ that is its isomorphism class. Furthermore, we let $\mathcal{R}$ be the subgroup of $\mathcal{F}$ generated by all expressions of the form $\tilde{B} - \tilde{A} - \tilde{C}$ whenever there exists a short exact sequence $0 \to A \to B \to C \to 0$. Notice that, since C is projective, the latter sequence splits and is equivalent to $B \cong A \oplus C$. We now let $\mathbf{K_0}(R) = \mathcal{F}/\mathcal{R}$ be the *projective Grothendieck group* of R. In particular, if $[P]$ is the image of $\tilde{P}$ in $\mathbf{K_0}(R)$, then $\mathbf{K_0}(R)$ is the abelian group generated by the symbols $[P]$ for all finitely generated projective R-modules P subject to the relations $[B] = [A] + [C]$ whenever $B \cong A \oplus C$. Obviously, $[0] = 0$.

We start with the projective analog of Lemma 12.2 and we paraphrase the hypothesis of part (i) by saying that θ' *respects direct sums.* The statement of part (ii) implicitly requires Theorem 5.9.

LEMMA 15.1 *Let R be a ring.*

i. Let $\mathcal{A}$ be an additive abelian group and let θ' be a map from the collection of finitely generated projective R-modules to $\mathcal{A}$. Suppose that $\theta'(B) = \theta'(A) + \theta'(C)$ whenever $B \cong A \oplus C$. Then θ' determines a group homomorphism $\theta\colon \mathbf{K_0}(R) \to \mathcal{A}$ given by $\theta([P]) = \theta'(P)$.

ii. Suppose R is right Artinian and let $P_1, P_2, \ldots, P_k$ be representatives of the isomorphism classes of the finitely many principal indecomposable R-modules. Then $\mathbf{K_0}(R)$ is the free abelian group on the generators $[P_1], [P_2], \ldots, [P_k]$.

PROOF (i) From $0 \cong 0 \oplus 0$ it follows that $\theta'(0) = 0 \in \mathcal{A}$. Next, if $B \cong C$, then $B \cong 0 \oplus C$, so $\theta'(B) = \theta'(C)$. Thus, since $\mathcal{F}$ is free abelian, we can define $\theta: \mathcal{F} \to \mathcal{A}$ by $\theta(\tilde{P}) = \theta'(P)$. But $\theta(\mathcal{R}) = 0$, so this map factors through $\mathbf{K_0}(R) = \mathcal{F}/\mathcal{R}$.

(ii) Now let R be Artinian. Since every finitely generated projective R-module is a direct sum of principal indecomposables, it follows that $\mathbf{K_0}(R)$ is spanned by $[P_1], [P_2], \ldots, [P_k]$. For independence, let $\mathcal{A}$ be the free abelian group on the generators $p_1, p_2, \ldots, p_k$ and for each finitely generated projective R-module P, define $\theta'(P) = \sum_j m_j p_j \in \mathcal{A}$, where m_j is the multiplicity of P_j, as a direct summand of P. Then θ' is well defined, by Theorem 5.9, and it respects direct sums. Thus by (i), θ' determines a homomorphism $\theta: \mathbf{K_0}(R) \to \mathcal{A}$. But $\theta([P_i]) = \theta'(P_i) = p_i$, so it is clear that $[P_1], [P_2], \ldots, [P_k]$ are also independent. □

We will return to Artinian rings shortly, but first it is appropriate to consider the relationship between $\mathbf{K_0}$ and $\mathbf{G_0}$ for arbitrary rings.

THEOREM 15.2 *Let R be a right Noetherian ring. Then there is a natural homomorphism $c: \mathbf{K_0}(R) \to \mathbf{G_0}(R)$ given by $c: [P] \mapsto [P]$. In addition, if every finitely generated R-module has finite projective dimension, then c is an isomorphism.*

PROOF The map c' that sends finitely generated projective R-modules P to $[P] \in \mathbf{G_0}(R)$ clearly respects direct sums. Thus c' determines a group homomorphism $c: \mathbf{K_0}(R) \to \mathbf{G_0}(R)$ given by $c: [P] \mapsto [P]$.

Now suppose that all finitely generated R-modules have finite projective dimension. Then, by Lemma 12.7(i), we know that c is onto. Furthermore, let $\mathcal{A} = \mathbf{K_0}(R)$ and define $\theta'(P) = [P] \in \mathcal{A}$ for all finitely generated projective R-modules P. Then clearly $\theta'(P_3) = \theta'(P_1) + \theta'(P_2)$ whenever $P_3 \cong P_1 \oplus P_2$, so Lemma 12.7(ii) implies that θ' determines a group homomorphism $\theta: \mathbf{G_0}(R) \to \mathcal{A}$ with $\theta: [P] \mapsto \theta'(P) = [P]$. But then the combined map

$$\mathbf{K_0}(R) \xrightarrow{c} \mathbf{G_0}(R) \xrightarrow{\theta} \mathbf{K_0}(R)$$

is the identity on $\mathbf{K_0}(R)$ and therefore c is one-to-one. □

As we mentioned in the paragraph preceding Lemma 12.7, if R has finite global dimension, then the finitely generated projective R-modules determine $\mathbf{G_0}(R)$. Indeed the fact that c is an isomorphism in this situation gives a precise meaning to that statement. The homomorphism $c\colon \mathbf{K_0}(R) \to \mathbf{G_0}(R)$ is called the *Cartan map*.

Now let us suppose that R is right Artinian. Then, by Theorem 5.9, there is a one-to-one correspondence between the isomorphism classes of principal indecomposable R-modules $P_1, P_2, \ldots, P_k$ and of the irreducible R-modules $V_1, V_2, \ldots, V_k$ given by $P_i/P_iN \cong V_i$, where $N = \mathrm{Nil}(R) = \mathrm{Rad}(R)$. In particular, it follows from Lemmas 12.2(ii) and 15.1(ii) that $\mathbf{G_0}(R)$ and $\mathbf{K_0}(R)$ are isomorphic. On the other hand, this isomorphism need not be achieved by the Cartan map. Indeed, c is neither surjective nor injective in general. Finally, note that if V_j occurs as a composition factor of P_i with multiplicity $c_{i,j}$, then

$$c\colon [P_i] \mapsto \sum_j c_{i,j}[V_j]$$

and the *Cartan matrix* $(c_{i,j})$ is precisely the matrix of the Cartan map with respect to the bases $\{[P_1], [P_2], \ldots, [P_k]\}$ and $\{[V_1], [V_2], \ldots, [V_k]\}$.

Next we see that the induced module map for $\mathbf{K_0}$ requires no flatness assumption.

LEMMA 15.3 *Let R and S be right Noetherian and let $\phi\colon R \to S$ be a ring homomorphism. Then the induced module map $P \mapsto P \otimes S$ determines a homomorphism $\theta\colon \mathbf{K_0}(R) \to \mathbf{K_0}(S)$.*

PROOF If P is a finitely generated projective R-module, then $P \otimes S$ is a finitely generated projective S-module by Lemma 9.11(i). Thus it makes sense to define $\theta'(P) = [P \otimes S] \in \mathbf{K_0}(S)$. Furthermore, since tensor product commutes with direct sums, it follows that θ' respects direct sums and Lemma 15.1(i) yields the result. □

We can now obtain the projective analog of Theorem 14.7.

THEOREM 15.4 (Serre's Theorem) *Let R be a right Noetherian ring and set $S = R[x; \sigma]$. If $\mathrm{gl\,dim}\, R < \infty$, then the induced module map determines an isomorphism $\theta\colon \mathbf{K_0}(R) \to \mathbf{K_0}(S)$.*

PROOF By Theorems 11.1 and 11.2, we know that S is right Noetherian with $\mathrm{gl\,dim}\, S < \infty$. In particular, Theorem 15.2 applies to both R and S

and we have the commutative diagram

$$\begin{array}{ccc} \mathbf{K_0}(S) & \xleftarrow{c^{-1}} & \mathbf{G_0}(S) \\ \uparrow \theta & & \uparrow \theta_1 \\ \mathbf{K_0}(R) & \xrightarrow{c_1} & \mathbf{G_0}(R) \end{array}$$

where θ and θ_1 denote the induced module maps and c and c_1 are the Cartan maps. But c_1, c^{-1} and θ_1 are isomorphisms, by Theorems 14.7 and 15.2, and therefore so is θ. □

We will obtain some rather powerful corollaries of this result once we take a closer look at $\mathbf{K_0}(R)$.

DEFINITION Let A and B be finitely generated R-modules. Then A and B are said to be *stably isomorphic* if $A \oplus R^n \cong B \oplus R^n$ for some free R-module R^n of finite rank n. Furthermore, A is *stably free* if $A \oplus R^n \cong R^m$ for some integers $m, n \geq 0$.

LEMMA 15.5 *Let P and Q be finitely generated projective R-modules.*

i. $[P] = [Q]$ *in* $\mathbf{K_0}(R)$ *if and only if P and Q are stably isomorphic.*

ii. $[P]$ *is in the cyclic subgroup of* $\mathbf{K_0}(R)$ *generated by* $[R]$ *if and only if P is stably free.*

iii. $\mathbf{K_0}(R)$ *is the cyclic group generated by* $[R]$ *if and only if all finitely generated projective R-modules are stably free.*

PROOF (i) If P and Q are stably isomorphic, then certainly $[P] = [Q]$ in $\mathbf{K_0}(R)$. For the converse, we work in the free abelian group $\mathcal{F}$ and we use all the notation given in the definition of $\mathbf{K_0}(R) = \mathcal{F}/\mathcal{R}$. In particular, if $[P] = [Q]$, then $\tilde{P} - \tilde{Q} \in \mathcal{R}$, so this element can be written as a finite sum and difference of relations. Say

$$\tilde{P} - \tilde{Q} = \sum_i (\tilde{B}_i - \tilde{A}_i - \tilde{C}_i) + \sum_j (\tilde{D}_j + \tilde{F}_j - \tilde{E}_j)$$

with $B_i \cong A_i \oplus C_i$ and $E_j \cong D_j \oplus F_j$. Thus

$$\tilde{P} + \sum_i \tilde{A}_i + \sum_i \tilde{C}_i + \sum_j \tilde{E}_j = \tilde{Q} + \sum_i \tilde{B}_i + \sum_j \tilde{D}_j + \sum_j \tilde{F}_j$$

and this means that the summands on the left must match, term for term, with the summands on the right. In particular, the direct sum of

all modules represented on the left must be isomorphic to the direct sum of all modules represented on the right. Hence we have $P \oplus V \cong Q \oplus V$, where V is the direct sum

$$\begin{aligned} V &\cong \oplus \sum_i A_i \oplus \sum_i C_i \oplus \sum_j E_j \\ &\cong \oplus \sum_i B_i \oplus \sum_j D_j \oplus \sum_j F_j \end{aligned}$$

But V is a finitely generated projective module, so $V \oplus U \cong R^n$ for some n. Thus, since

$$P \oplus R^n \cong P \oplus V \oplus U \cong Q \oplus V \oplus U \cong Q \oplus R^n$$

we conclude that P is stably isomorphic to Q.

(ii) If P is stably free with $P \oplus R^n \cong R^m$, for example, then $[P] = (m-n)[R]$ in $\mathbf{K_0}(R)$. Conversely, suppose $[P]$ is contained in the cyclic subgroup of $\mathbf{K_0}(R)$ generated by $[R]$ and say $[P] = n[R]$. If $n \geq 0$, then P is stably isomorphic to R^n, by (i), and hence P is stably free. On the other hand, if $n < 0$, then $P \oplus R^{(-n)}$ is stably isomorphic to 0 and again P is stably free. Thus (ii) is proved and (iii) is immediate. □

We can now obtain the key application of Theorem 15.4.

COROLLARY 15.6 *Let R be a ring satisfying the three conditions:*

i. It is right Noetherian.

ii. It has finite global dimension.

iii. All finitely generated projective modules are stably free.

If $S = R[x;\sigma]$, then S also satisfies (i), (ii), and (iii).

PROOF We already know from Theorems 11.1 and 11.2 that conditions (i) and (ii) are individually inherited by S. Now assume that R satisfies (i)–(iii). Then by Lemma 15.5(iii), $\mathbf{K_0}(R)$ is the cyclic group generated by $[R]$. Furthermore, by Theorem 15.4, $\mathbf{K_0}(S)$ is isomorphic to $\mathbf{K_0}(R)$ via the induced module map. But $R \otimes S \cong S$, so $\mathbf{K_0}(S)$ is the cyclic group generated by $[S]$ and Lemma 15.5(iii) yields the result. □

In particular, we have:

THEOREM 15.7 (Hilbert Syzygy Theorem) *Let $R = K[x_1, x_2, \ldots, x_n]$ be the ordinary polynomial ring in n variables over the field K. Then* gl dim $R = n$ *and all finitely generated projective R-modules are stably free.*

PROOF Note that the field K satisfies conditions (i)–(iii) of the previous result; thus, by induction on n, so does $R = K[x_1, x_2, \ldots, x_n]$. Since $\operatorname{gl\,dim} R = n$ by Corollary 11.5, the result follows. □

This is neither the original formulation nor the original proof of the Syzygy Theorem. In this context, *syzygy* means *relation* and the preceding result affords at least a partial description of all the finitely generated modules for the polynomial ring R. For example, suppose V is such a module with generating set $\{ v_1, v_2, \ldots, v_k \}$. Then every element of V is of the form $\sum_i v_i r_i$ with $r_i \in R$ but not necessarily uniquely so. Indeed, to understand V we must know when two such expressions are equal or, equivalently, when $\sum_i v_i r_i = 0$. To this end, map the free R-module $F = \cdot \sum_{i=1}^{k} f_i R$ onto V with $\alpha\colon f_i \mapsto v_i$. Then $\sum_i f_i r_i \in \operatorname{Ker}(\alpha)$ if and only if $\sum_i v_i r_i = 0$. In other words, $\operatorname{Ker}(\alpha)$ consists of all the relations satisfied by the set $\{ v_1, v_2, \ldots, v_k \}$ and it is called a *first syzygy* for V. Next, we know that $\operatorname{Ker}(\alpha)$ is finitely generated, but to better understand its module structure, we should also compute the syzygy of its generators. In this way we obtain, by definition, a *second syzygy* for V. If we continue in this manner then, since $\operatorname{gl\,dim} R = n$, it follows that the nth syzygy for V will be projective. But finitely generated projective R-modules are stably free, so an appropriate $(n+1)$st syzygy for V is free. The original Hilbert Theorem asserts that there exists an nth syzygy for V that is already free. We will obtain this sharper bound as a consequence of the affirmative solution of the Serre Conjecture.

We close this chapter by showing that the isomorphism $\theta\colon \mathbf{K_0}(R) \to \mathbf{K_0}(R[x;\sigma])$ can fail if $\operatorname{gl\,dim} R = \infty$. Indeed, we will construct a commutative counterexample in Lemma 15.10 once we accumulate a few preliminary observations.

LEMMA 15.8 *Let R be a commutative domain with quotient field K and let P and Q be R-submodules of K.*

i. If $PQ = R$, then P and Q are both finitely generated projective R-modules.

ii. If P is stably free, then $P = wR$ for some $w \in P$.

PROOF (i) We use the fact that $PQ \subseteq R$ and that $1 = \sum_1^n p_i q_i$ for suitable $p_i \in P$ and $q_i \in Q$. Define the R-module maps $\sigma\colon R^n \to P$ and $\tau\colon P \to R^n$ by

$$\sigma\colon (r_1, r_2, \ldots, r_n) \mapsto \sum_{i=1}^{n} p_i r_i$$

$$\tau: p \mapsto (q_1 p, q_2 p, \ldots, q_n p)$$

Then $\sigma\tau(p) = p$ for all $p \in P$, so σ is an epimorphism and τ splits the exact sequence $R^n \xrightarrow{\sigma} P \to 0$. Thus $P \mid R^n$ and P is a finitely generated projective R-module.

(ii) Suppose $P \neq 0$ is stably free so that $P \dot{+} R^n = V = R^m$. We first show that $m = n+1$. To this end, consider the K-vector space $P \otimes_R K$. If $0 \neq p_1, p_2 \in P \subseteq K$, then there exist nonzero $r_1, r_2 \in R$ with $p_1 r_1 = p_2 r_2$. Thus

$$\begin{aligned} p_1 \otimes K &= p_1 \otimes r_1 K = p_1 r_1 \otimes K \\ &= p_2 r_2 \otimes K = p_2 \otimes r_2 K = p_2 \otimes K \end{aligned}$$

and hence $\dim_K P \otimes K \leq 1$. On the other hand, the balanced map $P \times K \to K$ given by $(p, k) \mapsto pk$ certainly yields an epimorphism $P \otimes K \to K$. Thus $P \otimes K \cong K$ and, of course, $R \otimes K \cong K$. Since $P \dot{+} R^n = V = R^m$, we conclude that $V \otimes K$ is K-isomorphic to both K^{n+1} and K^m and hence that $m = n + 1$, as claimed.

Now let $\{ v_0, v_1, \ldots, v_n \}$ be an R-basis for $V = R^m = R^{n+1}$ and let $\{ w_1, \ldots, w_n \}$ be a basis for $W = R^n$, the complement for P in V. Then, for each $1 \leq j \leq n$, we have $w_j = \sum_{i=0}^{n} v_i r_{i,j}$ with $r_{i,j} \in R$ and we study the $(n+1) \times n$ matrix $M = (r_{i,j})$. Notice that if I is any maximal ideal of R, then

$$(P/PI) \dot{+} (R/I)^n = V/VI = (R/I)^{n+1}$$

so the elements $w_1, \ldots, w_n$ are (R/I)-linearly independent modulo VI. It follows that if $\bar{r}_{i,j} = r_{i,j} + I \in R/I$, then $\bar{M} = (\bar{r}_{i,j})$ must have rank n as a matrix over the field R/I. Hence at least one of the maximal $n \times n$ minors of $\bar{M}$ is not zero. Since I is an arbitrary maximal ideal, this implies that the set $\{ m_0, m_1, \ldots, m_n \}$ of maximal minors of M is unimodular, that is $\sum_{i=0}^{n} m_i R = R$. Indeed, if this were not the case, then the latter sum would be contained in some maximal ideal of R. Thus we can find elements $r_{i,0} \in R$ so that the augmented $(n+1) \times (n+1)$ matrix $M^* = (r_{i,j})$ has determinant 1 and hence is invertible. Finally, if we define $w_0 = \sum_{i=0}^{n} v_i r_{i,0}$, then $\{ w_0, w_1, \ldots, w_n \}$ must also be an R-basis for V by Lemma 2.5. Thus $P \dot{+} W = V = w_0 R \dot{+} W$ and $P \cong V/W \cong w_0 R$ is free of rank 1. □

With this we can prove:

PROPOSITION 15.9 *Let R be a commutative domain with quotient field K and suppose there exists $a \in K \setminus R$ with $a^2, a^3 \in R$. If S is the polynomial*

ring $S = R[x]$, then S has a finitely generated projective module that is not stably free.

PROOF Let $f = ax \in K[x]$ and let $P = (1 + f, 1 + f + f^2)$ be the $R[x]$-submodule of $K[x]$ generated by $1 + f$ and $1 + f + f^2$. Similarly, let $Q = (1 - f, 1 - f + f^2)$ and observe that

$$PQ = (1 - f^2, 1 + f^3, 1 - f^3, 1 + f^2 + f^4) \subseteq R[x]$$

since $a^2, a^3, a^4 \in R$. Furthermore, we have $2 = (1 + f^3) + (1 - f^3) \in PQ$ and $3 = (1 - f^2)(2 + f^2) + (1 + f^2 + f^4) \in PQ$. Thus $1 \in PQ$ and P is a finitely generated projective $R[x]$-module by Lemma 15.8(i).

Now suppose, by way of contradiction, that P is stably free. Then Lemma 15.8(ii) implies that $P = wR[x]$ for some $w \in K[x]$. Moreover, we have $P \cdot K[x] = K[x]$, since $(1 + f + f^2) - (1 + f)f = 1$, and thus $P = wR[x]$ implies that $K[x] = wK[x]$. In other words, w is a unit of $K[x]$ and hence $w \in K$. Now note that $wQ = PQ = R[x]$, so $w(1 - ax) = w(1 - f) \in wQ = R[x]$. Since $w \in K$, it therefore follows that $w \in R$. But then $1 + ax = 1 + f \in P = wR[x] \subseteq R[x]$, so $a \in R$, a contradiction, and we conclude that P is not stably free. □

Now we consider the example.

LEMMA 15.10 *Let F be a field and let R be the subring of the power series ring $F[[t]]$ consisting of all elements with t-coefficient 0. Then R is a Noetherian local domain and if S is the polynomial ring $S = R[x]$, then the induced module map θ: $\mathbf{K_0}(R) \to \mathbf{K_0}(S)$ is not surjective.*

PROOF We first briefly study the commutative domain $T = F[[t]]$. Suppose $\alpha = \sum_{i=0}^{\infty} a_i t^i$ and $\beta = \sum_{i=0}^{\infty} b_i t^i$ are two elements of this ring and set $\gamma = \alpha\beta = \sum_{i=0}^{\infty} c_i t^i$. Then by definition

$$c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0$$

for all $n \geq 0$. In particular, if α is given with $a_0 \neq 0$, then we can inductively solve for $b_0, b_1, b_2, \ldots$ in F so that $\alpha\beta = \gamma = 1$. In other words, every element α with $a_0 \neq 0$ is a unit of T and we conclude that T is a local ring with Jacobson radical $\mathrm{Rad}(T) = tT$. Furthermore, any nonzero element of T can then be written as a unit times t^m for some m and this implies that $T = F[[t]]$ is a ring whose only nonzero ideals are of the form $t^n T$ for $n = 0, 1, 2, \ldots$. Hence T is a commutative local Noetherian domain.

Let R be the set of all elements of T with t-coefficient 0, so that R is easily seen to be a subring of T. Since $R = 1 \cdot F[[t^2]] + t^3 \cdot F[[t^2]]$ and $F[[t^2]] \cong T$ is Noetherian, it follows from Lemma 6.6 that R is also Noetherian. Furthermore, if $\alpha \in R$ with $a_0 \neq 0$, then the equation $0 = c_1 = a_0 b_1 + a_1 b_0$ implies that $\alpha^{-1} \in R$. Thus R is a commutative local Noetherian domain with $\mathrm{Rad}(R) = R \cap tT$ and it follows from Theorem 10.8 that all projective R-modules are free. In particular, $\mathbf{K_0}(R)$ is the cyclic group generated by $[R]$.

Finally note that $t^2, t^3 \in R$ but that $t \notin R$. Thus, by the previous proposition, $S = R[x]$ has a finitely generated projective module that is not stably free. Lemma 15.5(iii) now implies that $\mathbf{K_0}(S)$ is not the cyclic group generated by $[S] = [R \otimes S]$ and hence the induced module map $\theta: \mathbf{K_0}(R) \to \mathbf{K_0}(S)$ cannot be surjective. □

As a consequence of the preceding, the ring R must have infinite global dimension. We can see this directly as follows. Let I be the set of elements of R with constant term 0. Then $I \lhd R$ and we have the short exact sequence

$$0 \to I \xrightarrow{\sigma} R \oplus R \xrightarrow{\tau} I \to 0$$

given by $\sigma: i \mapsto (i, it)$ and $\tau: (r_1, r_2) \mapsto r_1 t^3 - r_2 t^2$. We conclude, as in Lemma 8.5, that either $\mathrm{pd}_R I = \infty$ or I is projective and $R \oplus R \cong I \oplus I$. But $(R \oplus R)/(R \oplus R)I$ is two dimensional over F whereas $(I \oplus I)/(I \oplus I)I$ has F-dimension equal to 4. Thus $R \oplus R \ncong I \oplus I$ and $\mathrm{pd}_R I = \infty$.

EXERCISES

Let K be a field. In the following three problems, compute the Cartan matrix for the given Artinian rings.

1. Let R be the ring of upper triangular $n \times n$ matrices over K. Show that $\det(c_{i,j}) = 1$. Why is this not a surprise?
2. Describe the Cartan matrix in case R is a Wedderburn ring or $R = K[x \mid x^m = 0]$. In particular, note that c need not be surjective.
3. Write $A(a, b)$ and $B(a, b)$ for the sets of 4×4 upper triangular matrices

$$A(a,b) = \begin{pmatrix} a & * & 0 & 0 \\ & b & 0 & 0 \\ & & b & * \\ & & & a \end{pmatrix} \qquad B(a,b) = \begin{pmatrix} a & * & * & * \\ & b & * & * \\ & & b & * \\ & & & a \end{pmatrix}$$

with the $*$ entries arbitrary. Now let R and S be the four and eight dimensional subalgebras of $\mathrm{M}_4(K)$ given by

$$R = \{\, A(a,b) \mid a,b \in K \,\} \qquad S = \{\, B(a,b) \mid a,b \in K \,\}$$

Observe that $R/\mathrm{Rad}(R) \cong K \oplus K \cong S/\mathrm{Rad}(S)$ and describe the Cartan matrices of R and S. Conclude that c need not be injective in general.

4. Let R and S be right Noetherian rings and let M be an (R,S)-bimodule. Find conditions on M that guarantee that the map $A \mapsto A \otimes_R M$ determines a group homomorphism $\mathbf{G_0}(R) \to \mathbf{G_0}(S)$ or $\mathbf{K_0}(R) \to \mathbf{K_0}(S)$.
5. Let $R \subseteq S$ be Noetherian rings. Find conditions on the R-module S_R to guarantee that the restriction map $A \mapsto A_R$ determines a group homomorphism $\mathbf{G_0}(S) \to \mathbf{G_0}(R)$ or $\mathbf{K_0}(S) \to \mathbf{K_0}(R)$.
6. Modify the proof of Lemma 15.5(i) to show that $[X] = [Y]$ in $\mathbf{G_0}(R)$ if and only if there exist exact sequences $0 \to A \to B \oplus X \to C \to 0$ and $0 \to A \to B \oplus Y \to C \to 0$ with A, B, and C finitely generated R-modules.
7. Let R be an arbitrary ring and let P be a projective R-module. If $P \oplus Q \cong F$ is free, prove that $P \oplus F^\infty \cong F^\infty$, where F^∞ is a countably infinite direct sum of copies of F. This, of course, does not imply that P is stably free.
8. Let e be an idempotent of the Noetherian ring R and assume that $R = ReR$. Use the method of Exercise 12.5 to prove that $\mathbf{K_0}(R) \cong \mathbf{K_0}(eRe)$.
9. Let $S = S_0 \dot{+} S_1 \dot{+} \cdots$ be a graded ring and assume that every finitely generated projective S_0-module is stably free. Apply the result of Exercise 13.3 to deduce that every finitely generated graded-projective S-module is also stably free.
10. Obtain a power series analog of the Hilbert Basis Theorem. In other words, show that if R is right Noetherian, then so is $R[[t]]$. What about a version for the obvious skew power series ring $R[[t;\sigma]]$?

16. Patching Theorem

If R is a commutative polynomial ring over a field, then all finitely generated projective R-modules are free. This is the statement of the *Serre Conjecture*, which we prove in the next chapter. Of course, we already know that all finitely generated projective R-modules P are stably free, that is $P \oplus F' \cong F$ for suitable finitely generated free modules F' and F. Thus the goal is to show that F' can somehow be canceled from the preceding formula.

As we will see, cancellation is equivalent to the affirmative solution of a certain matrix problem. We begin here by describing that problem and we obtain some partial but rather key results. For the remainder of this and the next chapter, R always denotes a commutative ring.

DEFINITION Let $\mathbf{a} = (\, a_1 \quad a_2 \quad \cdots \quad a_n \,)$ be a *row matrix*, that is a $1 \times n$ matrix over R for some $n \geq 1$. We say that $\mathbf{a}$ is a *unimodular row* if $\sum_i a_i R = R$ or equivalently if there exist $c_i \in R$ with $\sum_i a_i c_i = 1$. We say that $\mathbf{a}$ is an *extendible row* if it is the first row of an invertible $n \times n$ matrix $\alpha \in \mathrm{M}_n(R)$.

Note that $\alpha \in \mathrm{M}_n(R)$ is invertible if and only if $\det \alpha$ is a unit of R. Thus for example if R is a field, then we need only have $\det \alpha \neq 0$. On the other hand, if $R = \mathbb{Z}$ is the ring of integers, then we must have $\det \alpha = \pm 1$.

Suppose now that α is invertible and that $\mathbf{a} = (\, a_1 \quad a_2 \quad \cdots \quad a_n \,)$ is its first row. Then, by computing the determinant of α by cofactors with respect to the first row, we have $\sum_i a_i c_i = \det \alpha = d$, where c_i is, of course, the cofactor of a_i. Thus $\sum_i a_i (c_i d^{-1}) = 1$ and it follows that $\mathbf{a}$ is unimodular. In other words, every extendible row is unimodular. We are concerned with the reverse question, namely is every unimodular row

extendible?

We start with two simple observations. Recall that the *elementary column operations* on R-matrices consists of (1) multiplying a column by a unit of R, (2) interchanging two columns, and (3) adding a multiple of one column to another. These operations can be applied to any size matrix, even a row, and they can all be achieved via right multiplication by appropriate invertible square matrices.

LEMMA 16.1 *i. Suppose row* $\mathbf{a}'$ *can be obtained from* $\mathbf{a}$ *by a sequence of elementary column operations. Then* $\mathbf{a}'$ *is extendible (or unimodular) if and only if* $\mathbf{a}$ *is extendible (or unimodular).*

ii. If $\mathbf{a} = (a_1 \quad a_2 \quad \cdots \quad a_n)$ *and* $a_1R + a_2R = R$, *then* $\mathbf{a}$ *is extendible.*

PROOF (i) By assumption we have $\mathbf{a}' = \mathbf{a}\gamma$ for some invertible matrix γ. Thus if $\mathbf{a}$ is the first row of the square matrix α, then $\mathbf{a}'$ is the first row of $\alpha\gamma$. In particular, if $\mathbf{a}$ is extendible, then we can take α invertible and thus $\mathbf{a}'$ is also extendible. Furthermore, if $\mathbf{a} = (a_1 \quad a_2 \quad \cdots \quad a_n)$ and $\mathbf{a}' = (a_1' \quad a_2' \quad \cdots \quad a_n')$, then $\mathbf{a}' = \mathbf{a}\gamma$ implies that $\sum_i a_i'R \subseteq \sum_i a_iR$. Thus, if $\mathbf{a}'$ is unimodular, then so is $\mathbf{a}$. The converses follow because $\mathbf{a} = \mathbf{a}'\gamma^{-1}$.

(ii) Now assume that $a_1R + a_2R = R$, so that $a_1b_1 - a_2b_2 = 1$ for some $b_1, b_2 \in R$. Then we see that $\mathbf{a}$ is the first row of the invertible matrix

$$\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ b_2 & b_1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

of determinant 1. □

We will freely use (i) without further comment. We remark that the matrix problem for $n = 1$ is trivially true and for $n = 2$ it is solved affirmatively in (ii). Thus it first becomes interesting when $n = 3$. In any case, in all our future computations we can assume that $n \geq 2$.

A commutative ring R is said to be *semilocal* if it has only finitely many maximal ideals. In particular, any local ring is semilocal.

LEMMA 16.2 *i. Let* R *be a semilocal ring and let* $\mathbf{a} = (a_1 \quad a_2 \quad \cdots \quad a_n)$ *be a unimodular row. Then there exist* $b_2, \ldots, b_n \in R$ *such that* $a_1 + \sum_{i=2}^n a_ib_i$ *is a unit of* R.

ii. If S is a commutative local ring and if $1 \neq p(x)$ is a monic polynomial in $S[x]$, then $S[x]/p(x)S[x]$ is a semilocal ring.

PROOF (i) Let $M_1, M_2, \ldots, M_k$ be the finitely many maximal ideals of R. We first show that, for each i, there exists $e_i \in R$ such that $e_i \equiv 1 \bmod M_i$ and $e_i \equiv 0 \bmod M_j$ for all $j \neq i$. To this end, note that for $j \neq i$ we have $M_i + M_j = R$, so there exist $m_j \in M_j$ and $m_j' \in M_i$ with $m_j' + m_j = 1$. In other words, $m_j \equiv 1 \bmod M_i$ and $m_j \equiv 0 \bmod M_j$. Now take $e_i = \prod_{j \neq i} m_j$.

Since $\mathbf{a} = (a_1 \quad a_2 \quad \cdots \quad a_n)$ is unimodular, $\sum_i a_i R = R$ and it follows that no maximal ideal of R contains all the a_i. In particular, for each maximal ideal M_j, if $a_1 \in M_j$, then there exists $a_{j'}$ with $j' \neq 1$ and $a_{j'} \notin M_j$. Set

$$b = a_1 + \sum_{a_1 \in M_j} e_j a_{j'}$$

Consider the maximal ideal M_i. If $a_1 \notin M_i$, then all e_j in the preceding sum for b are contained in M_i and hence $b \notin M_i$. On the other hand, if $a_1 \in M_i$, then $e_i a_{i'} \notin M_i$ occurs in the sum for b. Thus, since the remaining summands for b are all contained in M_i, we again have $b \notin M_i$. We conclude, therefore, that b is not contained in any maximal ideal of R and hence that b is a unit of R.

(ii) Suppose that $1 \neq p(x)$ is a monic polynomial of degree $k+1$. Our goal is to show that there are only finitely many maximal ideals M of $R = S[x]$ that contain $p(x)$. To this end, let M be such a maximal ideal and consider the irreducible R-module $V = R/M$. Since $p(x) \in M$ and $p(x)$ is monic, it follows that V is finitely generated as an S-module by the images of $1, x, \ldots, x^k$. Thus since $V \neq 0$, Nakayama's Lemma implies that $VJ \neq V$, where $J = \mathrm{Rad}(S)$. But VJ is certainly an R-submodule of V and V is irreducible, so $VJ = 0$ and hence $J \subseteq M$.

In other words, all maximal ideals of R that contain $p(x)$ also contain the Jacobson radical J of S. Thus they correspond to those maximal ideals of $R/JR = (S/J)[x]$ that contain the nonzero image $\bar{p}(x)$ of $p(x)$. But S is a local ring, so $S/J = F$ is a field. Thus $(S/J)[x] = F[x]$ is a principal ideal domain and hence a Dedekind domain. It follows that there are only finitely many maximal ideals of $F[x]$ that contain the nonzero ideal $\bar{p}(x)F[x]$. □

As a consequence we have:

PROPOSITION 16.3 *Let R be commutative and let $\mathbf{a} = (a_1 \quad a_2 \quad \cdots \quad a_n)$ be a unimodular row.*

i. If R/a_nR is a semilocal ring, then $\mathbf{a}$ *is extendible.*

ii. Suppose $R = S[x]$, with S a local ring. If a_n is a monic polynomial, then $\mathbf{a}$ *is an extendible row.*

PROOF (i) Let $\bar{}: R \to R/a_nR$ be the natural epimorphism. Since $\sum_i a_iR = R$, it follows that $\sum_i \bar{a}_i\bar{R} = \bar{R}$. Thus, by part (i) of the preceding lemma, there exist $b_i \in R$ with $\bar{b} = \bar{a}_1 + \sum_{i=2}^{n} \bar{a}_i\bar{b}_i$ a unit of $\bar{R}$. Define $\mathbf{a}' = (\, a_1' \quad a_2 \quad \cdots \quad a_n \,)$, where $a_1' = a_1 + \sum_{i=2}^{n} a_ib_i$. Then $\mathbf{a}'$ is obtained from $\mathbf{a}$ by a sequence of elementary column operations, so it suffices to show that $\mathbf{a}'$ is extendible. But observe that $\overline{a_1'} = \bar{b}$ is a unit of $\bar{R} = R/a_nR$ and hence $a_1'R + a_nR = R$. Lemma 16.1(ii) now implies that $\mathbf{a}'$ is extendible.

(ii) If $a_n = 1$, then $a_1R + a_nR = R$ and the proposition is proved. Otherwise, by part (ii) of the preceding lemma, $R/a_nR = S[x]/a_nS[x]$ is a semilocal ring and (i) yields the result. □

We now begin work on a key observation, the Patching Theorem. Recall that if T is a multiplicatively closed subset of a commutative integral domain S, then we can localize to form the ring of fractions ST^{-1}. We need to consider two such situations here. In one case, $T = \{1, f, f^2, \dots\}$ for some nonzero element $f \in S$ and we denote ST^{-1} by S_f. Alternatively, if M is a maximal ideal of S, then $T = S \setminus M$ is multiplicatively closed and we write S_M for ST^{-1}. These are, of course, all contained in the field of fractions SS^{-1}.

We are concerned with $n \times n$ matrices over the polynomial ring $S[x]$ and we note that these can all be viewed as polynomials in x over $\mathrm{M}_n(S)$. Thus we use polynomial notation for such matrices.

LEMMA 16.4 *Let S be a commutative integral domain, let f be a nonzero element of S and let $\theta(x)$ be an invertible matrix in $\mathrm{M}_n(S_f[x])$. Then there exists an integer $k \geq 1$ such that whenever $h_1, h_2 \in S$ satisfy $h_1 - h_2 \in f^kS$, then*

$$\phi(x) = \theta(h_1x)\theta(h_2x)^{-1}$$

is an invertible matrix in $\mathrm{M}_n(S[x])$.

PROOF Write $\theta(x) = \sum_0^p \alpha_i x^i$ and $\theta(x)^{-1} = \sum_0^q \beta_j x^j$, where $\alpha_i, \beta_j \in \mathrm{M}_n(S_f)$. Now choose an integer $k \geq 1$ so that $f^k\alpha_i\beta_j \in \mathrm{M}_n(S)$ for all i, j. If $s, t \in S$, define

$$\phi(x; s, t) = \theta\big((s + f^kt)x\big)\,\theta(sx)^{-1}$$

Then

$$\begin{aligned}\phi(x;s,t) &= 1 + \big[\theta\big((s+f^k t)x\big) - \theta(sx)\big]\theta(sx)^{-1} \\ &= 1 + \sum_i \alpha_i x^i \big[(s+f^k t)^i - s^i\big]\theta(sx)^{-1}\end{aligned}$$

Thus, since f^k divides $(s+f^k t)^i - s^i$, we see that $\phi(x;s,t)$ is a matrix in $\mathrm{M}_n(S[x])$.

Finally, let $h_1 - h_2 \in f^k S$, set $s = h_2$, and choose the element t so that $h_1 - h_2 = f^k t$. Then $\phi(x;s,t) = \theta(h_1 x)\theta(h_2 x)^{-1} = \phi(x)$ is a matrix in $\mathrm{M}_n(S[x])$. Similarly, $\theta(h_2 x)\theta(h_1 x)^{-1} \in \mathrm{M}_n(S[x])$, so $\phi(x)$ is invertible in $\mathrm{M}_n(S[x])$. □

LEMMA 16.5 *Let S be as before and suppose f, g are nonzero elements of S with $Sf + Sg = S$. Let $\mathbf{a}(x) = (\,a_1(x) \quad a_2(x) \quad \cdots \quad a_n(x)\,)$ be a unimodular row over $S[x]$ and assume that $\mathbf{a}(x)$ is extendible over the larger rings $S_f[x]$ and $S_g[x]$. If $\mathbf{a}(0) = (\,a_1(0) \quad a_2(0) \quad \cdots \quad a_n(0)\,)$ is extendible over S, then $\mathbf{a}(x)$ is extendible over $S[x]$.*

PROOF We start with some observations on matrix multiplication. If A and B are square matrices, then the first row of AB depends on all of B but only the first row of A. Thus if A and A' have the same first row, then so do AB and $A'B$. For example, if A has first row $\mathbf{i} = (1 \quad 0 \quad \cdots \quad 0)$, then A has the same first row as the identity matrix I and thus AB has the same first row as $IB = B$. Conversely, suppose A and B have the same first row and assume that B is invertible. Then AB^{-1} has the same first row as $BB^{-1} = I$, so AB^{-1} has first row $\mathbf{i}$. In particular, if B has first row $\mathbf{i}$, then so does $B^{-1} = IB^{-1}$.

Now for the proof. Let $\alpha_f(x)$ denote the given extension of the row $\mathbf{a}(x)$ to an invertible matrix in $\mathrm{M}_n(S_f[x])$ and let $\alpha_g(x)$ be the extension of $\mathbf{a}(x)$ to an invertible matrix in $\mathrm{M}_n(S_g[x])$. In addition, let β be an extension of the row $\mathbf{a}(0)$ to an invertible matrix in $\mathrm{M}_n(S)$. Then $\alpha'_f(x) = \beta\alpha_f(0)^{-1}\alpha_f(x)$ is also an invertible matrix in $\mathrm{M}_n(S_f[x])$ and it has first row $\mathbf{a}(x)$. Indeed, since β and $\alpha_f(0)$ have the same first row, $\beta\alpha_f(0)^{-1}$ has first row $\mathbf{i}$ and thus $\alpha'_f(x)$ has the same first row as $\alpha_f(x)$. Furthermore, since $\alpha'_f(0) = \beta$, we can now replace $\alpha_f(x)$ by $\alpha'_f(x)$ to assume that $\alpha_f(0) = \beta$. Similarly, we can assume that $\alpha_g(0) = \beta$ and, in particular, that $\alpha_f(0) = \alpha_g(0)$.

Define $\theta(x) = \alpha_f(x)\alpha_g(x)^{-1}$, so that $\theta(x)$ is clearly an invertible matrix in $\mathrm{M}_n(S_{fg}[x])$. Also $\theta(x)$ has first row $\mathbf{i}$ and $\theta(0) = I$. Since

$$S_{fg}[x] = (S_f)_g[x] = (S_g)_f[x]$$

we can apply the previous lemma in two different ways to the matrix $\theta(x)$ and we let k to be the larger of the two integers given by those applications.

Note that $S = (Sf + Sg)^{2k} = Sf^k + Sg^k$, so we can choose $h \in S$ with $h \in Sf^k$ and $1 - h \in Sg^k$. Since $\theta(0) = I$, we can write

$$\theta(x) = \left[\theta(x)\theta(hx)^{-1}\right]\left[\theta(0x)\theta(hx)^{-1}\right]^{-1}$$

and we consider, in turn, each of the two factors in square brackets.

First, we note that $\theta(x)$ is invertible in the ring $\mathrm{M}_n\big((S_f)_g[x]\big)$ and that $1 - h \in Sg^k \subseteq (S_f)g^k$. Thus, by the previous lemma, $\phi_f(x) = \theta(x)\theta(hx)^{-1}$ is invertible in $\mathrm{M}_n(S_f[x])$. Similarly, $\theta(x)$ is invertible in $\mathrm{M}_n\big((S_g)_f[x]\big)$ and $0 - h \in Sf^k \subseteq (S_g)f^k$, so the previous lemma also implies that $\phi_g(x) = \theta(0x)\theta(hx)^{-1}$ is invertible in $\mathrm{M}_n(S_g[x])$. Thus

$$\alpha_f(x)\alpha_g(x)^{-1} = \theta(x) = \phi_f(x)\phi_g(x)^{-1}$$

In other words, $\phi_f(x)^{-1}\alpha_f(x) = \phi_g(x)^{-1}\alpha_g(x)$ and we denote this common matrix by $\gamma(x)$.

Since $\theta(x)$ has first row $\mathbf{i}$, it follows that $\phi_f(x)$ and $\phi_f(x)^{-1}$ also have first row $\mathbf{i}$. Thus $\gamma(x)$ has the same first row as $\alpha_f(x)$, namely $\mathbf{a}(x)$. Furthermore, $\gamma(x)$ is an invertible matrix in both $\mathrm{M}_n(S_f[x])$ and $\mathrm{M}_n(S_g[x])$. Thus $\gamma(x)$ will be the appropriate extension for the row $\mathbf{a}(x)$ provided we show that $S_f[x] \cap S_g[x] = S[x]$ or, equivalently, that $S_f \cap S_g = S$. For the latter, let $w = s/f^j = t/g^j \in S_f \cap S_g$ with $s, t \in S$. Since $Sf^j + Sg^j = S$, there exist $u, v \in S$ with $uf^j + vg^j = 1$. But then

$$w = w(uf^j + vg^j) = us + vt \in S$$

and the lemma is proved. □

We can now quickly obtain the main result of this chapter.

THEOREM 16.6 (Quillen Patching Theorem) *Let S be a commutative integral domain and let $\mathbf{a}(x) = (\,a_1(x) \quad a_2(x) \quad \cdots \quad a_n(x)\,)$ be a unimodular row with entries in the polynomial ring $R = S[x]$. Suppose that $\mathbf{a}(0)$ is extendible in $\mathrm{M}_n(S)$ and that $\mathbf{a}(x)$ is extendible in $\mathrm{M}_n(S_M[x])$ for all maximal ideals M of S. Then $\mathbf{a}(x)$ is extendible in $\mathrm{M}_n(R) = \mathrm{M}_n(S[x])$.*

PROOF Let

$$A = \{\,0\,\} \cup \{\,0 \neq f \in S \mid \mathbf{a}(x) \text{ is extendible in } \mathrm{M}_n(S_f[x])\,\}$$

We claim that A is an ideal of S. To start with, suppose $0 \neq f \in A$ and $0 \neq g \in S$. Since $S_f[x] \subseteq S_{fg}[x]$, it follows that $\mathbf{a}(x)$ is extendible in $\mathrm{M}_n(S_{fg}[x])$. Thus $fg \in A$ and we see that A is closed under multiplication by S. To check closure of addition, it clearly suffices to consider $f, g \in A$ with f, g and $f+g$ all nonzero. The goal is to show that $f+g \in A$. If $S' = S_{f+g}$, then $S_f \subseteq S'_f$ and $S_g \subseteq S'_g$, so $\mathbf{a}(x)$ is extendible in both $\mathrm{M}_n(S'_f[x])$ and $\mathrm{M}_n(S'_g[x])$. Furthermore, $\mathbf{a}(0)$ is extendible in $\mathrm{M}_n(S) \subseteq \mathrm{M}_n(S')$. Thus, since $S'f + S'g = S'$, Lemma 16.5 implies that $\mathbf{a}(x)$ is extendible in $\mathrm{M}_n(S'[x])$. But $S' = S_{f+g}$ and therefore $f+g \in A$, as required.

We now know that A is an ideal of S. If $A \neq S$, then $A \subseteq M$ for some maximal ideal M of S and, by assumption, $\mathbf{a}(x)$ is the first row of an invertible matrix $\alpha(x) \in \mathrm{M}_n(S_M[x])$. In other words, both $\alpha(x)$ and $\alpha(x)^{-1}$ are contained in $\mathrm{M}_n(S_M)[x]$. Now let f be the product of all the denominators of all the finitely many entries of the $\mathrm{M}_n(S_M)$-coefficients of these two matrices. Then $\alpha(x), \alpha(x)^{-1} \in \mathrm{M}_n(S_f)[x] = \mathrm{M}_n(S_f[x])$ and hence $f \in A \subseteq M$. On the other hand, f is a product of elements of the multiplicatively closed set $S \setminus M$ and therefore $f \in S \setminus M$, a contradiction.

Thus $A = S$ and, in particular, $1 \in A$. But $S_1 = S$, so $\mathbf{a}(x)$ is extendible in $\mathrm{M}_n(S[x]) = \mathrm{M}_n(R)$ and the theorem is proved. □

EXERCISES

1. Let $P_1, P_2, \ldots, P_k$ be incomparable prime ideals in the commutative ring R. For each $i \neq j$, choose $a_{i,j} \in P_j \setminus P_i$ and define $e_i = \prod_{j \neq i} a_{i,j}$. Show that $e_i \in P_j$ for all $j \neq i$ but that $e_i \notin P_i$. Now let $I \lhd R$ and suppose that I is not contained in any P_i. If $b_i \in I \setminus P_i$, show that $b = \sum_i b_i e_i \in I \setminus \bigcup_i P_i$.
2. Assume that R is a commutative domain and that $P_1, P_2, \ldots P_k$ are as before. Show that $T = R \setminus \bigcup_i P_i$ is a multiplicatively closed subset of R and that RT^{-1} is a semilocal ring whose maximal ideals are $P_i T^{-1}$ for $i = 1, 2, \ldots, k$.
3. Let $S = \mathbb{Z}[a]$ be a polynomial ring in one variable over the integers $\mathbb{Z}$. Since $M = (2, a)$ is a maximal ideal of S, it follows that S_M is a local ring. Prove that $R = S_M[x]/(1 - ax)S_M[x]$ is not semilocal. For this, observe that for each integer $n \neq 0$, R has a homomorphism onto the rationals given by $a \mapsto 2n$ and $x \mapsto 1/(2n)$.
4. Let R be a commutative ring and let V be a finitely generated right R-module with generators $v_1, v_2, \ldots, v_n$. Suppose that $r_{i,j} \in R$ with $\sum_{i=1}^{n} v_i r_{i,j} = 0$ for $j = 1, 2, \ldots, n$. Multiply the matrix equation

$$(v_1 \quad v_2 \quad \cdots \quad v_n)(r_{i,j}) = 0$$

on the right by the adjoint of $(r_{i,j})$ to deduce that $V \cdot \det(r_{i,j}) = 0$. This is known as the *determinantal trick.*

In the remaining exercises, we assume that R is a principal ideal domain. We say that two $m \times n$ matrices A and B over R are *equivalent* and write $A \sim B$ if $A = PBQ$, where P is an invertible matrix in $\mathrm{M}_m(R)$ and Q is invertible in $\mathrm{M}_n(R)$. Obviously this is an equivalence relation and the goal is to show that each equivalence class contains a matrix having a particularly nice form. Recall that a principal ideal domain is also a unique factorization domain.

5. Suppose $a, b \in R$ have greatest common divisor $(a, b) = d$. Show that the matrix $A = \begin{pmatrix} a & b \\ r & s \end{pmatrix}$ is equivalent to a matrix of the form $\begin{pmatrix} d & * \\ * & * \end{pmatrix}$. To this end, note that $ax + by = d$ for suitable relatively prime elements $x, y \in R$.
6. Let A be an $m \times n$ matrix over R and assume, among all the matrices equivalent to A, that A has a nonzero entry q with the smallest number of prime factors. Prove that A is equivalent to the block matrix $\begin{pmatrix} q & 0 \\ 0 & A' \end{pmatrix}$, where q divides all entries of A'. To start with, use elementary row and column operations to shift q to the $(1,1)$ position. Then use the argument of Exercise 5 to deduce that q divides all entries in the first row and first column. Now apply row and column operations again.
7. For each $m \times n$ matrix A, define $D_k(A)$ to be the greatest common divisor of the determinants of all $k \times k$ submatrices of A. If $A \sim B$, show that $D_k(A)$ and $D_k(B)$ are *associates* for all k, that is they are unit multiples of each other.
8. Let A be an $m \times n$ matrix over R. Prove that A is equivalent to the $m \times n$ diagonal matrix $B = \mathrm{diag}\{q_1, q_2, \ldots, q_t\}$, where $t = \min\{m, n\}$ and where $q_i \mid q_{i+1}$ for all i. Furthermore, show that the q_i's are uniquely determined up to multiplication by a unit of R.
9. Suppose that W is an R-submodule of the free R-module $V = R^n$. Show that there exists a basis $\{v_1, v_2, \ldots, v_n\}$ of V and nonzero elements $q_1, q_2, \ldots, q_k \in R$ with $q_i \mid q_{i+1}$ such that $\{v_1 q_1, v_2 q_2, \ldots, v_k q_k\}$ is a basis for W. Furthermore, show that the q_i's are essentially

unique. For this, let $\{ v_1, v_2, \ldots, v_n \}$ be any basis for V. Since R is hereditary and Noetherian, W is also a free module with basis, say $\{ w_1, w_2, \ldots, w_m \}$. Write $w_i = \sum_j v_j a_{i,j}$ and observe that a change of basis in V and in W corresponds to multiplying the $m \times n$ matrix $(a_{i,j})$ on the right and on the left by invertible square matrices.

10. Finally, let M be a finitely generated module over the principal ideal domain R. Prove that M is isomorphic to a direct sum $\oplus \sum_1^n R/q_i R$, where $q_i \mid q_{i+1}$ for all i and no q_i is a unit. Furthermore, show that the q_i are appropriately unique. In case $R = \mathbb{Z}$ is the ring of integers, this result is the Fundamental Theorem of Abelian Groups. It follows from the previous exercise by observing that $M \cong V/W$ for some finitely generated free R-module V.

17. Serre Conjecture

In this chapter we complete the proof of the Serre Conjecture. Let K be a field and let $K[x_1, x_2, \ldots, x_m]$ be a commutative polynomial ring over K. By a *change of variables* we mean a collection of polynomials $t_1, t_2, \ldots, t_m$ that are algebraically independent over K and that generate the polynomial ring. In other words, $t_1, t_2, \ldots, t_m$ is a change of variables if and only if $K[x_1, x_2, \ldots, x_m] = K[t_1, t_2, \ldots, t_m]$. The following is a special case of a much more general result.

THEOREM 17.1 (Suslin Monic Polynomial Theorem) *Let A be a nonzero ideal of the polynomial ring $K[x_1, x_2, \ldots, x_m]$. Then there exists a change of variables $t_1, t_2, \ldots, t_m$ such that A contains a polynomial, written in terms of these new variables, that is monic in t_m.*

PROOF We proceed by induction on m, the case $m = 1$ being trivial. Now assume that $m \geq 2$, let $R = K[x_1, \ldots, x_{m-1}]$ and observe that

$$K[x_1, x_2, \ldots, x_m] = K[x_1, \ldots, x_{m-1}][x_m] = R[x_m]$$

Let B be the set of leading coefficients of elements of A, so that

$$B = \{\, r \in R \mid \sum_{i=0}^{k} r_i x_m^i \in A \text{ with } r_i \in R \text{ and } r_k = r \,\}$$

Then B is easily seen to be a nonzero ideal in the polynomial ring $R = K[x_1, \ldots, x_{m-1}]$ and induction applies in this smaller ring. Thus we can assume, by making a change of variables in R, that B contains a polynomial $f(x_1, \ldots, x_{m-1})$ that is monic in x_1. Furthermore, by definition of B, there is a polynomial $g \in A$ with

$$g = r_0 + r_1 x_m + \cdots + r_k x_m^k \in R[x_m]$$

such that $r_k = f$.

Finally choose an integer d larger than the total degree of each r_i and define a new change of variables by

$$t_i = \begin{cases} x_m - x_1^d & \text{if } i = 1 \\ x_i & \text{if } i \neq 1 \text{ or } m \\ x_1 & \text{if } i = m \end{cases}$$

It is clear that $t_1, t_2, \ldots, t_m$ generate the polynomial ring and that they are algebraically independent over K. Indeed, we have

$$x_i = \begin{cases} t_m & \text{if } i = 1 \\ t_i & \text{if } i \neq 1 \text{ or } m \\ t_1 + t_m^d & \text{if } i = m \end{cases}$$

Now in terms of these new variables, the ith summand of g becomes

$$r_i(t_m, t_2, \ldots, t_{m-1})(t_1 + t_m^d)^i$$

and for $i < k$, this polynomial has t_m degree strictly less than $d + di \leq dk$ by the choice of d. On the other hand, when $i = k$ we have $r_k = f$, so this summand is equal to

$$f(t_m, t_2, \ldots, t_{m-1})(t_1 + t_m^d)^k$$

and has t_m degree at least dk. Furthermore, since f is monic in its first variable, the latter summand looks like

$$(t_m^j + \text{lower degree terms in } t_m)(t_1 + t_m^d)^k$$

and hence is monic in t_m of degree $\geq dk$. It follows from all of this that $g \in A$ is monic in the variable t_m. □

As a consequence, we have the following classical result.

THEOREM 17.2 (Noether Normalization Theorem) *Let K be a field and let E be a finitely generated commutative K-algebra. Then E has a subalgebra E_0, isomorphic to a polynomial ring over K, with E a finite integral extension of E_0.*

PROOF Say E is generated over K by $\zeta_1, \zeta_2, \ldots, \zeta_m$. We proceed by induction on m, the case $m = 0$ being trivial. Assume now that $m \geq 1$ and map the polynomial ring $R = K[x_1, x_2, \ldots, x_m]$ onto E via $\theta: x_i \mapsto \zeta_i$.

If $\mathrm{Ker}(\theta) = 0$, then E is a polynomial ring and we are finished. Thus we may suppose that $A = \mathrm{Ker}(\theta) \neq 0$.

By the preceding theorem, there is a change of variables $t_1, t_2, \ldots, t_m$ in R such that A contains a polynomial monic in the variable t_m. Write $\eta_i = \theta(t_i)$ and let E' be the K-subalgebra of E generated by the elements $\eta_1, \eta_2, \ldots, \eta_{m-1}$. Since A contains a monic polynomial in t_m and since that polynomial maps to 0 in E, it follows that η_m is integral over E'. But E is generated by η_m and E', and hence we see that E is a finite integral extension of E'.

Finally, E' has $m-1$ generators, so, by induction, E' is a finite integral extension of a polynomial ring E_0. But an integral extension of an integral extension is integral, so it follows that E is a finite integral extension of E_0. □

We can now use the Monic Polynomial and Patching Theorems to solve the matrix problem.

THEOREM 17.3 *Let $R = K[x_1, x_2, \ldots, x_m]$ be a polynomial ring over the field K and let $\mathbf{a} = (a_1 \quad a_2 \quad \cdots \quad a_n)$ be a unimodular row. Then $\mathbf{a}$ is the first row of an invertible matrix in $\mathrm{M}_n(R)$.*

PROOF We can assume that $n \geq 2$ and that $a_1 \neq 0$. We proceed by induction on m, the number of variables that generate R. If $m = 0$, then $R = K$ is a field, so $a_1R + a_2R = R$ and $\mathbf{a}$ is extendible. Now assume that $m \geq 1$ and that the result holds for $m-1$.

Let $A = a_1R$ so that A is a nonzero ideal of R. By the Monic Polynomial Theorem, there exists a change of variables $t_1, t_2, \ldots, t_m$ such that A contains a polynomial $h = a_1r$ that is monic in t_m. Furthermore, by an elementary column operation, we can replace a_n in $\mathbf{a}$ by $a_n' = a_n + a_1rt_m^N = a_n + ht_m^N$ for any integer N. In particular, if we choose N sufficiently large, then a_n' is monic in t_m because h is.

In other words, by renaming the variables and entries, we can now assume that the variables are $x_1, x_2, \ldots, x_m$ and that a_n is monic in x_m. Set $S = K[x_1, \ldots, x_{m-1}]$ so that $R = S[x]$ with $x_m = x$. Then we can write the row $\mathbf{a}$ as $\mathbf{a}(x) = (a_1(x) \quad a_2(x) \quad \cdots \quad a_n(x))$, where the entries are all polynomials in $S[x]$.

Let M be any maximal ideal of S. Since $\sum_i a_i(x)R = R$, it follows that $\sum_i a_i(x)S_M[x] = S_M[x]$ and hence that $\mathbf{a}(x)$ is a unimodular row over $S_M[x]$. Thus, since $a_n(x)$ is a monic polynomial and S_M is a local ring, Proposition 16.3(ii) implies that $\mathbf{a}(x)$ is extendible over $S_M[x]$. Next, by evaluating at $x = 0$, we see that $\sum_i a_i(0)S = S$ and hence that $\mathbf{a}(0)$ is a unimodular row over S. But S is a polynomial ring in $m-1$ variables,

so induction implies that $\mathbf{a}(0)$ is extendible over S. We can now conclude from the Patching Theorem that $\mathbf{a}(x)$ is extendible over $R = S[x] = K[x_1, x_2, \ldots, x_m]$ and the result follows. □

It is now time to explain the relevance of this matrix problem to the Serre Conjecture.

LEMMA 17.4 *Let R be a commutative integral domain and let $F = R^n$ be a free R-module with basis $\{f_1, f_2, \ldots, f_n\}$. Let $\mathbf{a} = (a_1 \quad a_2 \quad \cdots \quad a_n)$ be a nonzero row and write $f = f_1a_1 + f_2a_2 + \cdots + f_na_n \in F$.*

i. $fR \mid F$ if and only if $\mathbf{a}$ is a unimodular row.

ii. fR has a free complement in F if and only if $\mathbf{a}$ is the first row of an invertible matrix in $\mathrm{M}_n(R)$.

PROOF (i) Since F is a torsion free R-module, we have $fR \cong R$. Suppose first that $fR \mid R^n$ and let $\pi\colon R^n \to fR$ be the projection homomorphism. If $\pi(f_i) = fr_i$ with $r_i \in R$, then

$$f = \pi(f) = \pi\Big(\sum_i f_ia_i\Big) = f\sum_i r_ia_i$$

Thus $1 = \sum_i r_ia_i$ and $\mathbf{a}$ is a unimodular row.

Conversely, suppose $\mathbf{a}$ is a unimodular row and say $1 = \sum_i a_is_i$. Define $\theta\colon R^n \to fR$ by $\theta\colon f_i \mapsto fs_i$. Then

$$\theta(f) = \theta\Big(\sum_i f_ia_i\Big) = f\sum_i s_ia_i = f$$

and thus θ is the identity on fR. In particular, $fR \cap \mathrm{Ker}(\theta) = 0$. Furthermore, if $v \in F$ is arbitrary, then $v = \theta(v) + \big(v - \theta(v)\big) \in fR + \mathrm{Ker}(\theta)$ and thus we conclude that $F = fR \dotplus \mathrm{Ker}(\theta)$.

(ii) Now suppose that $\mathbf{a}$ is the first row of the invertible matrix $(c_{i,j}) \in \mathrm{M}_n(R)$ and define the elements $g_i \in F$ by $g_i = \sum_j f_jc_{i,j}$. Since $(c_{i,j})$ is invertible, so is its transpose matrix and it follows from Lemma 2.5 that $\{g_1, g_2, \ldots, g_n\}$ is also a free basis for F. Furthermore,

$$g_1 = \sum_j f_jc_{1,j} = \sum_j f_ja_j = f$$

and thus $fR = g_1R$ has the free complement $\cdot \sum_{i=2}^n g_iR$.

Conversely, suppose fR has the free complement $W \cong R^t$. Since $fR \cong R$, we have $R^n = F \cong R^{t+1}$ and thus Lemma 2.6(iii) implies

that $n = t + 1$. Let W have basis $\{ h_2, h_3, \ldots, h_n \}$ and set $h_1 = f$. If $h_i = \sum_j f_j d_{i,j}$, then, since $\{ h_1, h_2, \ldots, h_n \}$ is also a free basis for F, Lemma 2.5 implies that the matrix $(d_{j,i})$ is invertible in $\mathrm{M}_n(R)$ and hence so is its transpose $(d_{i,j})$. But $\mathbf{a}$ is the first row of $(d_{i,j})$, so the lemma is proved. □

We can now quickly settle the Serre Conjecture. Its affirmative solution was obtained independently and at the same time by both Quillen and Suslin. Indeed, there are now at least three different proofs of the result, all of which use its equivalence to the matrix problem. The proof we chose, based on the Patching Theorem, seems to be of particular interest.

THEOREM 17.5 (Quillen-Suslin Theorem) *Let $R = K[x_1, x_2, \ldots, x_m]$ be a polynomial ring over the field K in $m < \infty$ variables. Then all finitely generated projective R-modules are free.*

PROOF By the Sygygy Theorem, all finitely generated projective R-modules are stably free. Thus we need only show that any stably free module is necessarily free.

Suppose first that P is a finitely generated R-module with $P \oplus R$ free. To be precise, say $P \dotplus A = F = R^n$, where $A \cong R$ and where R^n has free basis $\{ f_1, f_2, \ldots, f_n \}$. Since $A \cong R$, we have $A = fR$, with $f = \sum_1^n f_i a_i \neq 0$. By part (i) of the preceding lemma, $\mathbf{a} = (a_1 \quad a_2 \quad \cdots \quad a_n)$ is a unimodular row; then, by the affirmative solution of the matrix problem, it follows that $\mathbf{a}$ is extendible. Thus Lemma 17.4(ii) implies that $A = fR$ has a free complement, say F', in F. But then $P \dotplus A = F = F' \dotplus A$, so $P \cong F/A \cong F'$ and P is free.

Finally, if P is stably free, then $P \oplus R^t$ is free for some $t \geq 0$. If $t \geq 1$, then $(P \oplus R^{t-1}) \oplus R$ is free, so the preceding implies that $P \oplus R^{t-1}$ is also free. Continuing in this manner, canceling one R summand at a time, we conclude that P is free. □

It is reasonably easy to construct noncommutative counterexamples to the preceding theorem. Indeed, we have:

PROPOSITION 17.6 *Let D be a noncommutative division ring. Then the polynomial ring $S = D[x, y]$ has a stably free projective module that is not free.*

PROOF Since D is noncommutative, we can choose elements $a, b \in D$ with $ab - ba = d \neq 0$. Then d is a unit of D and hence of S. Define the right ideals $A = (x+a)S$ and $B = (y+b)S$ and note that $A_S \cong S_S \cong B_S$.

Furthermore, since x and y are central in S we have

$$(x+a)(y+b) - (y+b)(x+a) = d \qquad (*)$$

Thus $d \in A+B$ and hence $A+B=S$. It now follows from Lemma 6.8(i) that $A_S \oplus B_S \cong S_S \oplus C_S$, where $C = A \cap B$. In particular, since $A \oplus B \cong S \oplus S$, we see that C_S is projective and, in fact, stably free. Suppose by way of contradiction that C_S is free.

Note that the homomorphism $D[x,y] \to D$ given by $x, y \mapsto 0$ maps S to the IBN ring D. Thus, by Lemma 2.6(i), S is also an IBN ring. In particular, if C_S is free of rank n, then $S \oplus S \cong S \oplus C \cong S \oplus S^n$, so $n = 1$ and $C = f(x,y)S$ for some nonzero polynomial $f(x,y) \in S$. Of course, $f(x,y)$ is not uniquely determined, since we can certainly multiply it on the right by a nonzero element of D to obtain another generator of C.

We use $\deg_x$ and $\deg_y$ to denote the x- and y-degrees of a polynomial in S. Set $u = d^{-1}bd$ and multiply equation $(*)$ on the right by $y+u$. Since $d(y+u) = (y+b)d$, we obtain

$$(x+a)(y+b)(y+u) = (y+b)\big[(x+a)(y+u)+d\big]$$

so this expression is a nonzero element of $(x+a)S \cap (y+b)S = f(x,y)S$. In other words, $f(x,y)$ is a left divisor of $(x+a)(y+b)(y+u)$ and it follows that $\deg_x f(x,y) \leq 1$. Similarly $\deg_y f(x,y) \leq 1$, so we must have

$$f(x,y) = \alpha + \beta x + \gamma y + \delta xy$$

for suitable $\alpha, \beta, \gamma, \delta \in D$.

Now $f(x,y) \in (x+a)S$, so $f(x,y) = (x+a)g(x,y)$ for some $g(x,y) \in S$ and, by degree considerations, $g(x,y) = g(y)$ must be a polynomial in y with $\deg_y g(y) \leq 1$. Indeed, $\deg_y g(y) = 1$, since otherwise $\deg_y f(x,y) = 0$ contradicting the fact that $f(x,y) \in (y+b)S$. It follows from all this that $\delta \neq 0$; thus, by replacing $f(x,y)$ by $f(x,y)\delta^{-1}$, we can assume that $\delta = 1$. In particular, $f(x,y) = (x+a)g(y)$ now implies that $f(x,y) = (x+a)(y+b')$ for some $b' \in D$ and similarly we have $f(x,y) = (y+b)(x+a')$ for some a'. Thus

$$(x+a)(y+b') = f(x,y) = (y+b)(x+a')$$

and comparing coefficients yields $a = a'$, $b = b'$, and then $ab = ba$, a contradiction. Therefore, C is stably free but not free. □

Note that $D[x]$ is a principal ideal ring and hence, as in Corollary 6.4, all projective $D[x]$-modules are free. This shows that at least two variables are needed in the preceding. Examples also exist of commutative

Noetherian domains with stably free projective modules that are not free. At present, their construction seems to require the Hairy Ball Theorem, which asserts that an even dimensional real sphere does not possess a continuously differentiable field of unit tangent vectors. See Exercises 7–10 for an advanced calculus proof of this result.

PROPOSITION 17.7 *Let $\mathbb{R}$ be the field of real numbers and let*

$$R = \mathbb{R}[x, y, z]/(x^2 + y^2 + z^2 - 1)$$

Then R is a commutative integral domain, finitely generated over $\mathbb{R}$, and R has a stably free projective module that is not free.

PROOF Let $T = \mathbb{R}[a, b]$ be the polynomial ring in two variables over $\mathbb{R}$ and notice that $1 - a^2 - b^2$ does not have a square root in the rational function field $K = \mathbb{R}(a, b)$. Thus the polynomial $\zeta^2 - (1 - a^2 - b^2)$ is irreducible in $K[\zeta]$ and, if c is a root of this polynomial, then $K[c]$ is an algebraic field extension of K. Since the $\mathbb{R}$-homomorphism given by $x \mapsto a$, $y \mapsto b$, $z \mapsto c$ embeds $R = \mathbb{R}[x, y, z]/(x^2+y^2+z^2-1)$ into $K[c]$, we see that R is an integral domain. Furthermore, by way of this embedding, we can write $R = \mathbb{R}[a, b, c]$ subject to the relation $a^2 + b^2 + c^2 = 1$.

Now observe that evaluation yields a homomorphism from $\mathbb{R}[x, y, z]$ to $\mathbf{C}^\infty(\mathbb{S}^2)$, the ring of infinitely differentiable real valued functions defined on the 2-sphere

$$\mathbb{S}^2 = \{\, (\bar{x}, \bar{y}, \bar{z}) \in \mathbb{R}^3 \mid \bar{x}^2 + \bar{y}^2 + \bar{z}^2 = 1 \,\}$$

Indeed, since the polynomial $x^2 + y^2 + z^2 - 1$ maps to 0, this determines a homomorphism from R to $\mathbf{C}^\infty(\mathbb{S}^2)$. In particular, if $r \in R$, we let $r(s) \in \mathbb{R}$ denote the function r evaluated at $s \in \mathbb{S}^2$.

Let F be the free R-module of rank 3 with basis $\{ f_1, f_2, f_3 \}$ and set $f = f_1 a + f_2 b + f_3 c \in F$. Since $a^2 + b^2 + c^2 = 1$, we see that $\mathbf{a} = (a \quad b \quad c)$ is a unimodular row; thus, by Lemma 17.4(i), $fR \mid F$. In particular, if $F = fR \dotplus P$, then P is stably free, since $fR \cong R$. Moreover, to prove that P is not free, it suffices by Lemma 17.4(ii) to show that $\mathbf{a}$ is not the first row of an invertible matrix in $\mathrm{M}_3(R)$.

Suppose by way of contradiction that

$$\begin{pmatrix} a & b & c \\ u & v & w \\ u' & v' & w' \end{pmatrix}$$

is an invertible matrix in $\mathrm{M}_3(R)$ with determinant d, a unit of R. Thus d maps to a unit of $\mathbf{C}^\infty(\mathbb{S}^2)$ and, in particular, $d(s) \neq 0$ for all $s \in \mathbb{S}^2$.

Now let $A, U: \mathbb{S}^2 \to \mathbb{R}^3$ be the continuous vector valued funtions given by

$$A(s) = a(s)\vec{i} + b(s)\vec{j} + c(s)\vec{k}$$
$$U(s) = u(s)\vec{i} + v(s)\vec{j} + w(s)\vec{k}$$

Notice that $A(s)$ is the radial vector at s and that $U(s)$ is never in the same direction as $A(s)$ because $d(s) \neq 0$. Thus the cross product $A(s) \times U(s)$ is never zero and we can define

$$X(s) = \frac{A(s) \times U(s)}{\|A(s) \times U(s)\|}$$

Then $X: \mathbb{S}^2 \to \mathbb{R}^3$ is also an infinitely differentiable vector valued function. Furthermore, $X(s)$ is always a unit vector perpendicular to the radial vector $A(s)$. But the Hairy Ball Theorem asserts that no such function exists. Thus P_R is a stably free R-module that is not free. □

EXERCISES

1. Let K be a perfect field of characteristic $p > 0$ and let F be a finitely generated field extension of K. Prove that F/K is *separably generated*, that is there exists an intermediate field L with L/K purely transcendental and F/L separably algebraic. For this, suppose $F = K(a_1, a_2, \ldots, a_n)$ and proceed by induction on n. Choose m maximal so that all subsets of $\{ a_1, a_2, \ldots, a_n \}$ of size m are algebraically independent and suppose that $f(a_1, a_2, \ldots, a_{m+1}) = 0$ is an algebraic dependence of minimal degree. Show that some exponent in f is not divisible by p and if that exponent corresponds to the variable a_1, then F is a separable algebraic extension of $K(a_2, \ldots, a_n)$.
2. Let $R \subseteq S$ be commutative rings. If $\alpha \in S$, prove that the following are equivalent. (i) α is integral over R. (ii) $R[\alpha]$ is a finitely generated R-module. (iii) $\alpha \in T$, where T is an intermediate ring ($R \subseteq T \subseteq S$) that is finitely generated as an R-module. For (iii)⇒(i), let $t_1, t_2, \ldots, t_n$ generate the module T_R and observe that $t_j\alpha = \sum_i t_i r_{i,j}$ for suitable $r_{i,j} \in R$. If $\delta_{i,j} = 1$ when $i = j$ and 0 otherwise, conclude from the determinantal trick that $\det(\alpha\delta_{i,j} - r_{i,j})$ annihilates T. As a consequence, show that the set of elements of S integral over R is a subring of S.
3. Prove that an integral extension of an integral extension is integral.

4. Assume that R is Noetherian and let $I \lhd R$. If $\tilde{I} = \bigcap_{n=1}^{\infty} I^n$, use the Artin-Rees Lemma to show that $\tilde{I} \cdot I = \tilde{I}$. Then use the determinantal trick to conclude that

$$\tilde{I} = \{\, r \in R \mid r(1-i) = 0 \text{ for some } i \in I \,\}$$

This is the Krull Intersection Theorem. It follows that if R is a domain, then $\tilde{I}$ must be 0.

5. Suppose $I \lhd S$ with $\bigcap_{n=1}^{\infty} I^n = 0$. Then the *I-adic topology* on S is defined so that the cosets $s + I^n$ for $n = 1, 2, \ldots$ are a basic neighborhood system for $s \in S$. Show that addition and multiplication are continuous maps from $S \times S$ to S and that the I-adic topology on S is Hausdorff. Furthermore, show that a sequence $s_1, s_2, \ldots$ of elements of S is Cauchy if and only if $\lim_{i \to \infty} s_i = 0$. Note that Lemma 16.4 asserts that if h_1 is close to h_2 in the fS-adic topology, then $\theta(h_1 x)\theta(h_2 x)^{-1}$ is sufficiently close to the identity matrix to guarantee that it is invertible in $\mathrm{M}_n(S[x])$.
6. If R is a commutative Noetherian ring, prove that $\bigcap_{n=1}^{\infty} \mathrm{Rad}(R)^n = 0$. Now let $S = \begin{pmatrix} \mathbb{Z}_{(p)} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}$, where $\mathbb{Q}$ is the field of rationals and $\mathbb{Z}_{(p)}$ is the ring of integers localized at the maximal ideal (p). Show that S is right, but not left, Noetherian and that $e_{1,2} \in \bigcap_{n=1}^{\infty} \mathrm{Rad}(S)^n$. This is Herstein's counterexample to Jacobson's Conjecture.

In the remaining exercises, let $\mathbb{S}^2$ denote the real 2-sphere and let $v\colon \mathbb{S}^2 \to \mathbb{S}^2$ be a continuously differentiable function with $v(x) \perp x$ for all $x \in \mathbb{S}^2$. Extend v to a function on the punctured space $\mathbb{R}^3 \setminus 0$ by defining $v(x) = \|x\| \cdot v(x/\|x\|)$. Furthermore, let $\mathcal{A}$ be the compact region given by $\mathcal{A} = \{\, x \in \mathbb{R}^3 \mid 1/2 \le \|x\| \le 3/2 \,\}$.

7. Prove that v, as extended, is a continuously differentiable function and that it satisfies the Lipschitz condition $\|v(x) - v(y)\| \le c\,\|x - y\|$ for some real constant $c > 0$ and for all $x, y \in \mathcal{A}$.

Now let t be a real parameter with $0 < t < \min\{1/3, 1/c\}$ and define f_t on $\mathbb{R}^3 \setminus 0$ by $f_t(x) = x + tv(x)$. Note that $f_t(rx) = r f_t(x)$ for all positive real numbers r and that f_t maps the sphere $\mathbb{S}^2(r)$ of radius r into $\mathbb{S}^2(r\sqrt{1+t^2})$.

8. For any $u_0 \in \mathbb{S}^2$ and t as before, define $g(x) = u_0 - tv(x)$. Show that $g\colon \mathcal{A} \to \mathcal{A}$ and that g satisfies the Lipschitz condition $\|g(x) - g(y)\| \le ct\,\|x - y\|$. Since $0 < ct < 1$ and $\mathcal{A}$ is compact, prove that $\bigcap_{n=1}^{\infty} g^n(\mathcal{A})$ contains precisely one point z, which is necessarily a fixed point for

g. From $z = g(z) = u_0 - tv(z)$, deduce that $\|z\| = 1/\sqrt{1+t^2}$ and conclude that f_t maps $\mathbb{S}^2(1/\sqrt{1+t^2})$ onto $\mathbb{S}^2(1)$. Indeed, deduce that f_t maps $\mathbb{S}^2(r)$ onto $\mathbb{S}^2(r\sqrt{1+t^2})$ for any positive real number r.

9. Show that f_t maps $\mathcal{A}$ in a one-to-one manner onto

$$\mathcal{B}_t = \left\{ x \in \mathbb{R}^3 \mid (1/2)\sqrt{1+t^2} \leq \|x\| \leq (3/2)\sqrt{1+t^2} \right\}$$

Since the Jacobian $J(f_t)$ is a polynomial in the parameter t, use the formula

$$\mathrm{Vol}(\mathcal{B}_t) = \iiint_{\mathcal{B}_t} dV = \iiint_{\mathcal{A}} J(f_t)\, dV$$

to prove that the volume of $\mathcal{B}_t$ is also a polynomial function of t.

10. Finally, observe that $\mathrm{Vol}(\mathcal{B}_t) = (1+t^2)^{3/2}\,\mathrm{Vol}(\mathcal{A})$ and conclude that the function v does not exist. This is Milnor's proof of the Hairy Ball Theorem. It works equally well in all appropriate higher dimensions.

18. Big Projectives

In the previous chapters we were concerned with finitely generated projective modules over polynomial rings. Now we move on to the infinitely generated ones. As we will see, if R is any commutative Noetherian domain, then big projective R-modules are necessarily free.

DEFINITION Let R be an arbitrary ring and let V be an R-module. If X is any cardinal number, we let V^X denote the direct sum of X copies of V. In particular, R^X is the free R-module on X generators. If ∞ denotes the countably infinite cardinal and if X is infinite, then clearly $(V^X)^\infty \cong V^X \cong V^X \oplus V^X$.

PROPOSITION 18.1 (Eilenberg Trick) *Let X be an infinite cardinal and let P be a projective R-module with X generators. Then $R^X \cong R^X \oplus P$. In particular, if $R^X \mid P$, then $P \cong R^X$ is free.*

PROOF Since P has X generators, we can map R^X onto P and then, since P is projective, the map splits. Thus $R^X \cong P \oplus Q$ and, since X is infinite, we have

$$\begin{aligned} R^X \cong (R^X)^\infty &\cong (P \oplus Q) \oplus (P \oplus Q) \oplus (P \oplus Q) \oplus \cdots \\ &\cong P \oplus (Q \oplus P) \oplus (Q \oplus P) \oplus (Q \oplus P) \oplus \cdots \\ &\cong P \oplus R^X \end{aligned}$$

Finally, suppose $R^X \mid P$ and say $P \cong R^X \oplus M$. Then

$$\begin{aligned} R^X &\cong R^X \oplus P \cong R^X \oplus (R^X \oplus M) \\ &\cong (R^X \oplus R^X) \oplus M \cong R^X \oplus M \cong P \end{aligned}$$

as required. □

In other words, a projective module P is free if it has enough direct summands isomorphic to R. To obtain even one such summand, we study the R-module homomorphisms $\lambda: P \to R$. Indeed, if λ is an epimorphism, then the map splits and $R \mid P$. This leads to:

DEFINITION If V is an R-module, then the *trace ideal* of V, written $T(V)$, is the linear span of all images $\lambda(V)$ for all R-module homomorphisms $\lambda: V \to R$. Since each $\lambda(V)$ is a right ideal of R, it is clear that $T(V)$ is also a right ideal. Furthermore, if $r \in R$, then the composite map $V \xrightarrow{\lambda} R \xrightarrow{\tau} R$ given by $v \mapsto r\lambda(v)$ is an R-homomorphism with image $r\lambda(V)$. Thus $T(V)$ is indeed a two-sided ideal of R.

Unfortunately, $T(V)$ is not precise enough to determine whether V has a summand isomorphic to R. However, we do have:

LEMMA 18.2 *Let V be an R-module. Then $T(V) = R$ if and only if V^n has a summand isomorphic to R for some integer $n \geq 1$.*

PROOF If $R \mid V^n$, then there is an epimorphism $\theta: V^n \to R$ and clearly θ is of the form

$$\theta: (v_1, v_2, \ldots, v_n) \mapsto \lambda_1(v_1) + \lambda_2(v_2) + \cdots + \lambda_n(v_n)$$

where each $\lambda_i: V \to R$ is an R-homomorphism. Since θ is an epimorphism, we then have $1 \in \lambda_1(V) + \lambda_2(V) + \cdots + \lambda_n(V)$ and hence $T(V) = R$.

Conversely, if $T(V) = R$, then $1 \in T(V)$, so there exist $\lambda_1, \lambda_2, \ldots, \lambda_n$ and $v_1, v_2, \ldots, v_n$ such that $1 = \sum_i \lambda_i(v_i)$. In particular, if we define $\theta: V^n \to R$ as before, then θ is clearly an epimorphism. Since R_R is projective, it follows that θ splits and hence that $R \mid V^n$. □

By Theorem 10.5, any projective R-module is a direct sum of countably generated projectives. Thus the following result has more general applicability.

THEOREM 18.3 *Let R be a right Noetherian ring and let P be a countably generated projective R-module. Suppose that the module P/PM is not finitely generated for every maximal two-sided ideal M of R. Then P is a free R-module.*

PROOF Since P is countably generated, it is a homomorphic image of $R^\infty = F$. Furthermore, since the epimorphism splits, we have $F = P \dot{+} Q$. Let $\{ f_1, f_2, \ldots \}$ be a free basis for F and, for each $x \in F$, let $\lambda_i(x) \in R$ be

the coefficient of f_i when x is written in terms of this basis. In other words, x is the finite sum $\sum_i f_i\lambda_i(x)$ and it follows easily that each $\lambda_i: F \to R$ is an R-module epimorphism.

STEP 1 *For any integer $k \geq 0$, we have $\sum_{i\geq k+1} R\lambda_i(P) = R$.*

PROOF Observe that $\sum_{i\geq k+1} R\lambda_i(P)$ is a two-sided ideal of R. Thus if this sum is not equal to R, then it is contained in some maximal two-sided ideal M. In particular, $\lambda_i(P) \subseteq M$ for all $i \geq k+1$ and hence

$$P \subseteq \sum_{i=1}^{k} f_i R + FM$$

Now $F = P \dotplus Q$, so $FM = PM \dotplus QM$ and applying the natural projection $\pi_P: F \to P$ yields

$$P = \sum_{i=1}^{k} \pi_P(f_i) R + PM$$

But this implies that P/PM is a finitely generated R-module and thus we have the required contradiction. □

STEP 2 *For any integer $k \geq 0$, there exist $\ell \geq k+1$ and an R-homomorphism $\mu = \sum_{i=k+1}^{\ell} r_i\lambda_i$ such that $\mu(P) = R$.*

PROOF For each such μ as before, $\mu(P)$ is a right ideal of R. Thus since R is right Noetherian, we can assume that μ has been chosen with $\mu(P)$ maximal. We show that $\mu(P) = R$. First note that $\mu(P)$ is finitely generated, say by $s_1, s_2, \ldots, s_t$, and let $x_i \in P$ with $\mu(x_i) = s_i$. Since each x_i has only finitely many nonzero f_j-components, there exists $\ell' \geq \ell$ with $x_i \in P \cap \left(\sum_{j=1}^{\ell'} f_j R\right)$ for all i.

Let $j > \ell'$ and set $\mu' = \mu + r\lambda_j$ for any $r \in R$. Since $\lambda_j(x_i) = 0$, we have $\mu'(x_i) = \mu(x_i) = s_i$ and thus $\mu'(P) \supseteq \sum_i s_i R = \mu(P)$. The maximality of $\mu(P)$ now implies that $\mu'(P) = \mu(P)$. In particular, if y is any element of P, then $\mu(y)$ and $\mu'(y)$ are both contained in $\mu(P)$, so $r\lambda_j(y) \in \mu(P)$. But $y \in P$, $r \in R$, and $j > \ell'$ are arbitrary, so $\sum_{j>\ell'} R\lambda_j(P) \subseteq \mu(P)$ and Step 1 implies that $\mu(P) = R$. □

STEP 3 *P is free.*

PROOF We define a sequence of epimorphisms $\mu_n: P \to R$ as follows. First, take $k = 0$ in Step 2 to obtain $\mu_1 = \sum_1^{\ell_1} r_i\lambda_i$ and suppose $\mu_1(x_1) = 1$, where $x_1 \in P \cap \sum_1^{m_1} f_i R$ with $m_1 \geq \ell_1$. Next, take $k = m_1$ in

Step 2 to obtain $\mu_2 = \sum_{m_1+1}^{\ell_2} r_i\lambda_i$ and suppose $\mu_2(x_2) = 1$, where $x_2 \in P \cap \sum_1^{m_2} f_iR$ with $m_2 \geq \ell_2$. We continue in this manner, obtaining $\mu_n = \sum_{m_{n-1}}^{\ell_n} r_i\lambda_i$ and a corresponding $x_n \in P \cap \sum_1^{m_n} f_iR$. By the choice of parameters, it follows that $\mu_n(x_n) = 1$ and $\mu_k(x_n) = 0$ for all $k > n$.

Note that any $y \in P$ has only finitely many nonzero components and hence $\mu_n(y)$ can be nonzero for at most finitely many n. In particular, if F' is a free R-module with countable basis $\{ f_1', f_2', \dots \}$, then we can define $\theta: P \to F'$ by $\theta(y) = \sum_{n=1}^{\infty} f_n'\mu_n(y)$. Since $\mu_n(x_n) = 1$ and $\mu_k(x_n) = 0$ for all $k > n$, we then have

$$\theta(x_n) = f_n' + \sum_{j<n} f_j's_{n,j}$$

for suitable $s_{n,j} \in R$ and it follows by induction on n that each f_n' is in the image of θ. Thus θ is an epimorphism, so it splits and hence $F' \cong R^\infty$ is a direct summand of P. Proposition 18.1 now implies that $P \cong R^\infty$ is a free module. □

The main goal of this chapter is to sharpen the preceding result when R is a commutative integral domain. Thus we will assume, until Theorem 18.7 is proved, that R is such a ring.

DEFINITION Recall that an R-module V is *torsion free* if, for all $0 \neq v \in V$ and $0 \neq r \in R$, we have $vr \neq 0$. Thus R_R is torsion free and this property is inherited by submodules and direct sums. In particular, each free R-module and each projective R-module is torsion free.

Now let V be a torsion free R-module and let T be a multiplicatively closed subset of R. Then, just as we formed the ring of fractions RT^{-1}, we can also form the module VT^{-1}. Here VT^{-1} is the set of all formal fractions (or ordered pairs) vt^{-1} with $v \in V$, $t \in T$ and with equality given by $v_1t_1^{-1} = v_2t_2^{-1}$ if and only if $v_1t_2 = v_2t_1$. This equality of fractions is easily seen to be an equivalence relation, since V is torsion free.

Finally, VT^{-1} is an RT^{-1}-module with addition and multiplication defined by

$$v_1t_1^{-1} + v_2t_2^{-1} = (v_1t_2 + v_2t_1)(t_1t_2)^{-1}$$
$$(vt^{-1})(rs^{-1}) = (vr)(ts)^{-1}$$

for all appropriate parameters. It is obvious that the map $v \mapsto v1^{-1}$ is an R-module embedding of V into VT^{-1}. Furthermore, we have:

LEMMA 18.4 *If V is a torsion free R-module and if T is a multiplicatively closed subset of R, then $VT^{-1} \cong V \otimes_R RT^{-1}$.*

PROOF This is routine. First we must verify that the map $\alpha: VT^{-1} \to V \otimes RT^{-1}$ given by $vt^{-1} \mapsto v \otimes t^{-1}$ respects equality and addition. Then we verify that the map $\bar{\beta}: V \times RT^{-1} \to VT^{-1}$ given by $(v, rt^{-1}) \mapsto (vr)t^{-1}$ is balanced and therefore gives rise to an additive homomorphism $\beta: V \otimes RT^{-1} \to VT^{-1}$. Since α and β are clearly inverses of each other, they are both bijections. Finally, it is easy to check that α and β are both RT^{-1}-module homomorphisms. □

In view of the preceding, we can apply basic properties of induced modules to this situation. In particular, if X is any cardinal number, then $(V^X)T^{-1} \cong (VT^{-1})^X$ and if P is a projective R-module, then PT^{-1} is a projective RT^{-1}-module. We now require two lemmas. The first concerns localization at a maximal ideal.

LEMMA 18.5 *Let V be a torsion free R-module, let M be a maximal ideal of R, and set $T = R \setminus M$. Then $(VT^{-1})(MT^{-1}) = (VM)T^{-1}$ and*

$$VT^{-1}/(VM)T^{-1} \cong V/VM$$

as R-modules.

PROOF Since M is maximal, R/M is a field. In particular, if $t \in T$, then there exists $s \in T$ with $1 - ts \in M$. Notice that VM is an R-submodule of V, MT^{-1} is the maximal ideal of RT^{-1}, and $(VT^{-1})(MT^{-1}) = (VM)T^{-1}$.

We first show that $V + (VM)T^{-1} = VT^{-1}$. To this end, let $vt^{-1} \in VT^{-1}$ and choose s as before with $1 - ts \in M$. Then $t^{-1} - s \in MT^{-1}$, so $vt^{-1} - vs \in (VM)T^{-1}$ and therefore $vt^{-1} \in V + (VM)T^{-1}$.

Next, we observe that $V \cap (VM)T^{-1} = VM$ and one inclusion is obvious. For the converse, let $v \in V \cap (VM)T^{-1}$ and say $v = wt^{-1}$ with $w \in VM$. Since $v(1 - ts) \in VM$ and $vts = ws \in VM$, we conclude that $v \in VM$.

As a consequence, we have

$$\begin{aligned} VT^{-1}/(VM)T^{-1} &= \big(V + (VM)T^{-1}\big)/(VM)T^{-1} \\ &\cong V/\big(V \cap (VM)T^{-1}\big) = V/VM \end{aligned}$$

the required R-module isomorphism. □

This result is decidedly false if we localize at a nonmaximal prime. Note that if V is a finitely generated R-module, then VT^{-1} is a finitely generated RT^{-1}-module. We prove a partial converse.

LEMMA 18.6 *Let P be a projective R-module and let T be a multiplicatively closed subset of R. If PT^{-1} is a finitely generated RT^{-1}-module, then P is a finitely generated R-module.*

PROOF Suppose $p_1t_1^{-1}, p_2t_2^{-1}, \ldots, p_nt_n^{-1}$ are the finitely many generators for PT^{-1}. If p is an arbitrary element of P, then $p1^{-1} \in \sum_i (p_it_i^{-1})RT^{-1}$ and, by clearing denominators, it follows easily that $pr \in \sum_i p_iR$ for some $0 \neq r \in R$.

Since P is projective, $P \mid F$, where F is a free R-module with basis $\{f_i\}$. Furthermore, by relabeling this basis, we can assume that $p_1, p_2, \ldots, p_n \in F' = \sum_1^m f_iR$. Now, by the preceding, if $p \in P$, then there exists $0 \neq r \in R$ with $pr \in \sum_i p_iR \subseteq F'$. But $F = F' \dotplus F''$ and F'' is a torsion free R-module. Thus we conclude that $p \in F'$ and hence that $P \subseteq F'$. Finally, since $P \mid F$, the Modular Law implies that $P \mid F'$. Thus P is a homomorphic image of the finitely generated R-module F' and the lemma is proved. □

We can now obtain our main result on big projectives.

THEOREM 18.7 (Bass' Theorem) *Let R be a Noetherian commutative integral domain and let P be a projective R-module that is not finitely generated. Then P is free.*

PROOF Suppose first that P is countably generated but, of course, not finitely generated. Let M be a maximal ideal of R and set $T = R \setminus M$. Then $PT^{-1} \cong P \otimes RT^{-1}$ is a projective module for the local ring $RT^{-1} = R_M$ and hence, by Kaplansky's Theorem, PT^{-1} is free. Furthermore, since P is not finitely generated, the previous lemma implies that PT^{-1} is not a finitely generated RT^{-1}-module. Thus $PT^{-1} \cong (RT^{-1})^X$ for an infinite cardinal X. Two applications of Lemma 18.5 now yield

$$\begin{aligned} P/PM &\cong PT^{-1}/(PT^{-1})(MT^{-1}) \\ &\cong (RT^{-1})^X/(RT^{-1})^X(MT^{-1}) \\ &\cong \left[RT^{-1}/(RT^{-1})(MT^{-1})\right]^X \cong (R/M)^X \end{aligned}$$

where these are all R-isomorphisms. Thus, since X is an infinite cardinal, $P/PM \cong (R/M)^X$ is not finitely generated and Theorem 18.3 implies that P is indeed free.

Now suppose that P is not even countably generated. By Theorem 10.5, we know that P is a direct sum of nonzero countably generated projective R-modules and certainly this sum must be infinite. Thus we can suitably group these terms and write $P = \cdot\sum_i \left(\cdot \sum_{j=1}^{\infty} P_{i,j}\right)$. But, for each i, $P_i = \cdot \sum_{j=1}^{\infty} P_{i,j}$ is a countably generated projective R-module, which is clearly not finitely generated. Thus each P_i is free, by the work of the preceding paragraph, and hence $P = \cdot \sum_i P_i$ is free. □

In particular, in view of the preceding and the affirmative solution of the Serre Conjecture, we have:

COROLLARY 18.8 *If K is a field, then all projective modules for the polynomial ring $K[x_1, x_2, \ldots, x_m]$ are free.*

We close with a preliminary result needed for the next chapter.

DEFINITION Let R be an arbitrary noncommutative ring. Then R is said to be *filtered* if $R = \bigcup_{n=0}^{\infty} \mathcal{R}_n$ is the ascending union of the additive subgroups $\mathcal{R}_n$ and if $\mathcal{R}_i\mathcal{R}_j \subseteq \mathcal{R}_{i+j}$ for all i, j. In addition, we insist that $1 \in \mathcal{R}_0$, so that $\mathcal{R}_0$ is a subring of R.

Notice, for example, that the polynomial ring $R = K[x_1, x_2, \ldots, x_m]$ is filtered by defining $\mathcal{R}_n$ to be the set of all polynomials of total degree at most n. Furthermore, if $R = \cdot \sum_{i=0}^{\infty} R_i$ is a graded ring, then R is filtered by defining $\mathcal{R}_n = \cdot \sum_{i=0}^{n} R_i$. As we see in the next paragraph, there is a partial converse to this.

Suppose $R = \bigcup_{n=0}^{\infty} \mathcal{R}_n$ is an arbitrary filtered ring; for each $i \geq 0$, define $\bar{R}_i = \mathcal{R}_i/\mathcal{R}_{i-1}$, where we set $\mathcal{R}_{-1} = 0$. Then the multiplication map $\mathcal{R}_i \times \mathcal{R}_j \to \mathcal{R}_{i+j}$ gives rise to a map $\bar{R}_i \times \bar{R}_j \to \bar{R}_{i+j}$, which we again think of as multiplication. Specifically, if $\bar{x} = x + \mathcal{R}_{i-1} \in \bar{R}_i$ and $\bar{y} = y + \mathcal{R}_{j-1} \in \bar{R}_j$, then $\bar{x}\bar{y} \in \bar{R}_{i+j}$ is defined unambiguously by $\bar{x}\bar{y} = xy + \mathcal{R}_{i+j-1}$. Furthermore, it is easy to verify that this family of multiplication maps is associative. By this we mean that if $\bar{x}$ and $\bar{y}$ are as before and if $\bar{z} \in \bar{R}_k$, then $\bar{x}(\bar{y}\bar{z}) = (\bar{x}\bar{y})\bar{z} \in \bar{R}_{i+j+k}$. We now define $\bar{R} = \oplus \sum_{n=0}^{\infty} \bar{R}_n$ and, with the obvious addition and multiplication, $\bar{R}$ becomes a graded ring. We call $\bar{R} = \operatorname{gr} R$ the *associated graded ring* of R. It is determined by both R and the filtration on R.

Recall that a graded ring is said to be *graded right Noetherian* (or *graded right Artinian*) if every ascending (or descending) chain of graded right ideals eventually stabilizes. Obviously the ordinary Noetherian (or Artinian) condition implies its graded counterpart.

LEMMA 18.9 *Let $R = \bigcup_{n=0}^{\infty} \mathcal{R}_n$ be a filtered ring. If $\operatorname{gr} R$ is graded right*

Noetherian, then R is right Noetherian. Similarly, if gr R *is graded right Artinian, then R is right Artinian.*

PROOF Let I be a right ideal of R and, for each $n \geq 0$, let $\bar{I}_n$ be the image of $I_n = I \cap \mathcal{R}_n$ in $\bar{R}_n$. Then it follows easily that $\bar{I}_i \bar{R}_j \subseteq \bar{I}_{i+j}$ and hence that $\text{gr}\, I = \oplus \sum_{n=0}^{\infty} \bar{I}_n$ is a graded right ideal of gr R.

Now let J be a second right ideal of R and suppose that $I \subseteq J$. Then $I_n \subseteq J_n$ for all n and hence $\text{gr}\, I \subseteq \text{gr}\, J$. Furthermore, $\text{gr}\, I = \text{gr}\, J$ implies that $I = J$. Indeed, suppose we already know that $I_{n-1} = J_{n-1}$. Then we have

$$I_n \cap \mathcal{R}_{n-1} = I_{n-1} = J_{n-1} = J_n \cap \mathcal{R}_{n-1}$$

and also $I_n + \mathcal{R}_{n-1} = J_n + \mathcal{R}_{n-1}$, since $\bar{I}_n = \bar{J}_n$. But $I_n \subseteq J_n$, so the Modular Law implies that $I_n = J_n$ and it follows, by induction on n, that $I = J$.

In particular, any strictly increasing or decreasing chain of right ideals of R gives rise to a strictly increasing or decreasing chain of graded right ideals of gr R. With this, the result follows. □

EXERCISES

Let R be an arbitrary noncommutative ring. An R-module V is said to be a *generator* if, for each R-module W, there exists a cardinal number X and an epimorphism $V^X \to W$. A *progenerator* for R is a finitely generated projective R-module which is a generator. Recall that $T(V)$ is the trace ideal of V.

1. Prove that V is a generator if and only if $T(V) = R$.
2. Suppose $P \cong \oplus \sum_{i=1}^{\infty} P_i$ is an infinite direct sum of countably generated projective R-modules P_i with $T(P_i) = R$. If R is right Noetherian, show that there exists an epimorphism $\mu: P \to R$. Conclude from the Eilenberg Trick that P is free.
3. Suppose R is a right Noetherian ring and P is a finitely generated projective R-module. Prove that P is a progenerator if and only if $P^{\infty} \cong R^{\infty}$.
4. If I is a right ideal of R, show that $T(I_R) \supseteq RI$. Furthermore, if $I = eR$ for some idempotent e, prove that $T(eR) = ReR$.
5. Find an example of a nonzero finitely generated projective R-module that is not a progenerator. If R is a simple ring and I is a nonzero right ideal of R, prove that I_R is a generator.
6. Show that all nonzero R-modules are generators if and only if R is a simple Artinian ring. If R is assumed to be right Artinian, show that

all nonzero finitely generated projective R-modules are progenerators if and only if $R/\mathrm{Rad}(R)$ is simple.

7. Let P be a projective R-module and say $P \dot{+} Q = F = \cdot \sum_i f_i R$, where, of course, F is free. If $x \in P$, write $x = \sum_i f_i \lambda_i(x)$ and apply the projection map π_P to conclude that $P = PT(P)$. In particular, if $T(P) \neq R$, there exists a maximal ideal M of R with $P/PM = 0$.
8. If R is a Dedekind domain and $0 \neq A \triangleleft R$, show that $T(A_R) = A^{-1}A = R$. Conclude that all nonzero finitely generated projective R-modules are progenerators.
9. Now assume that R is a commutative domain and let V be a torsion free R-module. If T is a multiplicatively closed subset of R, verify all the steps in the construction of the module VT^{-1}. Furthermore, if $S \supseteq T$ is also a multiplicatively closed subset of R, prove that $(VT^{-1})S^{-1} \cong VS^{-1}$ as RS^{-1}-modules.
10. Let P be a prime ideal of the commutative integral domain R. If $R + PR_P = R_P$, prove that P is a maximal ideal of R. In particular, conclude that Lemma 18.5 fails for nonmaximal ideals.

19. Generic Flatness

In view of Corollary 18.8, we now completely understand the projective modules for the polynomial ring $R = K[x_1, x_2, \ldots, x_m]$. Thus it is time to move on to other aspects of the module theory of this ring. Specifically, we now consider the simple R-modules and the nature of the Jacobson radical of certain homomorphic images of R. Both of these topics actually fall under the province of the Hilbert Nullstellensatz and our goal is to prove this result in a mildly noncommutative setting.

DEFINITION If $R \supseteq S$ are rings, then R is said to be an *almost centralizing extension* of S provided that R is generated as a ring by S and the finitely many elements $x_1, x_2, \ldots, x_m$. Furthermore, we insist that each x_i commutes with S and that

$$x_i x_j - x_j x_i \in S + \sum_{k=1}^{m} S x_k$$

for all i, j. Notice that if S is commutative, then S must be central in R. Furthermore, if $S = K$ is a field, then R is called an *almost commutative K-algebra*. It is clear that if R is such a K-algebra, then so are all its homomorphic images.

Our goal in this and the next chapter is to prove an appropriate Nullstellensatz (Zero Set Theorem) for these almost commutative algebras. Since any polynomial ring is certainly of this form, we will thereby obtain the Hilbert Nullstellensatz as a corollary. Furthermore, there are certainly interesting noncommutative, almost commutative algebras. For example, we consider the Weyl algebras at the end of the next chapter.

Again, let R be an almost centralizing extension of S with generators $x_1, x_2, \ldots, x_m$. Set $\mathcal{R}_0 = S$ and $\mathcal{R}_n = \left(S + \sum_{k=1}^{m} Sx_k\right)^n$ for $n \geq 1$. Then it is clear that $R = \bigcup_{n=0}^{\infty} \mathcal{R}_n$ is a filtration of R and we consider the associated grade ring $\operatorname{gr} R = \oplus \sum_{n=0}^{\infty} \bar{R}_n$. Clearly $\bar{R}_0 = S$ and, since each $x_i \in \mathcal{R}_1$, we can set $\bar{x}_i = x_i + \mathcal{R}_0 \in \bar{R}_1$. Furthermore, since $x_i x_j - x_j x_i \in \mathcal{R}_1$, it follows that the $\bar{x}_i$ all commute in $\operatorname{gr} R$ and hence we see that $\operatorname{gr} R$ is a homomorphic image of the ordinary polynomial ring $S[\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_m]$. In particular, we conclude easily that every element $r \in R$ can be written as a finite sum $r = \sum_{\mathbf{a}} s_{\mathbf{a}} \mathbf{x}^{\mathbf{a}}$, where $\mathbf{a} = (a_1, a_2, \ldots, a_m)$ is an m-tuple of nonnegative integers, $\mathbf{x}^{\mathbf{a}} = x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}$ and $s_{\mathbf{a}} \in S$. Of course, this expression is not unique in general. Furthermore, if $\mathbf{b} = (b_1, b_2, \ldots, b_m)$, then $\mathbf{x}^{\mathbf{a}} \mathbf{x}^{\mathbf{b}} \equiv \mathbf{x}^{\mathbf{a}+\mathbf{b}} \bmod \mathcal{R}_{a+b-1}$ where $a = \deg \mathbf{a} = a_1 + \cdots + a_m$, $b = \deg \mathbf{b} = b_1 + \cdots + b_m$, and $\mathbf{a} + \mathbf{b} = (a_1 + b_1, a_2 + b_2, \ldots, a_m + b_m)$.

Notice that if S is Noetherian, then, by the Hilbert Basis Theorem, so is the polynomial ring $S[\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_m]$. Thus, since any homomorphic image of a Noetherian ring is Noetherian, Lemma 18.9 yields:

LEMMA 19.1 *Let R be an almost centralizing extension of S. If S is right Noetherian, then so is R.*

Our approach to the Nullstellensatz is based on the idea of generic flatness.

DEFINITION Let S be a commutative integral domain and let V be an S-module. We say that V is *α-free* for some $0 \neq \alpha \in S$ if V has a free S-submodule $\tilde{V}$ such that every element of $V/\tilde{V}$ is annihilated by some power of α. We say that V satisfies *generic flatness* if V is α-free for some such α. Recall that if α is a nonzero element of S, then S_α is the localization of S at the multiplicatively closed set $\{1, \alpha, \alpha^2, \ldots\}$. Part (i) of the following lemma partially explains the term *generic flatness*. Namely, it asserts that the induced module $V \otimes S_\alpha$ is free and hence flat. Furthermore, S_α is a flat extension of S.

LEMMA 19.2 *Let S be a commutative integral domain and let V be an S-module.*

i. If V is α-free, then $V \otimes_S S_\alpha$ is a free S_α-module.

ii. Let S be a principal ideal domain. If V is α-free, then so are all its submodules.

iii. If V is α-free, then it is $\alpha\beta$-free for any nonzero $\beta \in S$. In particular, if $V_1, V_2, \ldots, V_n$ are given and if V_i is α_i-free, then all V_i are α-free, where $\alpha = \prod_i \alpha_i$.

iv. Suppose $\mathcal{I}$ is a well-ordered set and that $\{V_i \mid i \in \mathcal{I}\}$ is an increasing family of submodules of V whose union is all of V. For each $i \in \mathcal{I}$, write $V_i^- = \bigcup_{j<i} V_j$ and suppose that V_i/V_i^- is α-free. Then V is α-free.

PROOF (i) First observe that $S_\alpha = \bigcup_{n=0}^{\infty} S\alpha^{-n}$ and that each $S\alpha^{-n}$ is a free left S-module. Thus, by Lemma 9.9(i)(iii), S_α is a flat left S-module. Now let $\tilde{V}$ be the free submodule of V given by the α-free definition and consider the exact sequence $0 \to \tilde{V} \to V \to V/\tilde{V} \to 0$. Then, since S_α is flat, we know that

$$0 \to \tilde{V} \otimes S_\alpha \to V \otimes S_\alpha \to (V/\tilde{V}) \otimes S_\alpha \to 0$$

is exact. But $\tilde{V} \otimes S_\alpha$ is free, by Lemma 9.11(i), and $(V/\tilde{V}) \otimes S_\alpha = 0$, since each element of the latter module is annihilated by some power of the unit $\alpha \in S_\alpha$. Thus $V \otimes S_\alpha \cong \tilde{V} \otimes S_\alpha$ is free.

(ii) If W is a submodule of V, then $\tilde{W} = \tilde{V} \cap W$ is free, by Corollary 6.4, since S is a principal ideal domain. But $W/\tilde{W}$ is isomorphic to a submodule of $V/\tilde{V}$, so this fact is proved. Part (iii) is, of course, obvious.

(iv) Since V_i/V_i^- is α-free, let $\mathcal{B}_i = \{ v_{i,j} \}$ be a set of elements of V_i which, modulo V_i^-, form a free basis for the appropriate free submodule of V/V_i^-. Let $\mathcal{B} = \bigcup_i \mathcal{B}_i$ and observe that the elements of $\mathcal{B}$ are S-independent. Indeed, if $\sum_{i,j} v_{i,j}s_{i,j} = 0$ is a finite dependence, let i_0 be the largest first subscript that occurs. Then, reading this equation modulo $V_{i_0}^-$, it follows that all $s_{i_0,j}$ terms are zero. We can now let $\tilde{V}$ be the free S-submodule of V generated by $\mathcal{B}$.

It remains to show that each element of $V/\tilde{V}$ is annihilated by a power of α and for this we proceed by induction on $i \in \mathcal{I}$. If $v \in V_i$, then, by definition of $\mathcal{B}_i$, we see that $v\alpha^n \equiv \sum_j v_{i,j}s_{i,j} \bmod V_i^-$ for suitable $s_{i,j} \in S$. Hence $w = v\alpha^n - \sum_j v_{i,j}s_{i,j} \in V_i^-$ and thus $w \in V_k$ for some $k < i$. By induction, $w\alpha^m \in \tilde{V}$ and hence $v\alpha^{n+m} \in \tilde{V}$, as required. □

If R is an almost centralizing extension of the ring S with generators $x_1, x_2, \ldots, x_m$, then the elements of R look like polynomials in these variables. Thus it is appropriate to study the exponents $\mathbf{a} = (a_1, a_2, \ldots, a_m) \in \mathbb{N}^m$, where $\mathbb{N}$ denotes the set of nonnegative integers. Now there are at least three different orderings we can put on these exponents. First, $\mathbb{N}^m$ can be ordered *lexicographically* by defining

$$(a_1, a_2, \ldots, a_m) <_\ell (b_1, b_2, \ldots, b_m)$$

if and only if $a_1 = b_1$, $a_2 = b_2$, ..., $a_{i-1} = b_{i-1}$ and $a_i < b_i$ for some subscript $1 \le i \le m$. Next, we write $\mathbf{a} \le \mathbf{b}$ if either $\deg \mathbf{a} < \deg \mathbf{b}$ or

$\deg \mathbf{a} = \deg \mathbf{b}$ and $\mathbf{a} \leq_\ell \mathbf{b}$. Either of these is a total order and, indeed, a well order. Finally, we have the *product ordering*, where

$$(a_1, a_2, \ldots, a_m) \leq_\pi (b_1, b_2, \ldots, b_m)$$

if and only if $a_i \leq b_i$ for all i. Note that the latter is only a partial order, but it has the following striking property.

LEMMA 19.3 *Any sequence* $\{x_1, x_2, \ldots\}$ *of elements in* $\mathbb{N}^m$ *contains a subsequence* $\{y_1, y_2, \ldots\}$ *with* $y_i \leq_\pi y_{i+1}$ *for all* i. *In particular, if* M *is a nonempty subset of* $\mathbb{N}^m$, *then* M *has only finitely many minimal elements under* $\leq_\pi$ *and each element of* M *contains at least one of these.*

PROOF The natural ordering on $\mathbb{N}$ has the property that every sequence has a nondecreasing subsequence. Therefore, the same holds for $\mathbb{N}^m$, by projecting the given sequence into each of the m coordinates in turn and, at each step, taking an appropriate subsequence. It follows that $\mathbb{N}^m$ cannot contain (i) infinitely many incomparable elements under $\leq_\pi$ or (ii) a strictly decreasing sequence. Thus the facts on $M \subseteq \mathbb{N}^m$ follow immediately. □

We can now prove:

THEOREM 19.4 (Generic Flatness Theorem) *Let* R *be an almost centralizing extension of the Noetherian commutative integral domain* S. *If* V *is a finitely generated* R*-module, then* V_S *satisfies generic flatness.*

PROOF Since V is finitely generated, it has R-submodules

$$0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V$$

such that each V_i/V_{i-1} is cyclic. Furthermore, by Lemma 19.2(iii)(iv), it suffices to show that each V_i/V_{i-1} satisfies generic flatness. Thus we may assume that V is cyclic and hence that $V = R/I$ for some right ideal I of the ring R.

Let R be generated over S by $x_1, x_2, \ldots, x_m$ and, for each exponent $\mathbf{a} = (a_1, a_2, \ldots, a_m)$, let $S(\mathbf{a})$ be the set of all finite sums $\sum_{\mathbf{b} \leq \mathbf{a}} s_\mathbf{b} \mathbf{x}^\mathbf{b}$ with $s_\mathbf{b} \in S$. In this way we obtain an increasing collection of right S-submodules of R whose union is all of R. Furthermore, let

$$L(\mathbf{a}) = \left\{ s \in S \mid \sum_{\mathbf{b} \leq \mathbf{a}} s_\mathbf{b} \mathbf{x}^\mathbf{b} \in I \text{ and } s = s_\mathbf{a} \right\}$$

In other words, $L(\mathbf{a})$ is the set of all "leading coefficients" of elements of $I \cap S(\mathbf{a})$. It is clear that $L(\mathbf{a})$ is an ideal of the central subring S.

STEP 1 *There are at most finitely many distinct* $L(\mathbf{a})$.

PROOF If $\deg \mathbf{b} < \deg \mathbf{a}$, then $\mathbf{b} < \mathbf{a}$, and if $\mathbf{b} \leq \mathbf{a}$, then $\mathbf{b} + \mathbf{c} \leq \mathbf{a} + \mathbf{c}$. It therefore follows that

$$\Big(\sum_{\mathbf{b} \leq \mathbf{a}} s_{\mathbf{b}} \mathbf{x}^{\mathbf{b}}\Big)\mathbf{x}^{\mathbf{c}} = \sum_{\mathbf{d} \leq \mathbf{a}+\mathbf{c}} s'_{\mathbf{d}} \mathbf{x}^{\mathbf{d}}$$

for suitable $s'_{\mathbf{d}} \in S$ and that the leading coefficients satisfy $s'_{\mathbf{a}+\mathbf{c}} = s_{\mathbf{a}}$. Thus, since I is a right ideal of R, we conclude that $L(\mathbf{a}) \subseteq L(\mathbf{a}+\mathbf{c})$ for all $\mathbf{a}$ and $\mathbf{c}$. In particular, by definition of the product ordering, $L(\mathbf{a}) \subseteq L(\mathbf{a}')$ for all $\mathbf{a} \leq_\pi \mathbf{a}'$.

Suppose, by way of contradiction, that $L(\mathbf{a_1}), L(\mathbf{a_2}), \ldots$ are infinitely many distinct ideals. By the previous lemma, the sequence $\{\mathbf{a_1}, \mathbf{a_2}, \ldots\}$ contains a nondecreasing subsequence $\{\mathbf{b_1}, \mathbf{b_2}, \ldots\}$ under the product ordering. But then $L(\mathbf{b_1}) \subset L(\mathbf{b_2}) \subset \cdots$ is a strictly increasing chain of ideals of S and this contradicts the fact that S is Noetherian. □

For each $\mathbf{a} \in \mathbb{N}^m$, define $V(\mathbf{a}) = \big(I + S(\mathbf{a})\big)/I$. In this way we obtain an increasing family of S-submodules of V whose union is all of V. Furthermore, we have

$$V(\mathbf{a})^- = \bigcup_{\mathbf{b}<\mathbf{a}} V(\mathbf{b}) = \big(I + S(\mathbf{a})^-\big)/I$$

where $S(\mathbf{a})^- = \bigcup_{\mathbf{b}<\mathbf{a}} S(\mathbf{b})$.

STEP 2 $V(\mathbf{a})/V(\mathbf{a})^- \cong S/L(\mathbf{a})$ *as* S*-modules.*

PROOF To start with, the map $\Lambda_{\mathbf{a}}\colon S \to \big(I+S(\mathbf{a})\big)/\big(I+S(\mathbf{a})^-\big)$ given by $s \mapsto s\mathbf{x}^{\mathbf{a}} + \big(I+S(\mathbf{a})^-\big)$ is an S-module epimorphism, since $S(\mathbf{a})^- + S\mathbf{x}^{\mathbf{a}} = S(\mathbf{a})$. Furthermore, $s \in \operatorname{Ker}(\Lambda_{\mathbf{a}})$ if and only if $s\mathbf{x}^{\mathbf{a}} \in I + S(\mathbf{a})^-$ and hence if and only if there exists $\sum_{\mathbf{b}<\mathbf{a}} s_{\mathbf{b}}\mathbf{x}^{\mathbf{b}} \in S(\mathbf{a})^-$ with $s\mathbf{x}^{\mathbf{a}} + \sum_{\mathbf{b}<\mathbf{a}} s_{\mathbf{b}}\mathbf{x}^{\mathbf{b}} \in I$. In other words, $\operatorname{Ker}(\Lambda_{\mathbf{a}}) = L(\mathbf{a})$ and therefore

$$\frac{S}{L(\mathbf{a})} \cong \frac{I + S(\mathbf{a})}{I + S(\mathbf{a})^-} \cong \frac{\big(I + S(\mathbf{a})\big)/I}{\big(I + S(\mathbf{a})^-\big)/I} \cong \frac{V(\mathbf{a})}{V(\mathbf{a})^-}$$

as required. □

STEP 3 V *has generic flatness.*

PROOF By Step 1, there are only finitely many distinct ideals $L(\mathbf{a})$. Thus, since S is an integral domain, there exists a nonzero element α contained in all the nonzero ideals of this form.

Now if $L(\mathbf{a}) = 0$, then $S/L(\mathbf{a}) \cong S$ is a free S-module and hence certainly α-free. On the other hand, if $L(\mathbf{a}) \neq 0$, then $\alpha \in L(\mathbf{a})$. Thus α annihilates the module $S/L(\mathbf{a})$ and $S/L(\mathbf{a})$ is again α-free. It therefore follows from Step 2 that $V(\mathbf{a})/V(\mathbf{a})^-$ is α-free for all such $\mathbf{a}$ and Lemma 19.2(iv) yields the result. □

Suppose R is an almost centralizing extension of S and that S is a commutative domain. If V is an irreducible R-module, then we are interested in the structure of the restricted module V_S. Suppose, for example, that V_S is isomorphic to a finite direct sum of copies of $F = SS^{-1}$, say $V = \cdot \sum_1^n v_i F$. If R is generated over S by $x_1, x_2, \ldots, x_m$, then the action of each x_i on V can be described by an $n \times n$ matrix over F. It follows that if α is a common denominator for the finitely many matrix entries for all these generators, then $\cdot \sum_1^n v_i S_\alpha$ is a nonzero R-submodule of V. But V is irreducible, so $\cdot \sum_1^n v_i S_\alpha = \cdot \sum_1^n v_i F$ and hence $S_\alpha = F$.

We say that a commutative domain S is a *G-domain* if there exists $0 \neq \alpha \in S$ with $S_\alpha = SS^{-1}$. Notice, for example, that if S is a unique factorization domain with infinitely many distinct primes, then S is not a G-domain. This follows because the elements of S_α have denominators that involve only the finitely many prime factors of α. Thus the ring of integers $\mathbb{Z}$ is not a G-domain and neither is the polynomial ring $K[x]$ over the field K. Indeed, $K[x]$ is a unique factorization domain and the algebraic closure of K is infinite. Thus there are infinitely many distinct monic minimal polynomials and each of these is irreducible.

Now suppose that R is a K-algebra, by which we mean that R contains K as a central subfield. If V is any right R-module and if $k \in K$, then the map $\rho(k)\colon v \mapsto vk$ is obviously an R-endomorphism of V. Furthermore, since K is a field, we see that $\rho\colon K \to \mathrm{End}_R(V)$ is a ring embedding and, in this way, we can think of K as being contained in $\mathrm{End}_R(V)$. But $\mathrm{End}_R(V)$ commutes with right multiplication by any $r \in R$ and, in particular, it centralizes $\rho(K)$. Thus $\mathrm{End}_R(V)$ becomes a K-algebra in a natural way. It is with this understanding that we state:

THEOREM 19.5 *Let R be an almost commutative K-algebra. If V is an irreducible R-module, then $D = \mathrm{End}_R(V)$ is a division ring that is finite dimensional over its central subfield K.*

PROOF By Schur's Lemma, $\mathrm{End}_R(V) = D$ is a division ring and, by our previous comments, K is a central subfield of D. The proof proceeds in

two steps.

STEP 1 *D is algebraic over K.*

PROOF Suppose, by way of contradiction, that some $d \in D$ is not algebraic over K. Then $K[d] \subseteq D$ is isomorphic to a polynomial ring over K and its field of fractions $F = K(d)$ is contained in the division ring D.

Form the polynomial ring $R' = R[x]$ and observe that R' is an almost centralizing extension of $S' = K[x]$ using the same set of generators. Since $d \in \mathrm{End}_R(V)$ commutes with the action of R, we can view V as an R'-module by letting x act like d. Then V is a cyclic R'-module and, since S' is a commutative Noetherian domain, the Generic Flatness Theorem implies that $V_{S'}$ is α-free for some $0 \neq \alpha \in S'$.

Choose any $0 \neq v \in V$ and observe that Fv is an S'-submodule of V. Thus, since S' is a principal ideal domain, Lemma 19.2(ii) implies that Fv is also α-free. But $F = K(d)$ and x acts on $Fv \cong F$ like multiplication by d. Thus, by changing to the variable x, it is clear that $K(x)$ is in fact an α-free $K[x]$-module.

Finally, suppose W is the free $K[x]$-submodule of $K(x)$ corresponding to the definition of α-free. Then W must have rank 1 and hence $W = \beta K[x]$ for some $0 \neq \beta \in K(x)$. Furthermore, since every element of $K(x)/W$ is annihilated by a power of α, it follows that $K(x) = WK[x]_\alpha = \beta K[x]_\alpha$. But, multiplying by β^{-1} yields $K(x) = K[x]_\alpha$ and this is a contradiction because $K[x]$ is not a G-domain. □

STEP 2 *Every maximal subfield of D is finite dimensional over K and hence* $\dim_K D < \infty$.

PROOF Let F be a maximal subfield of D, so that $F \supseteq K$. By the preceding, we know that F is an algebraic extension of K. Since $K \subseteq \mathrm{End}_R(V)$, it follows that V is a (K, R)-bimodule, and certainly F is an (F, K)-bimodule. Thus, by Lemma 9.3, $W = F \otimes_K V$ is an (F, R)-bimodule. In particular, there is a homomorphism $': R \to \mathrm{End}(W)$, with $\mathrm{End}(W)$ acting on the right. Notice that $R' \subseteq \mathrm{End}(W)$, being a homomorphic image of R, is also an almost commutative K-algebra. Next, since F is commutative and W is a left F-module, there is a homomorphism $': F \to \mathrm{End}(W)$ defined by $wf' = fw$ for all $w \in W$ and $f \in F$. Clearly $F \cong F' \subseteq \mathrm{End}(W)$ and, since W is an (F, R)-bimodule, it follows that F' and R' commute elementwise. Furthermore, since W is a tensor product over K, it follows from the nature of the embedding of K into D that both restriction maps $': K \to K' \subseteq \mathrm{End}(W)$ are identical.

We conclude from all this that $F'R'$, the subring of $\mathrm{End}(W)$ generated by F' and R', is an almost commutative F'-algebra whose generators

over F' are precisely the generators of R' over K'. Therefore, Lemma 19.1 implies that $F'R'$ is a Noetherian ring. Now fix $0 \neq v \in V$ and note that $W = (1 \otimes v)F'R'$ is a cyclic $F'R'$-module. Thus W is a Noetherian $F'R'$-module and, in particular, its submodules are finitely generated.

Finally, suppose by way of contradiction that $\dim_K F = \infty$. Since F/K is algebraic, we can find a strictly increasing chain of intermediate fields

$$K = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F$$

Then, for each $i \geq 0$, choose $f_i \in F_{i+1} \setminus F_i$ and set

$$w_i = f_i \otimes v - 1 \otimes f_i v \in W$$

Since the submodule $\sum_{i=0}^{\infty} w_i F'R'$ is finitely generated, it follows that $w_n \in \sum_{i<n} w_i F'R'$ for some $n \geq 0$.

Set $L = F_n$ and observe that $F \otimes_L V$ makes sense and that the map $F \times V \to F \otimes_L V$ given by $(f, v) \mapsto f \otimes_L v$ is balanced (over K). Thus there exists an additive group homomorphism $\theta\colon F \otimes_K V \to F \otimes_L V$ given by $f \otimes v \mapsto f \otimes_L v$. Furthermore, for any $f \in F$, $r \in R$ and $i < n$, we have

$$\begin{aligned} \theta\big(w_i(f'r')\big) &= \theta(f f_i \otimes vr - f \otimes f_i vr) \\ &= f f_i \otimes_L vr - f \otimes_L f_i vr = 0 \end{aligned}$$

since $f_i \in L$ can move across $\otimes_L$. Thus $w_n \in \sum_{i<n} w_i F'R' \subseteq \mathrm{Ker}(\theta)$. On the other hand, $\theta(w_n) = f_n \otimes_L v - 1 \otimes_L f_n v \in F \otimes_L V$ and $f_n \notin L$. Thus $\{1, f_n\}$ is part of an L-basis for F and the left analog of Lemma 9.7 implies that $\theta(w_n) \neq 0$, a contradiction. We conclude, therefore, that $\dim_K F < \infty$ and Lemma 4.8 yields the result. □

COROLLARY 19.6 *If D is a division ring that is an almost commutative K-algebra, then* $\dim_K D < \infty$.

PROOF $V = D$ is an irreducible right D-module and, by Lemma 4.3(ii), we have $\mathrm{End}_D(V) \cong D$. Now apply the preceding theorem. □

COROLLARY 19.7 (Zariski Nullstellensatz) *Suppose F is a field that is a finitely generated ring extension of its subfield K. Then F is a finite algebraic extension of K.*

The approach to the Nullstellensatz via generic flatness was discovered by P. Hall in his work on group rings of nilpotent groups. Duflo and

Quillen then went on to study almost commutative rings and proved the algebraic aspects of Theorem 19.5. The finite dimensional aspects of that theorem are due to Gabriel and Small. Results of McConnell on almost normalizing extensions are discussed in Exercises 5–10.

EXERCISES

1. If $R = \bigcup_{n=0}^{\infty} \mathcal{R}_n$ is a filtered ring, define $\deg r$ for $0 \neq r \in R$ to be the minimal n with $r \in \mathcal{R}_n$ and set $\deg 0 = -\infty$. Prove that $\deg rs = \deg r + \deg s$ for all $r, s \in R$ if and only if $\operatorname{gr} R$ is a domain. Now find an example of a domain R with $\operatorname{gr} R$ not a domain. For this, try a polynomial ring with a shifted degree.
2. Again let R be a filtered ring. If $I, J \lhd R$ with $IJ = 0$, prove that $(\operatorname{gr} I)(\operatorname{gr} J) = 0$. Conclude that if $\operatorname{gr} R$ is graded prime, then R must be prime, and, similarly, if $\operatorname{gr} R$ is graded semiprime, then R is semiprime. Here, a graded ring is *graded prime* if a product of nonzero graded ideals is necessarily nonzero. Similarly, *graded semiprime* means that there are no nonzero graded nilpotent ideals.
3. Let R be an almost centralizing extension of the integers $\mathbb{Z}$. If V is an irreducible R-module, use the argument of Theorem 19.5 (Step 1) to show that $\mathbb{Z}$ does not act faithfully on V. Conclude that $\operatorname{End}_R(V) = D$ is a finite division ring and hence a finite field.
4. If S is a commutative integral domain, prove that the following are equivalent. (i) S is a G-domain. (ii) SS^{-1} is an α-free S-module for some $0 \neq \alpha \in S$. (iii) The intersection of all nonzero prime ideals of S is not zero.

   We say that R is an *almost normalizing extension* of S if R is generated as a ring by S and the elements $x_1, x_2, \ldots, x_m$. Furthermore, we insist that $S + Sx_i = S + x_iS$ for all i and that

$$x_i x_j - x_j x_i \in S + \sum_{k=1}^{m} Sx_k$$

   for all i, j.

5. If R is an almost normalizing extension of the Noetherian ring S, prove that R is Noetherian. For this, use Exercise 11.7 along with the proof of Lemma 19.1.

   Suppose C is a commutative integral domain central in R. We say that R satisfies *generic flatness* with respect to C if every finitely

generated R-module V is α-free as a C-module for some $0 \neq \alpha \in C$. In the remaining problems let $R \supseteq S \supseteq C$.

6. Suppose that either R_S is finitely generated or R is an almost normalizing extension of S and S is Noetherian. If S satisfies generic flatness with respect to C, show that R does also. For this, generalize the proof of Theorem 19.4

   A family $\{ I(\mathbf{a}) \}$ of right ideals of R, indexed by $\mathbf{a} \in \mathbb{N}^k$, is called *weakly ascending* if $\mathbf{a} \leq_\pi \mathbf{b}$ implies that $I(\mathbf{a}) \subseteq I(\mathbf{b})$. We say that R satisfies *vector generic flatness* with respect to C if, for every $k \geq 1$ and every weakly ascending family $\{ I(\mathbf{a}) \mid \mathbf{a} \in \mathbb{N}^k \}$ of right ideals of R, there exists $0 \neq \alpha \in C$ such that all $R/I(\mathbf{a})$ are α-free C-modules. Notice that Exercises 8 and 9 have no Noetherian assumption.

7. Show that vector generic flatness with respect to C implies generic flatness with respect to C.
8. If S satisfies vector generic flatness with respect to C and if R_S is finitely generated, prove that R satisfies vector generic flatness with respect to C.
9. Suppose R is an almost normalizing extension of S. If S satisfies vector generic flatness with respect to C, prove that R does also. For this, merely observe that if $\{ I(\mathbf{a}) \mid \mathbf{a} \in \mathbb{N}^k \}$ is weakly ascending and if $I(\mathbf{a}, \mathbf{b})$ denotes the set of $\mathbf{b}$-leading coefficients of $I(\mathbf{a})$, then $\{ I(\mathbf{a}, \mathbf{b}) \mid \mathbf{a} \in \mathbb{N}^k, \ \mathbf{b} \in \mathbb{N}^m \}$ is a weakly ascending family with $(\mathbf{a}, \mathbf{b}) \in \mathbb{N}^{k+m}$. Now modify the proof of Exercise 6.
10. Suppose that C is Noetherian and that every nonzero right ideal of S meets C nontrivially. If S_C is a free C-module, prove that S satisfies vector generic flatness with respect to C.

20. Nullstellensatz

The main results of the preceding chapter, namely Theorem 19.5 and its corollaries, constitute the first half of the Nullstellensatz. We now move on to the second half and again we are concerned with an almost commutative K-algebra R. This time, the goal is to understand $\mathrm{Rad}(R)$. As in the classical commutative situation, the result will be proved by adjoining an additional variable to R. It is for this reason that we begin by studying the Jacobson radical of an arbitrary polynomial ring.

DEFINITION If $R \subseteq S$ are rings, then S is said to be a *finite centralizing extension* of R if S_R is a finitely generated R-module with generators that centralize R.

LEMMA 20.1 *Let $R \subseteq S$ be an extension of rings.*

i. If S is a finite centralizing extension of R and if V is an irreducible S-module, then V_R is a finite direct sum of irreducible R-modules. In particular, $\mathrm{Rad}(R) \subseteq R \cap \mathrm{Rad}(S)$.

ii. Suppose $S = R \dotplus U$, where U is a left R-submodule of S. Then every irreducible R-module is an R-submodule of an irreducible S-module. In particular, $R \cap \mathrm{Rad}(S) \subseteq \mathrm{Rad}(R)$.

PROOF (i) Write $S = \sum_{i=1}^{m} y_i R$, where each $y_i \in S$ centralizes R. Since V is an irreducible S-module, it is a cyclic S-module and hence a finitely generated R-module. Thus, by Nakayama's Lemma, $V \neq 0$ has a maximal R-submodule M.

For each i, observe that the map $y_i \colon V \to V$ given by $v \mapsto vy_i$ is an R-endomorphism; we let M_i be the complete inverse image of M. Thus

$M_i = \{ v \in V \mid vy_i \in M \}$ is an R-submodule of V and

$$\frac{V}{M_i} \cong \frac{Vy_i}{M_i y_i} = \frac{Vy_i}{Vy_i \cap M} \cong \frac{Vy_i + M}{M} \subseteq \frac{V}{M}$$

In particular, if V/M_i is not zero, then it is isomorphic to the irreducible R-module V/M.

Next, if $v \in \bigcap_{i=1}^m M_i$, then $vy_i \in M$ for all i and hence $vy_i R \subseteq M$. Thus $vS \subseteq M$ and, since V is an irreducible S-module, we conclude that $v = 0$. In other words, $\bigcap_{i=1}^m M_i = 0$ and hence the natural R-homomorphism $V \to \oplus \sum_{i=1}^m V/M_i$ is an embedding. But $\oplus \sum_{i=1}^m V/M_i$, being a finite direct sum of irreducible R-modules, is completely reducible and has finite composition length. Thus, by Lemmas 3.1 and 3.6, the same is true of V_R.

It follows, therefore, from Lemma 3.6(ii) that V_R is a finite direct sum of irreducible R-modules. In particular, $V \cdot \mathrm{Rad}(R) = 0$ and, since this is true for all such V, we conclude that $\mathrm{Rad}(R) \subseteq R \cap \mathrm{Rad}(S)$.

(ii) Now suppose that $S = R \dot{+} U$ with $RU \subseteq U$. If W is an irreducible R-module, then $W \cong R/M$ for some maximal right ideal M of R. Furthermore, $MS = M(R \dot{+} U) \subseteq M \dot{+} U$ and hence MS is a proper right ideal of S. We can therefore choose N to be a maximal right ideal of S containing MS. Since $R \supset R \cap N \supseteq M$, we have $R \cap N = M$ and hence

$$\frac{S}{N} \supseteq \frac{R+N}{N} \cong \frac{R}{R \cap N} = \frac{R}{M}$$

In other words, the irreducible S-module $V = S/N$ has $R/M \cong W$ as an R-submodule. Finally, $V \cdot \mathrm{Rad}(S) = 0$ implies that $W \cdot \mathrm{Rad}(S) = 0$; since this is true for all such W, we have $R \cap \mathrm{Rad}(S) \subseteq \mathrm{Rad}(R)$. □

We can now prove:

PROPOSITION 20.2 *If $S = \cdot \sum_{i=0}^{\infty} S_i$ is a graded ring, then the Jacobson radical of S is a graded ideal. In other words,* $\mathrm{Rad}(S) = \cdot \sum_{i=0}^{\infty} \big(S_i \cap \mathrm{Rad}(S)\big)$. *Furthermore, $S_m \cap \mathrm{Rad}(S)$ is nil for all $m > 0$.*

PROOF We first prove that $\mathrm{Rad}(S)$ is graded. Specifically, the goal is to show that if $s = \sum_i s_i$ is in $\mathrm{Rad}(S)$, then so is each s_i. We proceed by induction on the number n of nonzero components of s, over all choices of s and S. If $n = 0$ or 1, the result is clear, so assume that $n \geq 2$. Say $s_a \neq 0$ and fix any $s_b \neq 0$ with $b \neq a$.

Choose any rational prime $p > |b - a|$ and form the ring extension $\tilde{S} = S[\zeta]/(1 + \zeta + \cdots + \zeta^{p-1})$ of S. If ϵ denotes the image of ζ in $\tilde{S}$, then

ϵ commutes with S and $1 + \epsilon + \cdots + \epsilon^{p-1} = 0$, so $\epsilon^p = 1$. Furthermore, $\tilde{S} = S \dotplus S\epsilon \dotplus \cdots \dotplus S\epsilon^{p-2}$, so both parts of the preceding lemma imply that $\mathrm{Rad}(S) = \mathrm{Rad}(\tilde{S}) \cap S$. Note also that $\tilde{S}$ is graded with components $\tilde{S}_i = S_i \dotplus S_i\epsilon \dotplus \cdots \dotplus S_i\epsilon^{p-2}$. Thus $s = \sum_i s_i \in \mathrm{Rad}(\tilde{S})$ and s_i is the $\tilde{S}_i$-component of s.

Now observe that the map $\epsilon^{\#}\colon \tilde{S} \to \tilde{S}$ that multiplies each element of $\tilde{S}_i$ by ϵ^i is an automorphism of $\tilde{S}$. Thus since $\mathrm{Rad}(\tilde{S})$ is a characteristic ideal of $\tilde{S}$, we have $\sum_i \epsilon^i s_i = \epsilon^{\#}(s) \in \mathrm{Rad}(\tilde{S})$. It follows that

$$t = \sum_i \epsilon^i s_i - \epsilon^b \sum_i s_i \in \mathrm{Rad}(\tilde{S})$$

and this element has less than n nonzero components. We can therefore conclude by induction that $t_a = (\epsilon^a - \epsilon^b)s_a \in \mathrm{Rad}(\tilde{S})$, so $(\epsilon^c - 1)s_a \in \mathrm{Rad}(\tilde{S})$, where $c = |b - a|$. Furthermore, by the choice of p we have $p > c > 0$, so c is prime to p. Thus

$$(\epsilon^c - 1)\big(\epsilon^c + 2\epsilon^{2c} + \cdots + (p-1)\epsilon^{(p-1)c}\big) = p$$

and it follows that $ps_a \in \mathrm{Rad}(\tilde{S}) \cap S = \mathrm{Rad}(S)$. Since this is true for at least two distinct primes p, we conclude that $s_a \in \mathrm{Rad}(S)$, as required.

For the second part, let $u_m \in S_m \cap \mathrm{Rad}(S)$ and assume that $m > 0$. Then $1 - u_m$ is invertible in S with inverse $v = \sum_{i=0} v_i$. The equation $1 = (1 - u_m)v$ now implies that $v_0 = 1$ and that $u_m v_i = v_{i+m}$ for all i. In particular, we have $v_{jm} = (u_m)^j$ by induction on $j \geq 0$. But v_{jm} is eventually zero, so the result follows. □

In case $S = R[x]$ is an ordinary polynomial ring, there is the following sharper formulation.

THEOREM 20.3 (Amitsur's Theorem) *If R is any ring, then* $\mathrm{Rad}(R[x]) = N[x]$, *where N is some nil ideal of R.*

PROOF Let $S = R[x]$ and observe that S is graded with $S_i = Rx^i$. If $N = R \cap \mathrm{Rad}(S)$, then N is an ideal of R and $\mathrm{Rad}(S) \supseteq NS = N[x]$. Conversely, if $s = \sum_i r_i x^i \in \mathrm{Rad}(S)$, then, by the previous proposition, $r_i x^i \in \mathrm{Rad}(S)$ for all i. Therefore, it suffices to show that $rx^i \in \mathrm{Rad}(S)$ implies that $r \in N$. For this, observe that the map fixing R and sending x to $1 + x$ is a ring automorphism of S. Hence, since $\mathrm{Rad}(S)$ is a characteristic ideal,

$$r + irx + \cdots + rx^i = r(1 + x)^i \in \mathrm{Rad}(S)$$

and we can apply Proposition 20.2 to conclude that $r \in R \cap \mathrm{Rad}(S) = N$. Thus $\mathrm{Rad}(S) = N[x]$.

Finally, if $r \in N$, then $rx \in S_1 \cap \mathrm{Rad}(S)$, so rx is nilpotent. Thus r is also nilpotent and N is indeed a nil ideal of R. □

At present, there is no known intrinsic characterization of the ideal N for arbitrary rings. However, if R is assumed to be Noetherian, then the answer is easy.

DEFINITION If $a \in R$, then we recall that $\mathrm{r.ann}_R(a) = \{ r \in R \mid ar = 0 \}$ is a right ideal of R known as the *right annihilator* of a. We say that the ring R satisfies *max-ra*, the maximum condition on right annihilators, if every nonempty collection of right annihilator ideals contains a maximal member. Obviously, every right Noetherian ring satisfies max-ra. In addition, we say that R is *semiprime* if it has no nonzero nilpotent two-sided ideal.

LEMMA 20.4 *i. Let R be a semiprime ring with max-ra. Then R has no nonzero nil right or left ideal.*

ii. If R is right Noetherian, then $\mathrm{Nil}(R)$ is the unique maximal nilpotent two-sided ideal of R.

PROOF (i) Suppose by way of contradiction that I is a nonzero nil right or left ideal of R. If I is a right ideal, choose $0 \neq a \in I$ so that $aR \subseteq I$ is also a nil right ideal. Furthermore, since $(ra)^{n+1} = r(ar)^n a$ for all $r \in R$ and n, it follows that $Ra \neq 0$ is a nil left ideal of R. Thus we can now clearly assume that I is a left ideal. By max-ra, choose $0 \neq b \in I$ with $\mathrm{r.ann}_R(b)$ a maximal member of the set $\{ \mathrm{r.ann}_R(c) \mid 0 \neq c \in I \}$.

Suppose that x is an arbitrary element of R. Since I is a nil left ideal and $b \in I$, there exists $n \geq 0$ with $(xb)^n \neq 0$ but $(xb)^{n+1} = 0$. If $n = 0$, then $xb = 0$, so $bxb = 0$. If $n > 0$, then, since $\mathrm{r.ann}_R\big((xb)^n\big) \supseteq \mathrm{r.ann}_R(b)$, the maximality of $\mathrm{r.ann}_R(b)$ implies that these two right ideals are equal. But $xb \in \mathrm{r.ann}_R\big((xb)^n\big) = \mathrm{r.ann}_R(b)$, so again we have $bxb = 0$. In other words, $bRb = 0$ so $(RbR)^2 = 0$ and R is not semiprime, a contradiction.

(ii) By the Noetherian condition, R has a two-sided ideal N maximal with respect to the property of being nilpotent. Notice that if $N \subseteq I \lhd R$ and if $I^2 \subseteq N$, then I is also nilpotent and hence $I = N$. It follows that R/N is a semiprime ring. Furthermore, R/N is Noetherian and hence satisfies max-ra. Thus we conclude from (i) that $\mathrm{Nil}(R/N) = 0$. But nil ideals map to nil ideals under an epimorphism, so it is clear that $\mathrm{Nil}(R)$ is contained in N. On the other hand, the reverse inclusion is obvious, so the result follows. □

COROLLARY 20.5 *If R is a right Noetherian ring, then* $\mathrm{Rad}(R[x]) = \mathrm{Nil}(R)[x]$ *is nilpotent. In particular, if R is semiprime, then $R[x]$ is semiprimitive.*

PROOF According to Theorem 20.3 we have $\mathrm{Rad}(R[x]) \subseteq \mathrm{Nil}(R)[x]$ and, by Lemma 20.4(ii), $\mathrm{Nil}(R)$ is the largest nilpotent ideal of R. It then follows easily that $\mathrm{Nil}(R)[x]$ is a nilpotent ideal of $R[x]$ and thus we obtain the reverse inclusion $\mathrm{Nil}(R)[x] \subseteq \mathrm{Rad}(R[x])$. □

It is now a simple matter to prove the second half of the Nullstellensatz in this noncommutative setting.

THEOREM 20.6 *Let R be an almost commutative K-algebra. Then every semiprime homomorphic image of R is semiprimitive.*

PROOF Note that any homomorphic image of an almost commutative K-algebra is also a K-algebra of this form. Thus it suffices to show that if R is semiprime, then it is necessarily semiprimitive.

Suppose that R is semiprime. Since R is Noetherian, by Lemma 19.1, the preceding corollary implies that $S = R[x]$ is semiprimitive. In particular, if $0 \neq r \in R$, we can find an irreducible S-module V with $Vr \neq 0$. Notice that $S = R[x]$ is an almost commutative K-algebra whose generators are those of R along with the additional variable x. Thus, by Theorem 19.5, $\mathrm{End}_S(V)$ is finite dimensional over K and hence algebraic over K. But x is central in S, so the map $x\colon V \to V$ given by $v \mapsto vx$ is an S-endomorphism of V. Thus we conclude that x, in its action on V, is algebraic over K.

To make this precise, let $'\colon S \to \mathrm{End}(V)$ be the representation of S associated with the module V. Then $S' = R'[x']$ and x' is algebraic over $K' \subseteq R'$. Thus S' is a finite centralizing extension of R'. Furthermore, V is an irreducible S'-module, so Lemma 20.1 implies that $V_{R'}$ is a finite direct sum of irreducible R'-modules. Equivalently, V_R is a finite direct sum of irreducible R-modules. Since $Vr \neq 0$, it follows that r acts nontrivially on one of these irreducible direct summands and therefore $r \notin \mathrm{Rad}(R)$. Indeed, since this holds for all $0 \neq r \in R$, we have $\mathrm{Rad}(R) = 0$. □

Now let us see what all this has to do with zero sets.

DEFINITION Let K be a field, let $\tilde{K}$ denote its algebraic closure and let $R = K[x_1, x_2, \ldots, x_m]$ be an ordinary polynomial ring over K in m variables. If $f(x_1, x_2, \ldots, x_m) \in R$, then an m-tuple $(a_1, a_2, \ldots, a_m) \in \tilde{K}^m$ is called an *algebraic root*, or *zero*, of f if $f(a_1, a_2, \ldots, a_m) = 0$. We then let $\mathcal{Z}(f)$, the *zero set* of f, be the set of all the algebraic roots of f. Furthermore, if T is

any nonempty subset of R, then we use $\mathcal{Z}(T)$ to denote the set of common algebraic roots for all members of T. In other words, $\mathcal{Z}(T) = \bigcap_{f \in T} \mathcal{Z}(f)$.

Notice that $T_1 \subseteq T_2$ implies $\mathcal{Z}(T_1) \supseteq \mathcal{Z}(T_2)$ and that any common zero of T is also a zero of any R-linear combination of elements of T. It therefore follows that $\mathcal{Z}(T) = \mathcal{Z}(I)$, where I is the ideal of R generated by T. Because of this, we need only be concerned with the zero sets of ideals. Next observe that if I is an ideal of R and if $f^n \in I$ for some $n \geq 1$, then $\mathcal{Z}(f) \supseteq \mathcal{Z}(I)$. It follows that $\mathcal{Z}(I) = \mathcal{Z}(\sqrt{I})$, where

$$\sqrt{I} = \{ f \in R \mid f^n \in I \text{ for some } n \geq 1 \}$$

Since R is commutative, it is trivial to see that $\sqrt{I}$ is an ideal of R containing I. Indeed, $\sqrt{I}/I = \text{Nil}(R/I)$ and $R/\sqrt{I}$ is semiprime.

THEOREM 20.7 (Hilbert Nullstellensatz) *Let $R = K[x_1, x_2, \ldots, x_m]$ be a polynomial ring over the field K and let I be a proper ideal of R.*

i. The elements of I have a common algebraic root. Thus $\mathcal{Z}(I) \neq \emptyset$.

ii. Let $f \in R$. Then $f \in \sqrt{I}$ if and only if $\mathcal{Z}(f) \supseteq \mathcal{Z}(I)$.

PROOF We first translate these concepts into more ring theoretic language. Let $(a_1, a_2, \ldots, a_m) \in \tilde{K}^m$ and observe that the evaluation map $\phi: R \to \tilde{K}$ given by $f(x_1, x_2, \ldots, x_m) \mapsto f(a_1, a_2, \ldots, a_m)$ is a ring homomorphism. Furthermore, since each a_i is algebraic over K, $\phi(R) = K[a_1, a_2, \ldots, a_m]$ is a finite algebraic field extension of K. In particular, $\text{Ker}(\phi)$ is a maximal ideal of R. Note that $f \in \text{Ker}(\phi)$ if and only if $(a_1, a_2, \ldots, a_m)$ is an algebraic root of f.

Conversely, suppose M is a maximal ideal of R and observe that $R/M = K[\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_m]$, where $\bar{x}_i = x_i + M$. Thus R/M is a field that is finitely generated as a ring extension of K and the Zariski Nullstellensatz implies that R/M is an algebraic field extension of K. In other words, $(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_m)$ is contained in $\tilde{K}^m$ and the homomorphism $R \to R/M$ is the corresponding evaluation map as described in the preceding paragraph.

(i) Since I is a proper ideal of R, it is contained in a maximal ideal M. Furthermore, by the preceding, M is the kernel of the evaluation homomorphism $\phi: R \to \tilde{K}$ given by $\phi(f) = f(a_1, a_2, \ldots, a_m)$ for some m-tuple $(a_1, a_2, \ldots, a_m) \in \tilde{K}^m$. Since $I \subseteq M$, we conclude that $(a_1, a_2, \ldots, a_m)$ is a common algebraic root of all $f \in I$.

(ii) If $f \in \sqrt{I}$, then we know that $\mathcal{Z}(f) \supseteq \mathcal{Z}(I)$. Conversely, suppose that $\mathcal{Z}(f) \supseteq \mathcal{Z}(I)$ and let M be any maximal ideal of R containing $\sqrt{I}$. Since M is the kernel of the evaluation map at some $(a_1, a_2, \ldots, a_m) \in \tilde{K}^m$, it follows that $(a_1, a_2, \ldots, a_m) \in \mathcal{Z}(I) \subseteq \mathcal{Z}(f)$. In other words,

$f(a_1, a_2, \ldots, a_m) = 0$ and $f \in M$. Thus f is contained in all maximal ideals of R that contain $\sqrt{I}$.

Finally, observe that R is an almost commutative K-algebra and that $\bar{R} = R/\sqrt{I}$ is a semiprime homomorphic image. Thus, by the preceding theorem, $\bar{R}$ is semiprimitive and, in particular, the intersection of all its maximal ideals is 0. But this says that the intersection of all maximal ideals of R that contain $\sqrt{I}$ is precisely equal to $\sqrt{I}$ and therefore it follows that $f \in \sqrt{I}$. □

We close this chapter with an extremely interesting example of a noncommutative, almost commutative K-algebra.

DEFINITION Let $V = K[s_1, s_2, \ldots, s_m]$ be the polynomial ring in m variables, but think of V as just a K-vector space. Since multiplication by any element of $K[s_1, s_2, \ldots, s_m]$ is a K-linear transformation of V, we have an embedding $^-$ of this ring into $\mathrm{End}_K(V)$, acting on the right. Specifically, let $K[\bar{s}_1, \bar{s}_2, \ldots, \bar{s}_m]$ denote the image of $^-$ in $\mathrm{End}_K(V)$, so that $\bar{s}_i$ denotes multiplication by s_i. In addition, for each i, the operator $\partial/\partial s_i$ is also a K-linear transformation on V, which we denote by $\bar{t}_i \in \mathrm{End}_K(V)$. It is clear that $\bar{s}_i\bar{s}_j = \bar{s}_j\bar{s}_i$ and $\bar{t}_i\bar{t}_j = \bar{t}_j\bar{t}_i$ for all i, j and that $\bar{s}_i\bar{t}_j = \bar{t}_j\bar{s}_i$ for all $i \neq j$. Furthermore, for any $v \in V$ and i, we have

$$\begin{aligned} v(\bar{s}_i\bar{t}_i) &= \frac{\partial(vs_i)}{\partial s_i} \\ &= v\,\frac{\partial s_i}{\partial s_i} + \frac{\partial v}{\partial s_i}\,s_i = v + v(\bar{t}_i\bar{s}_i). \end{aligned}$$

so $\bar{s}_i\bar{t}_i - \bar{t}_i\bar{s}_i = 1$. Of course, K is central in $\mathrm{End}_K(V)$.

This motivates us to define the *Weyl algebra* $\mathrm{A}_m(K)$ to be the K-algebra generated by the $2m$ noncommuting variables

$$x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_m$$

subject to the relations

$$x_ix_j = x_jx_i, \quad y_iy_j = y_jy_i, \quad x_iy_j - y_jx_i = \delta_{i,j}$$

for all i, j. Here, $\delta_{i,j} = 1$ if $i = j$ and 0 otherwise. It is clear that $\mathrm{A}_m(K)$ is a noncommutative, almost commutative K-algebra. Furthermore, there is a ring homomorphism $\mathrm{A}_m(K) \to \mathrm{End}_K(V)$ given by $x_i \mapsto \bar{s}_i$, $y_i \mapsto \bar{t}_i$ and $k \mapsto k$ for all $k \in K$. In this way, V becomes a right $\mathrm{A}_m(K)$-module.

We sketch some basic properties.

THEOREM 20.8 *If K is a field of characteristic 0, then $A_m(K)$ is a simple Noetherian K-algebra. Furthermore, $A_m(K)$ is a domain and $\operatorname{gr} A_m(K)$ is isomorphic to a polynomial ring over K in $2m$ variables.*

PROOF Let x, y be elements of any K-algebra R with $xy - yx = 1$. Since

$$x^{n+1}y - yx^{n+1} = x(x^n y - yx^n) + (xy - yx)x^n$$

it follows immediately by induction on $n \geq 1$ that $x^n y - yx^n = nx^{n-1}$. In particular, if $f(x)$ is a polynomial in x with coefficients in K, then we have $f(x)y - yf(x) = \partial f/\partial x$. Similarly, $xg(y) - g(y)x = \partial g/\partial y$.

Now $A_m(K)$ is an almost commutative K-algebra, so we know that every element α of this ring can be written as a suitable finite sum $\alpha = \sum_{\mathbf{a},\mathbf{b}} k_{\mathbf{a},\mathbf{b}} \mathbf{x}^{\mathbf{a}} \mathbf{y}^{\mathbf{b}}$. Here $\mathbf{a} = (a_1, a_2, \ldots, a_m)$ and $\mathbf{b} = (b_1, b_2, \ldots b_m)$ are m-tuples in $\mathbb{N}^m$. Furthermore, $\mathbf{x}^{\mathbf{a}} = x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}$, $\mathbf{y}^{\mathbf{b}} = y_1^{b_1} y_2^{b_2} \cdots y_m^{b_m}$, and $k_{\mathbf{a},\mathbf{b}} \in K$. In particular, $\alpha = \sum_{\mathbf{a}} \mathbf{x}^{\mathbf{a}} f_{\mathbf{a}}(\mathbf{y})$, where each $f_{\mathbf{a}}$ is a polynomial in m variables. In the next paragraph we show that if some $f_{\mathbf{a}}$ is not identically zero as a polynomial and if $\alpha \in I \lhd A_m(K)$, then $I = A_m(K)$.

Thus suppose some $f_{\mathbf{a}}$ is not zero and choose $\mathbf{c} = (c_1, c_2, \ldots, c_m)$ maximal under the lexicographical ordering with $f_{\mathbf{c}} \neq 0$. Since I is closed under right and left multiplication, we have $\alpha y_i - y_i \alpha \in I$ for each i and, by the observation of the first paragraph, this implies that $\partial\alpha/\partial x_i \in I$. In particular, by the choice of $\mathbf{c}$, we have

$$c_1! c_2! \cdots c_m!\, f_{\mathbf{c}}(\mathbf{y}) = \frac{\partial^{c_1}}{\partial x_1^{c_1}} \frac{\partial^{c_2}}{\partial x_2^{c_2}} \cdots \frac{\partial^{c_m}}{\partial x_m^{c_m}} \alpha \in I$$

and thus, since $\operatorname{char} K = 0$, it follows that $f_{\mathbf{c}}(\mathbf{y}) \in I$. But $f_{\mathbf{c}}$ is not identically zero as a polynomial, so we can repeat this process, this time differentiating with respect to the y_j's, to conclude that $1 \in I$.

By Lemma 19.1, $A_m(K)$ is Noetherian and, by the preceding, this ring is simple. Furthermore, the representation of any element α as a polynomial in the x_i and y_j is unique, since otherwise we could describe 0 as a nontrivial polynomial and yet conclude that the ideal it generates is the whole ring. It now follows from a leading degree argument that $A_m(K)$ is a domain. Finally, write $\mathcal{A} = A_m(K)$ and recall that $\mathcal{A}$ is filtered by $\mathcal{A}_0 = K$ and

$$\mathcal{A}_n = (K + Kx_1 + \cdots + Kx_m + Ky_1 + \cdots + Ky_m)^n$$

for $n \geq 1$. Thus $\operatorname{gr} \mathcal{A}$ is a commutative K-algebra generated by the elements $\bar{x}_i = x_i + \mathcal{A}_0$ and $\bar{y}_j = y_j + \mathcal{A}_0$ for $i, j = 1, 2, \ldots, m$. Moreover,

the uniqueness of expression guarantees that all monomials in the $\bar{x}_i$ and $\bar{y}_j$ of total degree n are K-linearly independent. With this, it is clear that $\bar{x}_1, \ldots, \bar{x}_m$ and $\bar{y}_1, \ldots, \bar{y}_m$ are algebraically independent over K and hence generate a polynomial ring over K in the $2m$ variables. □

EXERCISES

1. What difference would it make in the definition of an almost centralizing extension $R \subseteq S$, if we assumed that the centralizing generators $x_1, x_2, \ldots, x_n$ satisfied the stronger condition $x_i x_j - x_j x_i \in \sum_{k=1}^{n} R x_k$ for all i, j? This has a simple one-line answer.
2. Let $\mathbb{Z}$ denote the ring of integers and let T be the multiplicatively closed subset of $\mathbb{Z}$ generated by the primes $p_1, p_2, \ldots$. Then $R = \mathbb{Z}T^{-1}$ can be filtered by defining R_n to be the set of all fractions of the form $z/p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ with $z \in \mathbb{Z}$ and all $a_i \leq n$. Prove that $\operatorname{gr} R \cong \mathbb{Z} \oplus xS[x]$, where S is the ring (without 1) given by $S = \oplus \sum_i \mathrm{GF}(p_i)$.
3. Use the preceding exercise to construct a filtered domain R such that $\operatorname{Rad}(R) \neq 0$ but $\operatorname{Rad}(\operatorname{gr} R) = 0$. Conversely, construct a semiprimitive filtered commutative domain R' with $\operatorname{Nil}(\operatorname{gr} R') \neq 0$.

   $R \subseteq S$ is a *finite normalizing extension* of rings if $S = \sum_{i=1}^{n} y_i R$ for suitable $y_i \in S$ with $y_i R = R y_i$ for all i.

4. Let $R \subseteq S$ be a finite normalizing extension and let V be an irreducible S-module. Prove that V_R is a finite direct sum of irreducible R-modules. If the extension is centralizing, show that all the irreducible R-summands of V are isomorphic.
5. Let V be the $\mathrm{A}_m(K)$-module described immediately preceding Theorem 20.8. Prove that V is irreducible if $\operatorname{char} K = 0$ but reducible otherwise.

   The next three problems discuss Amitsur's simple proof of the Nullstellensatz over uncountable fields.

6. Let R be an algebra over the field K and let $r \in R$. If $1 - kr$ is invertible for all $k \in K$ and if $\{(1 - kr)^{-1} \mid k \in K\}$ is K-linearly dependent, prove that r is algebraic over K. Furthermore, show that any $s \in \operatorname{Rad}(R)$ which is algebraic over K must necessarily be nilpotent.
7. Let R be a K-algebra and assume that $\dim_K R < |K|$, where this is an inequality of possibly infinite cardinals. Prove that $\operatorname{Rad}(R)$ is a nil ideal. Furthermore, if R is a division ring, prove that R is algebraic over K.

8. Suppose now that K is an uncountable field and that R is a finitely generated K-algebra. Prove that $\mathrm{Rad}(R)$ is nil. Furthermore, if V is an irreducible R-module, prove that the division ring $D = \mathrm{End}_R(V)$ is algebraic over K.

   If K is a countable field and R is a finitely generated K-algebra, then $\mathrm{Rad}(R)$ need not be nil. Although counterexamples exist in all characteristics, we will only offer a characteristic 0 example here. Its construction is analogous to the construction of the Weyl algebras.

   Let C be a commutative algebra over the field K and let $C[[\zeta]]$ be the power series ring over C in the variable ζ. View $V = C[[\zeta]]$ as a C-module and consider $\mathrm{End}_C(V)$, acting on the right. Since multiplication by any element of this ring is a C-endomorphism, we have an embedding of $C[[\zeta]]$ into $\mathrm{End}_C(V)$, say $C[[x]] \subseteq \mathrm{End}_C(V)$. In addition, let $y \in \mathrm{End}_C(V)$ denote the operator $\partial/\partial\zeta$ and let $e \in \mathrm{End}_C(V)$ be the map $v(\zeta) \mapsto v(0)$ that reads off the constant coefficient.

9. If $\alpha \in \mathrm{End}_C(V)$, prove that $e\alpha e = ec$, where $c = (1\alpha)(0) \in C$. Conclude that e is an idempotent and that $e\,\mathrm{End}_C(V)\,e = eC \cong C$, where the latter is a ring isomorphism. Next, if $\beta \in C[[x]]$, prove that $\beta y - y\beta = \partial\beta/\partial x$.
10. Now let K be a countable field of characteristic 0. Find a countable commutative K-algebra C such that C is a domain and $\mathrm{Rad}(C) \neq 0$. For example, take C to be a suitable localization of a polynomial ring over K. Next, let $C = \{c_0, c_1, c_2, \dots\}$ and define $\gamma \in \mathrm{End}_C(V)$ by $\gamma = \sum_{n=0}^{\infty} c_n x^n/n!$. If $R = K[e, \gamma, y]$ is the finitely generated K-subalgebra of $\mathrm{End}_C(V)$, prove that $eRe = eC$. Deduce that $\mathrm{Rad}(R) \supseteq \mathrm{Rad}(eRe) \cong \mathrm{Rad}(C)$ is not nil.

Part III
Injective Modules

21. Injective Modules

We start this chapter by taking another look at Hom_R. This time, we study it in much the same way we studied the tensor product. As we will see, Hom_R is left exact and there are two natural families of modules associated with it that are analogs of the flat modules. The first of these families consists of the projective modules; the second consists of the injective ones.

DEFINITION Let A_R and B_R be right R-modules and, as usual, let $\mathrm{Hom}_R(A, B)$ denote the additive abelian group of all R-homomorphisms from A to B, written on the left. We show next that when A or B is a bimodule, then $\mathrm{Hom}_R(A, B)$ inherits additional structure.

Thus suppose that A is an (S, R)-bimodule. If $\theta \in \mathrm{Hom}_R(A, B)$ and $s \in S$, then $\theta s\colon A \to B$ defined by

$$(\theta s)a = \theta(sa) \qquad \text{for all } a \in A$$

is easily seen to be an R-homomorphism. Indeed, in this way, $\mathrm{Hom}_R(A, B)$ becomes a right S-module. Similarly, suppose B is a (T, R)-bimodule. If $\theta \in \mathrm{Hom}_R(A, B)$ and $t \in T$, then we define $t\theta\colon A \to B$ by

$$(t\theta)a = t(\theta a) \qquad \text{for all } a \in A$$

It follows that $t\theta$ is an R-homomorphism and that $\mathrm{Hom}_R(A, B)$ is a left T-module. Furthermore, if A is an (S, R)-bimodule and B is a (T, R)-bimodule, then $\mathrm{Hom}_R(A, B)$ is a (T, S)-bimodule.

Again, suppose A_R and B_R are right R-modules. If $\sigma\colon B \to B'$ is an R-module homomorphism, then σ determines an additive group

homomorphism $\hat{\sigma}\colon \mathrm{Hom}_R(A, B) \to \mathrm{Hom}_R(A, B')$ given by $\hat{\sigma}(\theta) = \sigma\theta$. In other words, if $\theta\colon A \to B$, then $\hat{\sigma}(\theta)$ is the composite R-homomorphism

$$\hat{\sigma}(\theta)\colon A \xrightarrow{\theta} B \xrightarrow{\sigma} B'$$

As with the tensor product situation, $\hat{\sigma}$ preserves the direction of the arrows and hence is *covariant.*

Furthermore, if B and B' are (T, R)-bimodules and if σ is a bimodule homomorphism, then $\hat{\sigma}$ is easily seen to be a left T-module homomorphism. On the other hand, if A is an (S, R)-bimodule, then $\hat{\sigma}$ is a right S-module homomorphism.

Next, if $\mu\colon A \to A'$ is an R-module homomorphism, then μ determines an additive group homomorphism $\hat{\mu}\colon \mathrm{Hom}_R(A', B) \to \mathrm{Hom}_R(A, B)$ given by $\hat{\mu}(\theta) = \theta\mu$. In other words, if $\theta\colon A' \to B$, then $\hat{\mu}(\theta)$ is the composite R-homomorphism

$$\hat{\mu}(\theta)\colon A \xrightarrow{\mu} A' \xrightarrow{\theta} B$$

In this case, we see that the arrows reverse and hence $\hat{\mu}$ is said to be *contravariant.*

Again, if A and A' are (S, R)-bimodules and if μ is a bimodule homomorphism, then $\hat{\mu}$ is a right S-module map. Similarly, if B is a (T, R)-bimodule, then $\hat{\mu}$ is a left T-module homomorphism.

There are, of course, analogous definitions and properties in case A and B are left R-modules. The following lemma asserts that Hom_R is *left exact.* It applies equally well in the context of bimodules.

LEMMA 21.1 *Assume that the appropriate A's and B's that follow are all R-modules and that the given maps are all R-homomorphisms.*

i. If

$$0 \to B \xrightarrow{\sigma} B' \xrightarrow{\tau} B''$$

is exact, then so is

$$0 \to \mathrm{Hom}_R(A, B) \xrightarrow{\hat{\sigma}} \mathrm{Hom}_R(A, B') \xrightarrow{\hat{\tau}} \mathrm{Hom}_R(A, B'')$$

ii. If

$$A \xrightarrow{\mu} A' \xrightarrow{\eta} A'' \to 0$$

is exact, then so is

$$0 \to \mathrm{Hom}_R(A'', B) \xrightarrow{\hat{\eta}} \mathrm{Hom}_R(A', B) \xrightarrow{\hat{\mu}} \mathrm{Hom}_R(A, B)$$

PROOF (i) Since $\sigma: B \to B'$ is one-to-one, it is trivial to see that $\hat{\sigma}$ is also one-to-one with image

$$\mathrm{Im}(\hat{\sigma}) = \{\, \alpha \in \mathrm{Hom}_R(A, B') \mid \mathrm{Im}(\alpha) \subseteq \mathrm{Im}(\sigma) \,\}$$

On the other hand, $\beta \in \mathrm{Hom}_R(A, B')$ is in the kernel of $\hat{\tau}$ if and only if $\mathrm{Im}(\beta) \subseteq \mathrm{Ker}(\tau)$. But $\mathrm{Ker}(\tau) = \mathrm{Im}(\sigma)$, so we conclude that $\mathrm{Ker}(\hat{\tau}) = \mathrm{Im}(\hat{\sigma})$.

(ii) Since $\eta: A' \to A''$ is onto, it is easy to see that $\hat{\eta}$ is one-to-one with image

$$\mathrm{Im}(\hat{\eta}) = \{\, \alpha \in \mathrm{Hom}_R(A', B) \mid \mathrm{Ker}(\eta) \subseteq \mathrm{Ker}(\alpha) \,\}$$

On the other hand, $\beta \in \mathrm{Hom}_R(A', B)$ is in the kernel of $\hat{\mu}$ if and only if $\mathrm{Im}(\mu) \subseteq \mathrm{Ker}(\beta)$. Thus $\mathrm{Im}(\mu) = \mathrm{Ker}(\eta)$ implies that $\mathrm{Ker}(\hat{\mu}) = \mathrm{Im}(\hat{\eta})$. □

Let us see what is needed for exactness. In the first case, we would want

$$0 \to B \xrightarrow{\sigma} B' \xrightarrow{\tau} B'' \to 0$$

exact to imply that

$$0 \to \mathrm{Hom}_R(A, B) \xrightarrow{\hat{\sigma}} \mathrm{Hom}_R(A, B') \xrightarrow{\hat{\tau}} \mathrm{Hom}_R(A, B'') \to 0$$

is also exact. Equivalently, if $\tau: B' \to B''$ is an epimorphism, then we need $\hat{\tau}$ to be an epimorphism and this says that every R-homomorphism $\alpha: A \to B''$ lifts to a map from $A \to B'$. Thus we have the familiar diagram

$$\begin{array}{ccccc} & & A & & \\ & & \downarrow \alpha & & \\ B' & \xrightarrow{\tau} & B'' & \to & 0 \end{array}$$

which defines the property of being a projective module. In other words, A is a projective R-module if and only if $\mathrm{Hom}_R(A, -)$ preserves short exact sequences.

In the second case, we would want

$$0 \to A \xrightarrow{\mu} A' \xrightarrow{\eta} A'' \to 0$$

exact to imply that

$$0 \to \mathrm{Hom}_R(A'', B) \xrightarrow{\hat{\eta}} \mathrm{Hom}_R(A', B) \xrightarrow{\hat{\mu}} \mathrm{Hom}_R(A, B) \to 0$$

is also exact. Equivalently, if $\mu: A \to A'$ is a monomorphism, then we need $\hat{\mu}$ to be an epimorphism and this says that every R-homomorphism $\alpha: A \to B$ extends to a map from $A' \to B$.

DEFINITION An R-module Q is said to be *injective* if whenever

$$\begin{array}{ccccc} & & Q & & \\ & & \alpha \uparrow & & \\ 0 & \to & W & \xrightarrow{\beta} & V \end{array}$$

is given with the bottom row exact, then there exists an R-homomorphism $\gamma: V \to Q$ that makes the diagram commute. That is, given any R-monomorphism $\beta: W \to V$ and any R-homomorphism $\alpha: W \to Q$, then there exists $\gamma: V \to Q$ with $\gamma\beta = \alpha$. In view of the preceding remarks, B is an injective R-module if and only if $\mathrm{Hom}_R(-, B)$ preserves short exact sequences.

Since β is one-to-one, we can clearly view W as a submodule of V. Thus, Q is injective if and only if every homomorphism from a submodule $W \subseteq V$ to Q extends to a homomorphism from the entire module V. For example, if $R = K$ is a field, then $Q = K_K$ is injective, since any linear functional defined on W extends to one of V.

Let us formally restate the preceding observations.

LEMMA 21.2 *i. The R-module P is projective if and only if* $\mathrm{Hom}_R(P, -)$ *preserves short exact sequences.*

ii. The R-module Q is injective if and only if $\mathrm{Hom}_R(-, Q)$ *preserves short exact sequences.*

Notice that the difference between the definitions of projective and injective modules is that the arrows are reversed. Thus, this "duality" between the two families should imply that they share a variety of analogous properties. However, for the most part, we ignore these analogs in favor

of those results that are uniquely injective. Indeed, to start with, there is the question of the existence of "enough" injectives. Unlike the case of projective modules, where existence was simple because of the presence of free modules, here we have to work.

LEMMA 21.3 (Baer's Criterion) *The R-module Q is injective if and only if given any right ideal $I \subseteq R$ and any R-homomorphism $\sigma: I \to Q$, there exists an R-homomorphism $\sigma^*: R \to Q$ that extends σ.*

PROOF Suppose first that Q is injective. Since I is a submodule of R, any map $\sigma: I \to Q$ extends to a map $\sigma^*: R \to Q$.

Conversely, assume that Q has this extension property and let

$$\begin{array}{ccccc} & & Q & & \\ & & \alpha \uparrow & & \\ 0 & \to & W & \to & V \end{array}$$

be given with W a submodule of V. Consider the set of all pairs (C, φ) where $W \subseteq C \subseteq V$ and $\varphi: C \to Q$ extends α to the submodule C. We say that $(C_1, \varphi_1) \leq (C_2, \varphi_2)$ if and only if $C_1 \subseteq C_2$ and $\varphi_1 = (\varphi_2)_{C_1}$, the restriction of φ_2 to C_1. Note that any increasing chain $\{ (C_i, \varphi_i) \mid i \in \mathcal{I} \}$ of such pairs is bounded above. Indeed, an appropriate upper bound is (C', φ'), where $C' = \bigcup_i C_i$ and $\varphi'_{C_i} = \varphi_i$. Thus, since the set of pairs is nonempty, Zorn's Lemma implies that there exists (C, φ) maximal in this ordering. The goal is to show that $C = V$.

Let $a \in V$ and set $I = \{ r \in R \mid ar \in C \}$. Then I is a right ideal of R and we have an R-homomorphism $\sigma: I \to Q$ given by $\sigma(r) = \varphi(ar)$. By hypothesis, σ extends to $\sigma^*: R \to Q$ and we define $\varphi^*: C + aR \to Q$ by $c + ar \mapsto \varphi(c) + \sigma^*(r)$. Then φ^* is clearly an R-homomorphism extending φ provided we show that it is well defined. Thus suppose $c_1 + ar_1 = c_2 + ar_2$ with $c_1, c_2 \in C$ and $r_1, r_2 \in R$. Then $a(r_1 - r_2) = c_2 - c_1 \in C$, so $r_1 - r_2 \in I$ and hence

$$\begin{aligned} \sigma^*(r_1) - \sigma^*(r_2) &= \sigma^*(r_1 - r_2) = \sigma(r_1 - r_2) \\ &= \varphi\big(a(r_1 - r_2)\big) = \varphi(c_2 - c_1) \\ &= \varphi(c_2) - \varphi(c_1) \end{aligned}$$

Thus $\varphi(c_1) + \sigma^*(r_1) = \varphi(c_2) + \sigma^*(r_2)$ as required.

Since $(C, \varphi) \leq (C + aR, \varphi^*)$, the maximality of (C, φ) implies that $a \in C$. In particular, since $a \in V$ is arbitrary, we conclude that $C = V$ and the lemma is proved. □

Let us see what this says when $R = \mathbb{Z}$ is the ring of integers.

DEFINITION Let D be an additive abelian group. Then D is said to be *divisible* if, for each $d \in D$ and $0 \neq n \in \mathbb{Z}$, there exists $d' \in D$ with $d'n = d$. Note that we do not require d' to be unique. As an example of a divisible group we could take D to be the field of rationals $\mathbb{Q}$ or perhaps $F^\bullet$, the multiplicative group of nonzero elements of the algebraically closed field F. Of particular importance is $\mathbb{D} = \mathbb{Q}/\mathbb{Z}$. Note that every $\mathbb{Z}$-module is an abelian group and that conversely every abelian group is a $\mathbb{Z}$-module.

LEMMA 21.4 *A $\mathbb{Z}$-module D is injective if and only if it is divisible.*

PROOF The ideals of $\mathbb{Z}$ are all of the form $n\mathbb{Z}$. If $\sigma: n\mathbb{Z} \to D$ is given with $\sigma(n) = d$, then σ can be extended to $\sigma^*: \mathbb{Z} \to D$ if and only if there exists $d' = \sigma^*(1)$ with $d'n = d$. □

As we observed before, any abelian group V can be viewed as a left or right $\mathbb{Z}$-module. Indeed, if V is a left R-module, then it is an $(R, \mathbb{Z})$-bimodule, and if W is a right R-module, then it is a $(\mathbb{Z}, R)$-bimodule. It follows that, for any abelian group D, $\mathrm{Hom}_{\mathbb{Z}}({}_RV, D)$ is a right R-module and $\mathrm{Hom}_{\mathbb{Z}}(W_R, D)$ is a left R-module.

LEMMA 21.5 *Let R be a ring, D be a divisible abelian group, and F be a free left R-module. Then $\mathrm{Hom}_{\mathbb{Z}}(F, D)$ is an injective right R-module.*

PROOF Let $\{ f_j \mid j \in \mathcal{J} \}$ be a left R-basis for F, let $A = A_R$ be a right ideal of R, and let $\varphi: A \to \mathrm{Hom}_{\mathbb{Z}}(F, D)$ be a right R-module homomorphism, which we denote by $a \mapsto \varphi_a$. The goal is to show that φ extends to a map $\varphi^*: R \to \mathrm{Hom}_{\mathbb{Z}}(F, D)$ and for this we need to determine the image of 1.

To this end, we consider the additive subgroup AF of F. Since $F = \cdot\sum_j Rf_j$, it follows that $AF = \cdot\sum_j Af_j$ and hence we can define $\sigma: AF \to D$ by

$$\sigma: \sum_j a_j f_j \mapsto \sum_j \varphi_{a_j}(f_j)$$

where, of course, each $a_j \in A$. This is a well-defined map, easily seen to be additive, and thus σ is a $\mathbb{Z}$-module homomorphism. Since D is divisible and therefore injective as a $\mathbb{Z}$-module, σ extends to the $\mathbb{Z}$-homomorphism $\sigma^*: F \to D$.

Now define $\varphi^*: R \to \mathrm{Hom}_{\mathbb{Z}}(F, D)$ by $r \mapsto \varphi_r^* = \sigma^* r$. We claim that φ^* extends φ. Indeed, if $a \in A$, then, for any j and $r \in R$, we have

$$\varphi_a^*(rf_j) = (\sigma^* a)(rf_j) = \sigma^*(arf_j)$$

But $ar \in A$, so $arf_j \in AF$; since $\sigma^*_{AF} = \sigma$, we have

$$\varphi^*_a(rf_j) = \sigma(arf_j) = \varphi_{ar}(f_j)$$

Furthermore, $\varphi\colon A \to \mathrm{Hom}_{\mathbb{Z}}(F, D)$ is an R-homomorphism, so $\varphi_{ar} = \varphi_a r$ and hence

$$\varphi^*_a(rf_j) = (\varphi_a r)(f_j) = \varphi_a(rf_j)$$

Thus φ^* extends φ and Baer's Criterion yields the result. □

An alternate proof of the preceding is sketched in Exercise 7. The following is clearly the injective dual of Lemma 2.9(i).

THEOREM 21.6 (Baer's Theorem) *Every R-module is contained in an injective R-module.*

PROOF Let W be the given right R-module, let $\mathbb{D} = \mathbb{Q}/\mathbb{Z}$, and recall that $\mathbb{D}$ is a divisible abelian group. If $V = \mathrm{Hom}_{\mathbb{Z}}(W, \mathbb{D})$, then V is a left R-module and there exists an R-epimorphism $\gamma\colon F \to V$ with F a free left R-module. Thus, by Lemma 21.1(ii), $\hat{\gamma}\colon \mathrm{Hom}_{\mathbb{Z}}(V, \mathbb{D}) \to \mathrm{Hom}_{\mathbb{Z}}(F, \mathbb{D})$ is a right R-module monomorphism. In other words, we have embedded $\mathrm{Hom}_{\mathbb{Z}}(V, \mathbb{D})$ into $\mathrm{Hom}_{\mathbb{Z}}(F, \mathbb{D})$ and we know, by the previous lemma, that $\mathrm{Hom}_{\mathbb{Z}}(F, \mathbb{D})$ is injective. Thus it suffices to show that W embeds in $\mathrm{Hom}_{\mathbb{Z}}(V, \mathbb{D})$ and this is the usual double dual argument.

Define $\theta\colon W \to \mathrm{Hom}_{\mathbb{Z}}(V, \mathbb{D})$ by $\theta_w(v) = (w)v$ for all $v \in V = \mathrm{Hom}_{\mathbb{Z}}(W, \mathbb{D})$, acting on the right. Then θ is clearly additive and for any $r \in R$ we have

$$\begin{aligned}(\theta_w r)(v) &= \theta_w(rv) = (w)(rv)\\ &= (wr)v = \theta_{wr}(v)\end{aligned}$$

Thus θ is an R-module homomorphism and we need only show that θ is one-to-one. To this end, let $0 \neq w \in W$ and consider $\mathbb{Z}w \subseteq W$. If $\mathbb{Z}w \cong \mathbb{Z}$, map w to any nonzero element of $\mathbb{D}$. If $\mathbb{Z}w \cong \mathbb{Z}/\mathbb{Z}n$ with $n \neq 0$, map w to $1/n \in \mathbb{D}$. In either case, we obtain an abelian group homomorphism $\tau\colon \mathbb{Z}w \to \mathbb{D}$ with $(w)\tau \neq 0$. Furthermore, $\mathbb{D}$ is divisible, so τ extends to $v = \tau^* \in \mathrm{Hom}_{\mathbb{Z}}(W, \mathbb{D}) = V$. But then $\theta_w(v) = (w)v = (w)\tau \neq 0$ and hence $\theta_w \neq 0$. Thus W embeds isomorphically into $\mathrm{Hom}_{\mathbb{Z}}(V, \mathbb{D})$ and the result follows. □

Now that we know that injective modules are plentiful, it is worthwhile to list some of their basic properties. Suppose that $\{V_i \mid i \in \mathcal{I}\}$

is a family of R-modules. Then we let $V = \prod_{i\in\mathcal{I}} V_i$ denote their *strong*, or *complete, direct sum.* Thus the elements of V are $\mathcal{I}$-tuples $\prod_i v_i$ with $v_i \in V_i$ and with no assumption on the number of nonzero components. Of course, addition and scalar multiplication in V are defined componentwise and, if $\mathcal{I}$ is finite, then $\prod_i V_i = \oplus \sum_i V_i$. Note that $\prod_i V_i$ is also called the *direct product* of the V_i.

LEMMA 21.7 *i. If Q is an injective R-module and if A is a direct summand of Q, then A is injective.*

ii. If $\{ Q_i \mid i \in \mathcal{I} \}$ is a family of injective R-modules, then $\prod_{i\in\mathcal{I}} Q_i$ is injective.

PROOF (i) We can assume $A \subseteq Q$ and that there is an R-homomorphism $\pi: Q \to A$ that is the identity on A. Let $W \subseteq V$ be R-modules and let $\theta: W \to A$ be given. Then $\theta: W \to Q$ and, since Q is injective, θ extends to $\theta^*: V \to Q$. Finally, $\pi\theta^*: V \to A$ extends the map $\theta: W \to A$.

(ii) Let $W \subseteq V$ and suppose that $\theta: W \to Q = \prod_i Q_i$ is given. Then, for all $w \in W$, we have $\theta(w) = \prod_i \theta_i(w)$, where $\theta_i: W \to Q_i$ is an R-homomorphism. Since Q_i is injective, θ_i extends to $\theta_i^*: V \to Q_i$ and we can let $\theta^*: V \to Q$ be given by $\theta^*(v) = \prod_i \theta_i^*(v)$ for all $v \in V$. □

The proof of (ii) fails for direct sums, since it is quite possible for $\theta_i^*(v)$ to be nonzero for infinitely many i. We discuss this question in more detail later on. Finally, we have:

LEMMA 21.8 *An R-module Q is injective if and only if it is a direct summand of every module which contains it.*

PROOF Let Q be injective and suppose that $Q \subseteq V$. Then the identity map $\sigma: Q \to Q$ extends to a map $\sigma^*: V \to Q$ and thus $V = Q \dotplus \mathrm{Ker}(\sigma^*)$. Conversely, assume that Q is a direct summand of all larger modules and embed Q in an injective module Q'. Then $Q \mid Q'$, so Q is injective by the previous lemma. □

EXERCISES

1. Verify all the basic bimodule properties of $\mathrm{Hom}_R(A, B)$ as described in the beginning of this chapter.
2. Prove that a homomorphic image of a divisible group is divisible. Conclude that a nonzero divisible group has no proper subgroup of finite index. In particular, it is not true that every $\mathbb{Z}$-module is a homomorphic image of an injective $\mathbb{Z}$-module.

3. Let K be a field and suppose that R is a K-algebra. Then any R-module V is a K-vector space on either side and thus V_R is a (K,R)-bimodule. Show that the proofs of Lemma 21.5 and Theorem 21.6 carry over in this context using $\mathrm{Hom}_K(-,K)$ rather than $\mathrm{Hom}_{\mathbb{Z}}(-,\mathbb{D})$. Conclude that if $\dim_K V < \infty$, then V embeds in an injective R-module that is also finite dimensional over K.
4. Let R and S be rings and let A_R, ${}_RB_S$ and D_S be appropriate modules. Prove that there exists an isomorphism

$$\tilde{}: \mathrm{Hom}_R\big(A_R, \mathrm{Hom}_S({}_RB_S, D_S)\big) \to \mathrm{Hom}_S(A_R \otimes {}_RB_S, D_S)$$

To define $\tilde{}$, let $\theta \in \mathrm{Hom}_R\big(A, \mathrm{Hom}_S(B,D)\big)$ and denote the image of $a \in A$ under θ by θ_a. Show that the map $A \times B \to D$ given by $(a,b) \mapsto \theta_a(b)$ is balanced and hence gives rise to $\tilde{\theta} \in \mathrm{Hom}_S(A \otimes B, D)$. For the reverse map, let $\phi \in \mathrm{Hom}_S(A \otimes B, D)$ and, for each $a \in A$, define $\phi_a\colon B \to D$ by $\phi_a(b) = \phi(a \otimes b)$. Deduce that $\phi_a \in \mathrm{Hom}_S(B,D)$ and that the map $a \mapsto \phi_a$ belongs to $\mathrm{Hom}_R\big(A, \mathrm{Hom}_S(B,D)\big)$.
5. Prove that $\tilde{}$ as just defined is functorial. Specifically, suppose that $\alpha\colon A \to A'$ is an R-homomorphism and note that $\alpha \otimes 1\colon A \otimes B \to A' \otimes B$ is an S-homomorphism. Show that the diagram

$$\begin{array}{ccc} \mathrm{Hom}_R\big(A', \mathrm{Hom}_S(B,D)\big) & \xrightarrow{\ \tilde{}\ } & \mathrm{Hom}_S(A' \otimes B, D) \\ \downarrow \hat{\alpha} & & \downarrow (\alpha \otimes 1)\hat{} \\ \mathrm{Hom}_R\big(A, \mathrm{Hom}_S(B,D)\big) & \xrightarrow{\ \tilde{}\ } & \mathrm{Hom}_S(A \otimes B, D) \end{array}$$

commutes.

The remaining exercises describe the surprising relationship, discovered by Lambek, between the injective R-modules and the flat R-modules. If A is an abelian group, write $A^* = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{D})$, where $\mathbb{D} = \mathbb{Q}/\mathbb{Z}$.

6. If $\sigma\colon A \to B$ is a homomorphism of abelian groups, show that σ is one-to-one or onto if and only if $\hat{\sigma}\colon B^* \to A^*$ is onto or one-to-one, respectively.
7. Let F be a left R-module. Prove that F is flat if and only if F^* is an injective right R-module. To this end, suppose that $\alpha\colon A_R \to A'_R$ is a monomorphism and apply Exercises 4 and 5 with $B = F$, $S = \mathbb{Z}$, and $D = \mathbb{D}$ to obtain the commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}_R(A', F^*) & \xrightarrow{\sim} & (A' \otimes_R F)^* \\ \downarrow \hat{\alpha} & & \downarrow (\alpha\otimes 1)\hat{} \\ \mathrm{Hom}_R(A, F^*) & \xrightarrow{\sim} & (A \otimes_R F)^* \end{array}$$

where each $\tilde{}$ is an isomorphism. Now observe, by the previous exercise, that $\alpha \otimes 1$ is a monomorphism if and only if $(\alpha \otimes 1)\hat{}$ is onto and hence if and only if $\hat{\alpha}$ is onto. The definition of flatness and Lemma 21.2(ii) yield the result.

Now let R be a von Neumann regular ring. Thus, by Exercises 5.5 and 5.7, every finitely generated right or left ideal of R is generated by an idempotent.

8. Suppose ${}_RV$ is a left R-module and that D is an abelian group. Let A_R be a right ideal of R and let $\sigma\colon A_R \to \mathrm{Hom}_{\mathbb{Z}}({}_RV, D)$ be an R-homomorphism, which we denote by $a \mapsto \sigma_a$. Show that the abelian group homomorphism $\tau\colon AV \to D$ determined by $av \mapsto \sigma_a(v)$ is well defined. To this end, suppose $\sum_i a_i v_i = \sum_j b_j w_j$ with $a_i, b_j \in A$ and $v_i, w_j \in V$. Then $\sum_i a_i R + \sum_j b_j R = eR$ for some idempotent e and hence

$$\sigma_{a_i}(v_i) = \sigma_{ea_i}(v_i) = (\sigma_e a_i)(v_i) = \sigma_e(a_i v_i)$$

9. If $\sigma\colon A_R \to \mathrm{Hom}_{\mathbb{Z}}({}_RV, D)$ is as just described and if D is a divisible abelian group, show that there exists $\tau \in \mathrm{Hom}_{\mathbb{Z}}(V, D)$ with $\sigma_a = \tau a$ for all $a \in A$. Conclude from Baer's Criterion that $\mathrm{Hom}_{\mathbb{Z}}(V, D)$ is an injective right R-module.
10. Prove that all right and left R-modules are flat. This is the full converse to Exercise 9.3.

22. Injective Dimension

In this chapter we explore the injective analogs of certain projective concepts. In particular, we define the injective dimension of a module and the injective global dimension of a ring. However, for reasons that will soon become apparent, these dimensions do not lead to a spate of additional computations. We start with:

LEMMA 22.1 (Injective Schanuel's Lemma) *Let R be a ring and let*

$$0 \to A \to Q \to B \to 0$$
$$0 \to A \to Q' \to B' \to 0$$

be short exact sequences of R-modules with Q and Q' injective. Then we have $B \oplus Q' \cong B' \oplus Q$.

PROOF It suffices to assume that $A \subseteq Q$ and $A \subseteq Q'$. Then $Q \oplus Q'$ contains the submodule $\bar{A} = \{ a \oplus a \mid a \in A \}$ and we set $W = (Q \oplus Q')/\bar{A}$.

Since the map $A \oplus Q' \to Q'$ given by $a \oplus q' \mapsto -a + q'$ is an epimorphism with kernel $\bar{A}$, it follows that $Q' \cong (A \oplus Q')/\bar{A} = V'$. Furthermore,

$$W/V' \cong (Q \oplus Q')/(A \oplus Q') \cong Q/A \cong B$$

Finally, since $V' \cong Q'$ is injective, Lemma 21.8 implies that $V' \mid W$ and, for instance, $W = V' \dotplus C$. Then $C \cong W/V' \cong B$ and we conclude that $W = V' \dotplus C \cong Q' \oplus B$. Similarly, $W \cong Q \oplus B'$. □

As with projective modules, this leads to the following

DEFINITION Let A and A' be R-modules. We write $A \sim A'$ if and only if there exist injective R-modules Q and Q' with $A \oplus Q \cong A' \oplus Q'$. Obviously $\sim$

is an equivalence relation. Indeed, if $A \sim B$ and $B \sim C$, then $A \oplus Q_1 \cong B \oplus Q_1'$ and $B \oplus Q_2 \cong C \oplus Q_2'$ for suitable injective modules Q_1, Q_1', Q_2, Q_2'. Thus

$$\begin{aligned} A \oplus (Q_1 \oplus Q_2) &\cong B \oplus Q_1' \oplus Q_2 \\ &\cong B \oplus Q_2 \oplus Q_1' \cong C \oplus (Q_2' \oplus Q_1') \end{aligned}$$

and $A \sim C$, by Lemma 21.7(ii). We use $[A]$ to denote the equivalence class of A. Since any direct summand of an injective module is injective, by Lemma 21.7(i), it follows that $[0]$ is precisely the set of all injective R-modules.

We need a slight refinement of the preceding lemma.

LEMMA 22.2 *Suppose we are given the short exact sequences*

$$0 \to A \to Q \to B \to 0$$
$$0 \to A' \to Q' \to B' \to 0$$

with Q and Q' injective. If $A \sim A'$, then $B \sim B'$.

PROOF Since $A \sim A'$, we have $A \oplus Q_1 \cong A' \oplus Q_1'$ for suitable injective modules Q_1 and Q_1'. Thus we obtain the exact sequences

$$0 \to A \oplus Q_1 \to Q \oplus Q_1 \to B \oplus 0 \to 0$$
$$0 \to A' \oplus Q_1' \to Q' \oplus Q_1' \to B' \oplus 0 \to 0$$

and, since $A \oplus Q_1 \cong A' \oplus Q_1'$, Lemma 22.1 yields

$$B \oplus (Q' \oplus Q_1') \cong B' \oplus (Q \oplus Q_1)$$

Hence $B \sim B'$ as required. □

DEFINITION Let A be any R-module. By Baer's Theorem, there exists a short exact sequence $0 \to A \to Q \to B \to 0$ with Q injective and we define the *cokernel map* $\mathcal{C}$ by $\mathcal{C}\colon [A] \mapsto [B]$. In view of the preceding lemma, $\mathcal{C}$ is a well defined map on the $\sim$ equivalence classes of R-modules. That is, $\mathcal{C}$ is independent of the representative of the class and of the particular exact sequence chosen. Since $0 \to 0 \to 0 \to 0 \to 0$ is exact, we have $\mathcal{C}[0] = [0]$.

The *injective dimension* of A, written $\mathrm{id}_R A = \mathrm{id}\, A$, is defined to be the minimal integer n with $\mathcal{C}^n[A] = [0]$. Of course, if no such integer exists, then $\mathrm{id}\, A = \infty$. Modules with finite injective dimension are in

some sense "close to" the injective ones. For example, $\operatorname{id} A = 0$ if and only if A is injective.

Finally, the (right) *injective global dimension* of R is defined to be the supremum of the injective dimensions of all right R-modules. Thus $\operatorname{inj\,gl\,dim} R$ is either an integer or the symbol ∞.

Since there are injective modules that are not projective and projective modules that are not injective, it is obvious that the injective and projective dimensions of a module are not necessarily the same. On the other hand, as we will soon see, the injective and projective global dimensions of a ring are identical.

DEFINITION Let A_R and B_R be R-modules. We say that $\mathrm{E}(A, B) = 0$ if and only if every short exact sequence of the form

$$0 \to B \to X \to A \to 0$$

splits. Thus, by Theorem 2.8, the R-module P is projective if and only if $\mathrm{E}(P, B) = 0$ for all B. Similarly, by Lemma 21.8, the R-module Q is injective if and only if $\mathrm{E}(A, Q) = 0$ for all A.

Although we only require the definition $\mathrm{E}(A, B) = 0$ to prove equality of global dimensions, it is certainly worthwhile to describe $\mathrm{E}(A, B)$ is general. We sketch its construction next, relegating most of the tedious verifications to the exercises.

DEFINITION If A and B are R-modules, then an *extension of B by A* is a short exact sequence of the form

$$0 \to B \xrightarrow{\tau} X \xrightarrow{\sigma} A \to 0 \qquad (*)$$

If

$$0 \to B \xrightarrow{\tau'} X' \xrightarrow{\sigma'} A \to 0 \qquad (**)$$

is a second extension, then $(**)$ is said to be *equivalent* to $(*)$ if and only if there exists an isomorphism $\psi\colon X \to X'$ such that the diagram

$$\begin{array}{ccccccccc}
0 & \to & B & \xrightarrow{\tau} & X & \xrightarrow{\sigma} & A & \to & 0 \\
 & & \downarrow 1_B & & \downarrow \psi & & \downarrow 1_A & & \\
0 & \to & B & \xrightarrow{\tau'} & X' & \xrightarrow{\sigma'} & A & \to & 0
\end{array}$$

commutes. Of course, 1_B and 1_A denote the identity maps on B and A, respectively. It is easy to see that this is an equivalence relation and that the split extensions form a single equivalence class.

Again, if $(*)$ and $(**)$ are given, then we can define the *Baer sum* of these extensions as follows. First, let M and $\bar{B}$ be the submodules of $X \oplus X'$ given by $M = \{ x \oplus x' \mid \sigma x = \sigma' x' \}$ and $\bar{B} = \{ \tau b \oplus (-\tau' b) \mid b \in B \}$. Then $\bar{B} \subseteq \tau B \oplus \tau' B \subseteq M$ and we obtain the short exact sequence

$$0 \to (\tau B \oplus \tau' B)/\bar{B} \to M/\bar{B} \xrightarrow{\eta} A \to 0$$

where $\eta\colon (x \oplus x') + \bar{B} \mapsto \sigma x = \sigma' x'$. Since $(\tau B \oplus \tau' B)/\bar{B} \cong B$, we then obtain the extension

$$0 \to B \xrightarrow{\xi} Z \xrightarrow{\eta} A \to 0$$

where

$$\xi\colon b \mapsto (\tau b \oplus 0) + \bar{B} \in (\tau B \oplus \tau' B)/\bar{B} \subseteq M/\bar{B} = Z$$

By definition, this extension is the Baer sum of $(*)$ and $(**)$, and it is easily seen that equivalent extensions have equivalent Baer sums.

We can now let $\mathrm{E}(A, B)$ denote the set of all equivalence classes of extensions of B by A endowed with the Baer sum binary operation. Then $\mathrm{E}(A, B)$ turns out to be an additive abelian group called the *group of extensions* of B by A. Indeed, one easily verifies the commutative and associative laws and the fact that the equivalence class of split extensions is the zero element. Finally, the negative of the class of the extension $(*)$ is the class of

$$0 \to B \xrightarrow{\tau} X \xrightarrow{-\sigma} A \to 0 \qquad (-*)$$

where $(-\sigma)x = -(\sigma x)$ for all $x \in X$. To see this, note that the corresponding submodules M and $\bar{B}$ of $X \oplus X$ for the Baer sum can be characterized by

$$M = \{ x_1 \oplus x_2 \mid x_1, x_2 \in X \text{ and } x_1 + x_2 \in \tau(B) \}$$

and $\bar{B} = \{ \tau b \oplus (-\tau b) \mid b \in B \}$. In particular, if $C = \{ x \oplus (-x) \mid x \in X \}$, then C is a submodule of M with $C + (\tau B \oplus \tau B) = M$ and $C \cap (\tau B \oplus \tau B) = \bar{B}$. Thus

$$M/\bar{B} = (\tau B \oplus \tau B)/\bar{B} \dotplus C/\bar{B}$$

and the Baer sum of $(*)$ and $(-*)$ is split, as required.

Notice that $\mathrm{E}(A, B) = 0$ does indeed mean that all extensions of B by A are split.

Let A_R and B_R be R-modules. In homological algebra there is an interesting and important sequence of abelian groups constructed from A and B. These are denoted by $\mathrm{Ext}^n(A, B)$ for $n = 0, 1, 2, \ldots$ and they start with $\mathrm{Ext}^0(A, B) = \mathrm{Hom}_R(A, B)$. They are used to compensate for the fact that Hom is not an exact functor and their construction is analogous to that of Tor. Specifically, as we will see in the exercises, they can be constructed from either a projective resolution of A or an injective resolution of B and the answer is the same in either case. Furthermore, it turns out that $\mathrm{E}(A, B) \cong \mathrm{Ext}^1(A, B)$. The proof of the following proposition contains within it aspects of proof of this isomorphism.

PROPOSITION 22.3 *Let*

$$0 \to C \to P \xrightarrow{\alpha} A \to 0$$

$$0 \to B \to Q \xrightarrow{\beta} D \to 0$$

be short exact sequences of R-modules with P projective and Q injective. Then $\mathrm{E}(A, D) = 0$ if and only if $\mathrm{E}(C, B) = 0$.

PROOF We can assume that $C \subseteq P$ and that $B \subseteq Q$. The proofs of the two implications are obviously parallel. We consider each in turn.

CASE 1 $\mathrm{E}(C, B) = 0$ *implies* $\mathrm{E}(A, D) = 0$.

PROOF Let $0 \to D \to X \xrightarrow{\sigma} A \to 0$ be an extension of D by A and assume for convenience that $D \subseteq X$. Since P is projective, it follows that there exists a homomorphism $\theta: P \to X$ such that the diagram

$$\begin{array}{ccccccccc} 0 & \to & C & \to & P & \xrightarrow{\alpha} & A & \to & 0 \\ & & \downarrow \theta & & \downarrow \theta & & \downarrow 1_A & & \\ 0 & \to & D & \to & X & \xrightarrow{\sigma} & A & \to & 0 \end{array}$$

commutes. Indeed, since $\sigma: X \to A$ is surjective, $\theta: P \to X$ exists. Furthermore, $\sigma\theta(C) = \alpha(C) = 0$, so $\theta: C \to \mathrm{Ker}(\sigma) = D$ as required.

Next, let M be the submodule of $Q \oplus C$ given by $M = \{ q \oplus c \mid \beta q = \theta c \}$. If $\eta: B \to M$ and $\pi: M \to C$ are given by $\beta: b \mapsto b \oplus 0$ and $\pi: q \oplus c \mapsto c$, then it is easy to see that

$$0 \to B \xrightarrow{\eta} M \xrightarrow{\pi} C \to 0$$

is exact. Indeed, since β is onto, it follows that for every $c \in C$, there exists $q \in Q$ with $\beta q = \theta c$ and hence π is onto. Furthermore,

$$\mathrm{Ker}(\pi) = \{ q \oplus 0 \mid \beta q = 0 \} = \{ b \oplus 0 \mid b \in B \} = \mathrm{Im}(\eta)$$

and therefore we have constructed an extension of B by C. But $\mathrm{E}(C, B) = 0$ by assumption, so the sequence splits and an appropriate back map $C \to M$ exists. In view of the nature of π, this map has the form $c \mapsto \gamma c \oplus c \in M$, where $\gamma: C \to Q$. Thus, by definition of M, we must have $\beta\gamma = \theta$.

Now $\gamma: C \to Q$, Q is injective, and $C \subseteq P$. Thus γ extends to a map $\gamma^*: P \to Q$ and we let $\phi: P \to D$ be the composite map $\phi: P \xrightarrow{\gamma^*} Q \xrightarrow{\beta} D$. By definition of γ, this means that ϕ restricted to C is $\beta\gamma = \theta$. Equivalently, we see that the diagram

$$\begin{array}{ccccc} 0 & \to & C & \to & P \\ & & {\scriptstyle\theta}\downarrow & \swarrow{\scriptstyle\phi} & \\ & & D & & \end{array}$$

commutes. We now use ϕ to construct a back map $\tau: X \to D$ as follows.

Let $x \in X$. Since α is onto, there exists $p \in P$ with $\sigma x = \alpha p$ and we set $\tau x = x - \theta p + \phi p \in X$. Note that p is uniquely determined by x up to a summand $c \in C$. Thus, since $\theta c = \phi c$, it follows that τ is a well defined R-endomorphism of X. Next observe that

$$\sigma\tau x = \sigma x - \sigma\theta p + \sigma\phi p = \alpha p - \sigma\theta p = 0$$

since $\sigma\phi = 0$ and $\sigma x = \alpha p$. Thus $\tau x \in \mathrm{Ker}(\sigma) = D$ and $\tau \in \mathrm{Hom}_R(X, D)$. Finally, if $x \in D \subseteq X$, then $\sigma x = 0$, so, using $p = 0$ in the definition of τ, we obtain $\tau x = x$. In other words, $\tau: X \to D$ is the identity on D and therefore yields a splitting of the exact sequence $0 \to D \to X \to A \to 0$. Since the latter sequence was an arbitrary extension of D by A, we conclude that $\mathrm{E}(A, D) = 0$. □

CASE 2 $\mathrm{E}(A, D) = 0$ *implies* $\mathrm{E}(C, B) = 0$.

PROOF This time, let $0 \to B \to Y \xrightarrow{\sigma} C \to 0$ be an extension of B by C and assume for convenience that $B \subseteq Y$. Since Q is injective, it follows that there exist homomorphisms $\theta: Y \to Q$ and $\bar{\theta}: C \to D$ such that the

diagram

$$\begin{array}{ccccccccc} 0 & \to & B & \to & Y & \xrightarrow{\sigma} & C & \to & 0 \\ & & \downarrow 1_B & & \downarrow \theta & & \downarrow \bar{\theta} & & \\ 0 & \to & B & \to & Q & \xrightarrow{\beta} & D & \to & 0 \end{array}$$

commutes. Indeed, the map $B \xrightarrow{1_B} B \subseteq Q$ extends to $\theta: Y \to Q$. Furthermore, $\beta\theta(B) = \beta(B) = 0$, so $\beta\theta: Y \to D$ factors through $C \cong Y/B$ and $\bar{\theta}$ exists.

Next, we form the R-module $P \oplus D$ and let $\bar{C}$ be its submodule $\bar{C} = \{(-c) \oplus \bar{\theta}c \mid c \in C\}$. Since the epimorphism $P \oplus D \to A$ given by $p \oplus d \mapsto \alpha p$ has $\bar{C}$ in its kernel, we therefore obtain an R-epimorphism $\pi: (P \oplus D)/\bar{C} \to A$ given by $\pi: (p \oplus d) + \bar{C} \mapsto \alpha p$. Furthermore, if $\eta: D \to (P \oplus D)/\bar{C}$ is defined by $\eta: d \mapsto (0 \oplus d) + \bar{C}$, then we obtain the short exact sequence

$$0 \to D \xrightarrow{\eta} (P \oplus D)/\bar{C} \xrightarrow{\pi} A \to 0$$

Indeed, η is clearly one-to-one and $\mathrm{Ker}(\pi) = (C \oplus D)/\bar{C} = \mathrm{Im}(\eta)$. Thus the above short exact sequence is an extension of D by A and, since $\mathrm{E}(A, D) = 0$, the sequence splits and there is a back map $(P \oplus D)/\bar{C} \to D$. In view of the nature of η, this map must be given by $(p \oplus d) + \bar{C} \mapsto \delta p + d$, where $\delta: P \to D$. But this homomorphism vanishes on $\bar{C}$ and hence we have $\delta c = \bar{\theta}c$ for all $c \in C$.

Now $\beta: Q \to D$ is an epimorphism and $\delta: P \to D$. Thus since P is projective, there exists a homomorphism $\delta^*: P \to Q$ with $\beta\delta^* = \delta$. Furthermore, if we let ϕ denote δ^*_C, the restriction of δ^* to C, then $\beta\phi = \delta_C = \bar{\theta}$. Equivalently, we see that the diagram

$$\begin{array}{ccccc} & & C & & \\ & \phi \swarrow & \downarrow \bar{\theta} & & \\ Q & \xrightarrow{\beta} & D & \to & 0 \end{array}$$

commutes. We now use ϕ to construct a back map $\tau: Y \to B$ as follows.

Let $y \in Y$ and set $\tau y = \theta y - \phi\sigma y \in Q$. Since $\beta\phi = \bar{\theta}$ and $\beta\theta = \bar{\theta}\sigma$, we have

$$\beta\tau y = \beta\theta y - \beta\phi\sigma y = \beta\theta y - \bar{\theta}\sigma y = 0$$

and hence $\tau y \in \mathrm{Ker}(\beta) = B$. It is now clear that $\tau \in \mathrm{Hom}_R(Y, B)$. Furthermore, if $y \in B \subseteq Y$, then $\sigma y = 0$ so $\tau y = \theta y = y$, since $\theta_B = 1_B$. Thus τ is the identity on B and therefore yields a splitting of $0 \to B \to Y \to C \to 0$. Since the latter sequence was an arbitrary extension of B by C, we conclude that $\mathrm{E}(C, B) = 0$. □

With this, we can now quickly prove:

THEOREM 22.4 *If R is any ring, then* $\mathrm{inj\,gl\,dim}\, R = \mathrm{gl\,dim}\, R$.

PROOF For any integer $n \geq 0$, we will show below that $\mathrm{inj\,gl\,dim}\, R \leq n$ if and only $\mathrm{gl\,dim}\, R \leq n$. This will clearly yield the result. To avoid confusion, we use $[-]_{\mathrm{i}}$ to denote equivalence classes under the injective equivalence of this chapter and $[-]_{\mathrm{p}}$ to denote equivalence classes under the projective equivalence of Chapter 8.

Fix n and let A and B be any right R-modules. We can then define the R-modules A_i, P_i, B_i, Q_i inductively so that $A_0 = A$, $B_0 = B$, P_i is projective, Q_i is injective, and the sequences

$$0 \to A_{i+1} \to P_i \to A_i \to 0$$
$$0 \to B_j \to Q_j \to B_{j+1} \to 0$$

are exact for $i, j = 0, 1, \ldots, n-1$. In particular, $[A_n]_{\mathrm{p}} = \mathcal{K}^n[A]_{\mathrm{p}}$, $[B_n]_{\mathrm{i}} = \mathcal{C}^n[B]_{\mathrm{i}}$ and, by the preceding proposition, $\mathrm{E}(A_i, B_{j+1}) = 0$ if and only if $\mathrm{E}(A_{i+1}, B_j) = 0$. It follows by restricting our attention to $i + j + 1 = n$ that $\mathrm{E}(A, B_n) = 0$ if and only if $\mathrm{E}(A_n, B) = 0$.

Finally, suppose $\mathrm{gl\,dim}\, R \leq n$. Then $A_n \in \mathcal{K}^n[A]_{\mathrm{p}}$ is projective, so $\mathrm{E}(A_n, B) = 0$. Hence $\mathrm{E}(A, B_n) = 0$ by the preceding and, since this holds for all A, we conclude that B_n is injective. Thus $\mathrm{id}\, B \leq n$ and, since this holds for all such B, we have $\mathrm{inj\,gl\,dim}\, R \leq n$.

Conversely, suppose $\mathrm{inj\,gl\,dim}\, R \leq n$. This time, $B_n \in \mathcal{C}^n[B]_{\mathrm{i}}$ is injective, so $\mathrm{E}(A, B_n) = 0$. Hence $\mathrm{E}(A_n, B) = 0$ by the preceding and, since this holds for all B, we conclude that A_n is projective. Thus $\mathrm{pd}\, A \leq n$ and, since this holds for all such A, we have $\mathrm{gl\,dim}\, R \leq n$. As we mentioned earlier, this suffices to prove the result. □

EXERCISES

1. Let $\{ A_i \mid i \in \mathcal{I} \}$ be a collection of R-modules and set $A = \prod_i A_i$. Prove that $\mathrm{id}\, A = \sup \{ \mathrm{id}\, A_i \mid i \in \mathcal{I} \}$.
2. Suppose $0 \to A \to B \to C \to 0$ is an exact sequence of R-modules. Show that there exist modules D, E and Q with Q injective and sequences

$$0 \to B \to Q \to D \to 0$$
$$0 \to A \to Q \to E \to 0$$
$$0 \to C \to E \to D \to 0$$

that are exact. This is the injective analog of Lemma 8.6.

3. Suppose $0 \to A \to B \to C \to 0$ is exact. If any two of these modules have finite injective dimension, show that the third does also. Furthermore, prove that

$$\operatorname{id} A \leq \max\{1 + \operatorname{id} B, 1 + \operatorname{id} C\}$$
$$\operatorname{id} B \leq \max\{\operatorname{id} A, 1 + \operatorname{id} C\}$$
$$\operatorname{id} C \leq \max\{\operatorname{id} A, \operatorname{id} B\}$$

This is the injective analog of Lemma 8.7.

4. Verify the basic properties of $\mathrm{E}(A, B)$. In particular, show that the Baer sum respects the equivalence relation and that addition is associative and commutative. Furthermore, show that the split extensions form a single class, which corresponds to the zero element of $\mathrm{E}(A, B)$.
5. Let R be a ring. Prove directly, without using Theorem 22.4, that the following are equivalent.
   i. All right R-modules are injective.
   ii. All right ideals of R are injective.
   iii. R is a Wedderburn ring.
6. Let R be any ring. Show directly, without using Theorem 22.4, that the following are equivalent.
   i. Submodules of projective R-modules are projective.
   ii. Homomorphic images of injective R-modules are injective.

   For (i)⇒(ii), let Q be an injective module and U a submodule. Suppose $W \subseteq V$ and $\sigma: W \to Q/U$ are given. Map a projective module P onto V and let P' be the complete inverse image of W. By assumption, P' is also projective. Now σ extends to a map $\tau: P' \to W \to Q/U$ and, since P' is projective and $Q \to Q/U$ is onto, τ lifts to a map $\tau^*: P' \to Q$.

Let A_R and B_R be R-modules, let

$$\cdots \to P_2 \xrightarrow{\alpha_2} P_1 \xrightarrow{\alpha_1} P_0 \to A \to 0$$

be a projective resolution of A and let

$$0 \to B \to Q_0 \xrightarrow{\beta_1} Q_1 \xrightarrow{\beta_2} Q_2 \to \cdots$$

be an *injective resolution* of B. Of course, the latter is a long exact sequence with each Q_i injective. If we apply $\mathrm{Hom}_R(-, B)$ to the first sequence and $\mathrm{Hom}_R(A, -)$ to the second and then delete the $\mathrm{Hom}_R(A, B)$ term, we obtain the complexes

$$0 \xrightarrow{\hat{\alpha}_0} \mathrm{Hom}(P_0, B) \xrightarrow{\hat{\alpha}_1} \mathrm{Hom}(P_1, B) \xrightarrow{\hat{\alpha}_2} \mathrm{Hom}(P_2, B) \to \cdots$$

$$0 \xrightarrow{\hat{\beta}_0} \mathrm{Hom}(A, Q_0) \xrightarrow{\hat{\beta}_1} \mathrm{Hom}(A, Q_1) \xrightarrow{\hat{\beta}_2} \mathrm{Hom}(A, Q_2) \to \cdots$$

where, for convenience, we let $\hat{\alpha}_0$ and $\hat{\beta}_0$ denote the appropriate zero maps. The abelian groups $\mathrm{Ext}^n_R(A, B)$ are now defined by

$$\mathrm{Ext}^n_R(A, B) = \mathrm{Ext}^n(A, B) = \mathrm{Ker}(\hat{\beta}_{n+1})/\mathrm{Im}(\hat{\beta}_n)$$

for $n = 0, 1, 2, \ldots$. It can be shown that $\mathrm{Ext}^n(A, B)$ depends only on A and B and not on the particular injective resolution chosen for B. Furthermore,

$$\mathrm{Ext}^n_R(A, B) = \mathrm{Ext}^n(A, B) = \mathrm{Ker}(\hat{\alpha}_{n+1})/\mathrm{Im}(\hat{\alpha}_n)$$

7. Prove that $\mathrm{Ext}^0(A, B) \cong \mathrm{Hom}_R(A, B)$ and that Ext^n respects finite direct sums.
8. If $\mathrm{pd}\, A = k$ or $\mathrm{id}\, B = k$, show that $\mathrm{Ext}^n(A, B) = 0$ for all $n \geq k + 1$.
9. Suppose $0 \to C \to P \to A \to 0$ is exact with P projective. Prove that $\mathrm{Ext}^n(C, B) \cong \mathrm{Ext}^{n+1}(A, B)$ for all $n \geq 1$. Furthermore, show that

$$0 \to \mathrm{Hom}(A, B) \to \mathrm{Hom}(P, B) \to \mathrm{Hom}(C, B) \to \mathrm{Ext}^1(A, B) \to 0$$

is exact.

10. Suppose $0 \to B \to Q \to D \to 0$ is exact with Q injective. Prove that $\mathrm{Ext}^n_R(A, D) \cong \mathrm{Ext}^{n+1}(A, B)$ for all $n \geq 1$. Furthermore, show that

$$0 \to \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, Q) \to \mathrm{Hom}(A, D) \to \mathrm{Ext}^1(A, B) \to 0$$

is exact.

23. Essential Extensions

We now move on to those properties of injective modules that are more uniquely injective.

DEFINITION Let $W \subseteq V$ be R-modules. We say that V is an *essential extension* of W or that W is an *essential submodule* of V if and only if W has a nonzero intersection with every nonzero submodule of V. In other words, we write $W \operatorname{ess}_R V$ or $W \operatorname{ess} V$ if and only if $X \cap W \neq 0$ for all nonzero submodules $X \subseteq V$. For example, if $\mathbb{Z}$ denotes the ring of integers and $\mathbb{Q}$ the field of rationals, then certainly $\mathbb{Z} \operatorname{ess}_{\mathbb{Z}} \mathbb{Q}$.

Suppose $U \operatorname{ess} W$ and $W \operatorname{ess} V$. If X is a nonzero submodule of V, then $W \operatorname{ess} V$ implies that $X \cap W \neq 0$. But, $U \operatorname{ess} W$, so $(X \cap W) \cap U \neq 0$ and hence $X \cap U \neq 0$. Thus $U \operatorname{ess} V$ and we have proved the *transitivity of essential extensions.*

In this chapter, we explore the close relationship between this concept and injectivity. To start with, we have:

LEMMA 23.1 *The R-module V is injective if and only if it has no proper essential extension.*

PROOF If V is injective then, by Lemma 21.8, V is a direct summand of every module that contains it. Thus V has no proper essential extension.

Conversely, assume that V has no proper essential extension and, by Baer's Theorem, choose Q to be an injective module containing V. It follows from Zorn's Lemma that there exists a submodule $W \subseteq Q$ maximal with respect to the property that $V \cap W = 0$. Now observe that

$$V \cong V/(V \cap W) \cong (V + W)/W \subseteq Q/W$$

and we claim that $(V + W)/W \operatorname{ess} Q/W$. Indeed, if X/W is a nonzero submodule of Q/W, then $X \supset W$, so the maximality of W implies that $X \cap V \neq 0$. Furthermore, $X \cap V \not\subseteq W$, since $V \cap W = 0$, and thus $X \cap (V + W) \supset W$ as required. But $(V + W)/W \cong V$ has no proper essential extension, so it follows that $Q/W = (V + W)/W$. In other words, $V + W = Q$ and $V \cap W = 0$, so $V \mid Q$ and V is injective by Lemma 21.7(i). □

We can now obtain a key result.

THEOREM 23.2 *If V is an R-module, then there exists an injective R-module E containing V with $V \operatorname{ess} E$. Furthermore, E is uniquely determined up to an isomorphism which is the identity on V.*

PROOF First, let Q be any injective module containing V and consider the collection of all submodules E of Q with $V \subseteq E \subseteq Q$ and $V \operatorname{ess} E$. We show that a maximal such E exists. Thus suppose $E_1 \subseteq E_2 \subseteq \cdots$ is a chain of such submodules and set $E' = \bigcup_i E_i$. Then E' is certainly an R-submodule of Q containing V. Furthermore, if X is any nonzero submodule of E', then $X \cap E_i \neq 0$ for some i and therefore $(X \cap E_i) \cap V \neq 0$. Thus $X \cap V \neq 0$ and $V \operatorname{ess} E'$. By Zorn's Lemma, we can now choose E to be a maximal essential extension of V in Q.

Next, let L be any essential extension of E, not necessarily in Q. Since Q is injective, the embedding $1_E: E \to Q$ extends to a map $\sigma: L \to Q$. Furthermore, $\operatorname{Ker}(\sigma) \cap E = 0$ and $E \operatorname{ess} L$, so $\operatorname{Ker}(\sigma) = 0$. Thus $\bar{L} = \sigma(L) \cong L$ and it follows that $E \operatorname{ess} \bar{L}$. By transitivity of essential extensions, we have $V \operatorname{ess} \bar{L}$ and the maximality of E yields $\bar{L} = E$. Thus $E = L$ and the previous lemma implies that E is injective. In other words, there exists $E \supseteq V$ with E injective and $V \operatorname{ess} E$.

For uniqueness, let $\tilde{E}$ be another injective R-module with $V \operatorname{ess} \tilde{E}$. Then the embedding $1_V: V \to \tilde{E}$ extends to a map $\tau: E \to \tilde{E}$; again, since $\operatorname{Ker}(\tau) \cap V = 0$ and $V \operatorname{ess} E$, we conclude that $\operatorname{Ker}(\tau) = 0$. Thus $\tau(E) \cong E$ is an injective submodule of $\tilde{E}$, so Lemma 21.8 implies that $\tilde{E} = \tau(E) \dotplus Y$. Finally, $V \subseteq \tau(E)$ and $V \operatorname{ess} \tilde{E}$, so $Y = 0$ and τ is an appropriate isomorphism from E to $\tilde{E}$, which is the identity on V. □

DEFINITION Given the R-module V, we call the uniquely determined injective module E with $V \operatorname{ess} E$ the *injective hull* of V and write $E = \mathbf{E}(V)$.

Note that the projective analog of $\mathbf{E}(V)$ is the *projective cover*. Specifically, $P \to V \to 0$ is a projective cover of V if P is projective and if no proper submodule of P maps onto V. It is easy to see that

the projective cover, if it exists, is unique up to isomorphism. However, it may not exist. For example, let V be the $\mathbb{Z}$-module $V = \mathbb{Z}/2\mathbb{Z}$. If $P \to V \to 0$ is a projective cover, then $P3 \subset P$ and $P3$ maps onto V, a contradiction. On the other hand, as we have seen, injective hulls always exist.

Let us consider the injective hulls of certain $\mathbb{Z}$-modules. Recall that in this context, injective is the same as divisible. First, since $\mathbb{Z}$ ess $\mathbb{Q}$ and since $\mathbb{Q}$ is divisible, we have $\mathbf{E}(\mathbb{Z}) = \mathbb{Q}$. Next, let p be any prime, let $\mathbb{Z}_p$ denote $\mathbb{Z}$ localized at the multiplicatively closed set $\{1, p, p^2, \dots\}$, and let $\mathbb{C}_{p^\infty} = \mathbb{Z}_p/\mathbb{Z}$. Then $\mathbb{C}_{p^\infty}$ is an additive abelian group with all elements having order a power of p. It follows immediately that $\mathbb{C}_{p^\infty}$ is divisible by every integer k prime to p. On the other hand, by construction, $\mathbb{C}_{p^\infty}$ is certainly divisible by p. Thus $\mathbb{C}_{p^\infty}$ is a divisible abelian group and hence is an injective $\mathbb{Z}$-module. Finally, observe that $\mathbb{C}_{p^\infty}$ contains the cyclic subgroup

$$\mathbb{C}_{p^n} = \{0, 1/p^n, 2/p^n, \dots, (p^n - 1)/p^n\}$$

of order p^n and that $\mathbb{C}_{p^n}$ ess $\mathbb{C}_{p^\infty}$ for any $n \geq 1$. Therefore, we conclude that $\mathbb{C}_{p^\infty} = \mathbf{E}(\mathbb{C}_{p^n})$ for all $n \geq 1$.

LEMMA 23.3 *Let R be a ring and let the various U's, V's and W's be R-modules.*

i. If W ess V and $U \subseteq V$, then $(U \cap W)$ ess U.

ii. Let W_i ess V for $i = 1, 2, \dots, n$. If $W = \bigcap_1^n W_i$, then W ess V.

iii. Let W_i ess V_i for $i = 1, 2, \dots, n$. If $W = \oplus \sum_1^n W_i$ and $V = \oplus \sum_1^n V_i$, then W ess V.

PROOF (i) Let X be a nonzero submodule of U. Since W ess V, we have $X \cap W \neq 0$. But $X \subseteq U$, so $X = X \cap U$ and hence $X \cap (U \cap W) \neq 0$.

(ii) It suffices to consider $n = 2$. Since W_2 ess V, the preceding implies that $(W_1 \cap W_2)$ ess W_1. Thus, since W_1 ess V, transitivity of ess yields the result.

(iii) Again, it suffices to consider the case $n = 2$. Let X be a nonzero submodule of $V_1 \oplus V_2$ and choose $0 \neq x = v_1 \oplus v_2 \in X$. By symmetry, it suffices to assume that $v_1 \neq 0$. Since W_1 ess V_1, it follows that $v_1 R \cap W_1 \neq 0$. In particular, $0 \neq v_1 r \in W_1$ for some $r \in R$. Replacing x by $xr \in X$, we see that there exists $x = w_1 \oplus v_2 \in X$ with $0 \neq w_1 \in W_1$. If $v_2 = 0$, then $x \in X \cap (W_1 \oplus W_2)$ and we are done. Otherwise, $v_2 \neq 0$, so $v_2 R \cap W_2 \neq 0$ and there exists $s \in R$ with $0 \neq v_2 s \in W_2$. Then $0 \neq xs \in X \cap (W_1 \oplus W_2)$ and the lemma is proved. □

We remark that (iii) holds for arbitrary direct sums, since ess is a "local" property (see Exercise 6). As a consequence we have:

LEMMA 23.4 *Let U, W be R-submodules of V with $W \operatorname{ess} V$.*

i. $\mathbf{E}(W) = \mathbf{E}(V)$. *In particular, any essential extension of W is contained, up to isomorphism, in $\mathbf{E}(W)$.*

ii. If $W = W_1 \oplus W_2 \oplus \cdots \oplus W_n$, then $\mathbf{E}(V) = \mathbf{E}(W_1) \oplus \mathbf{E}(W_2) \oplus \cdots \oplus \mathbf{E}(W_n)$.

iii. There exists a submodule X of V with $(U \dotplus X) \operatorname{ess} V$. In particular, $\mathbf{E}(V) \cong \mathbf{E}(U) \oplus \mathbf{E}(X)$, so $\mathbf{E}(U) \mid \mathbf{E}(V)$.

PROOF (i) This is immediate, since $W \operatorname{ess} V$, $V \operatorname{ess} \mathbf{E}(V)$, and $\mathbf{E}(V)$ is injective.

(ii) Since $W_i \operatorname{ess} \mathbf{E}(W_i)$, it follows from the preceding lemma that $W = \oplus \sum_i W_i$ is an essential submodule of $E = \oplus \sum_i \mathbf{E}(W_i)$. Furthermore, since E is a finite direct sum of injective modules, E is injective and we conclude that $E = \mathbf{E}(W)$. Finally, (i) implies that $E = \mathbf{E}(W) = \mathbf{E}(V)$.

(iii) By Zorn's Lemma, we can choose $X \subseteq V$ maximal with the property that $U \cap X = 0$. Then certain $U + X = U \dotplus X$. Furthermore, if Y is a submodule of V disjoint from $U \dotplus X$, then $U \dotplus X \dotplus Y$ is a direct sum and $X \dotplus Y$ is disjoint from U. The maximality of X now implies that $Y = 0$ and hence we conclude that $(U \dotplus X) \operatorname{ess} V$. Part (ii) now yields the result. □

For example, suppose $R = \mathbb{Z}$ is the ring of integers and let V be a finitely generated abelian group. Then V is a direct sum of copies of $\mathbb{Z}$ and of cyclic groups $\mathbb{C}_{p^n} = \mathbb{Z}/p^n\mathbb{Z}$ for various prime powers $p^n > 1$. Thus $\mathbf{E}(V)$ is a direct sum of an appropriate number of copies of $\mathbb{Q}$ and of various $\mathbb{C}_{p^\infty}$.

DEFINITION Let V be an R-module. Then the *socle* of V, written $\operatorname{soc}(V)$, is the sum of all the irreducible submodules of V. If there are no such submodules, then $\operatorname{soc}(V) = 0$. In view of Theorem 3.3, $\operatorname{soc}(V)$ is the largest completely reducible submodule of V. Since a homomorphic image of a completely reducible module is completely reducible, we see that if $\alpha\colon V \to W$ is an R-homomorphism, then $\alpha\big(\operatorname{soc}(V)\big) \subseteq \operatorname{soc}(W)$.

If $V = R_R$, then $\operatorname{soc}(R_R)$ is certainly a right ideal of R. Furthermore, if $r \in R$, then left multiplication by r is an endomorphism of the right module R_R. Thus by the preceding, $r \cdot \operatorname{soc}(R) \subseteq \operatorname{soc}(R)$ and hence $\operatorname{soc}(R)$ is a two-sided ideal of R.

PROPOSITION 23.5 *Let V be an R-module. Then* $\operatorname{soc}(V)$ *is the intersection of all essential submodules of V.*

PROOF Write $S = \operatorname{soc}(V)$ and let T be the intersection of all essential submodules of V.

If $U \operatorname{ess} V$ and Z is a simple submodule of V, then $0 \neq U \cap Z \subseteq Z$ implies that $Z \subseteq U$. Thus $S = \operatorname{soc}(V) \subseteq U$ and, since U is arbitrary, we conclude that $S \subseteq T$.

For the reverse inclusion, it suffices to show that T is completely reducible. To this end, let X be a submodule of T and, by Lemma 23.4(iii), choose $Y \subseteq V$ so that $(X \dotplus Y) \operatorname{ess} V$. Then, by definition of T, we have $X \subseteq T \subseteq X \dotplus Y$, so the Modular Law implies that $T = X \dotplus (Y \cap T)$. Thus T is completely reducible and therefore it is contained in S. □

As an immediate consequence, we have:

LEMMA 23.6 *The R-module V is completely reducible if and only if it has no proper essential submodule. Furthermore, R is a Wedderburn ring if and only if it has no proper essential right ideal.*

Next we mention two comments of interest. The first is a slight modification of Baer's Criterion.

LEMMA 23.7 *Let Q be an R-module. Then Q is injective if and only if given any essential right ideal $I \subseteq R$ and any homomorphism $\sigma: I \to Q$, there exists a map $\sigma^*: R \to Q$ that extends σ.*

PROOF If Q is injective, then certainly the preceding condition is satisfied. For the converse, let $\sigma: I \to Q$ be given with I any right ideal of R. By Lemma 23.4(iii), there exists a right ideal J of R with $(I \dotplus J) \operatorname{ess} R$. Obviously, σ extends to $\sigma': I \dotplus J \to Q$ by defining $\sigma'(J) = 0$. Finally, by hypothesis, σ' extends to $\sigma^*: R \to Q$ and hence Q is injective by Baer's Criterion. □

LEMMA 23.8 *Let R be a commutative integral domain with field of fractions F. Then $\mathbf{E}(R_R) = F_R$.*

PROOF Certainly, $R \operatorname{ess}_R F$ and thus we need only show that F_R is injective. To this end, let I be a nonzero ideal of R and let $\sigma: I \to F$ be an R-module homomorphism. Then, for all $0 \neq a, b \in I$, we have

$$\sigma(b)a = \sigma(ba) = \sigma(ab) = \sigma(a)b$$

so $\sigma(a)/a = \sigma(b)/b$ in F. In particular, if $f \in F$ denotes this common ratio, then $\sigma(a) = fa$ for all $a \in I$, including $a = 0$. Thus σ extends to the map $\sigma^*: R \to F$ with $\sigma^*(r) = fr$. □

For any ring R, the regular module R_R is free and hence projective. On the other hand, it need not be injective.

DEFINITION A ring R is said to be *self-injective* if R_R is an injective R-module. Thus, for example, the preceding lemma implies that a commutative domain is self-injective if and only if it is a field. Furthermore, any Wedderburn ring is self-injective. This follows from Lemma 8.3(i) and Theorem 22.4, since $\operatorname{inj\,gl\,dim} R = \operatorname{gl\,dim} R = 0$ implies that all R-modules are injective. Artinian rings with nonzero radical can also be self-injective. For example, the ring $\mathbb{Z}/n\mathbb{Z}$ is self-injective for any integer $n \geq 2$. Other examples can be constructed from Lemmas 23.10 and 23.11. In particular, they imply that group algebras $K[G]$ with G finite are self-injective.

LEMMA 23.9 *Let R be a finite dimensional algebra over the field K and let $\lambda: R \to K$ be a K-linear functional. The following are equivalent.*

i. $\operatorname{Ker}(\lambda)$ *contains no nonzero right ideal of R.*

ii. $\operatorname{Ker}(\lambda)$ *contains no nonzero left ideal of R.*

iii. There exist "dual bases" $\{x_1, x_2, \ldots, x_n\}$ and $\{y_1, y_2, \ldots, y_n\}$ of R with $\lambda(x_i y_j) = \delta_{i,j}$. Here $\delta_{i,j} = 1$ if $i = j$ and 0 otherwise.

PROOF Since (iii) is right-left symmetric, it suffices to prove that (i) is equivalent to (iii).

(i) $\Rightarrow$(iii) Say $n = \dim_K R$ and let $\{y_1, y_2, \ldots, y_n\}$ be any basis for R. Define the K-linear transformation $\Lambda: R \to K^n$ by

$$\Lambda: r \mapsto \lambda(ry_1) \oplus \lambda(ry_2) \oplus \cdots \oplus \lambda(ry_n)$$

If $r \in \operatorname{Ker}(\Lambda)$, then $\lambda(rR) = 0$ and hence, by assumption, $r = 0$. Thus Λ is one-to-one and dimension considerations imply that Λ is onto. It follows that there exists $\{x_1, x_2, \ldots, x_n\} \subseteq R$ with $\lambda(x_i y_j) = \delta_{i,j}$. Finally, the x_i's are K-linearly independent, since $0 = \sum_i k_i x_i$ implies that

$$0 = \lambda(0) = \lambda\Big(\sum_i k_i x_i y_j\Big) = k_j$$

and hence $k_j = 0$ for all j.

(iii) $\Rightarrow$(i) If $r = \sum_i k_i x_i \in R$ and $\lambda(rR) = 0$, then

$$0 = \lambda(ry_j) = \lambda\Big(\sum_i k_i x_i y_j\Big) = k_j$$

Thus $k_j = 0$ for all j and $r = 0$. □

A finite dimensional K-algebra R with a linear functional $\lambda: R \to K$ that satisfies the above equivalent conditions is called a *Frobenius algebra*. Note that this definition is right-left symmetric.

LEMMA 23.10 *Any Frobenius algebra is both right and left self-injective.*

PROOF By symmetry it suffices to show that R_R is injective. Let $\lambda: R \to K$ be the linear functional given by the Frobenius definition and let $\langle\ ,\ \rangle: R \times R \to K$ be the bilinear form defined by $\langle x, y\rangle = \lambda(xy)$. Note that

$$\langle xr, y\rangle = \lambda(xry) = \langle x, ry\rangle$$

for all $x, y, r \in R$. Now let $\{x_1, x_2, \ldots, x_n\}$ and $\{y_1, y_2, \ldots, y_n\}$ be the dual bases for R given by the preceding lemma. If $r = \sum_i k_i x_i \in R$, then clearly $\langle r, y_j\rangle = k_j$ and thus $r = \sum_i \langle r, y_i\rangle x_i$.

Now suppose that A is a right ideal of R and that $\sigma: A \to R$ is an R-module homomorphism. Then the composite map $\tau: A \xrightarrow{\sigma} R \xrightarrow{\lambda} K$ is a linear functional on A that extends to a K-linear functional $\tau^*: R \to K$. Define $\sigma^*: R \to R$ by

$$\sigma^*: r \mapsto \sum_i \tau^*(ry_i)x_i$$

We claim that σ^* is an R-module homomorphism that extends σ. To start with, σ^* is certainly a K-linear transformation. Next, suppose $s \in R$ and write $sy_i = \sum_j y_j c_{i,j}$ and $x_j s = \sum_i d_{i,j} x_i$ with $c_{i,j}$ and $d_{i,j}$ in K. Then

$$c_{i,j} = \langle x_j, sy_i\rangle = \langle x_j s, y_i\rangle = d_{i,j}$$

and hence

$$\begin{aligned}\sigma^*(rs) &= \sum_i \tau^*(rsy_i)x_i = \sum_{i,j} \tau^*(ry_j c_{i,j})x_i \\ &= \sum_{i,j} \tau^*(ry_j)d_{i,j}x_i = \sum_j \tau^*(ry_j)x_j s = \sigma^*(r)s\end{aligned}$$

Thus σ^* is indeed an R-module homomorphism.

Finally, let $a \in A$. Then $ay_i \in A$, so

$$\begin{aligned}\tau^*(ay_i) &= \tau(ay_i) = \lambda\big(\sigma(ay_i)\big) \\ &= \lambda\big(\sigma(a)y_i\big) = \langle \sigma(a), y_i\rangle\end{aligned}$$

and hence

$$\sigma^*(a) = \sum_i \tau^*(ay_i)x_i = \sum_i \langle \sigma(a), y_i\rangle x_i = \sigma(a)$$

Thus σ^* extends σ and Baer's Criterion implies that R_R is injective. □

Some examples of Frobenius algebras are as follows.

LEMMA 23.11 *Let K be a field and let R be a finite dimensional K-algebra. If*

i. $R = R_1 \dot{+} R_2$ with each of R_1 and R_2 a Frobenius algebra, or

ii. R is a Wedderburn ring, or

iii. R is a group algebra $K[G]$,

then R is a Frobenius algebra.

PROOF (i) Let $\lambda_i: R_i \to K$ be the given linear functional for R_i. Then $\lambda: R \to K$, defined by $\lambda(r_1 \dot{+} r_2) = \lambda_1(r_1) + \lambda_2(r_2)$ with $r_i \in R_i$, is certainly a linear functional on R. Furthermore, since every right ideal I of R is of the form $I = I_1 \dot{+} I_2$, it follows immediately that $\mathrm{Ker}(\lambda)$ contains no nonzero right ideal of R.

(ii) In view of (i), we can assume that $R = \mathrm{M}_n(D)$, where D is a finite dimensional K-division algebra. Let $\mu: D \to K$ be any nonzero linear functional and define $\lambda: R \to K$ to be the composite of μ with the trace map $\mathrm{tr}: \mathrm{M}_n(D) \to D$. Note that $\mathrm{M}_n(D) \supseteq \mathrm{M}_n(K)$ and that if $\alpha \in \mathrm{M}_n(D)$ and $\beta \in \mathrm{M}_n(K)$, then $\mathrm{tr}(\alpha\beta) = \mathrm{tr}(\beta\alpha)$. Now suppose I is a right ideal of R contained in $\mathrm{Ker}(\lambda)$. Since $\mathrm{tr}(\mathrm{M}_n(K)I) = \mathrm{tr}(I\mathrm{M}_n(K)) \subseteq \mathrm{tr}(I)$, it follows that $\mathrm{M}_n(K)I \subseteq \mathrm{Ker}(\lambda)$. But $\mathrm{M}_n(K)I$ is easily seen to equal either 0 or $R = \mathrm{M}_n(D)$, and thus, since $\lambda \neq 0$, we conclude that $I = 0$.

(iii) Let $\lambda: K[G] \to K$ be defined by $\lambda: \sum_g k_g g \mapsto k_1$ and let I be a right ideal of $K[G]$ contained in $\mathrm{Ker}(\lambda)$. If $\alpha = \sum_g a_g g \in I$, then for all $x \in G$ we have $\alpha x^{-1} = \sum_g a_g g x^{-1} \in I$, so $a_x = \lambda(\alpha x^{-1}) = 0$. Thus $\alpha = 0$ as required. □

In particular, (iii) shows that Frobenius algebras need not be Wedderburn rings.

Finally, we remark that Lemma 23.8 is suggestive. It indicates that, for any ring R, the injective hull $\mathbf{E}(R_R)$ is somehow related to a ring of quotients of R. As we will see in the next chapter, this is indeed the case.

EXERCISES

1. Let

$$0 \to A \to Q_0 \xrightarrow{\alpha_1} Q_1 \xrightarrow{\alpha_2} Q_2 \to \cdots$$

$$0 \to A \to Q_0' \xrightarrow{\beta_1} Q_1' \xrightarrow{\beta_2} Q_2' \to \cdots$$

be two injective resolutions for the R-module A. Prove that

$$\begin{aligned}&\mathrm{Im}(\alpha_n) \oplus Q'_{n-1} \oplus Q_{n-2} \oplus Q'_{n-3} \oplus \cdots \\ &\quad \cong \mathrm{Im}(\beta_n) \oplus Q_{n-1} \oplus Q'_{n-2} \oplus Q_{n-3} \oplus \cdots\end{aligned}$$

for each integer $n \geq 1$. This is clearly an extension of the injective version of Schanuel's Lemma.

2. Let

$$\begin{aligned}0 &\to A \to P \to B \to 0 \\ 0 &\to C \to Q \to D \to 0\end{aligned}$$

be exact sequences of R-modules. If $\alpha\colon A \to C$ is a homomorphism, Q is injective and $\mathrm{Hom}_R(B, D) = 0$, show that α lifts to a map $\alpha^*\colon P \to C$. Similarly, if $\beta\colon B \to D$ is a homomorphism, P is projective and $\mathrm{Hom}_R(A, C) = 0$, show that β lifts to a map $\beta^*\colon B \to Q$.

3. Let Q be an injective right R-module and let $r_1, r_2, \ldots, r_n$ be elements of R. If no nonzero element of R annihilates all r_i on the right, prove that $Q = Qr_1 + Qr_2 + \cdots + Qr_n$. To this end, first observe that the map $\tau\colon R \to R^n$ given by $r \mapsto r_1 r \oplus r_2 r \oplus \cdots \oplus r_n r$ is an R-monomorphism. Next, let $q \in Q$ and define $\eta\colon R \to Q$ by $\eta r = qr$.
4. Suppose R is a commutative algebra over the field K and that $R = K \dotplus I$, where $I \neq 0$, $\dim_K I < \infty$, and $I^2 = 0$. Show that $R/I \cong \mathrm{Hom}_K(R/I, K)$ as left R-modules and then use Exercise 21.3 to deduce that $\mathbf{E}(R/I) \cong \mathrm{Hom}_K(R, K)$. Furthermore, observe that I_R is isomorphic to a finite direct sum of copies of $(R/I)_R$ and find $\mathbf{E}(R)$.
5. Let K be a field and set $R = \begin{pmatrix} K & K \\ 0 & K \end{pmatrix}$. Again use Exercise 21.3 to find $\mathbf{E}(e_{1,1}R)$, $\mathbf{E}(e_{2,2}R)$, and $\mathbf{E}(R)$.
6. Let $W_i \operatorname{ess} V_i$ for $i = 1, 2, \ldots$. Prove that $\oplus \sum_i W_i$ is essential in $\oplus \sum_i V_i$. On the other hand, show by example that $\prod_i W_i$ need not be essential in $\prod_i V_i$.
7. If R is a ring with no zero divisors, prove that R is self-injective if and only if it is a division ring.
8. Show that $\mathbb{Z}/n\mathbb{Z}$ is self-injective for all integers $n \geq 2$.

In the remaining two problems, let K be a field and let R be the ring of row finite, countably infinite matrices over K. The goal is to show that R is left but not right self-injective. Let $\{ e_{i,j} \}$ denote the usual matrix units in R.

9. Let B be a left ideal of R and let $\phi: B \to R$ be a left R-module homomorphism. The restricted map $\phi': e_{1,1}B \to e_{1,1}R$ is K-linear and hence can be extended to a K-linear map $\phi'': e_{1,1}R \to e_{1,1}R$. Show that ϕ'' is equal to right multiplication by a row finite matrix $\Phi \in R$. Then prove that ϕ is right multiplication by Φ and hence observe that ϕ can be extended to all of R. Conclude that R is left self-injective.
10. Let $A = \cdot \sum_i e_{i,i}R$, so that A is the right ideal of R consisting of all matrices with only finitely many nonzero rows. For any $a \in A$, let $\theta(a)$ be the matrix in R whose first row is the sum of all rows of a and whose other rows are 0. Show first that $\theta: A \to R$ is a right R-module homomorphism. Then show that θ is not left multiplication by any matrix $\Theta \in R$. Conclude that θ cannot be extended to R and hence that R is not right self-injective.

24. Maximal Ring of Quotients

We now show how the injective hull $\mathbf{E}(R_R)$ gives rise to a ring of quotients for R.

DEFINITION Let R be a ring and set $E = \mathbf{E}(R)$. To avoid confusion, we assume throughout that the copy of R_R in E is e_0R with $e_0 \in E$. In other words, we have $R \cong e_0R$ via the map $r \mapsto e_0r$ and e_0R is an essential submodule of the injective module E. Let $H = \mathrm{End}_R(E)$ with H acting on the left. Then E is a left H-module and we set $Q = \mathrm{End}_H(E)$ acting on the right. Note that $Q \supseteq R$, since R acts faithfully on R_R and hence on E and since H commutes with the action of R. Furthermore, E is a right Q-module. We call $Q = \mathbf{Q}_{\max}(R)$ the *maximal ring of quotients* of R.

As we will see, $\mathbf{Q}_{\max}(R)$ can be appreciably larger than R. For example, the properties of being countable or of being a domain can be lost when R is extended to $Q = \mathbf{Q}_{\max}(R)$. Furthermore, with the preceding definition, the computation of Q can frequently be quite tedious. However, under reasonable hypotheses, Q can be described in a fairly concrete manner. The latter result is one of the aims of this chapter. We start with some easy examples.

LEMMA 24.1 *i. If R is a commutative integral domain with field of fractions F, then $\mathbf{Q}_{\max}(R) = F$.*

ii. If R is self-injective, then $\mathbf{Q}_{\max}(R) = R$.

PROOF (i) It follows from Lemma 23.8 that $E = \mathbf{E}(R) = F$. Furthermore, any map $h: F \to F$ that commutes with multiplication by R certainly also commutes with multiplication by F. Thus $H = \mathrm{End}_F(F_F) = F$ and therefore $Q = \mathrm{End}_F({}_FF) = F$.

(ii) Here $E = R_R$, by assumption, so $H = \mathrm{End}_R(R_R) = R$, acting on the left. Thus $Q = \mathrm{End}_R({}_R R) = R$, acting on the right. □

Our first goal is to show that $\mathbf{Q}_{\max}(Q) = Q$ or, equivalently, that $\mathbf{Q}_{\max}$ is a closure operation. For this, we need:

LEMMA 24.2 *With the preceding notation, we have*

i. $E = He_0$.

ii. $Q \cong e_0 Q$ *as right* Q*-modules via the map* $q \mapsto e_0 q$.

iii. If B *is any* Q*-module and* $\beta: B \to E$ *is an* R*-homomorphism, then* β *is a* Q*-homomorphism.*

PROOF (i) Let e be an arbitrary element of E and let $\sigma: e_0 R \to E$ be given by $e_0 r \mapsto er$. Since $e_0 R \subseteq E$ and since E is injective, σ extends to an R-module homomorphism $h: E \to E$. Thus $h \in H = \mathrm{End}_R(E)$ and $e = \sigma(e_0) = he_0 \in He_0$.

(ii) The map $\tau: Q \to e_0 Q$ given by $q \mapsto e_0 q$ is certainly a Q-module epimorphism. Furthermore, if $e_0 q = 0$, then $Eq = (He_0)q = H0 = 0$, so $q = 0$. Thus τ is an isomorphism.

(iii) Fix $b \in B$ and let $\psi_b: e_0 Q \to E$ be given by $e_0 q \mapsto \beta(bq) - \beta(b)q$. Then ψ_b is an R-homomorphism and, since $e_0 Q \subseteq E$ and E is injective, ψ_b extends to a map $h_b: E \to E$. Note that $h_b \in H$ and hence h_b commutes with the action of Q. Since $h_b e_0 = \psi_b(e_0) = 0$, it follows that

$$\psi_b(e_0 Q) = h_b(e_0 Q) = (h_b e_0)Q = 0$$

Thus $\beta(bq) = \beta(b)q$ for all $b \in B$ and $q \in Q$, so β is a Q-homomorphism and the lemma is proved. □

Note that (iii) generalizes the obvious fact used in the proof of Lemma 24.1(i) that any element of $\mathrm{End}(F)$ that commutes with R also commutes with F. We can now prove:

THEOREM 24.3 *Let* R *be a ring and set* $E = \mathbf{E}(R_R)$ *and* $Q = \mathbf{Q}_{\max}(R)$. *Then* $E_Q \cong \mathbf{E}(Q_Q)$ *and* $\mathbf{Q}_{\max}(Q) = Q$.

PROOF We use all of the preceding notation. Note that E is a Q-module and that $E \supseteq e_0 Q \cong Q$. Furthermore, we have $e_0 R \operatorname{ess} E$ as R-modules. In particular, if X is a nonzero Q-submodule of E, then, since X is an R-submodule, it follows that $X \cap e_0 R \neq 0$ and hence $X \cap e_0 Q \neq 0$. Thus $e_0 Q \operatorname{ess} E$ as Q-modules.

Next, we show that E_Q is injective. To this end, let $A \subseteq B$ be Q-modules and let $\alpha: A \to E$ be a Q-homomorphism. Then α is an R-homomorphism and, since E_R is an injective R-module, it follows that

α extends to an R-homomorphism $\beta: B \to E$. But, by (iii) of the previous lemma, β must also be a Q-homomorphism and thus E_Q is indeed injective. We conclude that $E_Q = \mathbf{E}(e_0 Q) \cong \mathbf{E}(Q_Q)$.

Finally, since $Q \supseteq R$, we have $\mathrm{End}_Q(E_Q) \subseteq \mathrm{End}_R(E_R) = H$. On the other hand, by definition of Q, it follows that H commutes with the action of Q. Thus $H = \mathrm{End}_Q(E_Q)$ and $\mathbf{Q}_{\max}(Q) = \mathrm{End}_H({}_H E) = Q$. □

Our next goal is to understand $\mathbf{Q}_{\max}(R)$ in a totally different way, independent of E.

DEFINITION If I is a right ideal of R and $x \in R$, then we define the *residual* $x^{-1}I$ by

$$x^{-1}I = \{ r \in R \mid xr \in I \}$$

Thus $x^{-1}I$ is the largest subset of R with $x \cdot x^{-1}I \subseteq I$. Basic properties are as follows.

LEMMA 24.4 *Let I and J be right ideals of R and let $x, y \in R$.*

i. $x^{-1}I$ *is a right ideal of* R.
ii. $y^{-1}(x^{-1}I) = (xy)^{-1}I$.
iii. $x^{-1}(I \cap J) = (x^{-1}I) \cap (x^{-1}J)$.

PROOF (i) Since $x \cdot (x^{-1}I)R \subseteq IR \subseteq I$, it follows that $(x^{-1}I)R \subseteq x^{-1}I$.

(ii) Note that $r \in y^{-1}(x^{-1}I)$ if and only if $yr \in x^{-1}I$ and hence if and only if $xyr \in I$.

(iii) Clearly $r \in x^{-1}(I \cap J)$ if and only if $xr \in I$ and $xr \in J$. □

DEFINITION If A is a subset of R, we recall that

$$\mathrm{l.ann}_R(A) = \mathrm{l.ann}(A) = \{ r \in R \mid rA = 0 \}$$

is called the left annihilator of A in R. If D is any right ideal of R, then D is said to be *dense* if and only if $\mathrm{l.ann}_R(x^{-1}D) = 0$ for all $x \in R$. We list some elementary properties.

LEMMA 24.5 *Let D and D' be dense right ideals of R and let I be a right ideal of R.*

i. If $I \supseteq D$, then I is dense.
ii. If $x \in R$, then $x^{-1}D$ is dense.
iii. $D \cap D'$ is dense.
iv. D is essential in R_R.

v. If $I \lhd R$, then I is dense if and only if $\mathrm{l.ann}(I) = 0$.

PROOF (i) This is clear since $x^{-1}I \supseteq x^{-1}D$ for all $x \in R$.

(ii) This follows since $y^{-1}(x^{-1}D) = (xy)^{-1}D$.

(iii) Fix $x \in R$ and let $a \in \mathrm{l.ann}\big(x^{-1}(D \cap D')\big)$. For any $y \in x^{-1}D'$, let $J = (xy)^{-1}D = y^{-1}(x^{-1}D)$. Then $yJ \subseteq x^{-1}D$ and $yJ \subseteq x^{-1}D'$, since $x^{-1}D'$ is a right ideal containing y. Thus $yJ \subseteq (x^{-1}D) \cap (x^{-1}D') = x^{-1}(D \cap D')$ and hence $ayJ = 0$. But D is dense, so $\mathrm{l.ann}(J) = 0$ and we have $ay = 0$. Since this holds for all $y \in x^{-1}D'$, it follows that $a \in \mathrm{l.ann}(x^{-1}D') = 0$ and hence $D \cap D'$ is dense.

(iv) Let X be a right ideal of R disjoint from D. If $x \in X$, then $x(x^{-1}D) \subseteq D \cap X = 0$. Thus $x \in \mathrm{l.ann}(x^{-1}D) = 0$, so $X = 0$ and $D \operatorname{ess} R$.

(v) This follows since $I \lhd R$ implies that $I \subseteq x^{-1}I$ for all $x \in R$. □

We now consider the relationship between dense right ideals and the injective hull $E = \mathbf{E}(R)$.

LEMMA 24.6 *Let D be a right ideal of R. Then D is dense if and only if* $0 = \mathrm{l.ann}_E(D) = \{\, e \in E \mid eD = 0 \,\}$.

PROOF Suppose first that D is dense and let $0 \neq e \in E$. Since $e_0R \operatorname{ess} E$ and $eR \neq 0$, there exists $x \in R$ with $ex \in e_0R \setminus 0$. Thus, since $e_0R \cong R$ and $\mathrm{l.ann}_R(x^{-1}D) = 0$, it follows that $ex \cdot x^{-1}D \neq 0$. But $x \cdot x^{-1}D \subseteq D$, so $eD \neq 0$.

Now suppose $\mathrm{l.ann}_E(D) = 0$, fix $x \in R$ and let $a \in \mathrm{l.ann}_R(x^{-1}D)$. We consider the map $\sigma\colon D + xR \to e_0R \subseteq E$ given by $d + xr \mapsto e_0ar$. This map is easily seen to be well defined. Indeed, if $d + xr = 0$, then $xr \in D$, so $r \in x^{-1}D$ and $ar = 0$. Now E is injective and $D + xR \subseteq R$, so σ extends to $\sigma^*\colon R \to E$. But then $0 = \sigma(D) = \sigma^*(D) = \sigma^*(1)D$, so $\sigma^*(1) \in \mathrm{l.ann}_E(D) = 0$ and therefore $\sigma^* = 0$. In particular, $\sigma = 0$, so $0 = \sigma(x) = e_0a$ and $a = 0$. It follows that $\mathrm{l.ann}_R(x^{-1}D) = 0$ and hence D is dense. □

LEMMA 24.7 *Let $q \in Q = \mathbf{Q}_{\max}(R)$ and let D' be a dense right ideal of R. Then $D = \{\, r \in R \mid qr \in D' \,\}$ is also a dense right ideal of R.*

PROOF It is clear that D is a right ideal of R. In view of the preceding lemma, it suffices to show that $\mathrm{l.ann}_E(D) = 0$. To this end, choose $e \in \mathrm{l.ann}_E(D)$ and define $\sigma\colon e_0D' + e_0qR \to E$ by $e_0d' + e_0qr \mapsto er$. This map is easily seen to be well defined. Indeed, if $e_0d' + e_0qr = 0$, then $qr = -d' \in D'$ by Lemma 24.2(ii), so $r \in D$ and $er = 0$. Since σ is clearly an R-homomorphism, $e_0D' + e_0qR \subseteq E$ and E is injective, it

follows that σ extends to a map $h \in \mathrm{End}_R(E) = H$. Now $\sigma(e_0D') = 0$, so $(he_0)D' = h(e_0D') = 0$ and hence $he_0 = 0$ by the previous lemma. Thus $e = h(e_0q) = (he_0)q = 0$ and we conclude that $\mathrm{l.ann}_E(D) = 0$. □

With these results in hand, we can now obtain the following abstract characterization of $\mathbf{Q}_{\max}(R)$. For convenience, let $\mathcal{D} = \mathcal{D}(R)$ denote the collection of dense right ideals of R.

THEOREM 24.8 *The maximal ring of quotients $Q = \mathbf{Q}_{\max}(R)$ of the ring R satisfies*

i. $Q \supseteq R$ with the same 1.
ii. If $q \in Q$, then there exists $D \in \mathcal{D}(R)$ with $qD \subseteq R$.
iii. If $q \in Q$ and $D \in \mathcal{D}$, then $qD = 0$ implies $q = 0$.
iv. If $D \in \mathcal{D}$ and $\sigma: D \to R$ is a right R-module homomorphism, then there exists $q \in Q$ with $\sigma d = qd$ for all $d \in D$.

Furthermore, if Q' is any ring satisfying these four conditions, then Q' is isomorphic to Q via an isomorphism that is the identity on R.

PROOF We first verify that Q has the preceding properties. (i) is, of course, obvious and (ii) follows from the preceding lemma, since R is dense by Lemma 24.5(v). For (iii), observe that $qD = 0$ implies $EqD = 0$ and hence $Eq = 0$ by Lemma 24.6. But Q acts faithfully on E, so we conclude that $q = 0$.

To prove (iv), let $\sigma: D \to R$ be given and define $\sigma': D \to E$ by $\sigma': d \mapsto e_0\sigma(d)$. Then σ' is also an R-homomorphism and, since E is injective, σ' extends to an R-homomorphism $\sigma^*: R \to E$. Notice that if $h \in H$ and $d \in D$, then

$$h\sigma^*(1)d = h\sigma^*(d) = h\sigma'(d) = he_0\sigma(d)$$

In particular, if $he_0 = 0$, then $h\sigma^*(1)D = 0$ and hence $h\sigma^*(1) = 0$ by Lemma 24.6. Now recall, by Lemma 24.2(i), that $E = He_0$ and observe that the preceding remark implies that the map $q: E \to E$ given by $(he_0)q = h\sigma^*(1)$ is well defined. Thus q is an H-endomorphism of E, so $q \in Q$ and, for all $d \in D$, we have

$$he_0qd = h\sigma^*(1)d = he_0\sigma(d)$$

Thus $E\big(qd - \sigma(d)\big) = 0$ and we conclude that $qd = \sigma(d)$, as required.

For uniqueness, suppose $Q' \supseteq R$ also satisfies (i)–(iv). Let $q \in Q$ and, by (ii), choose $D \in \mathcal{D}(R)$ with $qD \subseteq R$. Then the map $\sigma_q: D \to R$ given by $d \mapsto qd$ is an R-homomorphism; hence, by (iv) applied to Q',

there exists $q' \in Q'$ with $q'd = \sigma_q d = qd$ for all $d \in D$. Indeed, by (iii) applied to Q', we see that $q' \in Q'$ is uniquely determined by the equation

$$q'd = qd \qquad \text{for all } d \in D \tag{$*$}$$

Furthermore, if we had chosen a second dense right ideal D_1 with $qD_1 \subseteq R$ and if $q_1' \in Q'$ was the corresponding element obtained, then $q_1'd = qd = q'd$ for all $d \in D \cap D_1$. But $D \cap D_1$ is also dense, by Lemma 24.5(iii), so $q_1' = q'$ by assumption (iii). In other words, q' is uniquely determined by q and equation $(*)$, independent of the choice of D, and therefore we have a well-defined map $\theta\colon Q \to Q'$ given by $q \mapsto q'$. It is clear that θ restricted to R is the identity map.

Now suppose $q_1, q_2 \in Q$ with $q_1D_1 \subseteq R$ for some dense right ideal D_1. By Lemma 24.7, there exists $D_2 \in \mathcal{D}(R)$ with $q_2D_2 \subseteq D_1 \subseteq R$. If $\theta(q_i) = q_i'$, then we have

$$(q_1' + q_2')d = (q_1 + q_2)d \qquad \text{for all } d \in D_1 \cap D_2$$

and

$$(q_1'q_2')d = (q_1q_2)d \qquad \text{for all } d \in D_2$$

Thus $q_1' + q_2' = \theta(q_1 + q_2)$ and $q_1'q_2' = \theta(q_1q_2)$, so θ is a ring homomorphism. Finally, by reversing the roles of Q and Q', we obtain an analogous map $\theta'\colon Q' \to Q$. In view of the symmetry of equation $(*)$, it is clear that θ' is the inverse of θ and therefore that θ is an isomorphism. □

It is now a simple matter to prove:

THEOREM 24.9 (Utumi's Theorem) *Let D be a dense right ideal of the ring R.*

i. $\mathrm{End}_R(D)$ *is isomorphic to a subring of* $\mathbf{Q}_{\max}(R)$.

ii. If D is a minimal member of $\mathcal{D}(R)$, then D is the unique minimum dense right ideal of R, $D \lhd R$, and $\mathbf{Q}_{\max}(R) \cong \mathrm{End}_R(D)$. *Here R embeds in* $\mathrm{End}_R(D)$ *as left multiplication.*

PROOF (i) If $\sigma \in \mathrm{End}_R(D)$, then conditions (iii) and (iv) of the preceding theorem imply that there exists a unique $q_\sigma \in Q$ with $\sigma d = q_\sigma d$ for all $d \in D$. The map $\mathrm{End}_R(D) \to Q$ given by $\sigma \mapsto q_\sigma$ is easily seen to be a ring monomorphism.

(ii) Suppose D' is a dense right ideal of R. Then $D' \cap D$ is dense and $D' \cap D \subseteq D$, so the minimality of D yields $D' \supseteq D$. Thus D is the unique minimum element of $\mathcal{D}(R)$. Next, for any $x \in R$, we have $x^{-1}D$ dense. Thus $x^{-1}D \supseteq D$, so $xD \subseteq x \cdot x^{-1}D \subseteq D$ and $D \lhd R$.

By (i), the map $\theta: \mathrm{End}_R(D) \to Q$ is a ring embedding and we need only show that θ is onto. To this end, let $q \in Q$ and observe that, by Lemma 24.7, $\{ r \in R \mid qr \in D \}$ is dense. Hence this right ideal must contain D and we conclude that $qD \subseteq D$. Now the map $\sigma: D \to D$ given by $\sigma d = qd$ is certainly an R-endomorphism and, by definition of θ, we have $\theta(\sigma) = q$. Thus θ is onto and hence it is an isomorphism. Since the endomorphism of D associated with q is left multiplication by q, the result follows. □

If R is right Artinian, then $\mathcal{D}(R)$ necessarily contains a minimal member and the preceding applies. Moreover, we have:

COROLLARY 24.10 *Let R be a ring with $\mathrm{l.ann}_R\big(\mathrm{soc}(R)\big) = 0$. Then $\mathbf{Q}_{\max}(R) \cong \mathrm{End}_R\big(\mathrm{soc}(R)\big)$.*

PROOF Since $\mathrm{soc}(R) \lhd R$ with left annihilator zero, Lemma 24.5(v) implies that $\mathrm{soc}(R)$ is dense. On the other hand, if D' is any dense right ideal of R, then $D' \operatorname{ess} R$, by Lemma 24.5(iv), and hence $D' \supseteq \mathrm{soc}(R)$, by Proposition 23.5. Thus $\mathrm{soc}(R)$ is the minimum dense right ideal of R and the preceding theorem yields the result. □

We close this chapter with an example and a comment. Let K be a field, let X be a set of variables, and let $R = K\langle X \rangle$ be the free K-algebra generated by the variables in X. If D is the *augmentation ideal* of R, namely the two-sided ideal of R generated by X, then D is easily seen to be a free right R-module with basis X. Note that R is a domain and $D \lhd R$, so D is dense. Thus, by Theorem 24.9(i), $\mathrm{End}_R(D)$ embeds as a subring of $Q = \mathbf{Q}_{\max}(R)$. If $|X| = n < \infty$, then $\mathrm{End}_R(D) \cong \mathrm{M}_n(R)$, so $\mathrm{M}_n(R)$ embeds in Q and Q is not a domain even though R is. Furthermore, suppose K is countable and that X is countably infinite. Then R is a countable ring, but $\mathrm{End}_R(D)$ is uncountable and hence so is Q. Thus the properties of being a domain or of being countable are not inherited by Q. On the other hand, we have:

LEMMA 24.11 *The center of $\mathbf{Q}_{\max}(R)$ is the set of elements of this ring that commute with R. In particular, if R is commutative, then so is $\mathbf{Q}_{\max}(R)$.*

PROOF If q is in the center of $Q = \mathbf{Q}_{\max}(R)$, then it certainly commutes with R. Conversely, suppose q commutes with R and let $q' \in Q$. Choose a dense right ideal D' of R with $q'D' \subseteq R$ and let $d' \in D'$. Then q commutes with both d' and $q'd'$, so $q(q'd') = (q'd')q = q'(qd')$. Thus $(qq' - q'q)D' = 0$ and hence $qq' - q'q = 0$ by Theorem 24.8(iii).

Finally, if R is commutative, then the preceding implies that R is central in Q. But then every element of Q commutes with R, so Q is central in Q and hence it is commutative. □

EXERCISES

1. Let R be a Frobenius algebra with linear functional $\lambda: R \to K$. If A is a right ideal of R, prove that $\text{l.ann}_R(A) = \{ r \in R \mid \lambda(rA) = 0 \}$. Similarly, if B is a left ideal of R, show that $\text{r.ann}_R(B) = \{ r \in R \mid \lambda(Br) = 0 \}$. Conclude that

$$\dim A + \dim \text{l.ann}_R(A) = \dim R = \dim B + \dim \text{r.ann}_R(B)$$

and that $\text{r.ann}_R\big(\text{l.ann}_R(A)\big) = A$.

2. Suppose R is an almost commutative K-algebra whose generators are $x_1, x_2, \ldots, x_m$. Assume that $x_i^{n_i+1} \in K + \sum_{j=1}^{m} Kx_j$ and that every element $r \in R$ is uniquely a polynomial in the x_i's of the form $r = \sum_{\mathbf{a}} k_{\mathbf{a}} \mathbf{x}^{\mathbf{a}}$, where the exponents are bounded above in the product ordering by $\mathbf{n} = (n_1, n_2, \ldots, n_m)$. Use the coefficient of $\mathbf{x}^{\mathbf{n}}$ to deduce that R is a Frobenius algebra.
3. Show that $\text{soc}(R) \subseteq \text{l.ann}_R\big(\text{Rad}(R)\big)$ with equality when R is right Artinian.
4. If $R = K\langle x, y \rangle$, prove that $\text{M}_n(R)$ embeds in $Q = \mathbf{Q}_{\text{max}}(R)$ for all $n \geq 1$ and that Q is uncountable.
5. Suppose K is a field and R is the ring of $n \times n$ upper triangular matrices over K. Find the socle of R and also the left socle, that is the sum of all minimal left ideals. Compute $\mathbf{Q}_{\text{max}}(R)$.
6. Let R be a local ring with Jacobson radical J and assume that J is nilpotent. Show that R is the unique minimal dense right ideal of R and conclude that $\mathbf{Q}_{\text{max}}(R) = R$. Suppose, in addition, that R has nonzero right ideals A and B with $A \cap B = 0$. Show that R is not self-injective and find a commutative example of such a ring.

In the remaining exercises we assume that R is a prime ring. In view of Lemma 24.5(v), this implies that all nonzero two-sided ideals of R are dense. Let

$$\mathbf{Q}_{\text{r}}(R) = \{ q \in \mathbf{Q}_{\text{max}}(R) \mid qB \subseteq R \text{ for some } 0 \neq B \lhd R \}$$

Then $\mathbf{Q}_{\text{r}}(R)$ is a subring of $\mathbf{Q}_{\text{max}}(R)$ called the (right) *Martindale ring of quotients* of R. Furthermore, if

$$\mathbf{Q}_{\mathrm{s}}(R) = \{\, q \in \mathbf{Q}_{\max}(R) \mid Aq, qB \subseteq R \text{ for some } 0 \neq A, B \lhd R \,\}$$

then $\mathbf{Q}_{\mathrm{s}}(R)$ is subring of $\mathbf{Q}_{\max}(R)$ called the *symmetric Martindale ring of quotients* of R.

7. Verify that $\mathbf{Q}_{\mathrm{r}}(R)$ and $\mathbf{Q}_{\mathrm{s}}(R)$ are subrings of $\mathbf{Q}_{\max}(R)$. Obtain an abstract characterization of $\mathbf{Q}_{\mathrm{r}}(R)$ analogous to that given for $\mathbf{Q}_{\max}(R)$ in Theorem 24.8.
8. If R is a domain, prove that $\mathbf{Q}_{\mathrm{s}}(R)$ is also a domain. What about $\mathbf{Q}_{\mathrm{r}}(R)$? If R is a simple ring, show that $\mathbf{Q}_{\mathrm{r}}(R) = \mathbf{Q}_{\mathrm{s}}(R) = R$.
9. Prove that the centers of $\mathbf{Q}_{\max}(R)$, $\mathbf{Q}_{\mathrm{r}}(R)$, and $\mathbf{Q}_{\mathrm{s}}(R)$ are all equal. This common center is called the *extended centroid* of R. Show that, in this context, the extended centroid F is a field.
10. Let a, b, c, d be nonzero elements of R and suppose that $arb = crd$ for all $r \in R$. Prove that there exists a nonzero element f in the extended centroid of R with $c = af$ and $d = f^{-1}b$. This result is due to Martindale. To start with, let $A = RaR$ and $C = RcR$ and define the maps $\sigma\colon A \to C$ and $\tau\colon C \to A$ by

$$\sigma\colon \sum_i x_i a y_i \mapsto \sum_i x_i c y_i$$
$$\tau\colon \sum_i x_i c y_i \mapsto \sum_i x_i a y_i$$

To see that these are well defined, assume that $\sum_i x_i a y_i = 0$ and consider the expression $0 = \left(\sum_i x_i a y_i\right) rb$ for all $r \in R$. If σ and τ determine the elements $f, g \in \mathbf{Q}_{\mathrm{r}}(R)$ as in Exercise 7, prove that $g^{-1} = f \in F$ and that f has the appropriate properties.

25. Classical Ring of Quotients

We now move on to the more natural and familiar classical ring of quotients. Let R be a ring and let T be a *multiplicatively closed* subset of R. By definition, this means that $1 \in T$ and if $a, b \in T$, then $ab \in T$. In order to form an appropriate ring of fractions RT^{-1} with the elements of T in the denominator, it is clear that T must consist of regular elements, that is elements that are not zero divisors in R. Specifically, $r \in R$ is said to be *regular* if and only if $\text{r.ann}_R(r) = \text{l.ann}_R(r) = 0$.

DEFINITION Let R be a ring and let T be a multiplicatively closed subset of regular elements of R. We say that RT^{-1} is a *right ring of quotients* of R provided

1. RT^{-1} is a ring containing R with the same 1.
2. Every element of T is invertible in RT^{-1}.
3. Every element of RT^{-1} is of the form rt^{-1} with $r \in R$ and $t \in T$.

Unlike the commutative situation, we cannot always form RT^{-1}. Indeed, there is at least one obvious additional requirement. Thus suppose RT^{-1} exists and let $r \in R$ and $t \in T$ be arbitrary. Then $r, t^{-1} \in RT^{-1}$, so $t^{-1}r \in RT^{-1}$ and (3) implies that there exist $r_1 \in R$ and $t_1 \in T$ with $t^{-1}r = r_1 t_1^{-1}$. Multiplying by t and t_1 on the appropriate sides then yields $rt_1 = tr_1$, an equation in the ring R.

DEFINITION Let T be a multiplicatively closed set of regular elements of R. We say that T is a *right denominator set* if for all $r \in R$ and $t \in T$ there exist $r_1 \in R$ and $t_1 \in T$ with $rt_1 = tr_1$.

In view of the preceding remarks, we have:

LEMMA 25.1 *Let T be a multiplicatively closed set of regular elements of R. If RT^{-1} exists, then T is a right denominator set.*

As we will shortly see, the converse to the above result is also true. To prove this, we first need:

LEMMA 25.2 *Let T be a right denominator set in R and suppose that S is a ring containing R with the property that each $t \in T$ is invertible in S. If $RT^{-1} \subseteq S$ is defined by*

$$RT^{-1} = \{ rt^{-1} \mid r \in R,\ t \in T \}$$

then

i. $T^{-1}R \subseteq RT^{-1}$.

ii. RT^{-1} *is a subring of* S *containing* R.

iii. The arithmetic in RT^{-1} *is solely determined by* R *and* T, *independent of the arithmetic in* S.

iv. Any finite number of elements of RT^{-1} *can be written with a common denominator. Specifically, if* $r_1t_1^{-1}, r_2t_2^{-1}, \ldots, r_nt_n^{-1} \in RT^{-1}$, *then there exist* $s_i \in r_iR$ *and* $t \in T$ *with* $r_it_i^{-1} = s_it^{-1}$ *for all* $i = 1, 2, \ldots, n$.

PROOF We proceed in a series of steps. Since we are concerned with (iii) as well as (ii), it is important to observe that the conclusions of each of these steps can be achieved solely from a knowledge of R and T. In other words, these conclusions are independent of the arithmetic in the ring S.

STEP 1 $T^{-1}R \subseteq RT^{-1}$.

PROOF Let $t \in T$ and $r \in R$. By the right denominator condition in R, there exist $r_1 \in R$ and $t_1 \in T$ with $tr_1 = rt_1$. Now multiply by t^{-1} and t_1^{-1} on the appropriate sides to obtain $t^{-1}r = r_1t_1^{-1} \in RT^{-1}$. Notice that r_1 and t_1 are determined in R by r and t. They are, of course, not uniquely determined. □

STEP 2 *Common denominators exist.*

PROOF Let $r_1t_1^{-1}, r_2t_2^{-1}, \ldots, r_nt_n^{-1} \in RT^{-1}$. We show by induction on n that there exist $s_i \in r_iR$ and $t \in T$ with $r_it_i^{-1} = s_it^{-1}$. Furthermore, we show that such s_i and t are computable in R. Now, by induction, there exist $\tilde{s}_i \in r_iR$ and $\tilde{t} \in T$ with $r_it_i^{-1} = \tilde{s}_i\tilde{t}^{-1}$ for $i = 1, 2, \ldots, n-1$. In addition, Step 1 implies that by working in R we can find $s \in R$ and $t \in T$ with $t_n^{-1}\tilde{t} = st^{-1}$. Thus, when $i \leq n-1$, we have

$$r_it_i^{-1} = \tilde{s}_i\tilde{t}^{-1} = \tilde{s}_itt^{-1}\tilde{t}^{-1} = (\tilde{s}_it)(\tilde{t}t)^{-1}$$

and, since $t_n^{-1} = st^{-1}\tilde{t}^{-1}$, we also have

$$r_n t_n^{-1} = r_n s t^{-1}\tilde{t}^{-1} = (r_n s)(\tilde{t}t)^{-1}$$

In particular, since $\tilde{s}_i t \in r_i R$ for $i \leq n-1$ and since $r_n s \in r_n R$, this step is proved. □

STEP 3 *RT^{-1} is closed under addition and multiplication. Furthermore, these operations, along with equality, are all determined in R.*

PROOF Let $r_1 t_1^{-1}, r_2 t_2^{-1} \in RT^{-1}$. By the preceding step, we can write $r_1 t_1^{-1} = s_1 t^{-1}$ and $r_2 t_2^{-1} = s_2 t^{-1}$ just working in R. Thus $r_1 t_1^{-1} + r_2 t_2^{-1} = (s_1 + s_2)t^{-1}$, so RT^{-1} is closed under addition and addition is determined in R. Moreover $r_1 t_1^{-1} = r_2 t_2^{-1}$ if and only if $s_1 t^{-1} = s_2 t^{-1}$ and hence if and only if $s_1 = s_2$. Finally, Step 1 implies that by working in R we can find $s_3 \in R$ and $t_3 \in T$ with $t_1^{-1} r_2 = s_3 t_3^{-1}$. Thus

$$r_1 t_1^{-1} \cdot r_2 t_2^{-1} = r_1 s_3 t_3^{-1} t_2^{-1} = (r_1 s_3)(t_2 t_3)^{-1} \in RT^{-1}$$

and the lemma is proved. □

We can now obtain:

THEOREM 25.3 (Ore's Theorem) *If T is a right denominator set in the ring R, then the right ring of quotients RT^{-1} exists and is unique up to an isomorphism, which is the identity on R.*

PROOF In view of the preceding lemma, it suffices to find an extension ring $S \supseteq R$ in which all elements of T are invertible. For this we will use $S = \mathbf{Q}_{\max}(R)$. Thus, let $E = \mathbf{E}(R_R)$, let $H = \mathrm{End}_R(E_R)$, and recall that $\mathbf{Q}_{\max}(R) = \mathrm{End}_H({}_H E)$. Let $t \in T$.

If $r \in R$, then there exist $r_1 \in R$ and $t_1 \in T$ with $rt_1 = tr_1 \in tR$. Thus t_1 is contained in the residual $r^{-1}(tR)$ and hence, since t_1 is regular, we conclude that $\mathrm{l.ann}_R\big(r^{-1}(tR)\big) = 0$ for all $r \in R$. It follows that tR is a dense right ideal of R and we conclude from Lemma 24.6 that $\mathrm{l.ann}_E(tR) = 0$. In particular, $\mathrm{l.ann}_E(t) = 0$.

Next, let $e \in E$ be arbitrary. Since $\mathrm{r.ann}_R(t) = 0$, the map $\sigma: tR \to E$ given by $tr \mapsto er$ is a well-defined R-homomorphism. Since E is injective, σ extends to $\sigma^*: R \to E$ and thus

$$e = \sigma(t) = \sigma^*(t) = \sigma^*(1)t \in Et$$

In other words, we have shown that $E = Et$.

Finally, since $E = Et$ and $\mathrm{l.ann}_E(t) = 0$, the map $q: E \to E$ given by $et \mapsto e$ is a well-defined left H-module endomorphism of E. Thus $q \in \mathbf{Q}_{\max}(R) = S$. But clearly, $etq = e$ for all $e \in E$ and $fqt = f$ for all $f \in Et = E$. It therefore follows that $tq = qt = 1$, so $t^{-1} = q \in S$ and the preceding lemma yields the result. □

This is, of course, not the original proof of Ore's Theorem. That proof began by considering the collection of all formal fractions rt^{-1} with $r \in R$, $t \in T$ and by defining the equivalence of fractions as in the equality part of Lemma 25.2. After showing that this is indeed an equivalence relation, addition and multiplication were then defined via the formulas given in Lemma 25.2. At this point, it was necessary to show that these operations respect the equivalence relation and therefore define an addition and multiplication on the set of equivalence classes. Finally, all the ring axioms were verified. This was clearly a formidable and uninspiring task, some aspects of which are included in the exercises.

We remark that there is an obvious left analog to all the previous definitions and results. In particular, we can speak of *left denominator sets* and of the *left ring of quotients* $T^{-1}R$. The following result is an immediate consequence of Lemma 25.2 and Theorem 25.3.

LEMMA 25.4 *If T is a right and left denominator set in R, then $RT^{-1} = T^{-1}R$.*

If T is the set of all regular elements of R, then T is certainly a multiplicatively closed subset of R. In this case, the right denominator condition is usually called the *Ore condition*. Indeed, if T satisfies the Ore condition, then R is said to be an *Ore ring* and we call RT^{-1} the *classical right ring of quotients* of R. Thus $\mathbf{Q}_{\mathrm{cl}}(R)$ is certainly a natural ring extension of R. If, in addition, R is a domain, then R is called an *Ore domain*.

COROLLARY 25.5 *Let R be a ring.*

i. R is an Ore ring if and only if $\mathbf{Q}_{\mathrm{cl}}(R)$ exists.

ii. R is an Ore domain if and only if $\mathbf{Q}_{\mathrm{cl}}(R)$ is a division ring.

iii. If $\mathbf{Q}_{\mathrm{cl}}(R)$ exists, then it is unique up to an isomorphism, which is the identity on R.

PROOF (i) and (iii) are immediate consequences of Ore's Theorem. For (ii), if $\mathbf{Q}_{\mathrm{cl}}(R)$ is a division ring, then R is certainly a domain and hence an Ore domain. Conversely, if R is an Ore domain, then $\mathbf{Q}_{\mathrm{cl}}(R)$ exists and every nonzero element of R is invertible in this ring. Thus, since every element of $\mathbf{Q}_{\mathrm{cl}}(R)$ is a quotient of elements of R, it is clear that $\mathbf{Q}_{\mathrm{cl}}(R)$ is a division ring. □

If $R = K\langle x, y\rangle$ is the free algebra over the field K in the variables x and y, then R is obviously a domain. On the other hand, the equation $xs = yt$ has no nonzero solutions $s, t \in R$. Thus R is not an Ore domain and $\mathbf{Q}_{\mathrm{cl}}(R)$ does not exist. As we will see in Exercise 4, R can in fact be embedded in a division ring D, but of course $D \neq \mathbf{Q}_{\mathrm{cl}}(R)$.

Note that if all regular elements of a ring R are invertible, then the uniqueness of $\mathbf{Q}_{\mathrm{cl}}(R)$ implies that $R = \mathbf{Q}_{\mathrm{cl}}(R)$.

LEMMA 25.6 *Let R be a right Artinian ring.*

i. If $t \in R$ with $\mathrm{r.ann}_R(t) = 0$, then t is invertible in R.

ii. If $t \in R$ with $\mathrm{l.ann}_R(t) = 0$, then t is invertible in R.

iii. $\mathbf{Q}_{\mathrm{cl}}(R) = R$.

PROOF (i) Since $\mathrm{r.ann}_R(t) = 0$, the map $R \to tR$ given by $r \mapsto tr$ is an R-module isomorphism. In particular, R and tR have the same composition length and thus R/tR has length 0. In other words, $tR = R$ and there exists $s \in R$ with $ts = 1$. But this implies that $\mathrm{r.ann}_R(s) = 0$, so we conclude similarly that there exists $u \in R$ with $su = 1$. It follows that s is invertible with inverse $t = u$.

(ii) This proof is more complicated. By the Hopkins-Levitzki Theorem, R_R has finite composition length and we proceed by induction on this parameter. To start with, if R_R has length 1, then R is a division ring and t is obviously invertible. Now, for the general case, observe that if I is a nonzero two-sided ideal of R, then the length of R/I is less than that of R. Thus, by induction, we may assume that the result holds in all proper homomorphic images of R.

Let $N = \mathrm{Nil}(R)$. If $N = 0$, then R is a Wedderburn ring and hence also a left Artinian ring by the Artin-Wedderburn Theorem. Thus the left analog of (i) implies that t is invertible. We may therefore suppose that $N \neq 0$; hence, since N is nilpotent, we see that $A = \mathrm{r.ann}_R(N) \neq 0$. Furthermore, since $NR = N$, we have $0 = NA = N(RA)$ and it follows that A is a nonzero two-sided ideal of R.

Let $\bar{t} = t + A$ denote the image of t in R/A. If $s \in R$ with $\bar{s}\bar{t} = 0$, then $st \in A = \mathrm{r.ann}_R(N)$ and thus $Nst = 0$. But $\mathrm{l.ann}_R(t) = 0$, so $Ns = 0$ and hence $s \in A$. In other words, $\bar{s} = 0$ and $\mathrm{l.ann}_{R/A}(\bar{t}) = 0$. By induction, $\bar{t}$ is invertible, so there exists $r \in R$ with $\bar{r}\bar{t} = 1$. Thus $1 - rt \in \mathrm{r.ann}_R(N)$, so $N(1 - rt) = 0$ and it follows that $N = Nt$.

Finally, let $' : R \to R/N$ denote the natural map and let $t' = t + N$ denote the image of t in this proper homomorphic image of R. If $x't' = 0$, then $xt \in N = Nt$, so $xt = nt$ for some $n \in N$. Since $\mathrm{l.ann}_R(t) = 0$, this yields $x = n$, so $x' = 0$ and $\mathrm{l.ann}_{R/N}(t') = 0$. Again, induction implies that t' is invertible and hence there exists $y \in R$ with $y't' = 1$. Thus

$1 - yt \in N = Nt$ and in particular $1 - yt = mt$ for some $m \in N$. We conclude that $1 = (y + m)t$, so $\mathrm{r.ann}_R(t) = 0$ and part (i) now yields the result.

(iii) This follows from (i) and the observation immediately preceding this lemma. □

LEMMA 25.7 *Let R be a ring.*

i. If $T_1 \subseteq T_2$ are right denominator sets in R, then T_2 is a right denominator set in RT_1^{-1} and $(RT_1^{-1})T_2^{-1} = RT_2^{-1}$.

ii. If R is an Ore ring and $Q = \mathbf{Q}_{\mathrm{cl}}(R)$, then $\mathbf{Q}_{\mathrm{cl}}(Q) = Q$. In other words, when it exists, the classical ring of quotients is a closure operation.

PROOF (i) Notice that $RT_1^{-1} \subseteq RT_2^{-1}$, so it follows that T_2 is a multiplicatively closed set of regular elements in RT_1^{-1}. Since every element of RT_2^{-1} is of the form rt^{-1} with $t \in T_2$ and $r \in R \subseteq RT_1^{-1}$, it follows that $RT_2^{-1} = (RT_1^{-1})T_2^{-1}$. In particular, T_2 must be a right denominator set in RT_1^{-1}.

(ii) Let T be the set of regular elements of R, so that $Q = \mathbf{Q}_{\mathrm{cl}}(R) = RT^{-1}$. If rt^{-1} is a regular element of Q, then certainly $\mathrm{l.ann}_R(r) = 0$. Furthermore, if $0 \neq s \in R$, then $ts \neq 0$, so $0 \neq rt^{-1} \cdot ts = rs$ and it follows that $\mathrm{r.ann}_R(r) = 0$. Thus $r \in T$ and rt^{-1} is an invertible element of Q. As we observed earlier, this implies that $\mathbf{Q}_{\mathrm{cl}}(Q) = Q$. □

If R is a commutative domain, then $\mathbf{Q}_{\mathrm{cl}}(R)$ exists and is a field. Thus a natural noncommutative question is to classify those R for which $\mathbf{Q}_{\mathrm{cl}}(R)$ exists and is a divison ring or, more generally, a Wedderburn ring. Indeed, this is the goal of the remainder of this chapter and of the next. As we will see, the answer concerns certain weak forms of the Noetherian condition. Thus it is reasonable to start by considering the relationship between the right ideals of R and of RT^{-1}. Note that once we know that RT^{-1} exists, then Lemma 25.2(iv) with $S = RT^{-1}$ implies that common denominators exist in this ring of fractions.

LEMMA 25.8 *Let T be a right denominator set in R.*

i. If I is a right ideal of R, then $IT^{-1} = \{ rt^{-1} \mid r \in I,\ t \in T \}$ is a right ideal of RT^{-1}.

ii. If I is an essential right ideal of R, then IT^{-1} is an essential right ideal of RT^{-1}.

iii. If $I_1 \dotplus I_2 \dotplus \cdots \dotplus I_n$ is a direct sum of right ideals of R, then

$$I_1T^{-1} \dotplus I_2T^{-1} \dotplus \cdots \dotplus I_nT^{-1} \subseteq RT^{-1}$$

is also a direct sum.

PROOF (i) Let $r_1t_1^{-1}, r_2t_2^{-1} \in IT^{-1}$. Then Lemma 25.2(iv) implies that there exist $s_i \in r_iR \subseteq I$ and $t \in T$ with $r_it_i^{-1} = s_it^{-1}$. Thus $r_1t_1^{-1} + r_2t_2^{-1} = (s_1 + s_2)t^{-1} \in IT^{-1}$ and IT^{-1} is closed under addition. Furthermore, since $T^{-1}R \subseteq RT^{-1}$, we have

$$IT^{-1} \cdot RT^{-1} \subseteq IR \cdot T^{-1}T^{-1} = IT^{-1}$$

and IT^{-1} is a right ideal of RT^{-1}.

(ii) Now suppose that X is a right ideal of RT^{-1} disjoint from IT^{-1}. Since $IT^{-1} \cap R \supseteq I$, it follows that $X \cap R$ is a right ideal of R disjoint from I. But $I \operatorname{ess} R$, so $X \cap R = 0$. Finally, if $rt^{-1} \in X$, then $r = (rt^{-1})t \in X \cap R = 0$, so $rt^{-1} = 0$ and $X = 0$.

(iii) Let $r_it_i^{-1} \in I_iT^{-1}$ for $1 \leq i \leq n$ and suppose that $\sum_1^n r_it_i^{-1} = 0$. By Lemma 25.2 there exist $s_i \in r_iR \subseteq I_i$ and $t \in T$ with $r_it_i^{-1} = s_it^{-1}$ for all i. Thus $0 = \left(\sum_1^n s_i\right)t^{-1}$, so $0 = \sum_1^n s_i$. But $s_i \in I_i$ and $\cdot \sum_i I_i$ is direct, so we conclude that each $s_i = 0$ and hence that each $r_it_i^{-1} = 0$. With this, it follows that the sum $\sum_1^n I_iT^{-1}$ is direct. □

In the other direction, we have:

LEMMA 25.9 *Let T be a right denominator set in R.*

i. If X is a right ideal of RT^{-1}, then $X \cap R$ is a right ideal of R and $X = (X \cap R)T^{-1} = (X \cap R)(RT^{-1})$.

ii. If X is an essential right ideal of RT^{-1}, then $X \cap R$ is an essential right ideal of R.

iii. If $X_1 \dotplus X_2 \dotplus \cdots \dotplus X_n$ is a direct sum of right ideals of RT^{-1}, then

$$(X_1 \cap R) \dotplus (X_2 \cap R) \dotplus \cdots \dotplus (X_n \cap R) \subseteq R$$

is also a direct sum.

PROOF (i) Certainly $X \supseteq (X \cap R)T^{-1}$. Conversely, if $rt^{-1} \in X$, then $r = (rt^{-1})t \in X \cap R$ and $rt^{-1} \in (X \cap R)T^{-1}$.

(ii) Let I be a right ideal of R disjoint from $X \cap R$. Since $(X \cap R) \dotplus I$ is a direct sum, it follows from the preceding lemma that $(X \cap R)T^{-1} \dotplus IT^{-1}$ is also direct. But $(X \cap R)T^{-1} = X$ and $X \operatorname{ess} RT^{-1}$, so we must have $IT^{-1} = 0$ and hence $I = 0$.

(iii) This is obvious. □

We need the following observation.

LEMMA 25.10 *i. Let $W \subseteq V$ be R-modules with $W \operatorname{ess} V$. If $v \in V$, then $\{ r \in R \mid vr \in W \}$ is an essential right ideal of R.*

ii. Let I be an essential right ideal of R. If $x \in R$, then $(x^{-1}I) \operatorname{ess} R$.

PROOF (i) It is clear that $J = \{ r \in R \mid vr \in W \}$ is a right ideal of R. Let X be a nonzero right ideal of R. If $vX = 0$, then $vX \subseteq W$, so $X \subseteq J$ and $X \cap J \neq 0$. On the other hand, if $vX \neq 0$, then vX is a nonzero submodule of V. Thus, since $W \operatorname{ess} V$, we have $vX \cap W \neq 0$; clearly $X \cap J \neq 0$, by the definition of J. Thus $X \cap J \neq 0$ in all cases and $J \operatorname{ess} R$.

(ii) Note that $x^{-1}I = \{ r \in R \mid xr \in I \}$. Thus (ii) follows from (i) with $V = R$ and $W = I$. □

We close this chapter with a key result. It offers the sufficient condition we will use in the next chapter for the existence of a Wedderburn ring of quotients.

LEMMA 25.11 *Let T be a multiplicatively closed set of regular elements of R. Suppose that*

i. $t \in T$ implies $(tR) \operatorname{ess} R$, and

ii. $I \operatorname{ess} R$ implies $I \cap T \neq \emptyset$.

Then T is a right denominator set in R and RT^{-1} is a Wedderburn ring.

PROOF We first show that T is a right denominator set. To this end, let $r \in R$ and $t \in T$. Then $(tR) \operatorname{ess} R$ by (i) and hence $r^{-1}(tR) \operatorname{ess} R$ by Lemma 25.10. It now follows from assumption (ii) that $r^{-1}(tR) \cap T \neq \emptyset$ and, say, $t_1 \in r^{-1}(tR) \cap T$. Thus $rt_1 \in tR$, so $rt_1 = tr_1$ as required.

We now know that RT^{-1} exists and let X be any essential right ideal of this ring of quotients. Then $(X \cap R) \operatorname{ess} R$ by Lemma 25.9(ii), so assumption (ii) implies that $X \cap T$ is nonempty. But every element of T is invertible in RT^{-1}, so we conclude that $X = R$. In other words, RT^{-1} has no proper essential right ideal; therefore, Lemma 23.6 implies that RT^{-1} is a Wedderburn ring. □

EXERCISES

1. Let R be a prime ring. Show that the symmetric Martindale ring of quotients $Q = \mathbf{Q}_s(R)$ can be uniquely characterized by the following four properties.
   i. $Q \supseteq R$ with the same 1.
   ii. If $q \in Q$, then there exist $0 \neq A, B \lhd R$ with $Aq, qB \subseteq R$.
   iii. If $0 \neq q \in Q$ and $0 \neq I \lhd R$, then $Iq \neq 0$ and $qI \neq 0$.

iv. Let $0 \neq A, B \lhd R$ and let $f: {}_RA \to {}_RR$ and $g: B_R \to R_R$ be R-module homomorphisms. If $(af)b = a(gb)$ for all $a \in A$, $b \in B$, then there exists $q \in Q$ with $af = aq$ and $gb = qb$ for all $a \in A$ and $b \in B$.

2. Let T be a right denominator set in R. Characterize those right ideals X of R with $(XT^{-1}) \cap R = X$. If R is right Noetherian, prove that the same is true of RT^{-1}.
3. Suppose R is a domain. Show that R is an Ore domain if and only if every two nonzero right ideals of R have a nonzero intersection. If R is right Noetherian, prove that $\mathbf{Q}_{\mathrm{cl}}(R)$ exists. For the latter, let $0 \neq r, t \in R$ and observe that the right ideal $\sum_{k=0}^{\infty} t^k r R$ must be finitely generated.
4. Let K be a field and let F be the rational function field over K generated by the countably many algebraically independent elements x_i for $i = 0, \pm 1, \pm 2, \ldots$. Then there exists a K-automorphism σ of F determined by the shift map $x_i \mapsto x_{i+1}$ and we let R be the skew polynomial ring $R = F[y; \sigma]$. Observe that R is a Noetherian domain and, hence, by the preceding problem $\mathbf{Q}_{\mathrm{cl}}(R) = D$ exists and is a division ring. On the other hand, prove that the K-subalgebra of R generated by $x = x_0$ and y is the free algebra on these two generators. Thus conclude that the free algebra $K\langle x, y\rangle$ embeds in a division ring.
5. If $R = \begin{pmatrix} K & K[x] \\ 0 & K[x] \end{pmatrix}$, prove that R has a classical right ring of quotients but not a left one.

The remaining exercises outline a direct proof of Corollary 25.5(i). Thus suppose that R is an Ore ring and let T denote the set of its regular elements. The goal is to show that $\mathbf{Q}_{\mathrm{cl}}(R) = RT^{-1}$ exists.

6. If $c, d \in T$ and $r \in R$ with $cr = d$, prove that $r \in T$. In particular, deduce that if $a, b \in T$ then there exist $x, y \in T$ with $ax = by$.
7. Consider the collection of formal fractions with denominators in T and define $ra^{-1} \sim sb^{-1}$ if and only if there exist $x, y \in T$ with $ax = by$ and $rx = sy$. Prove that $\sim$ is an equivalence relation and then let $[ra^{-1}]$ denote the class of ra^{-1}.
8. Define $[ra^{-1}] + [sb^{-1}] = [(rx + sy)(ax)^{-1}]$, where $x, y \in T$ are any elements with $ax = by$. Prove that this sum is well defined. To this end, first show that the sum is independent of the choice of auxiliary elements x and y. Then show that the sum is independent of the representative of the class $[ra^{-1}]$.
9. If RT^{-1} denotes the set of all such equivalence classes, prove that

RT^{-1} is an abelian group under the addition given previously.

10. Now define $[ra^{-1}][sb^{-1}] = [(rv)(bx)^{-1}]$, where $x \in T$ and $v \in R$ are any elements with $av = sx$. Verify that multiplication is well defined and that in this way RT^{-1} becomes a ring. Finally, show that the map $r \mapsto [r1^{-1}]$ identifies R as a subring of RT^{-1} and that, with this identification, we have $RT^{-1} = \mathbf{Q}_{\mathrm{cl}}(R)$.

26. Goldie Rings

The goal now is to determine those rings having a Wedderburn classical ring of quotients. As we mentioned earlier, this classification involves conditions that are somewhat weaker than being Noetherian. In addition, the existence, or rather the nonexistence, of nonzero nilpotent ideals also comes into play.

Recall that R is a *prime ring* if for all nonzero ideals $A, B \lhd R$ we have $AB \neq 0$. Furthermore, we say that $P \lhd R$ is a *prime ideal* of R if R/P is a prime ring. Thus P is a prime ideal if and only if for all $A, B \lhd R$, the inclusion $AB \subseteq P$ implies $A \subseteq P$ or $B \subseteq P$. Alternately, P is prime if and only if $A, B \supset P$ implies $AB \not\subseteq P$. It is clear, by induction, that if P is prime and if $A_1 A_2 \cdots A_n \subseteq P$, then at least one of the ideals A_i must be contained in P. Recall that R is said to be a *semiprime ring* if R has no nonzero nilpotent two-sided ideal.

LEMMA 26.1 *Let R be a ring. The following are equivalent.*

i. R is a semiprime ring.

ii. The intersection of all prime ideals of R is equal to 0.

iii. If $A \lhd R$ with $A^2 = 0$, then $A = 0$.

iv. R has no nonzero nilpotent right or left ideal.

PROOF (i)⇒(iv) If I is a right ideal of R with $I^n = 0$, then $A = RI$ is a two-sided ideal of R containing I. Furthermore, $IR = I$ implies that

$$A^n = (RI)(RI)\cdots(RI) = RI^n = 0$$

and thus, since R is semiprime, we conclude that $A = 0$ and $I = 0$.

(iv)⇒(iii) This is obvious.

(iii)⇒(ii) Let $0 \neq r \in R$ be arbitrary and construct a sequence $S = \{ r_0, r_1, r_2, \ldots \}$ of nonzero elements of R inductively as follows. First, we let $r_0 = r$. Next, if $r_n \neq 0$ is given, then $0 \neq Rr_nR \triangleleft R$ and hence, by assumption, $(Rr_nR)^2 \neq 0$. Thus $r_nRr_n \neq 0$ and we can choose $0 \neq r_{n+1} \in r_nRr_n$. Now $0 \notin S$, so the zero ideal is disjoint from S and Zorn's Lemma implies that there exists $P \triangleleft R$ maximal with the property that $P \cap S = \emptyset$. We claim that P is prime. Indeed, suppose A and B are ideals of R properly containing P. By the maximality of P, we have $r_n \in A$ for some subscript n and hence for all larger subscripts by the manner in which S is constructed. Similarly, $r_m \in B$. Thus if $t = \max\{ n, m \}$, then r_t is in both A and B and hence $r_{t+1} \in r_tRr_t \subseteq AB$. But $r_{t+1} \notin P$, so $AB \not\subseteq P$ and therefore P is prime. Finally, $r = r_0 \notin P$, so, since $0 \neq r \in R$ was chosen arbitrarily, we conclude that the intersection of all prime ideals of R is 0.

(ii)⇒(i) Let $A \triangleleft R$ with $A^n = 0$. If P is any prime ideal of R, then $A^n = 0 \subseteq P$ and hence $A \subseteq P$. Thus A is contained in the intersection of all prime ideals of R and therefore $A = 0$. □

In particular, R is a semiprime ring if and only if it is a subdirect product of prime rings. This, of course, explains the name *semiprime*. Now we move on to the relevant Noetherian-like conditions.

DEFINITION Suppose V is a right R-module. We say that V satisfies *max-c*, the maximum condition on complements, if V contains no infinite direct sum of nonzero submodules. Obviously, any module with the ascending or descending chain condition satisfies max-c. If $V = R_R$ satisfies max-c, then we say that R has *max-rc*. Here the r reminds us that we are viewing R as a *right* R-module.

Next, recall that R satisfies *max-ra* if the set $\{ \text{r.ann}_R(x) \mid x \in R \}$ of right annihilators of elements of R satisfies the maximum condition or, equivalently, the ascending chain condition.

Finally, we say that R is a right *Goldie ring* if it satisfies both max-rc and max-ra. Obviously, any Noetherian ring is Goldie. On the other hand, any commutative domain also satisfies these conditions. Thus max-rc and max-ra together are weaker than the Noetherian property.

As usual, we view Artinian and Noetherian conditions on the right unless otherwise indicated.

LEMMA 26.2 *Let T be a right denominator set in R. If RT^{-1} is either Artinian or Noetherian, then R is a Goldie ring.*

PROOF Since Artinian implies Noetherian, by the Hopkins-Levitzki The-

orem, it suffices to assume that RT^{-1} is Noetherian. Thus RT^{-1} cannot have an infinite direct sum of nonzero right ideals. Now suppose $\cdot \sum_{i\in\mathcal{I}} I_i$ is a direct sum of nonzero right ideals of R. Since a sum is direct if and only if every finite subsum is direct, it follows from Lemma 25.8(iii) that $\cdot \sum_{i\in\mathcal{I}} I_i T^{-1}$ is also direct. Thus, by the preceding, $\mathcal{I}$ is finite and R satisfies max-rc.

Now let $\text{r.ann}_R(x_1) \subseteq \text{r.ann}_R(x_2) \subseteq \cdots$ be an ascending chain of right annihilators of elements in R. Set $X_n = \{x_n, x_{n+1}, \dots\}$, so that clearly $\text{r.ann}_R(x_n) = \text{r.ann}_R(X_n)$. Now let $S = RT^{-1}$ and observe that $X_n \supseteq X_{n+1}$ for all $n \geq 1$. It follows that $\text{r.ann}_S(X_1) \subseteq \text{r.ann}_S(X_2) \subseteq \cdots$ is an ascending chain of right ideals of S and, since S is Noetherian, this chain must terminate. But $\text{r.ann}_S(X_n) \cap R = \text{r.ann}_R(X_n) = \text{r.ann}_R(x_n)$, so $\text{r.ann}_R(x_1) \subseteq \text{r.ann}_R(x_2) \subseteq \cdots$ must also terminate. □

In other words, if $\mathbf{Q}_{\text{cl}}(R)$ exists and is a Wedderburn ring, then R must be a Goldie ring. For the converse, we use the Goldie assumption in a number of ways. To start with, Lemma 20.4(i) states that any semiprime ring with max-ra has no nonzero nil right or left ideal. In addition, the next result uses max-rc to prove an essential version of Fitting's Lemma.

LEMMA 26.3 *Let R satisfy max-rc and let $a \in R$ with $\text{r.ann}_R(a) = \text{r.ann}_R(a^2)$. Then $\big(aR \dotplus \text{r.ann}_R(a)\big)$ ess R.*

PROOF First, if $x \in aR \cap \text{r.ann}_R(a)$, then $x = ar$ for some $r \in R$ and $0 = ax = a^2 r$. Thus $r \in \text{r.ann}_R(a^2) = \text{r.ann}_R(a)$ and $x = ar = 0$. In other words, $aR \cap \text{r.ann}_R(a) = 0$ and hence $aR \dotplus \text{r.ann}_R(a)$ is direct.

Next, we claim that $\text{r.ann}_R(a^n) = \text{r.ann}_R(a)$ for all $n \geq 1$. Indeed, let $n > 1$ and suppose by induction that $\text{r.ann}_R(a^{n-1}) = \text{r.ann}_R(a)$. If $y \in \text{r.ann}_R(a^n)$, then $ay \in \text{r.ann}_R(a^{n-1}) = \text{r.ann}_R(a)$ and hence $a^2 y = 0$. Thus $y \in \text{r.ann}_R(a^2) = \text{r.ann}_R(a)$ and this fact is proved.

Finally let I be any nonzero right ideal of R and consider the infinite sum $\sum_{i=1}^{\infty} a^i I$. By max-rc, this cannot be a direct sum of nonzero right ideals of R and thus there must exist a relation

$$a^n b_0 + a^{n+1} b_1 + \cdots + a^{n+m} b_m = 0$$

with all $b_i \in I$ and $b_0 \neq 0$. Note that $n \geq 1$, by our assumption on the powers in the infinite sum, and

$$b_0 + a b_1 + \cdots + a^m b_m \in \text{r.ann}_R(a^n)$$

Thus $b_0 \in aR + \text{r.ann}_R(a^n) = aR \dotplus \text{r.ann}_R(a)$ and, since $b_0 \in I \setminus 0$, we conclude that $I \cap \big(aR \dotplus \text{r.ann}_R(a)\big) \neq 0$. But $I \neq 0$ is arbitrary and therefore $aR \dotplus \text{r.ann}_R(a)$ is essential in R. □

DEFINITION If V is an R-module, then

$$\mathrm{Sing}(V) = \{\, v \in V \mid \mathrm{r.ann}_R(v) \operatorname{ess} R \,\}$$

is called the *singular submodule* of V. In particular, V is said to be *nonsingular* when $\mathrm{Sing}(V) = 0$. If $V = R_R$, then $\mathrm{Sing}(R)$ is called the (right) *singular ideal* of R and if $\mathrm{Sing}(R) = 0$, then R is a *nonsingular ring*. The following lemma justifies all this nomenclature.

LEMMA 26.4 *Let V be an R-module.*

i. $\mathrm{Sing}(V)$ *is a submodule of* V.

ii. If $W \subseteq V$, *then* $\mathrm{Sing}(W) = W \cap \mathrm{Sing}(V)$. *Furthermore, if* $V = \oplus \sum_{i=1}^{n} V_i$, *then* $\mathrm{Sing}(V) = \oplus \sum_{i=1}^{n} \mathrm{Sing}(V_i)$.

iii. $\mathrm{Sing}(R)$ *is a two-sided ideal of* R.

PROOF (i) Let $v, w \in \mathrm{Sing}(V)$. Then $\mathrm{r.ann}_R(v)$ and $\mathrm{r.ann}_R(w)$ are both essential right ideals of R and hence so is $\mathrm{r.ann}_R(v) \cap \mathrm{r.ann}_R(w)$, by Lemma 23.3(ii). Thus, since $\mathrm{r.ann}_R(v+w) \supseteq \mathrm{r.ann}_R(v) \cap \mathrm{r.ann}_R(w)$, we have $\mathrm{r.ann}_R(v+w) \operatorname{ess} R$ and $v + w \in \mathrm{Sing}(V)$. Now let $s \in R$. Since the residual $s^{-1}\mathrm{r.ann}_R(v)$ is essential in R, by Lemma 25.10(ii), and $vs \cdot s^{-1}\mathrm{r.ann}_R(v) \subseteq v \cdot \mathrm{r.ann}_R(v) = 0$, we have $\mathrm{r.ann}_R(vs) \supseteq s^{-1}\mathrm{r.ann}_R(v)$ and $\mathrm{r.ann}_R(vs) \operatorname{ess} R$. Thus $vs \in \mathrm{Sing}(V)$.

(ii) The first part is clear, since membership in $\mathrm{Sing}(V)$ is an elementwise condition. The second follows immediately from Lemma 23.3(ii), since $\mathrm{r.ann}_R(\oplus_i v_i) = \bigcap_i \mathrm{r.ann}_R(v_i)$.

(iii) We already know that $\mathrm{Sing}(R)$ is a right ideal of R. Now let $x \in \mathrm{Sing}(R)$ and let $r \in R$. Since $\mathrm{r.ann}_R(rx) \supseteq \mathrm{r.ann}_R(x)$, it follows that $\mathrm{r.ann}_R(rx) \operatorname{ess} R$ and therefore $rx \in \mathrm{Sing}(R)$. □

The singular submodule is not a *radical* in the sense that $V/\mathrm{Sing}(V)$ need not be nonsingular. Furthermore, we remark that the left and right singular ideals of a ring need not be equal. See the exercises for more details.

LEMMA 26.5 *Let R be a Goldie ring.*

i. $\mathrm{Sing}(R)$ *is a nil ideal. In particular, if R is semiprime, then R is nonsingular.*

ii. If $d \in R$ *with* $\mathrm{r.ann}_R(d) = 0$, *then* $dR \operatorname{ess} R$. *In particular, if R is nonsingular, then d is regular in R.*

PROOF (i) Suppose by way of contradiction that $\mathrm{Sing}(R)$ is not nil. Then, by max-ra, we can choose $a \in \mathrm{Sing}(R)$ to be a nonnilpotent element

whose right annihilator $\mathrm{r.ann}_R(a)$ is maximal in the set

$$\{\,\mathrm{r.ann}_R(b) \mid b \in \mathrm{Sing}(R) \text{ and } b \text{ is not nilpotent}\,\}$$

Note that $\mathrm{r.ann}_R(a^2) \supseteq \mathrm{r.ann}_R(a)$ and that a^2 is also a nonnilpotent element of $\mathrm{Sing}(R)$. Thus $\mathrm{r.ann}_R(a^2) = \mathrm{r.ann}_R(a)$, by the maximality of $\mathrm{r.ann}_R(a)$, and Lemma 26.3 implies that the sum $aR \dotplus \mathrm{r.ann}_R(a)$ is direct. But $a \in \mathrm{Sing}(R)$, so $\mathrm{r.ann}_R(a) \operatorname{ess} R$ and hence $aR = 0$, a contradiction. It follows that $\mathrm{Sing}(R)$ is nil and, therefore, if R is semiprime, then Lemma 20.4(i) implies that R is nonsingular.

(ii) Since $\mathrm{r.ann}_R(d) = 0$, it follows that $\mathrm{r.ann}_R(d^2) = 0 = \mathrm{r.ann}_R(d)$. Thus $dR = dR \dotplus \mathrm{r.ann}_R(d)$ is essential in R, by Lemma 26.3. Furthermore, if $x \in \mathrm{l.ann}_R(d)$, then $\mathrm{r.ann}_R(x) \supseteq dR$ and therefore $\mathrm{r.ann}_R(x) \operatorname{ess} R$. In other words, $\mathrm{l.ann}_R(d) \subseteq \mathrm{Sing}(R) = 0$ as required. □

As we mentioned at the end of the previous chapter, Lemma 25.11 will be used to prove the existence of a Wedderburn ring of quotients. Indeed, part (ii) already yields hypothesis (i) of that lemma and the key hypothesis (ii) is proved next.

LEMMA 26.6 *Let R be a semiprime Goldie ring. If I is an essential right ideal of R, then I contains a regular element of R.*

PROOF We first note that any nonzero right ideal X of R contains a nonzero element x with $\mathrm{r.ann}_R(x) = \mathrm{r.ann}_R(x^2)$. Indeed, since R is semiprime, we know that X is not nil by Lemma 20.4(i). Thus, we can choose x to be a nonnilpotent element of X such that $\mathrm{r.ann}_R(x)$ is maximal in the set

$$\{\,\mathrm{r.ann}_R(y) \mid y \in X \text{ and } y \text{ is not nilpotent}\,\}$$

Since x^2 is not nilpotent and $\mathrm{r.ann}_R(x^2) \supseteq \mathrm{r.ann}_R(x)$, it follows that these two annihilators are equal.

Suppose, by way of contradiction, that I contains no element d with $\mathrm{r.ann}_R(d) = 0$. We construct, by induction on n, a sequence $a_0, a_1, \ldots$ of nonzero elements of I satisfying

1. $\mathrm{r.ann}_R(a_i) = \mathrm{r.ann}_R(a_i^2)$ for all i,
2. $a_i a_j = 0$ for all $i < j$, and
3. $a_1R \dotplus a_2R \dotplus \cdots \dotplus a_nR$ is a direct sum.

To start with, the $n = 1$ case follows from the observation of the preceding paragraph. Now suppose $a_1, a_2, \ldots, a_n$ are given satisfying (1)–(3) and set

$$b = a_1 + a_2 + \cdots + a_n \in a_1R \dotplus a_2R \dotplus \cdots \dotplus a_nR$$

Since the latter sum is direct, it follows that $0 \neq b \in I$ and $\text{r.ann}_R(b) = \bigcap_1^n \text{r.ann}_R(a_i)$.

Now by assumption, I contains no right regular element, so we have $\text{r.ann}_R(b) \neq 0$ and hence $X = \text{r.ann}_R(b) \cap I \neq 0$, since $I \operatorname{ess} R$. The observation of the first paragraph therefore implies that there exists $0 \neq a_{n+1} \in X$ with $\text{r.ann}_R(a_{n+1}) = \text{r.ann}_R(a_{n+1}^2)$. Moreover, since $a_{n+1} \in \text{r.ann}_R(b) = \bigcap_1^n \text{r.ann}_R(a_i)$, we have $a_i a_{n+1} = 0$ for all $i < n+1$. Finally, let

$$y \in (a_1 R \dotplus a_2 R \dotplus \cdots \dotplus a_n R) \cap a_{n+1} R$$

and write $y = \sum_{j=1}^n a_j r_j$ with $r_j \in R$. We show in turn that each summand $a_j r_j$ is zero. Indeed, suppose $a_j r_j = 0$ for all $j < i \leq n$. Since $y \in a_{n+1} R$ and $y = \sum_{j=i}^n a_j r_j$, we have

$$0 = a_i y = \sum_{j=i}^{n} a_i a_j r_j = a_i^2 r_i$$

by (2). Thus $r_i \in \text{r.ann}_R(a_i^2) = \text{r.ann}_R(a_i)$ and $a_i r_i = 0$. We conclude that all $a_j r_j = 0$ and hence $y = 0$. In other words, we have shown that $\sum_{i=1}^{n+1} a_i R$ is a direct sum and therefore the inductive statement is proved.

But (3) implies that $\cdot \sum_{i=1}^{\infty} a_i R$ is an infinite direct sum of nonzero right ideals, a conclusion that contradicts max-rc. Thus I must contain an element $d \neq 0$ with $\text{r.ann}_R(d) = 0$. Since R is semiprime, the preceding lemma implies that $\text{l.ann}_R(d) = 0$ and therefore $d \in I$ is regular. □

We need just one more fact.

LEMMA 26.7 *Suppose $A \lhd R$ and that $B = \text{l.ann}_R(A)$.*

i. $B \lhd R$.

ii. If T is a right denominator set in R, then $BT^{-1} \lhd RT^{-1}$.

iii. If A is nilpotent, then $B \operatorname{ess} R$.

PROOF (i) It is clear that B is a left ideal of R. Furthermore, $(BR)A \subseteq BA = 0$, so $BR \subseteq B$.

(ii) By Lemma 25.8(i), BT^{-1} is at least a right ideal of R. To show that it is closed under left multiplication, let $b \in B$ and $t \in T$. Then, by the right denominator condition, there exist $b_1 \in R$ and $t_1 \in T$ with $tb_1 = bt_1 \in B$. In particular, $tb_1 A = 0$ and, since t is regular, it follows that $b_1 A = 0$ and $b_1 \in B$. Thus $t^{-1}b = b_1 t_1^{-1}$ implies that $T^{-1}B \subseteq BT^{-1}$ and therefore

$$(RT^{-1})(BT^{-1}) \subseteq R(BT^{-1})T^{-1} = BT^{-1}$$

(iii) Let X be a nonzero right ideal of R. Since A is nilpotent, we can choose $n \geq 0$ maximal with $XA^n \neq 0$. Then $XA^n \subseteq \text{l.ann}_R(A) = B$, so $0 \neq XA^n \subseteq X \cap B$ and $B \operatorname{ess} R$. □

We can now obtain the main result of this chapter.

THEOREM 26.8 (Goldie's Theorem) *The ring R has a Wedderburn classical ring of quotients $\mathbf{Q}_{\text{cl}}(R)$ if and only if R is semiprime and satisfies max-rc and max-ra.*

PROOF Let T denote the multiplicatively closed set of regular elements of R and suppose that R is a semiprime Goldie ring. Then Lemma 26.5(ii) implies that $tR \operatorname{ess} R$ for all $t \in T$ and, by Lemma 26.6, any essential right ideal of R contains an element of T. It therefore follows from Lemma 25.11 that $\mathbf{Q}_{\text{cl}}(R)$ exists and is a Wedderburn ring.

Conversely suppose $\mathbf{Q}_{\text{cl}}(R) = RT^{-1}$ is a Wedderburn ring. Then RT^{-1} is Artinian, so R is a Goldie ring by Lemma 26.2. Futhermore, if N is a nilpotent two-sided ideal of R, then the preceding lemma implies that $B = \text{l.ann}_R(N)$ is an essential right ideal of R and hence $BT^{-1} \operatorname{ess} RT^{-1}$ by Lemma 25.8(ii). But RT^{-1} is a Wedderburn ring and therefore it has no proper essential right ideal. It follows that $1 \in BT^{-1}$, so $B \cap T$ is nonempty; since $(B \cap T)N = 0$, we conclude that $N = 0$. □

COROLLARY 26.9 *The ring R has a simple Wedderburn ring of quotients $\mathbf{Q}_{\text{cl}}(R)$ if and only if R is prime and satisfies max-ra and max-rc.*

PROOF If $\mathbf{Q}_{\text{cl}}(R) = RT^{-1}$ is a simple Wedderburn ring, then R is certainly a Goldie ring. Furthermore, let A be an ideal of R with $B = \text{l.ann}_R(A) \neq 0$. Then $B \lhd R$ and $0 \neq BT^{-1} \lhd RT^{-1}$ by Lemma 26.7. Since RT^{-1} is simple, this implies that $1 \in BT^{-1}$, so $B \cap T \neq \emptyset$. But $(B \cap T)A = 0$, so $A = 0$ and R is a prime ring.

Conversely, let R be a prime Goldie ring. Then $\mathbf{Q}_{\text{cl}}(R)$ exists and is a Wedderburn ring. Let $I, J \lhd \mathbf{Q}_{\text{cl}}(R)$ with $IJ = 0$. Then $(I \cap R)(J \cap R) = 0$ and, since R is prime, one of these intersection ideals must be zero. But $I \cap R = 0$ implies $I = 0$, so we conclude that $\mathbf{Q}_{\text{cl}}(R)$ is prime. Finally, since a prime Wedderburn ring is clearly simple, the result follows. □

As we observed in the last chapter, the free algebra $R = K\langle x, y\rangle$ is a domain and hence is a semiprime ring with max-ra. But R does not have a classical ring of quotients. Thus R cannot satisfy max-rc and indeed it is easy to see that the sum $\sum_{n=0}^{\infty} y^n xR$ is direct.

Now it turns out that nonsingular rings also play an important role in the study of the maximal ring of quotients and indeed they were originally defined in that context. We close this chapter by discussing the structure of $\mathbf{Q}_{\max}(R)$ when R is assumed to be nonsingular. To start with, we need:

LEMMA 26.10 *Suppose R is a nonsingular ring and write $E = \mathbf{E}(R)$ and $H = \mathrm{End}_R(E)$.*

i. E is a nonsingular R-module.

ii. Every essential right ideal of R is dense.

iii. If $V \operatorname{ess} E$ and $hV = 0$ for some $h \in H$, then $h = 0$.

PROOF (i) This is immediate from Lemma 26.4(ii), since $e_0R \operatorname{ess} E$ and $e_0R \cong R$ is a nonsingular R-module.

(ii) If I is an essential right ideal of R, then $\mathrm{l.ann}_R(I) \subseteq \mathrm{Sing}(R) = 0$. Furthermore, by Lemma 25.10(ii), the residual $r^{-1}I$ is also essential. Thus $\mathrm{l.ann}_R(r^{-1}I) = 0$ for all $r \in R$ and I is dense.

(iii) Let $e \in E$ be arbitrary. Since $V \operatorname{ess} E$, Lemma 25.10(i) implies that there exists an essential right ideal I of R with $eI \subseteq V$. Thus $heI = 0$ and, since I is dense by (ii), Lemma 24.6 implies that $he = 0$. In other words, $hE = 0$ and hence $h = 0$. □

DEFINITION A ring R is said to be *von Neumann regular* if and only if every cyclic right ideal of R is generated by an idempotent. To see what this entails, let $r \in R$ and let $f = rr'$ be an idempotent that generates rR. Then we have $fr = r$ and hence $rr'r = r$. Conversely, suppose we know that r' exists with $rr'r = r$ and set $f = rr'$. Then $fr = rr'r = r$ and $f^2 = frr' = rr' = f$, so f is an idempotent with $fR = rR$. In other words, R is von Neumann regular if and only if for all $r \in R$, there exists $r' \in R$ with $rr'r = r$. Obviously the latter condition is right-left symmetric.

Finally, we prove:

THEOREM 26.11 (Johnson's Theorem) *If R is a nonsingular ring, then $\mathbf{Q}_{\max}(R)$ is a von Neumann regular, self-injective ring.*

PROOF As usual, let $E = \mathbf{E}(R) \supseteq e_0R \cong R$ and write $H = \mathrm{End}_R(E)$ and $Q = \mathbf{Q}_{\max}(R)$. Since $e_0R \operatorname{ess} E$, it follows from part (iii) of the preceding lemma that no nonzero element of H can annihilate e_0. Thus, since $E = He_0$ by Lemma 24.2(i), we see that the map $H \to E$ given by $h \mapsto he_0$ is an H-module isomorphism. In other words, E is isomorphic to the left regular H-module ${}_HH$ and, of course, $\mathrm{End}_H({}_HH) \cong H$ acting on the right. Thus we conclude that $Q = \mathrm{End}_H({}_HE)$ is isomorphic to H

and, since $1H = H$ and 1 corresponds to e_0, we have $e_0Q = E$. But, by Lemma 24.2(ii) and Theorem 24.3, E is the injective hull of the Q-module $e_0Q \cong Q$. Thus $E = e_0Q$ implies that Q is self-injective.

Now let h be a fixed element of H and set $A = \{ e \in E \mid he = 0 \}$. Then A is an R-submodule of E and, by Lemma 23.4(iii), we can choose the R-submodule B of E with $(A \dotplus B)$ ess E. Since B is disjoint from A, the map $\sigma: hB \to E$ given by $hb \mapsto b$ is a well defined R-homomorphism. Thus, since $hB \subseteq E$ and E is injective, σ extends to an R-module endomorphism $h': E \to E$. In other words, $h' \in H$ and $h'hb = b$ for all $b \in B$. Finally, if $a \in A$ and $b \in B$, then $h(a + b) = hb$, so

$$hh'h(a + b) = hh'hb = hb = h(a + b)$$

Thus $hh'h - h \in H$ annihilates the essential R-submodule $A \dotplus B$ and Lemma 26.10(iii) implies that $hh'h - h = 0$. Since $h \in H$ was arbitrary, it follows that H is von Neumann regular. But $Q \cong H$ and therefore the same is true of Q. □

EXERCISES

1. Let $Q = \mathbf{Q}_{\max}(R)$ or $\mathbf{Q}_{\mathrm{r}}(R)$ or $\mathbf{Q}_{\mathrm{s}}(R)$ or $\mathbf{Q}_{\mathrm{cl}}(R)$. If I is a nonzero ideal of Q, prove that $I \cap R \neq 0$. Conclude that if R is prime or semiprime, then the same is true of Q.
2. Let K be a field. Show that the Artinian ring $R = \begin{pmatrix} K & K \\ 0 & K \end{pmatrix}$ is both right and left nonsingular. Conclude that $\mathbf{Q}_{\max}(R) \ncong \mathbf{Q}_{\mathrm{cl}}(R)$. (See Exercise 24.5.)
3. Show that the right and left Noetherian ring $R = \begin{pmatrix} \mathbb{Z} & \mathbb{Z}/2\mathbb{Z} \\ 0 & \mathbb{Z}/2\mathbb{Z} \end{pmatrix}$ is right nonsingular but not left nonsingular. Find an element $d \in R$ with $\mathrm{l.ann}_R(d) = 0$ but $\mathrm{r.ann}_R(d) \neq 0$.
4. Let $W \subseteq V$ be R-modules. If W and V/W are nonsingular, prove that V is nonsingular. Show that $(\mathrm{Sing}(V) + W)/W \subseteq \mathrm{Sing}(V/W)$ but that equality need not occur.
5. Show that $\mathrm{Sing}(R)$ contains no nonzero idempotents. Deduce that a von Neumann regular ring must be nonsingular. In particular, if R is a nonsingular ring, conclude that $\mathbf{Q}_{\max}(R)$ is also nonsingular.
6. Prove that a commutative ring is nonsingular if and only if it is semiprime. If R is the ring of continuous functions on the closed interval $[0, 1]$, show that $\mathbf{Q}_{\max}(R)$ is a commutative von Neumann regular ring with no minimal ideals.

7. If V is an R-module and $V \supseteq W \supseteq \mathrm{Sing}(V)$, define $W^* \supseteq W$ by $W^*/W = \mathrm{Sing}(V/W)$. Prove that $W \operatorname{ess} W^*$ and then use $W \operatorname{ess} W^{**}$ and Lemma 25.10(i) to deduce that $W^* = W^{**}$. In particular, if we define $\mathrm{Sing}_2(V) = \mathrm{Sing}(V)^*$, conclude that $V/\mathrm{Sing}_2(V)$ is nonsingular.
8. Let $V = (\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z})$ be the natural right module for the ring $R = \begin{pmatrix} \mathbb{Z}/4\mathbb{Z} & \mathbb{Z}/4\mathbb{Z} \\ 0 & \mathbb{Z}/4\mathbb{Z} \end{pmatrix}$. Compute $\mathrm{Sing}(V)$ and $\mathrm{Sing}_2(V)$.
9. Assume that $\mathbf{Q}_{\mathrm{cl}}(R)$ exists. If every essential right ideal of R contains a regular element, prove that $\mathbf{Q}_{\max}(R) = \mathbf{Q}_{\mathrm{cl}}(R)$. In particular, if R is a semiprime Goldie ring, conclude that $\mathbf{Q}_{\max}(R) = \mathbf{Q}_{\mathrm{cl}}(R)$.
10. Let R be a semiprime Goldie ring and let V be a right R-module. Assume that, for every $v \in V$ and regular element $t \in R$, there exists a *unique* $v' \in V$ with $v't = v$. Prove that V is injective. In particular, deduce that every $\mathbf{Q}_{\mathrm{cl}}(R)$-module is injective as an R-module.

27. Uniform Dimension

If R is a semiprime Goldie ring, then, by Goldie's Theorem, $\mathbf{Q}_{\mathrm{cl}}(R)$ exists and is a Wedderburn ring. In particular, $\mathbf{Q}_{\mathrm{cl}}(R)$ is a finite direct sum of full matrix rings over division rings. Now it is obviously of interest to determine the sizes of these matrix rings; as we will see, this can be achieved by using uniform dimension.

DEFINITION Let V be an R-module. The *uniform dimension* of V, written $\mathrm{u.dim}\, V = \mathrm{u.dim}_R\, V$, is the largest integer n such that V contains a direct sum $X_1 \dotplus X_2 \dotplus \cdots \dotplus X_n$ of nonzero submodules. If no such maximum exists, then $\mathrm{u.dim}\, V = \infty$. By definition, $\mathrm{u.dim}\, V = 0$ if and only if $V = 0$.

Some elementary properties are as follows.

LEMMA 27.1 *Let W be a submodule of V.*

i. $\mathrm{u.dim}\, W \leq \mathrm{u.dim}\, V$ *with equality if* $W \operatorname{ess} V$.

ii. If $\mathrm{u.dim}\, W = \mathrm{u.dim}\, V < \infty$, *then* $W \operatorname{ess} V$.

iii. If V has composition length k, then $\mathrm{u.dim}\, V \leq k$.

iv. If V is the direct sum of k simple modules, then $\mathrm{u.dim}\, V = k$.

PROOF (i) It is clear that $\mathrm{u.dim}\, W \leq \mathrm{u.dim}\, V$. For the reverse inequality, assume that $W \operatorname{ess} V$. If $X_1 \dotplus X_2 \dotplus \cdots \dotplus X_n$ is a direct sum of nonzero submodules of V, then $Y_i = X_i \cap W \neq 0$ and $Y_1 \dotplus Y_2 \dotplus \cdots \dotplus Y_n$ is a direct sum of nonzero submodules of W.

(ii) If $W \cap X = 0$, then $W \dotplus X \subseteq V$ and clearly

$$\mathrm{u.dim}\, W + \mathrm{u.dim}\, X \leq \mathrm{u.dim}(W \dotplus X) \leq \mathrm{u.dim}\, V = \mathrm{u.dim}\, W$$

Thus $\mathrm{u.dim}\, X = 0$ and $X = 0$.

(iii) This follows since any direct sum $X_1 \dot{+} X_2 \dot{+} \cdots \dot{+} X_n$ of nonzero submodules of V gives rise to a series $0 \subset X_1 \subset X_1 \dot{+} X_2 \subset \cdots$, which has length n.

(iv) Here V has composition length k and V contains a direct sum of k nonzero submodules. □

DEFINITION An R-module U is said to be *uniform* if $\text{u.dim}\, U = 1$. Obviously, such modules are nonzero and we have:

LEMMA 27.2 *If U is a nonzero R-module, then the following are equivalent.*

i. U is uniform.

ii. For all $0 \neq X, Y \subseteq U$, we have $X \cap Y \neq 0$.

iii. For all $0 \neq X \subseteq U$, we have $X \operatorname{ess} U$.

As we indicated earlier, uniform dimension will be used to translate certain numerical information from R to $\mathbf{Q}_{\text{cl}}(R)$. We first require a few simple observations, which we tabulate next.

LEMMA 27.3 *Let T be a right denominator set in R and write $S = RT^{-1}$.*

i. $\text{u.dim}_R R = \text{u.dim}_S S$.

ii. If S is Artinian, then $S = \mathbf{Q}_{\text{cl}}(R)$.

iii. Let A be an ideal of S and let $^-: R \to R/(R \cap A)$ be the natural epimorphism. Then $\bar{T}$ is a right denominator set in $\bar{R}$ and $\bar{R}\bar{T}^{-1} \cong S/A$.

PROOF (i) This is immediate from Lemmas 25.8(iii) and 25.9(iii), since every direct sum of nonzero right ideals of R gives rise to a direct sum of nonzero right ideals of S and vice versa.

(ii) In view of the definition of $\mathbf{Q}_{\text{cl}}(R)$, it suffices to show that every regular element of R is invertible in S. To this end, let $r \in R$ with $\text{r.ann}_R(r) = 0$. If $bt^{-1} \in RT^{-1} = S$ with $r(bt^{-1}) = 0$, then $rb = 0$ and hence $b = 0$. Thus $\text{r.ann}_S(r) = 0$ and Lemma 25.6(i) yields the result.

(iii) Let $^-: S \to S/A$ denote the natural ring epimorphism. If $t \in T$, then t is invertible in S and hence $\bar{t}$ is invertible in $\bar{S}$. It follows that every element of $\bar{S}$ is of the form $\bar{r}\bar{t}^{-1}$ with $r \in R$ and $t \in T$. Since $\bar{T} \subseteq \bar{R}$ is clearly a multiplicative closed set of elements invertible in $\bar{S}$, we conclude that $\bar{S} = \bar{R}\bar{T}^{-1}$. In particular, by Lemma 25.1, $\bar{T}$ is a right denominator set in $\bar{R}$. Finally, since $\bar{R} \cong R/(R \cap A)$, the result follows. □

DEFINITION An ideal P of R is said to be a *minimal prime* if P is a prime ideal that properly contains no other prime. In particular, if P_1 and P_2 are distinct minimal primes, then P_1 and P_2 are *incomparable*. By this we mean that $P_1 \not\supseteq P_2$ and $P_2 \not\supseteq P_1$. A Zorn's Lemma argument shows

that every prime ideal of R contains a minimal prime. More to the point, we have:

LEMMA 27.4 *Let $P_1, P_2, \ldots, P_m$ be incomparable primes of R with product $P_1P_2\cdots P_m = 0$. Then $\{P_1, P_2, \ldots, P_m\}$ is precisely the set of minimal primes of R.*

PROOF If P is a prime ideal of R, then $P \supseteq 0 = P_1P_2\cdots P_m$ and hence $P \supseteq P_i$ for some i. In particular, the minimal primes of P must be contained in the set $\{P_1, P_2, \ldots, P_m\}$. Finally, if some P_j were not minimal, then $P_j \supset P$ for some prime P and $P \supseteq P_i$ by the preceding. Thus $P_j \supset P_i$ and this contradicts the assumed incomparability. □

It is now a simple matter to put this all together.

PROPOSITION 27.5 *Let R be a semiprime Goldie ring with Wedderburn classical ring of quotients given by*

$$\mathbf{Q}_{\mathrm{cl}}(R) = \cdot\sum_{k=1}^{m} \mathrm{M}_{n_k}(D_k)$$

a finite direct sum of full matrix rings over division rings. Then

i. R has precisely m minimal primes $P_1, P_2, \ldots, P_m$ and $\bigcap_i P_i = 0$.

ii. R/P_k is a prime Goldie ring with $\mathbf{Q}_{\mathrm{cl}}(R/P_k) \cong \mathrm{M}_{n_k}(D_k)$ for $k = 1, 2, \ldots, m$.

iii. $n_k = \mathrm{u.dim}_{R/P_k} R/P_k$ and $n_1 + n_2 + \cdots + n_k = \mathrm{u.dim}_R R$.

PROOF By Goldie's Theorem, R has a Wedderburn classical ring of quotients and, by the Artin-Wedderburn Theorem, $S = \mathbf{Q}_{\mathrm{cl}}(R) = \cdot\sum_{k=1}^{m} S_k$, where $S_k \cong \mathrm{M}_{n_k}(D_k)$. For each $k = 1, 2, \ldots, m$, let $A_k = \cdot\sum_{i\neq k} S_i$, so that $A_k \lhd S$ with $S/A_k \cong S_k$. In particular, if we set $P_k = R \cap A_k$, then Lemma 27.3(iii) implies that S_k is isomorphic to a right ring of quotients of R/P_k. Indeed, since S_k is Artinian, we have $S_k \cong \mathbf{Q}_{\mathrm{cl}}(R/P_k)$ by Lemma 27.3(ii). Furthermore, since S_k is a simple ring, Corollary 26.9 implies that R/P_k is a prime Goldie ring. Thus each P_k is a prime ideal of R and (ii) is proved.

Next observe that $\bigcap_k A_k = 0$ and hence $\bigcap_k P_k = 0$. Furthermore the A_k's are clearly incomparable and, since $A_k = P_kS$ by Lemma 25.9(i), it follows that the P_k's are also incomparable. Thus, since

$$P_1P_2\cdots P_m \subsetneq \bigcap_k P_k = 0$$

the previous lemma implies that $P_1, P_2, \ldots, P_m$ are precisely the distinct minimal prime ideals of R and (i) is proved.

Finally, Lemma 27.3(i) implies that $\text{u.dim}_R R = \text{u.dim}_S S$ and, since S_S is completely reducible, Lemma 27.1(iv) implies that $\text{u.dim}_S S$ is equal to the composition length of S_S. Thus Theorem 4.5(i)(ii) yields $\text{u.dim}_R R = n_1 + n_2 + \cdots + n_k$. Moreover, since $\mathbf{Q}_{\text{cl}}(R/P_k) \cong \text{M}_{n_k}(D_k)$, we have $\text{u.dim}_{R/P_k} R/P_k = n_k$ by the case $m = 1$. This completes the proof. □

It follows from the preceding proposition that if R is a semiprime Goldie ring, then R_R has finite uniform dimension. But this can be proved more directly by other means. Indeed, as we will show, if R is any ring and if V is an R-module with max-c, then $\text{u.dim}\, V < \infty$. To start with, we need:

LEMMA 27.6 *Let V be an R-module with max-c and suppose W is a submodule of V.*

i. If $W \neq 0$, then W contains a uniform module.

ii. There exist finitely many uniform submodules $U_1, U_2, \ldots, U_n$ of V such that $W \dotplus U_1 \dotplus U_2 \dotplus \cdots \dotplus U_n$ is essential in V.

PROOF (i) Suppose by way of contradiction that W has no uniform submodule and set $Y_0 = W$. We show by induction on $n = 1, 2, \ldots$ that W contains nonzero submodules X_n and Y_n with $Y_{n-1} \supseteq X_n \dotplus Y_n$. Indeed, if $Y_{n-1} \neq 0$ exists, then Y_{n-1} is not uniform and hence it contains a direct sum of two nonzero submodules. If we label these as X_n and Y_n, then the induction step is proved. But then $\cdot \sum_1^\infty X_i$ is an infinite direct sum and this contradicts the fact that V has max-c.

(ii) Again suppose the result is false. We show by induction on $n = 0, 1, 2, \ldots$ that there exist uniform submodules $U_1, U_2, \ldots$ of V such that the sum $W \dotplus U_1 \dotplus \cdots \dotplus U_n$ is direct. The case $n = 0$ is, of course, trivial. Now suppose that $U_1, \ldots, U_{n-1}$ exist with $W' = W \dotplus U_1 \dotplus \cdots \dotplus U_{n-1}$ a direct sum. Since the result is assumed false, W' is not essential in V. Thus there exists a nonzero submodule X of V disjoint from W' and, by (i), X contains a uniform submodule U_n. In particular, $W' \cap U_n = 0$, so $W \dotplus U_1 \dotplus \cdots \dotplus U_n = W' \dotplus U_n$ is a direct sum and the inductive step is proved. But then $\cdot \sum_1^\infty U_i$ is an infinite direct sum of nonzero submodules of V and this contradicts max-c. □

Next, we prove an analog of the Replacement Theorem from linear algebra.

LEMMA 27.7 *Suppose E is an essential submodule of V and assume that $E = U_1 \dotplus U_2 \dotplus \cdots \dotplus U_n$ is a direct sum of $n < \infty$ uniform modules. Then $n = \text{u.dim}\, V$.*

PROOF It is clear that $\text{u.dim}\, V \geq n$. For the reverse inequality, suppose by way of contradiction that V contains a direct sum $W_1 \dotplus W_2 \dotplus \cdots \dotplus W_{n+1}$ of $n+1$ nonzero submodules W_i. We show by induction on $i = 0, 1, \ldots, n$ that, for a suitable relabeling of the uniform modules U_j, we have the direct sum

$$V_i = U_1 \dotplus \cdots \dotplus U_i \dotplus W_{i+1} \dotplus \cdots \dotplus W_{n+1}$$

The case $i = 0$ is given.

Now suppose that V_i exists for some $i < n$ and set

$$V_i' = U_1 \dotplus \cdots \dotplus U_i \dotplus W_{i+2} \dotplus \cdots \dotplus W_{n+1}$$

Then $V_i = V_i' \dotplus W_{i+1}$ and, in particular, V_i' is not essential in V. Consider the submodule X of E given by

$$X = (U_1 \cap V_i') \dotplus (U_2 \cap V_i') \dotplus \cdots \dotplus (U_n \cap V_i')$$

If $U_j \cap V_i' \neq 0$ for all j, then, since U_j is uniform, we have $(U_j \cap V_i') \operatorname{ess} U_j$ and hence $X \operatorname{ess} E$ by Lemma 23.3(iii). Thus since $E \operatorname{ess} V$, the transitivity of essential extensions implies that $X \operatorname{ess} V$. But $V_i' \supseteq X$, so this yields $V_i' \operatorname{ess} V$, a contradiction. In other words, there exists a subscript j with $U_j \cap V_i' = 0$ and clearly $j \neq 1, 2, \ldots, i$. By relabeling, we can therefore assume that $j = i + 1$ and hence

$$\begin{aligned} V_{i+1} &= V_i' \dotplus U_{i+1} \\ &= U_1 \dotplus \cdots \dotplus U_i \dotplus U_{i+1} \dotplus W_{i+2} \dotplus \cdots \dotplus W_{n+1} \end{aligned}$$

exists. The inductive statement is therefore proved.

Finally, when $i = n$, we obtain $V_n = E \dotplus W_{n+1}$; this is a contradiction, since $E \operatorname{ess} V$. □

As an immediate consequence, we have:

PROPOSITION 27.8 *Let V and V' be R-modules.*

i. $\text{u.dim}\, V < \infty$ *if and only if V satisfies max-c.*

ii. $\text{u.dim}(V \oplus V') = \text{u.dim}\, V + \text{u.dim}\, V'$. *In particular, if V and V' satisfy max-c, then so does $V \oplus V'$.*

PROOF (i) Obviously u.dim $V < \infty$ implies that V satisfies max-c. Conversely, assume that V has max-c. By Lemma 27.6, there exist uniform submodules $U_1, U_2, \ldots, U_n$ such that $E = U_1 \dotplus U_2 \dotplus \cdots \dotplus U_n$ is essential in V. By the preceding lemma, u.dim $V = n < \infty$.

(ii) If either u.dim V or u.dim V' is infinite, then so is u.dim$(V \oplus V')$. Thus we may assume that u.dim V and u.dim V' are both finite and, in particular, that V and V' satisfy max-c. As in the preceding argument, it follows that both V and V' contain uniform submodules U_i and U_j' such that $E = U_1 \dotplus U_2 \dotplus \cdots \dotplus U_s$ is essential in V and $E' = U_1' \dotplus U_2' \dotplus \cdots \dotplus U_t'$ is essential in V'. Furthermore, $s =$ u.dim V and $t =$ u.dim V'. Thus, since $(E \oplus E')$ ess$(V \oplus V')$ by Lemma 23.3(iii) and since $E \oplus E'$ is a direct sum of $s + t$ uniform submodules, we conclude from the previous lemma that u.dim$(V \oplus V') = s + t =$ u.dim $V +$ u.dim V'. □

Next we discuss the behavior of uniform dimension with respect to short exact sequences. To start with, suppose $R = \mathbb{Z}$ is the ring of integers and consider the sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. Then u.dim $\mathbb{Z} =$ u.dim $\mathbb{Q} = 1$, but u.dim $\mathbb{Q}/\mathbb{Z} = \infty$, since $\mathbb{Q}/\mathbb{Z}$ contains a cyclic group of prime order p for each prime p. Thus, in general, u.dim does not add over short exact sequences. Nevertheless, we have:

LEMMA 27.9 *i. Let $W \subseteq V$ be R-modules. If W ess V, then* Sing$(V/W) = V/W$. *Conversely, if* Sing$(V/W) = V/W$ *and if* Sing$(V) = 0$, *then W ess V.*

ii. Let $0 \to A \to B \to C \to 0$ be an exact sequence of R-modules. If Sing$(C) = 0$, *then* u.dim $B =$ u.dim $A +$ u.dim C.

PROOF (i) If W ess V and $v \in V$, then $I = \{ r \in R \mid vr \in W \}$ is an essential right ideal of R by Lemma 25.10(i). But I is the annihilator in R of the element $v + W \in V/W$, so $V/W =$ Sing(V/W).

Conversely, assume that $V/W =$ Sing(V/W) and that Sing$(V) = 0$. Let X be a submodule of V disjoint from W and let $x \in X$. Since $V/W =$ Sing(V/W), there exists an essential right ideal I of R with $xI \subseteq W$. Thus $xI \subseteq W \cap X = 0$ and hence $x \in$ Sing$(V) = 0$. In other words, $X = 0$ and W is essential in V.

(ii) We can assume that $A \subseteq B$ and that $C = B/A$. Furthermore, by Lemma 23.4(iii), we can choose $X \subseteq B$ with $E = A \dotplus X$ essential in B. Since

$$\text{u.dim } B = \text{u.dim } E = \text{u.dim } A + \text{u.dim } X$$

by Lemma 27.1(i) and Proposition 27.8(ii), it clearly suffices to prove that u.dim $X =$ u.dim C. In fact, since $X \cong E/A \subseteq B/A = C$, we need

only show that $\bar{E}$ ess $\bar{B}$, where $\bar{E} = E/A$ and $\bar{B} = B/A$. To this end, observe that E ess B, so (i) implies that $B/E = \text{Sing}(B/E)$ and hence $\bar{B}/\bar{E} = \text{Sing}(\bar{B}/\bar{E})$, since $\bar{B}/\bar{E} \cong B/E$. But $\text{Sing}(\bar{B}) = \text{Sing}(C) = 0$, by assumption, so we conclude from part (i) again that $\bar{E}$ is indeed essential in $\bar{B}$. □

The following lovely theorem has consequences that will not be considered here. We include the result because its proof ties together many of the concepts studied throughout this book. In particular, it uses the fact that modules of finite projective dimension are "close to" being projective and similarly that stably free projective modules are "close to" being free.

THEOREM 27.10 (Walker's Theorem) *Let R be a ring satisfying*

i. R is semiprime and right Noetherian,

ii. $\text{gl dim } R < \infty$, *and*

iii. All finitely generated projective R-modules are stably free.

Then R is a domain.

PROOF Since R is right Noetherian, R is a Goldie ring and all finitely generated R-modules satisfy the ascending chain condition and hence max-c. Furthermore, since R is semiprime, we have $\text{Sing}(R) = 0$ by Lemma 26.5(i). Set $\text{u.dim } R = t$.

Let A be a finitely generated R-module with $\text{Sing}(A) = 0$. We prove that t divides $\text{u.dim } A$. Suppose first that A is free. Then $A \cong R^m$ for some integer $m \geq 0$, so $\text{u.dim } A = m(\text{u.dim } R) = mt$ by Proposition 27.8(ii). Next, suppose that A is projective. Then by assumption, A is stably free and there exist finitely generated free modules F' and F'' with $A \oplus F'' \cong F'$. Thus, by Proposition 27.8(ii) again, $\text{u.dim } A = \text{u.dim } F' - \text{u.dim } F''$ and hence t divides $\text{u.dim } A$. Since $\text{gl dim } R < \infty$, we can now proceed by induction on the projective dimension d of the module A. We have, of course, already considered the case $d = 0$. On the other hand, if $d > 0$, map a finitely generated free R-module F onto A to obtain the short exact sequence $0 \to B \to F \to A \to 0$. Then $\text{pd } B = (\text{pd } A) - 1 = d - 1$ and, since R is Noetherian, B is also finitely generated. Furthermore, since $\text{Sing}(R) = 0$, we have $\text{Sing}(F) = 0$ and hence $\text{Sing}(B) = 0$ by Lemma 26.4(ii). Thus, by induction, t divides $\text{u.dim } B$. But $\text{u.dim } B + \text{u.dim } A = \text{u.dim } F$ by the previous lemma and we know that t divides both $\text{u.dim } B$ and $\text{u.dim } F$. Thus t divides $\text{u.dim } A$ as required.

Now let I be any nonzero right ideal of R. Since $\text{Sing}(R) = 0$, it follows that I is a finitely generated nonsingular right R-module and hence t divides $\text{u.dim } I$. But $0 \neq I \subseteq R$, so $0 < \text{u.dim } I \leq \text{u.dim } R = t$. Thus we

conclude that u.dim I = u.dim R and therefore I ess R by Lemma 27.1(ii). Finally, let $x, y \in R$ with $xy = 0$ and $y \neq 0$. Then r.ann$_R(x) = Y$ is a nonzero right ideal of R, which must be essential by the preceding. Thus $x \in \text{Sing}(R) = 0$ and we conclude that R is a domain. □

As a consequence, since all projective modules of a local ring are free, we have:

COROLLARY 27.11 *Let R be a local ring that is both right Noetherian and semiprime. If* gl dim $R < \infty$, *then R is a domain.*

The next result follows easily from the existence of common denominators in RT^{-1}.

LEMMA 27.12 *Let T be a right denominator set in R.*

i. RT^{-1} is a flat left R-module.

ii. If V is a right RT^{-1}-module and W is an R-submodule with $V = W(RT^{-1})$, then $V \cong W \otimes_R RT^{-1}$.

iii. If V is a finitely generated right RT^{-1}-module, then there exists a finitely generated right R-module W with $V \cong W \otimes_R RT^{-1}$.

PROOF Write $S = RT^{-1}$ and observe, from Lemma 25.2(iv), that any finite set of elements of S can be written with a common denominator.

(i) It follows from the preceding that the collection of all Rt^{-1} with $t \in T$ is a local system of left R-submodules of S. Since each of these submodules is free and hence flat, we conclude from Lemma 9.9(i) that ${}_RS$ is also flat.

(ii) Since the map $W \times S \to V$ given by $(w, s) \mapsto ws$ is easily seen to be balanced, it follows that there exists an additive group homomorphism $\varphi: W \otimes_R S \to V$ determined by $w \otimes s \mapsto ws$. Furthermore, φ is clearly an S-module homomorphism and indeed an epimorphism, since $V = WS$. Thus it suffices to prove that φ is one-to-one.

To this end, let $\sum_i w_i \otimes s_i \in W \otimes S$ and write each s_i as $r_i t^{-1}$, where t is a common denominator. Then

$$\sum_i w_i \otimes s_i = \sum_i w_i \otimes (r_i t^{-1}) = \left(\sum_i w_i r_i\right) \otimes t^{-1}$$

and it follows that every element of $W \otimes S$ can be written as $w \otimes t^{-1}$ for suitable $w \in W$ and $t \in T$. Finally, if $w \otimes t^{-1} \in \text{Ker}(\varphi)$, then $0 = wt^{-1}$, so $w = 0$ and $w \otimes t^{-1} = 0$ as required.

(iii) Finally, if $V = \sum_1^n v_i S$, set $W = \sum_1^n v_i R$. Then $V = WS$ and part (ii) yields the result. □

It is easy to see that hypotheses (ii) and (iii) of Walker's Theorem imply that the Grothendieck group of R is generated by the class $[R]$. Thus the following result extends Theorem 27.10 with a somewhat different proof.

THEOREM 27.13 (Walker's Theorem Revisited) *Let R be a semiprime right Noetherian ring and let H be the subgroup of elements of finite order in $G = \mathbf{G_0}(R)$. If G is generated by H and the element $[R]$, then R is a domain.*

PROOF By Goldie's Theorem, R has a Wedderburn classical right ring of quotients $Q = \mathbf{Q_{cl}}(R)$ and, by the preceding lemma, ${}_RQ$ is flat. Thus Lemma 12.3 implies that the induced module map $A \mapsto A \otimes_R Q$ determines a group homomorphism $\theta: \mathbf{G_0}(R) \to \mathbf{G_0}(Q)$ given by $[A] \mapsto [A \otimes Q]$. Indeed, by Lemma 27.12(iii), this map is onto and, by Lemma 12.2, $\mathbf{G_0}(Q)$ is the free abelian group whose generators $[V_1], [V_2], \ldots, [V_k]$ correspond to the isomorphism classes of the finitely many simple Q-modules. It follows that $\mathbf{G_0}(Q)$ has no nonzero elements of finite order, so $\theta(H) = 0$ and the hypothesis implies that $\mathbf{G_0}(Q)$ is generated by $\theta([R]) = [R \otimes_R Q] = [Q]$. In particular, we must have $k = 1$. Furthermore, if V_1 occurs as a composition factor of Q_Q with multiplicity m, then $[Q] = m[V_1]$ and, since $[V_1]$ is a multiple of $[Q]$, we conclude that $m = 1$. In other words, Q is an irreducible right Q-module, so Q is a division ring and $R \subseteq Q$ is certainly a domain. □

EXERCISES

1. Use Zorn's Lemma to prove that every prime ideal of R contains a minimal prime. Conclude that R is semiprime if and only if the intersection of all its minimal primes is zero.
2. Let F be a field and let R be the subring of the strong direct sum $\prod_{n=0}^{\infty} F$ consisting of all sequences that are eventually constant. Thus R consists of all elements $\prod_{n=0}^{\infty} a_n$ such that $a_n \in F$ and $a_k = a_{k+1}$ for all sufficiently large k. First verify that R is a commutative von Neumann regular ring. Next, let I be the ideal of R consisting of all sequences that are eventually 0 and define the R-module homomorphism $\sigma: I \to R$ by $\prod_{n=0}^{\infty} a_n \mapsto \prod_{n=0}^{\infty} f_n a_n$, where $f_n = 0$ for n even and $f_n = 1$ for n odd. Show that σ does not extend to an R-homomorphism $\sigma^*: R \to R$ and conclude that R is not self-injective.
3. Let $R = R_1 \dotplus R_2 \dotplus \cdots \dotplus R_n$ be the direct sum of the n rings R_i. If D is a right ideal of R, prove that $D = D_1 \dotplus D_2 \dotplus \cdots \dotplus D_n$, where

$D_i = D \cap R_i$ and that D is dense if and only if each D_i is dense in R_i. Conclude from Theorem 24.8 that $\mathbf{Q}_{max}(R) = \cdot \sum_i \mathbf{Q}_{max}(R_i)$. Furthermore, prove that $\mathbf{Q}_{cl}(R) = \cdot \sum_i \mathbf{Q}_{cl}(R_i)$ if either side of this equality is assumed to exist.

In the next three problems assume that $I \subseteq R \subseteq S$, where R and S are rings and where $I \lhd S$ with $\text{l.ann}_S(I) = 0$. For example, we could take $S = \mathbb{Z}[\omega]$, where $\omega = (-1 + \sqrt{-3})/2$ is a primitive cube root of 1, $R = \mathbb{Z}[\sqrt{-3}]$, and $I = 2S$.

4. Let $E = \mathbf{E}(S_S)$ so that $R \subseteq S \subseteq E$. Prove that $\text{l.ann}_E(I) = 0$ and that $R_R \text{ ess } E_R$. Furthermore, show that E is an injective R-module. For the latter, first prove that if J is a right ideal of R and if $\sigma: J \to E$ is an R-homomorphism, then σ extends to an S-module homomorphism $\sigma': JS \to E$.
5. Prove that $\mathbf{Q}_{max}(R) = \mathbf{Q}_{max}(S)$. For this, observe that E_R is the injective hull of R_R and note that $\text{End}_R(E) = \text{End}_S(E)$. Furthermore, if R is prime, deduce that $\mathbf{Q}_r(R) = \mathbf{Q}_r(S)$ and $\mathbf{Q}_s(R) = \mathbf{Q}_s(S)$.
6. Now assume that I contains a regular element of S. Prove that $\mathbf{Q}_{cl}(R) = \mathbf{Q}_{cl}(S)$ if either of these two quotient rings is assumed to exist.

Let R be a semiprime ring and let $A, B \lhd R$. Since $(A \cap B)^2 \subseteq AB \subseteq A \cap B$, it follows that $AB = 0$ if and only if $A \cap B = 0$. In particular, $AB = 0$ if and only if $BA = 0$ and hence $\text{r.ann}_R(A) = \text{l.ann}_R(A)$. We use $\text{ann}_R(A)$ to denote this common annihilator. In the next two exercises assume that $P_1, P_2, \ldots, P_n$ are incomparable prime ideals of R with $\bigcap_1^n P_i = 0$.

7. Prove that $N_i = \text{ann}_R(P_i) = \bigcap_{j \neq i} P_j$ and that $\text{ann}_R(N_i) = P_i$. Furthermore, show that $N = \cdot \sum_i N_i$ is an ideal of R with $\text{ann}_R(N) = 0$.
8. Define S to be the ring direct sum $S = \oplus \sum_1^n R/P_i$ and let $\bar{}: R \to S$ be the natural ring embedding. Prove that $\bar{N} \subseteq \bar{R} \subseteq S$ with $\bar{N} \lhd S$ and $\text{ann}_S(\bar{N}) = 0$. Conclude from Exercises 3, 5, and 6 that $\mathbf{Q}_{max}(R) \cong \oplus \sum_i \mathbf{Q}_{max}(R/P_i)$ in general and that $\mathbf{Q}_{cl}(R) \cong \oplus \sum_i \mathbf{Q}_{cl}(R/P_i)$ under appropriate hypotheses.

If R is a Dedekind domain, then the *class group* of R is defined to be the multiplicative group of nonzero fractional ideals of R modulo the subgroup of principal fractional ideals. For example, if R is a principal ideal domain, then $\mathbf{Cl}(R) = \{1\}$ and if R is the ring of integers in an algebraic number field, then it is known that $\mathbf{Cl}(R)$ is finite.

9. Suppose R is a Dedekind domain. If A is a nonzero fractional ideal of R, let $\tilde{A}$ denote its natural image in $\mathbf{Cl}(R)$. Use Lemma 7.6 and Theorem 7.7(i) to prove that $\mathbf{K_0}(R) \cong \mathbb{Z} \oplus \mathbf{Cl}(R)$ via the map determined by $[A] \mapsto 1 \oplus \tilde{A}$. In particular, conclude that $\mathbf{K_0}(R) = \langle [R] \rangle \dotplus H$ with $\langle [R] \rangle$ infinite cyclic and with $H \cong \mathbf{Cl}(R)$. What about the structure of $\mathbf{G_0}(R)$?
10. Let R be a Noetherian domain with division ring of fractions D. If H is the kernel of the induced module map $\mathbf{G_0}(R) \to \mathbf{G_0}(D)$, prove that $\mathbf{G_0}(R)$ is generated by $[R]$ and H. Obtain an analogous result for $\mathbf{K_0}(R)$.

28. Uniform Injective Modules

Our goal in this chapter is to classify the injective R-modules when R is a right Noetherian ring. We start with a key observation, which settles the natural question of whether arbitrary direct sums of injective modules are injective.

PROPOSITION 28.1 *An arbitrary direct sum of injective R-modules is injective if and only if R is a right Noetherian ring.*

PROOF Suppose first that R is Noetherian and let $\{E_i \mid i \in \mathcal{I}\}$ be a collection of injective R-modules. Set $E = \oplus \sum_i E_i$ and let $\sigma: I \to E$ be an R-module homomorphism with I a right ideal of R. Then I_R is finitely generated and, since the image of each generator has only finitely many nonzero components, it follows that $\sigma(I)$ has only finitely many nonzero components. Say $\sigma(I) \subseteq E'$, where $E' = \oplus \sum_{i=1}^{n} E_i$. Since E' is a finite direct sum of injectives, it follows that E' is injective and hence the map $\sigma: I \to E'$ extends to an R-homomorphism $\sigma^*: R \to E' \subseteq E$. Baer's Criterion now implies that E is injective.

For the converse, let $I_1 \subseteq I_2 \subseteq \cdots$ be an increasing sequence of right ideals of R and set $I = \bigcup_n I_n$ so that I is also a right ideal of R. For each n, the injective hull $E_n = \mathbf{E}(R/I_n)$ is an injective R-module and hence, by assumption, $E = \oplus \sum_{n=1}^{\infty} E_n$ is also injective. Now define $\sigma: I \to E$ by $\sigma: x \mapsto \oplus_n (x + I_n)$. Since $I = \bigcup_n I_n$, any such $x \in I$ is contained in some I_m and hence in all I_n with $n \geq m$. Thus $\sigma(x)$ has only finitely many nonzero components and it is indeed contained in E. Since E is injective, σ extends to a map $\sigma^*: R \to E$; say $\sigma^*(1) \in E' = \oplus \sum_{n=1}^{k-1} E_n$. Then $\sigma(I) \subseteq \sigma^*(R) = \sigma^*(1)R$ is also contained in E'. Thus the k-component of each $\sigma(x)$ is zero and we conclude that $I = I_k$. In other words, the

given ascending chain of right ideals stabilizes at k and it follows that R is right Noetherian. □

For the remainder of this chapter, we will assume that R is right Noetherian. A proper right ideal A of R is said to be *meet irreducible* if $A = B \cap C$, for right ideals B and C, implies that $A = B$ or $A = C$. It is clear that A is meet irreducible if and only if 0 is not an intersection of two nonzero submodules of R/A and hence if and only if R/A is a uniform right R-module.

LEMMA 28.2 *Let I be a nonzero injective R-module. The following are equivalent.*

i. I is uniform.

ii. I is the injective hull of a uniform module.

iii. I is isomorphic to the injective hull of some R/A, where A is a meet irreducible right ideal of R.

iv. I is the injective hull of all its nonzero submodules.

v. I is indecomposable; equivalently, it is not the direct sum of nonzero submodules.

PROOF (v)⇒(iv) If $0 \neq X \subseteq I$, then, by Lemma 23.4(iii), $\mathbf{E}(X)$ is a direct summand of $\mathbf{E}(I) = I$. Since I is indecomposable and $\mathbf{E}(X) \neq 0$, we have $\mathbf{E}(X) = I$.

(iv)⇒(iii) Let $0 \neq x \in I$ and set $X = xR \subseteq I$. If Y is any nonzero submodule of X, then, by assumption, $\mathbf{E}(Y) = I$ so $Y \operatorname{ess} I$. It follows that $Y \operatorname{ess} X$ and hence that X is a uniform R-module. Next observe that the map $r \mapsto xr$ is an R-epimorphism from R to X with kernel $A = \operatorname{r.ann}_R(x)$. Thus $X = xR \cong R/A$ and, since X is uniform, A is meet irreducible. Finally, $I = \mathbf{E}(X) \cong \mathbf{E}(R/A)$ as required.

(iii)⇒(ii) This is clear since R/A is uniform.

(ii)⇒(i) If $I = \mathbf{E}(U)$ with U a uniform submodule, then $U \operatorname{ess} I$. Thus $\operatorname{u.dim} I = \operatorname{u.dim} U = 1$ and I is uniform.

(i)⇒(v) This is obvious. □

As we will see, these uniform injectives are the building blocks of the theory. For the uniqueness aspect, we first need:

LEMMA 28.3 *Let $V = \cdot\sum_\beta J_\beta$ be a direct sum of uniform injectives and suppose that $V \supseteq I_1 \dot{+} I_2 \dot{+} \cdots \dot{+} I_n$, a finite direct sum of uniform injectives. Then there exist distinct $\beta_1, \beta_2, \ldots, \beta_n$ such that $I_i \cong J_{\beta_i}$.*

PROOF We proceed by induction on $n \geq 1$ and let $x \in I_1 \setminus 0$. Then $U = xR$ is a uniform cyclic submodule of the uniform module I_1 and, since

$x \in V = \cdot\sum_\beta J_\beta$, we can assume that $U = xR \subseteq V' = J_1 \dot{+} J_2 \dot{+} \cdots \dot{+} J_k$. Let $\pi_i: V \to J_i$ be the natural projection and write $K_i = \mathrm{Ker}(\pi_i)$. Since $U \subseteq V'$, we have $\bigcap_{i=1}^k (U \cap K_i) = 0$; hence, since U is uniform, one of these intersecting submodules must be zero, say $U \cap K_1 = 0$. Now $U \operatorname{ess} I_1$, since I_1 is uniform, and $(I_1 \cap K_1) \cap U = 0$. Thus $I_1 \cap K_1 = 0$ and $I_1 \dot{+} K_1$ is a direct sum. Next note that $I_1 \cong \pi_1(I_1) \subseteq J_1$, so, since J_1 is a uniform injective and $\pi_1(I_1)$ is a nonzero injective submodule, the preceding lemma implies that $\pi_1(I_1) = J_1$ and, in particular, $I_1 \cong J_1$. Furthermore, since $I_1 \dot{+} K_1$ contains the kernel of π_1 and maps onto $\pi_1(V) = J_1$, it follows that $V = I_1 \dot{+} K_1$ and hence $I_2 \dot{+} \cdots \dot{+} I_n$ is contained isomorphically in

$$V/I_1 \cong K_1 = \cdot\sum_{\beta \neq 1} J_\beta$$

The result now clearly follows by induction. □

Recall that if $W \subseteq V$ are R-modules with V injective, then the embedding $\sigma: W \to V$ extends to an R-homomorphism $\sigma^*: \mathbf{E}(W) \to V$. Furthermore, since $W \operatorname{ess} \mathbf{E}(W)$, it follows that σ^* is one-to-one and hence V contains an isomorphic copy of $\mathbf{E}(W)$.

THEOREM 28.4 *Let V be an injective R-module with R a right Noetherian ring. Then V is uniquely a direct sum of uniform injectives.*

PROOF We consider existence and uniqueness separately.

STEP 1 *Existence.*

PROOF Let $\{ J_\alpha \mid \alpha \in \mathcal{A} \}$ be the possibly empty collection of all uniform injective submodules of V. By Zorn's Lemma, there exists a subset $\mathcal{B} \subseteq \mathcal{A}$ maximal with the property that $J = \cdot\sum_{\beta \in \mathcal{B}} J_\beta$ is direct. Since R is Noetherian, Proposition 28.1 implies that J is an injective R-module and hence J is a direct summand of V. Say $V = J \dot{+} X$ so that X, being a direct summand of V, is also injective.

If $X \neq 0$, choose $0 \neq x \in X$. Then xR is a Noetherian R-module, so it satisfies max-c and, by Lemma 27.6(i), it contains a nonzero uniform submodule U. But X is injective, so X contains the uniform injective module $\mathbf{E}(U)$ and hence $J \dot{+} \mathbf{E}(U)$ is a larger direct sum of uniform injectives, a contradiction. Thus $X = 0$ and $J = V$ as required. □

STEP 2 *Uniqueness.*

PROOF Write $V = \cdot\sum_{\beta\in\mathcal{B}} J_\beta$ as before. Let I be a fixed uniform injective R-module and set $\mathcal{C} = \{\beta \in \mathcal{B} \mid J_\beta \cong I\}$. We need to show that V and I determine $|\mathcal{C}|$, a possibly infinite cardinal. Indeed, we will prove that

$$|\mathcal{C}| = \max\{|\mathcal{D}| \mid V \supseteq \cdot\sum_{\delta\in\mathcal{D}} I_\delta \text{ with } I_\delta \cong I\}$$

Since the right-hand side depends only on V and I, this will surely yield the result.

Now $|\mathcal{C}|$ is certainly bounded above by $\max\{|\mathcal{D}|\}$, so we need only obtain the reverse inequality. To this end, suppose that $V \supseteq \cdot\sum_{\delta\in\mathcal{D}} I_\delta$ with all $I_\delta \cong I$. If $\mathcal{C}$ is finite, then the preceding lemma implies that $\mathcal{D}$ is also finite and that $|\mathcal{D}| \leq |\mathcal{C}|$. Thus we may suppose that $\mathcal{C}$ is infinite and hence also that $\mathcal{D}$ is infinite. Write $W = \cdot\sum_{\beta\in\mathcal{B}\setminus\mathcal{C}} J_\beta$, so that none of these summands is isomorphic to I, and note that $V = W \dot{+} \cdot\sum_{\gamma\in\mathcal{C}} J_\gamma$. For each I_δ choose a fixed nonzero element $x_\delta \in I_\delta$ and set $U_\delta = x_\delta R$. Then $I_\delta = \mathbf{E}(U_\delta)$ and we construct a map θ from $\mathcal{D}$ to the finite subsets of $\mathcal{C}$ as follows. Let $\delta \in \mathcal{D}$. Then $x_\delta \in W \dot{+} \cdot\sum_{\gamma\in\mathcal{C}} J_\gamma$ and $\theta(\delta)$ is defined to be the unique minimal finite subset of $\mathcal{C}$ with $x_\delta \in W \dot{+} \cdot\sum_{\gamma\in\theta(\delta)} J_\gamma$.

Now suppose that $\delta_1, \delta_2, \ldots, \delta_t$ are distinct elements of $\mathcal{D}$ having the same image, say $\mathcal{T} \subseteq \mathcal{C}$, under θ. Then, by definition, $U_{\delta_1}, U_{\delta_2}, \ldots, U_{\delta_t}$ are all contained in $Y = W \dot{+} \cdot\sum_{\gamma\in\mathcal{T}} J_\gamma$. Obviously Y is an injective submodule of V and, since

$$Z = U_{\delta_1} \dot{+} U_{\delta_2} \dot{+} \cdots \dot{+} U_{\delta_t} \subseteq Y$$

it follows that Y contains an isomorphic copy of

$$\begin{aligned}\mathbf{E}(Z) &\cong \mathbf{E}(U_{\delta_1}) \oplus \mathbf{E}(U_{\delta_2}) \oplus \cdots \oplus \mathbf{E}(U_{\delta_t}) \\ &\cong I_{\delta_1} \oplus I_{\delta_2} \oplus \cdots \oplus I_{\delta_t} \cong I^t\end{aligned}$$

Thus, by the preceding lemma, $t \leq |\mathcal{T}| < \infty$ and hence the map θ is clearly finite-to-one. In particular, since $\mathcal{C}$ and $\mathcal{D}$ are both infinite sets, this implies that $|\mathcal{D}| \leq |\mathcal{C}|$ and the theorem is proved. □

There are two special cases of particular interest. The first, which we consider next, deals with Artinian rings. The second, which requires some additional preliminaries, deals with commutative Noetherian rings and is contained in Theorem 28.10.

COROLLARY 28.5 *Let R be a right Artinian ring and let $V_1, V_2, \ldots, V_k$ be a complete set of representatives of the irreducible right R-modules. Then*

every injective R-module is uniquely a direct sum of copies of $\mathbf{E}(V_i)$ for $i = 1, 2, \ldots, k$.

PROOF By the Hopkins-Levitzki Theorem, R is Noetherian, so the preceding result applies. Thus it suffices to prove that every uniform injective I is isomorphic to a unique $\mathbf{E}(V_i)$. For this, observe that any nonzero finitely generated submodule of I is Artinian and hence contains a minimal submodule. Thus I contains a minimal submodule V and indeed V is unique, since I is uniform. Thus $I = \mathbf{E}(V) \cong \mathbf{E}(V_i)$ for some unique i. Finally, since each V_j is uniform, we conclude that each $\mathbf{E}(V_j)$ is a uniform injective. □

For the remainder of this chapter, we assume that R is a commutative Noetherian ring.

DEFINITION Let Q be a proper ideal of R. Then Q is said to be a *primary ideal* if $ab \in Q$ implies that $a \in Q$ or $b^n \in Q$ for some integer $n \geq 1$. Thus, for example, any prime ideal of R is primary. Furthermore, if $R = \mathbb{Z}$, then Q is primary if and only if $Q = p^m\mathbb{Z}$ for some prime p. Our interest in primary ideals stems from the following.

LEMMA 28.6 *Let R be a commutative Noetherian ring.*

i. Every ideal of R is a finite intersection of meet irreducible ideals.

ii. Every meet irreducible ideal is primary.

PROOF (i) If this is false, then, since R is Noetherian, we can choose $A \lhd R$ to be a maximal counterexample. Clearly A is not meet irreducible, so $A = B \cap C$ with B and C ideals of R properly larger than A. But $B, C \supset A$ implies that each of B and C is a finite intersection of meet irreducibles. Therefore, the same is true of A, contradiction. Note that, by definition, meet irreducible ideals are proper. Thus it is necessary to view R as an empty intersection of such ideals.

(ii) Let Q be a meet irreducible ideal of R and let V be the uniform right R-module R/Q. Suppose $a, b \in R$ with $ab \in Q$. Since V satisfies a.c.c. on R-submodules, the ascending chain $\text{l.ann}_V(b) \subseteq \text{l.ann}_V(b^2) \subseteq \cdots$ must stabilize and hence $\text{l.ann}_V(b^n) = \text{l.ann}_V(b^{2n})$ for some integer $n \geq 1$.

If $v \in Vb^n \cap \text{l.ann}_V(b^n)$, then $v = v'b^n$ and $0 = vb^n = v'b^{2n}$. Hence $v' \in \text{l.ann}_V(b^{2n}) = \text{l.ann}_V(b^n)$ and $v = v'b^n = 0$. In other words, $Vb^n \cap \text{l.ann}_V(b^n) = 0$ and, since $V = R/Q$ is uniform, one of the latter intersecting submodules must be zero. Note that $ab \in Q$ implies that $a + Q \in \text{l.ann}_V(b) \subseteq \text{l.ann}_V(b^n)$. Thus if $\text{l.ann}_V(b^n) = 0$, then $a \in Q$, whereas if $Vb^n = 0$, then certainly $b^n \in Q$. □

We remark that primary ideals need not be meet irreducible in general. Now it is clear that parts (i) and (ii) combine to yield a *primary decomposition* for every ideal of R. However we seek a somewhat sharper result, along with the appropriate uniqueness. To start with, we show that these primary ideals are close to being prime powers.

Let $I \lhd R$. Then P is said to be a *minimal covering prime* of I if P is a prime ideal containing I and if there exist no primes P' with $P \supset P' \supseteq I$. It is clear that the minimal covering primes of I correspond naturally to the minimal primes of the ring R/I.

LEMMA 28.7 *Let Q be a primary ideal of R and set*

$$P = \sqrt{Q} = \{ r \in R \mid r^n \in Q \text{ for some } n \geq 1 \}$$

Then P is a prime ideal of R containing Q and $P^m \subseteq Q$ for some $m \geq 1$. Furthermore, P is the unique minimal covering prime of Q.

PROOF Since R is commutative, $\sqrt{Q}$ is an ideal of R containing Q. Indeed, $\sqrt{Q}/Q = \text{Nil}(R/Q)$. Now suppose $a, b \in R$ with $ab \in P = \sqrt{Q}$. Then $a^n b^n = (ab)^n \in Q$ for some $n \geq 1$ and, since Q is primary, we conclude that either $a^n \in Q$ or that $b^{nj} \in Q$ for some $j \geq 1$. In either case, a or b is in P and P is prime.

Next, since R is Noetherian, $\sqrt{Q}$ is finitely generated and hence clearly nilpotent modulo Q. In other words, $P^m \subseteq Q$ for some $m \geq 1$. Finally, if P' is a prime ideal containing Q, then $P' \supseteq Q \supseteq P^m$, so $P' \supseteq P$ and P is the unique minimal covering prime of Q. □

It is not true that every primary ideal is a prime power, nor is every prime power a primary ideal (see Exercises 6–10). If Q is primary and if $P = \sqrt{Q}$, then we say that Q is *P-primary*. Notice that Q is P-primary if and only if $ab \in Q$ implies $a \in Q$ or $b \in P$. In particular, if P is a prime, then P is P-primary.

LEMMA 28.8 *Let P be a prime ideal of R.*

i. A finite intersection of P-primary ideals is P-primary.

ii. If Q is P-primary and if X is a nonzero submodule of the R-module R/Q, then X contains a nonzero submodule Y such that $\text{r.ann}_R(y) = P$ for all $0 \neq y \in Y$.

PROOF (i) Suppose $Q_1, Q_2, \ldots, Q_n$ are P-primary and let $Q = \bigcap_1^n Q_i$. If $c \in P$, then some power of c is in each Q_i and hence in Q. It follows that $P = \sqrt{Q}$. Furthermore, if $ab \in Q$ and $b \notin P$, then $a \in Q_i$ for all i, so $a \in Q$.

(ii) Write $X = J/Q$. By the previous lemma, we can choose m minimal with $JP^m \subseteq Q$ and clearly $m \geq 1$. Thus $Y = (JP^{m-1}+Q)/Q$ is a *nonzero* submodule of J/Q and certainly $YP = 0$, since $JP^m \subseteq Q$. On the other hand, suppose $0 \neq y \in Y$ so that $y = a+Q$ for some $a \in R \setminus Q$. If $yb = 0$ with $b \in R$, then $ab \in Q$ and, since $a \notin Q$, we must have $b \in P$. Thus $\text{r.ann}_R(y) = P$ for all such y. □

We say that $I = Q_1 \cap Q_2 \cap \cdots \cap Q_n$ is a *normal primary decomposition* of the ideal I if: (1) the intersection is irredundant, so that no Q_i can be deleted, and (2) each Q_i is P_i-primary and the primes P_i are all distinct. We can now prove:

THEOREM 28.9 (Lasker-Noether Theorem) *If R is a commutative Noetherian ring, then every ideal I of R has a normal primary decomposition. Furthermore, if $I = Q_1 \cap Q_2 \cap \cdots \cap Q_n$ is such a decomposition with Q_i a P_i-primary ideal, then the following hold:*

i. The set $\{P_1, P_2, \ldots, P_n\}$ of corresponding prime ideals contains all the minimal covering primes of I and is uniquely determined by I.

ii. If P_i is a minimal covering prime of I, then the P_i-primary component Q_i is uniquely determined by I.

PROOF It follows from Lemma 28.6 that I is a finite intersection of primary ideals. Furthermore, if several of these are P-primary for the same prime P, then they can be replaced by their intersection, which is also P-primary by Lemma 28.8(i). In this way, we can write $I = Q_1 \cap Q_2 \cap \cdots \cap Q_n$, where each Q_i is a P_i-primary ideal with the P_i's distinct. Finally, delete the redundant Q_i's to obtain a normal primary decomposition for I.

Now suppose $I = Q_1 \cap Q_2 \cap \cdots \cap Q_n$ is such a decomposition with Q_i a P_i-primary ideal and say $P_i^{m_i} \subseteq Q_i$.

(i) If P is a prime ideal of R containing I, then

$$P \supseteq \bigcap_{i=1}^{n} Q_i \supseteq \prod_{i=1}^{n} Q_i \supseteq \prod_{i=1}^{n} P_i^{m_i}$$

Thus $P \supseteq P_i$ for some i and it follows that the minimal elements of the set $\{P_1, P_2, \ldots, P_n\}$ are precisely the minimal covering primes of I.

Again let P be a prime ideal of R. We will show that $P = P_i$ for some i if and only if the R-module $V = R/I$ has a nonzero submodule X with $\text{r.ann}_R(x) = P$ for all $0 \neq x \in X$. Since the latter property depends only on I, this will prove that the set $\{P_1, P_2, \ldots, P_n\}$ is uniquely determined by the ideal I.

To start with, we observe that each P_i has the preceding property. To this end, note that $J_i = \bigcap_{j \neq i} Q_j$ is properly larger than I by irredundancy. Next, since $J_i \cap Q_i = I$, it follows that

$$0 \neq J_i/I = J_i/(J_i \cap Q_i) \cong (J_i + Q_i)/Q_i \subseteq R/Q_i$$

Thus, by Lemma 28.8(ii), $J_i/I \subseteq R/I$ contains a nonzero submodule X_i with $\mathrm{r.ann}_R(x) = P_i$ for all $0 \neq x \in X_i$.

Conversely, suppose P is a prime ideal of R having the property that there exists a nonzero submodule X of V with $\mathrm{r.ann}_R(x) = P$ for all $0 \neq x \in X$. Among all such X, assume that $X = J/I$ is chosen so that J is contained in the largest number of primary components Q_j. Now $J \supset I$, so J is not contained in all Q_j and say $J \not\subseteq Q_i$. We claim that $P = P_i$. First, note that $XP = 0$, so $JP \subseteq I \subseteq Q_i$. Hence, since $J \not\subseteq Q_i$ and since Q_i is P_i-primary, we have $P \subseteq P_i$. On the other hand, observe that $(J \cap Q_i)/I \subseteq J/I = X$ and that $J \cap Q_i$ is contained in more primary components than J. Thus, by the choice of $X = J/I$, it follows that $(J \cap Q_i)/I = 0$ and hence that $J \cap Q_i = I$. But then $JP_i^{m_i} \subseteq JQ_i \subseteq I$, so $P_i^{m_i} \subseteq \mathrm{r.ann}_R(X) = P$ and $P_i \subseteq P$ as required.

(ii) Finally, let P_1 be a minimal covering prime of I and write $J = \bigcap_{i=2}^{n} Q_i$. Then it is clear that the latter intersection is actually a normal primary decomposition for J and hence, by (i), the minimal covering primes of J belong to the set $\{P_2, P_3, \ldots, P_n\}$. In particular, $J \not\subseteq P_1$, since otherwise P_1 would contain one of the minimal covering primes of J, say P_2, and then $P_1 \supset P_2 \supseteq I$, a contradiction.

Consider the R-module $V = R/I$ and notice that $(Q_1/I)J = 0$ because $Q_1 J \subseteq Q_1 \cap J = I$. Thus if

$$X_1 = \{\, v \in V \mid vb = 0 \text{ for some } b \in R \setminus P_1 \,\}$$

then $Q_1/I \subseteq X_1$, since $J \not\subseteq P_1$. On the other hand, if $v = a + I \in X_1$, then $vb = 0$ for some $b \in R \setminus P_1$ and hence $ab \in I \subseteq Q_1$. But Q_1 is P_1-primary, so we conclude that $a \in Q_1$ and $v \in Q_1/I$. In other words, $Q_1/I = X_1$ and, since X_1 is uniquely determined by I and P_1, the result follows. □

Not every prime in the set $\{P_1, P_2, \ldots, P_n\}$ is a minimal covering prime of I. The remaining ones are called the *embedded primes* and their corresponding primary components need not be unique in general.

We close with the promised characterization of injective R-modules.

THEOREM 28.10 (Matlis' Theorem) *Let R be a commutative Noetherian ring.*

i. Every injective R-module is uniquely a direct sum of uniform injective R-modules.

ii. The map $P \mapsto \mathbf{E}(R/P)$ yields a one-to-one correspondence between the prime ideals P of R and the isomorphism classes of uniform injective R-modules.

iii. If P is a prime ideal of R, then every element of $\mathbf{E}(R/P)$ is annihilated by some power of P.

PROOF (i) This is just a special case of Theorem 28.4.

(ii) Let P be a prime ideal of R. If $A, B \lhd R$ with $P = A \cap B$, then $AB \subseteq P$, so $A = P$ or $B = P$. In other words, P is meet irreducible and, by Lemma 28.2, $\mathbf{E}(R/P)$ is a uniform injective R-module. It remains to show that the map $\eta: P \mapsto \mathbf{E}(R/P)$ is one-to-one and onto.

Let I be a uniform injective R-module and let x be any nonzero element of I. If $Q = \text{r.ann}_R(x)$, then $xR \cong R/Q$ and $I = \mathbf{E}(xR) \cong \mathbf{E}(R/Q)$. Furthermore, xR is a uniform module, so Q is meet irreducible and hence P-primary, for some prime P, by Lemmas 28.6(ii) and 28.7. In addition, by Lemma 28.8(ii), R/Q has a nonzero submodule Y with $\text{r.ann}_R(y) = P$ for all $0 \neq y \in Y$. Thus $I \supseteq yR \cong R/P$ and $I = \mathbf{E}(yR) \cong \mathbf{E}(R/P)$. We have, therefore, proved that the map η is onto.

Finally, suppose $\mathbf{E}(R/P) \cong I \cong \mathbf{E}(R/P')$ for primes P and P'. Then I contains an isomorphic copy of R/P and, since P is P-primary, it follows from Lemma 28.8(ii) that I has a nonzero submodule Z with $\text{r.ann}_R(z) = P$ for all $0 \neq z \in Z$. Similarly, I has a nonzero submodule Z' with $\text{r.ann}_R(z') = P'$ for all $0 \neq z' \in Z'$. But I is uniform, so $Z \cap Z' \neq 0$ and by computing the annihilator of any nonzero element of this intersection, we conclude that $P = P'$. Thus η is one-to-one.

(iii) Let $I = \mathbf{E}(R/P)$ and let x be any nonzero element of I. By the preceding, if $Q' = \text{r.ann}_R(x)$, then Q' is P'-primary and $I \cong \mathbf{E}(R/P')$. Uniqueness now implies that $P' = P$ and hence $P^m \subseteq Q'$ for some integer $m \geq 1$. In particular, P^m annihilates x. □

As a consequence, we have:

COROLLARY 28.11 *The uniform injective $\mathbb{Z}$-modules are, up to isomorphism, $\mathbb{Q}$ and $\mathbb{C}_{p^\infty}$ for the various primes p. Furthermore, every injective $\mathbb{Z}$-module is uniquely a direct sum of these.*

PROOF We know that $\mathbb{Z}$ is a commutative Noetherian ring and if P is a prime ideal of $\mathbb{Z}$, then either $P = 0$ or $P = p\mathbb{Z}$ for some prime p. Now $\mathbb{Z}/0 \cong \mathbb{Z}$ and $\mathbf{E}(\mathbb{Z}) \cong \mathbb{Q}$, as we observed in Chapter 23. Furthermore,

$\mathbb{Z}/p\mathbb{Z} \cong \mathbb{C}_p$ and $\mathbf{E}(\mathbb{C}_p) \cong \mathbb{C}_{p^\infty}$. Matlis' Theorem now clearly yields the result. □

EXERCISES

1. Let R be a ring with the property that every projective module is injective and vice versa. Prove that R is Noetherian and self-injective. Furthermore, show that every finitely generated uniform R-module is isomorphic to a submodule of R_R.
2. Conversely, if R is Noetherian and self-injective, show that any projective R-module is injective. If, in addition, every cyclic uniform R-module is isomorphic to a submodule of R, prove that every injective R-module is projective.
3. Suppose R is right Noetherian and that the left regular module ${}_RR$ is injective. Use Exercise 23.3 to show that every proper right ideal of R has a nonzero left annihilator. Conclude that every irreducible R-module is isomorphic to a submodule of R_R.
4. Let V be an R-module with submodules $W_1, W_2, \ldots, W_n$ and asume that $0 = \bigcap_1^n W_i$ is an irredundant intersection. Prove that $\text{u.dim}\, V \geq n$. In particular, if each V/W_i is uniform, show that V is isomorphic to an essential submodule of $\oplus \sum_1^n V/W_i$ and hence that $\mathbf{E}(V) \cong \oplus \sum_1^n \mathbf{E}(V/W_i)$.
5. Suppose V is an R-module with R right Noetherian. Prove that $\text{u.dim}\, V = n < \infty$ if and only if $\mathbf{E}(V)$ is a direct sum of n uniform injectives.
6. Let R be a commutative Noetherian ring, let P be a prime ideal of R, and let $Q \lhd R$ with $P \supseteq Q \supseteq P^m$. If Q is primary, prove that Q is P-primary. If in addition P is a maximal ideal of R, prove that Q is necessarily primary.
7. Let F be a field and set $R = F[x, y]$. If P is the maximal ideal $P = (x, y)$, prove that $Q_1 = (x, y^2)$ is P-primary but not a power of P. Furthermore, observe that $Q_2 = P^2 = (x, y^2) \cap (x^2, y)$ and conclude that Q_2 is a primary ideal that is not meet irreducible.
8. Now suppose R is the polynomial ring $F[x, y, z]$ and let P be the kernel of the homomorphism $R \to F[t]$ given by $x \mapsto t^3$, $y \mapsto t^4$ and $z \mapsto t^5$. Then P is a prime ideal of R containing the polynomials $f_1 = y^2 - xz$, $f_2 = yz - x^3$, and $f_3 = z^2 - x^2y$. If $f \in R$, prove that

$$f \equiv x^2A(z) + xyB(z) + xC(z) + yD(z) + E(z) \mod (f_1, f_2, f_3)$$

for suitable polynomials $A(z), \ldots, E(z)$. Conclude therefore that $P = (f_1, f_2, f_3)$.

9. We continue with the preceding example and show that P^2 is not P-primary and hence not primary. To this end, observe that $f_2^2 - f_1 f_3 = xg$, where $g = x^5 - 3x^2yz + xy^3 + z^3$, and note that $f_2^2 - f_1 f_3 \in P^2$ but that $x \notin P$ and $g \notin P^2$. The latter follows since P^2 is generated by all $f_i f_j$ and hence no element of P^2 can contain a monomial of degree less than 4.
10. Finally, let $R = F[x, y]$ again and consider the ideal $I = (x^2, xy) = (x)(x, y)$. First prove that $I = (x) \cap (y + ax, x^2)$ for any $a \in F$. Next observe that (x) is a prime ideal and that $(x, y)^2 \subseteq (y+ax, x^2) \subseteq (x, y)$ so that $(y + ax, x^2)$ is (x, y)-primary. Conclude that the embedded components in a normal primary decomposition for the ideal I are not unique.

29. Reduced Rank

In this final chapter we consider two related themes in the context of noncommutative Noetherian rings. The first concerns the reduced rank of a module. As we will see, this rank respects short exact sequences and is therefore somewhat better behaved than uniform dimension. The second theme concerns the existence of an Artinian classical ring of quotients. As we will see, there is a beautiful characterization of the rings with this property.

DEFINITION Suppose first that Q is an Artinian ring. Then we recall from the Hopkins-Levitzki and Jordan-Hölder Theorems that every finitely generated Q-module V has a well-defined composition length $\operatorname{len} V = \operatorname{len}_Q V$. Furthermore, if $0 \to U \to V \to W \to 0$ is a short exact sequence, then $\operatorname{len} V = \operatorname{len} U + \operatorname{len} W$ and $\operatorname{len} V = 0$ if and only if $V = 0$.

Now let R be a semiprime Noetherian ring. Then Goldie's Theorem implies that R has a Wedderburn classical right ring of quotients $Q = \mathbf{Q}_{\mathrm{cl}}(R)$. In particular Q is Artinian and, by Lemma 9.11(i), if V is a finitely generated R-module, then $V \otimes_R Q$ is a finitely generated Q-module. The *reduced rank* of V is then defined to be the nonnegative integer

$$\rho(V) = \rho_R(V) = \operatorname{len}_Q(V \otimes_R Q)$$

Basic properties are as follows.

LEMMA 29.1 *Let R be a semiprime Noetherian ring and let V be a finitely generated R-module.*

i. If $0 \to U \to V \to W \to 0$ *is exact, then* $\rho_R(V) = \rho_R(U) + \rho_R(W)$.

ii. If $\eta: V \to V \otimes Q$ *is the natural* R*-module homomorphism given by* $v \mapsto v \otimes 1$, *then the kernel of* η *is equal to*

$$\mathrm{Sing}(V) = \{ v \in V \mid vc = 0 \text{ for some regular element } c \in R \}$$

In particular, $\rho_R(V) = 0$ *if and only if* $V = \mathrm{Sing}(V)$.

PROOF Let $Q = \mathbf{Q}_{\mathrm{cl}}(R)$ so that, by Lemma 27.12(i), ${}_RQ$ is a flat left R-module.

(i) If $0 \to U \to V \to W \to 0$ is exact, then flatness implies that

$$0 \to U \otimes Q \to V \otimes Q \to W \otimes Q \to 0$$

is an exact sequence of Q-modules. In particular, since $V \otimes Q$ has finite composition length and since composition length respects short exact sequences, we conclude that

$$\begin{aligned} \rho_R(V) = \mathrm{len}(V \otimes Q) &= \mathrm{len}(U \otimes Q) + \mathrm{len}(W \otimes Q) \\ &= \rho_R(U) + \rho_R(W) \end{aligned}$$

(ii) Since R is a semiprime Goldie ring, Lemmas 26.5(ii) and 26.6 imply that a right ideal of R is essential if and only if it contains a regular element. Thus

$$\begin{aligned} \mathrm{Sing}(V) &= \{ v \in V \mid \mathrm{r.ann}_R(v) \operatorname{ess} R \} \\ &= \{ v \in V \mid vc = 0 \text{ for some regular element } c \in R \} \end{aligned}$$

In particular, if $v \in \mathrm{Sing}(V)$ and $vc = 0$, then $v \otimes 1 = vc \otimes c^{-1} = 0$ and $v \in \mathrm{Ker}(\eta)$.

Conversely, suppose $v \in \mathrm{Ker}(\eta)$. Since ${}_RQ$ is flat, the natural map $vR \otimes Q \to V \otimes Q$ is one-to-one and, since $0 = v \otimes 1 \in V \otimes Q$, we conclude that $vR \otimes Q = 0$. Furthermore, the map $R \to vR$ given by $r \mapsto vr$ determines an exact sequence $0 \to A \to R \to vR \to 0$, where $A = \mathrm{r.ann}_R(v)$ and hence

$$0 \to A \otimes Q \to R \otimes Q \to vR \otimes Q \to 0$$

is also exact. But $vR \otimes Q = 0$ and, by Lemma 27.12(ii), we have $A \otimes Q \cong AQ$ and $R \otimes Q \cong Q$. Thus $Q = AQ = AT^{-1}$, where T is the set of regular elements of R and hence $1 = at^{-1}$ for suitable $a \in A$ and $t \in T$. In other words, $\mathrm{r.ann}_R(v) \cap T = A \cap T \neq \emptyset$ and hence $v \in \mathrm{Sing}(V)$ as required.

Finally, note that $\rho_R(V) = 0$ if and only if $0 = V \otimes Q = (V \otimes 1)Q$ and hence, by the preceding, if and only if $V = \mathrm{Sing}(V)$. □

This characterization of $\mathrm{Sing}(V)$, when R is a semiprime Noetherian ring, leads to the following more general consideration.

DEFINITION Let T be a multiplicatively closed subset of R. An R-module V is said to be *T-torsion* if every $v \in V$ is annihilated by some $t \in T$. Similarly, V is *T-torsion-free* if $vt = 0$ for $v \in V$, $t \in T$ implies that $v = 0$. In general, a module V need not contain a "torsion submodule," but we do have:

LEMMA 29.2 *Let T be a right denominator set in R.*

i. If V is an R-module, then

$$V_0 = \{ v \in V \mid vt = 0 \text{ for some } t \in T \}$$

is a T-torsion R-submodule of V and V/V_0 is T-torsion-free.

ii. Let $A \lhd R$ with R/A a T-torsion-free left and right R-module. Then $AT^{-1} \lhd RT^{-1}$ and $(AT^{-1}) \cap R = A$. Furthermore, if A is nilpotent, then so is AT^{-1}.

PROOF (i) Suppose $v_1, v_2 \in V_0$ with $v_1 t_1 = v_2 t_2 = 0$ and let $r \in R$. By the right denominator condition, there exist $t_3, t_4 \in T$ and $s_3, s_4 \in R$ with $t_1 t_3 = t_2 s_3$ and $r t_4 = t_1 s_4$. Since $(v_1 + v_2)t_1 t_3 = 0$ and $(v_1 r)t_4 = 0$, it follows that $v_1 + v_2$ and $v_1 r$ are both contained in V_0. In other words, V_0 is an R-submodule of V. Finally, if $v \in V$ has T-torsion modulo V_0, then $vt \in V_0$ for some $t \in T$, so $v(tt') = (vt)t' = 0$ and $v \in V_0$.

(ii) We already know from Lemma 25.8(i) that AT^{-1} is a right ideal of RT^{-1}. To show that it is closed under left multiplication, we proceed as follows. Let $a \in A$ and $t \in T$. By the right denominator condition, there exist $r' \in R$ and $t' \in T$ with $tr' = at' \in A$. In particular, r' corresponds to a T-torsion element in ${}_R(R/A)$ and thus, by assumption, $r' \in A$. Since $t^{-1}a = r'(t')^{-1}$, it therefore follows that $T^{-1}A \subseteq AT^{-1}$ and hence

$$(RT^{-1})(AT^{-1}) \subseteq R(AT^{-1})T^{-1} = AT^{-1}$$

as required.

Next, if $r \in (AT^{-1}) \cap R$, then $r = at^{-1}$ for some $a \in A$ and $t \in T$, so $rt = a \in A$. In this case, r corresponds to a T-torsion element of $(R/A)_R$ so, again by assumption, $r \in A$. Finally, if $A^n = 0$, then $T^{-1}A \subseteq AT^{-1}$ and $T^{-1}T^{-1} = T^{-1}$ yield $(AT^{-1})^n \subseteq A^n T^{-1} = 0$ and the lemma is proved. □

Thus $\mathrm{Sing}(V)$, as described in Lemma 29.1, is the T-torsion submodule of V for T the set of regular elements of R. Furthermore, $\rho_R(V) = \rho_R(V/\mathrm{Sing}(V))$, so ρ_R is, in some sense, the torsion-free rank of V.

DEFINITION Now suppose R is a right Noetherian ring that is not necessarily semiprime. Then, by Lemma 20.4(ii), $N = \mathrm{Nil}(R)$ is the unique largest nilpotent two-sided ideal of R and, say, $N^{k+1} = 0$. Since $\mathrm{Nil}(R/N) = 0$, it follows that R/N is semiprime and therefore N is an intersection of prime ideals of R. On the other hand, if P is any prime of R, then $P \supseteq 0 = N^{k+1}$, so $P \supseteq N$. Thus N is the intersection of all the prime ideals of R and, by definition, N is the *prime radical* of R. Again, since $\bar{R} = R/N$ is a semiprime Noetherian ring, we note that the reduced rank $\rho_{\bar{R}}$ has already been defined.

Let V be a finitely generated R-module and set $V_i = VN^i$ for $i = 0, 1, \ldots, k+1$. Then

$$0 = V_{k+1} \subseteq V_k \subseteq \cdots \subseteq V_0 = V$$

is a series of R-submodules of V with each quotient $\bar{V}_i = V_i/V_{i+1}$ annihilated by N. Thus $\bar{V}_i$ is naturally an $\bar{R}$-module. Furthermore, since R is Noetherian, each V_i is finitely generated and hence so is $\bar{V}_i$. We can now define the *reduced rank* $\rho_R(V)$ to be

$$\rho_R(V) = \sum_{i=0}^{k} \rho_{\bar{R}}(\bar{V}_i)$$

Notice that $\rho_R(V)$ is a nonnegative integer and that if R is semiprime, then $N = 0$, so $\bar{R} = R$ and this new definition agrees with the earlier one.

For the remainder of this chapter we assume that R is a right Noetherian ring with prime radical N satisfying $N^{k+1} = 0$ and we set $\bar{R} = R/N$.

LEMMA 29.3 *Let V be a finitely generated R-module and suppose that*

$$0 = X_{n+1} \subseteq X_n \subseteq \cdots \subseteq X_0 = V$$

is a series of R-submodules with each quotient $\bar{X}_i = X_i/X_{i+1}$ annihilated by N. Then $\bar{X}_i$ is an $\bar{R}$-module and

$$\rho_R(V) = \sum_{i=0}^{n} \rho_{\bar{R}}(\bar{X}_i)$$

PROOF Let $\mathcal{X}$ denote the given X-series and define

$$\sigma(\mathcal{X}) = \sum_{i=0}^{n} \rho_{\bar{R}}(\bar{X}_i)$$

We claim that $\sigma(\mathcal{X}) = \sigma(\mathcal{Y})$ for any two such series $\mathcal{X}$ and $\mathcal{Y}$. Indeed, since $\mathcal{X}$ and $\mathcal{Y}$ have a common refinement by the Schreier-Zassenhaus Lemma, it merely suffices to show that $\sigma(\mathcal{X}) = \sigma(\mathcal{X}')$ when $\mathcal{X}'$ is obtained from $\mathcal{X}$ by adding one more submodule, say X' with $X_{j+1} \subseteq X' \subseteq X_j$. To this end, we note that $\sigma(\mathcal{X}')$ is obtained from $\sigma(\mathcal{X})$ by replacing the summand $\rho_{\bar{R}}(X_j/X_{j+1})$ with $\rho_{\bar{R}}(X_j/X') + \rho_{\bar{R}}(X'/X_{j+1})$. Furthermore,

$$0 \to X'/X_{j+1} \to X_j/X_{j+1} \to X_j/X' \to 0$$

is a short exact sequence of $\bar{R}$-modules and we know that $\rho_{\bar{R}}$ respects such sequences by Lemma 29.1(i). Thus

$$\rho_{\bar{R}}(X_j/X_{j+1}) = \rho_{\bar{R}}(X_j/X') + \rho_{\bar{R}}(X'/X_{j+1})$$

and $\sigma(\mathcal{X}')$ is indeed equal to $\sigma(\mathcal{X})$.

It follows that $\sigma(\mathcal{X}) = \sigma(\mathcal{Y})$ for all such $\mathcal{Y}$. In particular, if $Z_i = VN^i$, then $\sigma(\mathcal{X}) = \sigma(\mathcal{Z})$ and, by definition, $\sigma(\mathcal{Z}) = \rho_R(V)$. □

If I is any ideal of R, we define $\mathcal{C}(I)$ to be the set of elements of R that are regular modulo I. In other words, these are the elements of R that map to the regular elements of R/I. Equivalently, $c \in \mathcal{C}(I)$ if and only if $cr \in I$ or $rc \in I$ implies $r \in I$. Notice that $\mathcal{C}(I)$ is multiplicatively closed and that $\mathcal{C}(0)$ is precisely the set of regular elements of R.

LEMMA 29.4 *Let R be a Noetherian ring and let V be a finitely generated R-module.*

i. If $0 \to U \to V \to W \to 0$ is exact, then $\rho_R(V) = \rho_R(U) + \rho_R(W)$.

ii. $\rho_R(V) = 0$ if and only if V is a $\mathcal{C}(N)$-torsion module.

PROOF (i) We can assume that $U \subseteq V$ and that $W = V/U$. If $U_i = UN^i$ and $X_i = VN^i + U$ for $i = 0, 1, \ldots, k+1$, then

$$0 = U_{k+1} \subseteq \cdots \subseteq U_0 = U = X_{k+1} \subseteq \cdots \subseteq X_0 = V$$

is a series of submodules of V with each quotient annihilated by N. Thus the previous lemma implies that

$$\rho_R(V) = \sum_{i=0}^{k} \rho_{\bar{R}}(U_i/U_{i+1}) + \sum_{i=0}^{k} \rho_{\bar{R}}(X_i/X_{i+1})$$

On the other hand, the first sum here is just $\rho_R(U)$ and, since

$$\frac{X_i}{X_{i+1}} \cong \frac{(VN^i + U)/U}{(VN^{i+1} + U)/U} \cong \frac{WN^i}{WN^{i+1}}$$

the second sum is $\rho_R(W)$. Thus $\rho_R(V) = \rho_R(U) + \rho_R(W)$ as required.

(ii) Now let $V_i = VN^i$ for $i = 0, 1, \ldots, k+1$ and set $\bar{V}_i = V_i/V_{i+1}$. Since $\rho_R(V) = \sum_{i=0}^{k} \rho_{\bar{R}}(\bar{V}_i)$, we see that $\rho_R(V) = 0$ if and only if $\rho_{\bar{R}}(\bar{V}_i) = 0$ for all i. In other words, by Lemma 29.1(ii), $\rho_R(V) = 0$ if and only if each $\bar{V}_i$ is a $\mathcal{C}(N)$-torsion module.

Suppose first that each $\bar{V}_i$ is $\mathcal{C}(N)$-torsion. If $v \in V$, then, by definition, we can choose $c_1, c_2, \ldots, c_k \in \mathcal{C}(N)$ inductively so that $vc_1c_2 \cdots c_i \in V_{i+1}$. Thus, since $V_{k+1} = 0$ and $c_1c_2 \cdots c_k \in \mathcal{C}(N)$, we conclude that V is $\mathcal{C}(N)$-torsion. Conversely if V is $\mathcal{C}(N)$-torsion, then so is every submodule and factor module. In particular, each $\bar{V}_i$ inherits this property. □

As a consequence, we prove a "pseudo-Ore condition" for R.

LEMMA 29.5 *Let $r \in R$ and $c \in \mathcal{C}(0)$. Then there exist $r' \in R$ and $c' \in \mathcal{C}(N)$ with $rc' = cr'$. Furthermore, $\mathcal{C}(0) \subseteq \mathcal{C}(N)$.*

PROOF Since c is regular in R, the map $R \to cR$ given by $s \mapsto cs$ is an R-module isomorphism. In particular, $\rho_R(R) = \rho_R(cR)$, so the previous lemma implies that $\rho_R(R/cR) = 0$ and hence that R/cR is a $\mathcal{C}(N)$-torsion module. By applying this condition to the element $r + cR \in R/cR$, we conclude that there exists $c' \in \mathcal{C}(N)$ with $rc' \in cR$ and thus $rc' = cr'$ for some $r' \in R$.

Finally let $c \in \mathcal{C}(0)$ and apply the pseudo-Ore condition with $r = 1$. Then there exist $d \in \mathcal{C}(N)$ and $s \in R$ with $cs = d$. In particular, if

$$\bar{}: R \to R/N \subseteq \mathbf{Q}_{\mathrm{cl}}(R/N) = Q$$

is the natural homomorphism, then $\bar{c}\bar{s} = \bar{d}$ and, since $\bar{d}$ is invertible in Q, we have $\bar{c}\bar{s}\bar{d}^{-1} = 1$. Thus $\mathrm{l.ann}_Q(\bar{c}) = 0$ and, since Q is Artinian, Lemma 25.6 implies that $\bar{c}$ is invertible in Q. It follows that $\bar{c}$ is regular in R/N and hence that $c \in \mathcal{C}(N)$. □

As we will see, this is a key ingredient in the characterization of Noetherian rings with an Artinian classical right ring of quotients. Indeed, all that remains in the way of preliminaries is the following:

LEMMA 29.6 *Let S be a Noetherian ring.*

i. If T is a right denominator set of S, then ST^{-1} is also Noetherian.

ii. If S has a nilpotent ideal M with S/M an Artinian ring, then S is also Artinian.

PROOF (i) This is immediate from Lemma 25.9(i).

(ii) If $M^{n+1} = 0$, consider the series

$$0 = M^{n+1} \subseteq M^n \subseteq \cdots \subseteq M^1 \subseteq M^0 = S$$

of two-sided ideals of S. Since S is Noetherian, each M^i and each quotient $\bar{S}_i = M^i/M^{i+1}$ is a finitely-generated S-module. Furthermore, since M annihilates $\bar{S}_i$, it follows that $\bar{S}_i$ is naturally a finitely generated module for the Artinian ring $\bar{S} = S/M$. Thus each $\bar{S}_i$ is an Artinian $\bar{S}$-module and hence also an Artinian S-module. In particular, S_S has a finite series with Artinian factors, so we conclude that S_S is also Artinian. □

We can now obtain the promised characterization.

THEOREM 29.7 (Small's Theorem) *Let R be a right Noetherian ring with prime radical N. Then R has an Artinian classical right ring of quotients if and only if $\mathcal{C}(N) = \mathcal{C}(0)$.*

PROOF Suppose first that $\mathcal{C}(N) = \mathcal{C}(0)$ and call this common set T. Then the pseudo-Ore condition of Lemma 29.5 implies that T is a right denominator set of R. In particular, we can form $Q = RT^{-1} = \mathbf{Q}_{\mathrm{cl}}(R)$ and the goal is to show that Q is Artinian. By the previous lemma, we know at least that Q is Noetherian.

Since $T = \mathcal{C}(N)$, it follows that R/N is T-torsion-free as a right and left R-module. Thus Lemma 29.2(ii) implies that $M = NT^{-1}$ is a nilpotent ideal of Q with $M \cap R = N$. Furthermore, by Lemma 27.3(iii), if $^- : R \to R/N$ is the natural ring homomorphism, then $Q/M = \bar{R}\bar{T}^{-1}$. But $T = \mathcal{C}(N)$, so $\bar{T}$ is the set of regular elements of the semiprime Noetherian ring $\bar{R}$ and hence $\bar{R}\bar{T}^{-1} = \mathbf{Q}_{\mathrm{cl}}(R/N)$ is a Wedderburn ring by Goldie's Theorem. In other words, Q is a Noetherian ring having a nilpotent ideal M with Q/M Artinian. The previous lemma now implies that Q is also Artinian.

Conversely, suppose $Q = \mathbf{Q}_{\mathrm{cl}}(R)$ is Artinian and set $T = \mathcal{C}(0)$. By Lemma 29.5, we know that $T = \mathcal{C}(0) \subseteq \mathcal{C}(N)$ and therefore R/N is T-torsion-free as a right and left R-module. Again Lemma 29.2(ii) implies that $M = NT^{-1}$ is a nilpotent ideal of Q with $M \cap R = N$.

Finally, let $c \in \mathcal{C}(N)$. If $c(rt^{-1}) \in M$ for some $r \in R$ and $t \in T$, then $cr \in M \cap R = N$. Since $c \in \mathcal{C}(N)$, it follows that $r \in N$ and hence that $rt^{-1} \in M$. In other words, we have shown that the image of c is right

regular in the Artinian ring Q/M, so Lemma 25.6 implies that this image is invertible. Thus there exists $q \in Q$ with $cq = 1 - m$ and $qc = 1 - m'$ for suitable $m, m' \in M$. But m and m' are nilpotent, so it follows from Lemma 5.1(i) that cq and qc are both invertible in Q and hence so is c. In particular, c is regular in Q and therefore $c \in \mathcal{C}(0)$. We conclude that $\mathcal{C}(N) \subseteq \mathcal{C}(0)$ and the theorem is proved. □

We close with an example of interest. Let K be a field and set $R = K[x, y]/(x^2, xy)$. Then R is a commutative K-algebra generated by the images $\bar{x}$ and $\bar{y}$ of x and y. Furthermore, $N = \text{Nil}(R) = \bar{x}R$ and $R/N \cong K[\bar{y}]$. Thus $\bar{y} \in \mathcal{C}(N)$, but $\bar{x}\bar{y} = 0$, so $\bar{y} \notin \mathcal{C}(0)$. In other words, $\mathcal{C}(N) \neq \mathcal{C}(0)$ and Small's Theorem implies that R does not have an Artinian classical ring of quotients. On the other hand, as we will see in the exercises, every commutative Noetherian ring is embeddable in an Artinian ring.

EXERCISES

1. If S is a ring with one of the following properties, show that S is not embeddable in an Artinian ring.
   i. S has arbitrarily large finite subsets of orthogonal idempotents.
   ii. S does not satisfy the maximal or minimal condition on right annihilators of subsets.
   iii. There exist infinitely many rational primes p with $\text{ann}_S(p) \neq 0$.
2. Suppose S is a subring of the Artinian ring Q. If V is a finitely generated S-module, define $\sigma(V) = \text{len}_Q(V \otimes_S Q)/\text{len}_Q(Q)$. Show that
   i. $\sigma(V)$ is a nonnegative rational number with $\sigma(S) = 1$.
   ii. $\sigma(V_1 \oplus V_2) = \sigma(V_1) + \sigma(V_2)$.
   iii. If $U \to V \to W \to 0$ is an exact sequence, then $\sigma(W) \leq \sigma(V) \leq \sigma(U) + \sigma(W)$.
   Such a function σ is called a *Sylvester rank function.* Amazingly, Schofield has proved that every algebra with a Sylvester rank function is embeddable in an Artinian ring.
3. Let X be a subset of the ring S and assume that S is contained in a right Artinian ring or in a left Noetherian ring. Prove that there exists a finite subset $X_0 \subseteq X$ with $\text{r.ann}_S(X) = \text{r.ann}_S(X_0)$.
4. Let e and f be idempotents in a ring S. Suppose first that $e = uv$ and $f = vu$ for some $u, v \in S$ and define $\alpha: eS \to S$ by $\alpha(es) = ves$. Prove that α determines an S-isomorphism from eS to fS. Conversely,

suppose that there exists an S-isomorphism $\alpha\colon eS \to fS$. Prove that $e = uv$ and $f = vu$ for some $u, v \in S$.

5. Suppose R is a right Noetherian ring containing the Wedderburn ring S and write $S = \cdot\sum_{i=1}^{k} S_i$, a direct sum of simple rings. If f_i is a primitive idempotent of S_i, prove that

$$\text{u.dim}_R R = \sum_{i=1}^{k} (\text{u.dim}_S S_i)(\text{u.dim}_R f_i R)$$

To this end, first observe that $S_i \cong \mathrm{M}_{n_i}(D_i)$ has a family of orthogonal primitive idempotents $\{ f_{i,1}, f_{i,2}, \ldots, f_{i,n_i} \}$ with $n_i = \text{u.dim}_S S_i$ and $f_{i,j} S_S \cong f_i S_S$. Then note that $\{ f_{i,j} \}$ is an orthogonal decomposition of 1 in R and hence that $R = \cdot\sum_{i,j} f_{i,j} R$. Finally, use the preceding exercise to conclude that $f_{i,j} R_R \cong f_i R_R$. This is a special case of the *additivity principle.*

6. Let R be the ring $R = \begin{pmatrix} \mathbb{Z} & \mathbb{Z}/p\mathbb{Z} \\ 0 & \mathbb{Z}/p\mathbb{Z} \end{pmatrix}$, where p is any prime. Show that R is right and left Noetherian and that $N = \text{Nil}(R) = \begin{pmatrix} 0 & \mathbb{Z}/p\mathbb{Z} \\ 0 & 0 \end{pmatrix}$. Prove that $\mathcal{C}(N) \neq \mathcal{C}(0)$ and that the right and left reduced ranks of the (R, R)-bimodule N are distinct.

7. Suppose $A = \mathrm{A}_1(K)$ is the first Weyl algebra over a field K of characteristic 0 and let $0 \subset B \subset A$ be a proper right ideal of A. Note that $A/B = \text{Sing}(A/B)$, since $B \operatorname{ess} A$, and that $\text{r.ann}_A(A/B) = 0$, since this annihilator must be a proper two-sided ideal of A. Now define $R = \begin{pmatrix} K & A/B \\ 0 & A \end{pmatrix}$ and observe that R has a natural ring structure and as such it is a right Noetherian ring. If $X = \begin{pmatrix} 0 & A/B \\ 0 & 0 \end{pmatrix}$, show that every finite subset X_0 of X is annihilated by some $\begin{pmatrix} 0 & 0 \\ 0 & E \end{pmatrix}$ with $E \operatorname{ess} A$. Conclude from Exercise 3 that R cannot be embedded in a right Artinian ring or a left Noetherian ring.

In the remaining problems, let R denote a commutative Noetherian ring.

8. Let P be a prime ideal of R. For each integer $n \geq 1$, show that there exists a unique P-primary component for the ideal P^n. We denote this component by $P^{(n)}$ and call it the nth *symbolic power* of P. Suppose in addition that R is an integral domain and set $R_P = RT^{-1}$, where $T = R \setminus P$. If $P' = PR_P$, prove that $(P')^n \cap R = P^{(n)}$.

9. If R_R is a uniform module, use Lemma 26.3 to show that every element of R is either nilpotent or regular. Conclude that every element of $Q = \mathbf{Q}_{\mathrm{cl}}(R)$ is either nilpotent or invertible and hence that Q is a semiprimary ring. Deduce that Q is also Artinian.
10. Now apply Lemma 28.6 and the previous problem to conclude that any commutative Noetherian ring can be embedded in a commutative Artinian ring. Find an example of a commutative ring that cannot be embedded in an Artinian ring.

Suggested Additional Reading

1. F. Anderson and K. Fuller, "*Rings and Categories of Modules*", Springer-Verlag, Berlin, 1974.
2. M. F. Atiyah and I. G. Macdonald, "*Introduction to Commutative Algebra*", Addison-Wesley, Reading, 1969.
3. K. R. Goodearl and R. B. Warfield, Jr., "*An Introduction to Noncommutative Noetherian Rings*", Cambridge Univ. Press, Cambridge, 1989.
4. I. N. Herstein, "*Noncommutative Rings*", Carus Math. Monograph, AMS, Providence, 1968.
5. N. Jacobson, "*Basic Algebra*", Freeman, San Francisco, 1974 and 1980.
6. I. Kaplansky, "*Commutative Rings*", Univ. of Chicago Press, Chicago, 1974.
7. I. Kaplansky, "*Fields and Rings*", Univ. of Chicago Press, Chicago, 1972.
8. T. Y. Lam, "*Serre's Conjecture*", Springer-Verlag, Berlin, 1978.
9. J. Lambek, "*Lectures on Rings and Modules*", Blaisdell, Waltham, 1966.
10. J. C. McConnell and J. C. Robson, "*Noncommutative Noetherian Rings*", Wiley-Interscience, New York, 1987.
11. D. S. Passman, "*Infinite Crossed Products*", Academic Press, Boston, 1989.
12. J. Rotman, "*An Introduction to Homological Algebra*", Academic Press, New York, 1979.
13. L. Rowen, "*Ring Theory*", Academic Press, Boston, 1988.

Index

A.c.c., *See* ascending chain condition.
Abelian group, divisible, 208.
  structure, 160.
Additivity principle, 292.
Algebra, almost commutative, 180.
  Clifford, 52, 55.
  free, 21, 250.
  Frobenius, 228–230.
  Grassmann, 52.
  group, 41.
  quaternion, 52.
  Weyl, 196.
Algebraic root, 194.
Almost centralizing extension, 180.
Almost commutative algebra, 180.
  Nullstellensatz, 194.
Almost normalizing extension, 188.
α-free module, 181.
Amitsur's Theorem, 192.
$A_m(K)$, *See* Weyl algebra.
Artin-Rees Lemma, 123.
Artin-Wedderburn Theorem, 36.
Artinian module, 28.
Artinian quotient ring, 290.
Artinian ring, 28, 45–50, 52, 81.
  classical quotient ring, 246.
  Grothendieck group, 117.
  injective module, 276.
  projective Grothendieck group, 143.
Ascending chain condition, 58.
Associated graded ring, 177.
Associativity, tensor product, 88.
Automorphism, 6.

Backmap, 14.
Baer sum, 216.
Baer's Criterion, 207, 227.
Baer's Theorem, 209.
Balanced map, 84.
Basis, 16.
Basis Theorem, 106.
Bass' Theorem, 176.
Bimodule, 87, 203.
Bimodule homomorphism, 87.

$\mathbb{C}_{p^n}$, 225–226, 281.
$\mathbb{C}_{p^\infty}$, 225–226, 281.
$c[P]$, *See* Cartan map.
$\mathcal{C}[A]$, *See* cokernel map.
$\mathcal{C}(I)$, 288.
Cartan map, 144.

Cartan matrix, 144, 150.
Change of variables, 161.
Checkered matrix ring, 34, 42.
Chevalley-Jacobson Theorem, 39.
Chinese Remainder Theorem, 31.
Class group, 271.
Classical quotient ring, 245.
  Artinian ring, 246.
  simple Wedderburn, 258.
  Wedderburn, 258.
Clifford algebra, 52, 55.
Closure operation, 234, 247.
Cokernel, 12.
Cokernel map, 214.
Column operations, elementary, 153.
Commutative Noetherian ring, 277–281.
Commuting diagram, 3.
Complete direct sum, *See* strong direct sum.
Completely reducible module, 23–25.
Complex, 13, *See* zero sequence.
Composition, 3.
  left notation, 4.
  right notation, 3.
Composition factors, 26.
Composition length, 26, 284.
Composition series, 26, 47.
  factors, 26.
  length, 26.
Conjugate module, 107.
Contravariant, 204.
Countably generated module, 98.
Covariant, 204.
Cuts across the grade, 128.
Cyclic module, 10, 81.

$\mathbb{D}$, 208.
$\mathcal{D}(R)$, *See* dense ideal.
D.c.c., *See* descending chain condition.
Decomposable module, 49.
Dedekind domain, 66–72.
  class group, 271.
Degree, total, 128.
Denominator set, left, 245.
  right, 242–245.
Dense ideal, 235–238.
  minimum, 238.
Dense ring of transformations, 39.
Density Theorem, 39.
Derivation, 113.
  inner, 113.
Descending chain condition, 28.
Determinantal trick, 159.
Diagram, commuting, 3.
Dimension, global, 76, 81.
  injective, 214.
  projective, 75–81.
  uniform, 262, 264, 266–267.
Direct product, 210.
Direct sum, external, 7.
  internal, 7, 24.
  strong, 7, 210.
  tensor product, 88.
  weak, 7.
Direct summand, 15, 23.
Directed system, 94.
Distributive law, 12.
Divisible abelian group, 208.
Division algebra, finite dimensional, 185.
Division ring, 40.
Domain, 268–270.
  Dedekind, 66–72, 271.
  hereditary, 66–68.
  Ore, 245.
Doubly transitive, 43.
Dual basis, 228.

$\mathrm{E}(A, B)$, *See* extension group.
$\mathrm{E}(A, B) = 0$, 215, 217–220.

$\mathbf{E}(V)$, *See* injective hull.
Eilenberg Trick, 171.
Element, homogeneous, 124.
  normal, 110.
  regular, 256.
Elementary column operations, 153.
Embedded prime ideal, 280.
$\mathrm{End}(V)$, 5.
Endomorphism, 5, 6.
$\mathrm{End}_R(V)$, 6, 33–36.
Epimorphism, 13.
Equivalent extension, 215.
Equivalent matrices, 159.
Equivalent series, 25.
Essential extension, 223.
  transitivity, 223.
Essential ideal, 256.
Essential submodule, 223, 226.
ess_R, *See* essential extension.
Exact, left, 204.
Exact at, 13.
Exact sequence, 13.
Extended centroid, 241.
Extendible row, 152, 163.
Extension, 215.
  almost centralizing, 180.
  almost normalizing, 188.
  Baer sum, 216.
  equivalent, 215.
  essential, 223.
  finite centralizing, 190.
  finite normalizing, 198.
  group, 216.
External direct sum, 7.
$\mathrm{Ext}^n(A, B)$, 217, 222.

Factors through, 8.
Faithful module, 38.
Faithfully flat module, 94.
Field extension, separably generated, 168.
Filtered ring, 177.
Finite centralizing extension, 190.
Finite dimensional division algebra, 185.
Finite normalizing extension, 198.
Finitely generated module, 10, 59.
First Isomorphism Theorem, 8.
Fitting's Lemma, 62–63.
  essential version, 254.
Five Lemma, 21.
Fixed ring, 131.
Flat module, 89–92, 211.
Fractional ideal, 68–70, 271.
Free algebra, 21, 250.
Free basis, 16.
Free module, 16–18.
  rank, 17.
Free resolution, 82.
Frobenius algebra, 228–230.
Function on 2-sphere, 167.
Functional, linear, 228.
Fundamental Theorem of Abelian Groups, 160.

G-domain, 185.
G-graded ring, 131.
$\mathbf{G}_0(R)$, *See* Grothendieck group.
Generator, 178.
Generic flatness, 181, 183, 188.
  vector, 189.
Generic Flatness Theorem, 183.
$\mathrm{gl\,dim}\, R$, *See* global dimension.
Global dimension, 76, 81, 107–113, 220.
  finite, 268.
  injective, 215, 220.
Goldie ring, 253, 256.
  prime, 258, 264.
  semiprime, 258, 264.
Goldie's Theorem, 258.
$\mathrm{gr}\, R$, *See* associated graded ring.

$\mathbf{gr}\,\mathbf{G_0}(R)$, *See* graded Grothendieck group.
Graded, homomorphism, 125.
module, 124–130.
prime ring, 188.
ring, 124–130.
semiprime ring, 188.
submodule, 125.
Graded Artinian ring, 177.
Graded Grothendieck group, 127–130.
Graded Nakayama's Lemma, 127.
Graded Noetherian ring, 130, 177.
Graded ring, 124–130.
graded prime, 188.
graded semiprime, 188.
Jacobson radical, 191.
Graded-free module, 126.
Graded-projective module, 126.
Grassmann algebra, 52.
Grothendieck group, 115–121, 270.
Artinian ring, 117.
graded, 127–130.
integers, 118.
projective, 142–146.
skew polynomial ring, 137–139.
Grothendieck-Quillen Theorem, 138.
Group algebra, 41.
Group ring, 41, 83.

Hairy Ball Theorem, 167, 169–170.
Hereditary domain, 66–68.
Hereditary module, 56.
Hereditary ring, 57, 65, 76.
Herstein's counterexample, 169.
Hilbert Basis Theorem, 106.
Hilbert Nullstellensatz, 195.
Hilbert Syzygy Theorem, 113, 146.
$\mathrm{Hom}(A, B)$, 5.
Homogeneous element, 124.
Homomorphism, 4.
automorphism, 6.
endomorphism, 6.
factors through, 8.
graded, 125.
isomorphism, 6.
module, 6.
ring, 6.
$\mathrm{Hom}_R(A, B)$, 6, 33–36, 203–206.
Hopkins-Levitzki Theorem, 47, 59.

I-adic topology, 169.
IBN ring, 18, 21, 42.
$\mathrm{id}_R V$, *See* injective dimension.
Ideal, dense, 235–238.
essential, 256.
fractional, 68–70, 271.
integral, 68.
invertible, 64–66.
meet irreducible, 274.
minimal prime, 263–264.
nil, 44.
P-primary, 278.
primary, 277, 282.
prime, 60, 66–69, 252, 281, 287, 292.
primitive, 50.
projective, 65.
quasi-regular, 50.
residual, 235.
Idempotent, 29.
lifted, 48.
primitive, 53.
Idempotents, orthogonal, 53.
$\mathrm{Im}(\theta)$, 7.
Image, 7.
Incomparable prime ideal, 263.
Indecomposable module, 49, 63.
Indecomposable projective module, 50.
Induced module, 92, 135–136.
Induced module map, 117, 144.
Infinitely divisible, 21.

inj gl dim R, *See* injective global dimension.
Injective dimension, 214.
Injective global dimension, 215, 220.
Injective hull, 224–226.
Injective module, 206–210, 223.
  Artinian ring, 276.
  integers, 225–226, 281.
  Noetherian ring, 273, 275, 281.
  uniform, 274–276.
Injective resolution, 222.
Injective Schanuel's Lemma, 213–214, 231.
Injective $\mathbb{Z}$-module, 225–226, 281.
Inner, derivation, 113.
Integers, Grothendieck group, 118.
  injective module, 281.
Integral element, 66.
Integral extension, 71.
Integral ideal, 68.
Integrally closed, 66.
Internal direct sum, 7, 24.
Intersection Theorem, 169.
Invariant basis number, 18.
Invertible ideal, 64–66.
Invertible matrix, 17.
Irreducible module, *See* simple module.
Isomorphic modules, 6.
Isomorphism, 6.
Isomorphism invariant, 20.
Isomorphism Theorem, First, 8.
  Second, 9.
  Third, 9.

Jacobson radical, 50–52, 95.
  graded ring, 191.
  not nil, 199.
  polynomial ring, 192.
Jacobson's Conjecture, 169.
Johnson's Theorem, 259.
Jordan-Hölder Theorem, 26.

$\mathcal{K}[A]$, *See* kernel map.
$\mathbf{K_0}(R)$, *See* projective Grothendieck group.
Kaplansky's Theorem, 101.
$\mathrm{Ker}(\theta)$, 7.
Kernel, 7.
Kernel map, 75.
Krull Intersection Theorem, 169.
Krull-Schmidt Theorem, 63.

Lasker-Noether Theorem, 279.
Left exact, 204.
Left module, 5.
Left notation, 4.
Left quotient ring, 245.
$\mathrm{len}\, V$, *See* composition length.
Lexicographical order, 182.
Lifted idempotent, 48.
Linear functional, 228.
Local ring, 96–101, 269.
  projective module, 97, 101.
Local system, 91, 94.
Localization, 97, 174.

Martindale quotient ring, 240.
  symmetric, 241, 249.
Maschke's Theorem, 41, 131.
Matlis' Theorem, 281.
Matrices, equivalent, 159.
Matrix, invertible, 17.
Matrix ring, checkered, 34, 42.
Max, *See* maximum condition.
Max-c, *See* maximum condition, complement.
Max-ra, *See* maximum condition, right annihilator.
Max-rc, *See* maximum condition, complement.
Maximal quotient ring, 233–240.
  center, 239.

Maximum condition, 58.
complement, 253.
right annihilator, 193, 253.
Meet irreducible ideal, 274.
Min, *See* minimum condition.
Minimal covering prime ideal, 278, 279.
Minimal prime ideal, 263–264.
Minimal right ideal, 28.
Minimum condition, 28.
Modular Law, 10.
Module, 5.
α-free, 181.
Artinian, 28.
completely reducible, 23–25.
conjugate, 107.
countably generated, 98.
cyclic, 10, 81.
decomposable, 49.
faithful, 38.
faithfully flat, 94.
finitely generated, 10, 59.
flat, 89–92, 211.
free, 16–18.
graded, 124–130.
graded-free, 126.
graded-projective, 126.
hereditary, 56.
indecomposable, 49, 63.
induced, 92, 135–136.
infinitely divisible, 21.
injective, 206–210, 223, 273, 281.
irreducible, 23, 46.
left, 5.
Noetherian, 58.
nonsingular, 255.
principal indecomposable, 50, 143.
projective, 18–20, 47, 49, 91, 98, 120, 172, 176, 205.
regular, 7.
right, 5.
simple, 23, 46, 49.
stably free, 145, 165.
submodule, 7.
torsion, 286.
torsion free, 92, 174, 286.
uniform, 263.
uniform injective, 274–276.
unital, 6.
Modules, isomorphic, 6.
Monic polynomial, 161.
Monic Polynomial Theorem, 161, 163.
Monomorphism, 13.
Morita correspondence, 122.
Multiplicatively closed, 97.
Multiplicatively closed set, 242.

n-fir, 62.
Nakayama's Lemma, 95.
graded, 127.
Nil(R), *See* nil radical.
Nil ideal, 44.
Nil radical, 45, 52.
Nilpotent element, 44.
Nilpotent right ideal, 28.
Nilpotent subset, 28.
Noether Normalization Theorem, 162.
Noetherian module, 58.
Noetherian ring, 59, 106, 287–291.
commutative, 277–281.
injective module, 273, 275, 281.
semiprime, 268, 270.
Nonsingular, 255.
Nonsingular ring, 259.
Normal element, 110.
Normal primary decomposition, 279.
Normalization Theorem, 162.
Nullstellensatz, 190–199.
almost commutative algebra, 194.
Hilbert, 195.
uncountable field, 198.
Zariski, 187.

Order, lexicographical, 182.
product, 183.
Ore condition, 245.
pseudo, 289.
Ore domain, 245.
Ore extension, 113.
global dimension, 114.
Ore ring, 245, 250.
Ore's Theorem, 244, 250.
Orthogonal idempotents, 53.

P-primary ideal, 278.
Patching Theorem, 157, 163.
$\mathrm{pd}_R V$, *See* projective dimension.
Polynomial, 105.
monic, 161.
Polynomial ring, Jacobson radical, 192.
projective module, 177.
Primary decomposition, 278, 282.
normal, 279.
Primary ideal, 277, 282.
Prime ideal, 60, 66–69, 252, 281, 287, 292.
embedded, 280.
incomparable, 263.
minimal, 263–264.
minimal covering, 278, 279.
Prime radical, 287.
Prime ring, 60, 240, 252.
Primitive ideal, 50.
Primitive idempotent, 53.
Primitive ring, 38–40, 50.
Principal ideal domain, 58, 159.
Principal indecomposable module, 50, 143.
Product order, 183.
Progenerator, 178.
Projective cover, 102, 224.
Projective dimension, 75–81.
Projective Grothendieck group, 142–146.
Artinian ring, 143.
skew polynomial ring, 144.
Projective ideal, 65.
Projective indecomposable module, *See* principal indecomposable module.
Projective module, 18–20, 47, 49, 91, 98, 120, 205.
integer, 22.
local ring, 97, 101.
not finitely generated, 172, 176.
polynomial ring, 177.
Projective resolution, 82, 140.
Projective $\mathbb{Z}$-module, 22.
Pseudo Ore condition, 289.

$\mathbb{Q}$, 225–226, 281.
$\mathbf{Q}_{\mathrm{cl}}(R)$, *See* classical quotient ring.
$\mathbf{Q}_{\max}(R)$, *See* maximal quotient ring.
$\mathbf{Q}_{\mathrm{r}}(R)$, *See* quotient ring, right.
$\mathbf{Q}_{\mathrm{s}}(R)$, *See* quotient ring, symmetric.
Quasi-regular ideal, 50.
Quaternion algebra, 52.
Quillen Patching Theorem, 157, 163.
Quillen-Suslin Theorem, 165.
Quotient ring, classical, 245.
left, 245.
Martindale, 240.
maximal, 233–240.
right, 242–249.
symmetric, 241, 249.

$\mathbb{R}$, 167.
$R[G]$, *See* group ring.
$R[x]$, *See* polynomial ring.
$R[x; \delta]$, *See* Ore extension.
$R[x; \sigma]$, *See* skew polynomial ring.
$R*G$, *See* skew group ring.

R-homomorphism, *See* homomorphism.
R-module, *See* module.
R-submodule, *See* submodule.
$\mathrm{Rad}(R)$, *See* Jacobson radical.
Radical, Jacobson, 50–52, 95.
  nil, 45, 52.
  prime, 287.
Rank, reduced, 284, 287–288.
  torsion-free, 287.
Rank of free module, 17.
Reduced rank, 284, 287–288.
Refinement, 25.
Regular element, 256.
Regular module, 7.
Relation, 115, 127, 147.
Replacement Theorem, 265.
Representation, 6.
Residual ideal, 235.
Resolution, free, 82.
  injective, 222.
  projective, 82, 140.
Respects direct sums, 142.
Respects short exact sequences, 116.
  graded, 128.
$\rho_R(V)$, *See* reduced rank.
Right annihilator, 77.
  maximum condition, 193.
Right exact, tensor product, 88.
Right ideal, minimal, 28.
  nilpotent, 28.
Right module, 5.
Right notation, 3.
Right quotient ring, 242–249.
  Artinian, 290.
Ring, Artinian, 28, 45–50, 52, 81, 276.
  commutative Noetherian, 277–281.
  division ring, 40.
  filtered, 177.
  fixed, 131.
  G-graded, 131.
  Goldie, 253, 256.
  graded, 124–130.
  graded Artinian, 177.
  graded Noetherian, 130, 177.
  group, 41, 83.
  hereditary, 57, 65, 76.
  IBN, 18, 21, 42.
  local, 96–101, 269.
  n-fir, 62.
  Noetherian, 59, 106, 273, 275, 287–291.
  nonsingular, 255, 259.
  Ore, 245, 250.
  prime, 60, 240, 252.
  prime Goldie, 258, 264.
  primitive, 38–40, 50.
  self-injective, 228–229, 259.
  semigroup, 83.
  semihereditary, 72.
  semilocal, 153.
  semiprimary, 54, 63.
  semiprime, 193, 252.
  semiprime Goldie, 258, 264.
  semiprime Noetherian, 268, 270, 284.
  semiprimitive, 50.
  simple, 38.
  simple Artinian, 38.
  skew group, 131.
  skew polynomial, 105–109.
  strongly G-graded, 131.
  von Neumann regular, 54, 93, 212, 259.
  Wedderburn, 28, 30, 36, 45–50, 76, 227, 249.
Ring homomorphism, 6.
Root, algebraic, 194.
Row, extendible, 152, 163.
  unimodular, 152, 163.
Row matrix, 152.

Schanuel's Lemma, 74–75, 82.
  injective, 213–214, 231.
Schreier-Zassenhaus Lemma, 25.
Schur's Lemma, 36.
Second Isomorphism Theorem, 9.
Self-injective ring, 228–229, 259.
Semigroup ring, 83.
Semihereditary ring, 72.
Semilocal ring, 153.
Semiprimary ring, 54, 63.
Semiprime Noetherian ring, 284.
Semiprime ring, 193, 252.
Semiprimitive ring, 50.
Separably generated, 168.
Sequence, exact, 13.
  short exact, 14.
  zero, 13.
Series, 25.
  composition, 26, 47.
  equivalent, 25.
  factors, 25.
  length, 25.
  refinement, 25.
Serre Conjecture, 152, 165.
Serre's Theorem, 144.
Short exact sequence, 14.
  split, 14.
Simple Artinian ring, 38.
Simple module, 23, 46, 49.
Simple ring, 38.
$\mathrm{Sing}(V)$, *See* singular submodule.
Singular ideal, 255.
Singular submodule, 255, 285.
Skew group ring, 131.
Skew polynomial ring, 105–109.
  global dimension, 107, 112.
  Grothendieck group, 137–139.
  Noetherian, 106.
  projective Grothendieck group, 144.
Small's Theorem, 290.
$\mathrm{soc}(V)$, *See* socle.
Socle, 226, 239.
Split, 14.
Splitting backmap, 14.
Stably free module, 145.
  not free, 165.
Stably isomorphic, 145.
Strong direct sum, 7, 210.
Strongly G-graded ring, 131.
Submodule, 7.
  essential, 223, 226.
  graded, 125.
  singular, 255, 285.
  torsion, 286.
Subring, 5.
Suslin Monic Polynomial Theorem, 161, 163.
Sylvester rank function, 291.
Symbolic power, 292.
Symmetric difference, 52.
Symmetric quotient ring, 241, 249.
Syzygy, 147.
Syzygy Theorem, 113, 146.

$\mathrm{T}(V)$, *See* trace ideal.
Tensor product, 84–93.
  associativity, 88.
  maps, 87.
  right exact, 88.
Third Isomorphism Theorem, 9.
$\mathrm{Tor}_1(A, R) = 0$, 134.
$\mathrm{Tor}_2(A, R) = 0$, 134.
$\mathrm{Tor}_n(A, B)$, 140.
Torsion free module, 92, 174, 286.
Torsion free rank, 287.
Torsion module, 286.
Torsion submodule, 286.
Total degree, 128.
Trace ideal, 172.
Trace map, 21.
Transitive, 36, 43.
Transitivity, essential extension, 223.

Transitivity of induction, 93.
Triangular matrix, 82.

u.dim V, *See* uniform dimension.
Uniform dimension, 262, 264, 266–267.
Uniform injective module, 274–276.
Uniform module, 263.
Unimodular row, 152, 163.
Unital module, 6.
Utumi's Theorem, 238.

Vector generic flatness, 189.
von Neumann regular ring, 54, 93, 212, 259.

Walker's Theorem, 268.
Walker's Theorem Revisited, 270.
Weak direct sum, 7.
Weakly ascending, 189.
Wedderburn ring, 28, 30, 36, 45–50, 76, 227, 249.
Weyl algebra, 196.

$\mathbb{Z}$, *See* integers.
$\mathcal{Z}(f)$, *See* zero set.
Zariski Nullstellensatz, 187.
Zero, algebraic, 194.
Zero sequence, 13.
Zero set, 194.