Free Ideal Rings and Localization in General Rings

Proving that a polynomial ring in one variable over a field is a principal ideal domain can be done by means of the Euclidean algorithm, but this does not extend to more variables. However, if the variables are not allowed to commute, giving a free associative algebra, then there is a generalization, the weak algorithm, which can be used to prove that all one-sided ideals are free.

This book presents the theory of free ideal rings (firs) in detail. Particular emphasis is placed on rings with a weak algorithm, exemplified by free associative algebras. There is also a full account of localization, which is treated for general rings, but the features arising in firs are given special attention. Each section has a number of exercises, including some open problems, and each chapter ends in a historical note.

PAUL COHN is Emeritus Professor of Mathematics at the University of London and Honorary Research Fellow at University College London.

NEW MATHEMATICAL MONOGRAPHS

For information about Cambridge University Press mathematics publications visit
http://publishing.cambridge.org/stm/mathematics

Already published in New Mathematical Monographs:

Representation Theory of Finite Reductive Groups
Marc Cabanes, Michel Enguehard

Harmonic Measure
John B. Garnett, Donald E. Marshall

Heights in Diophantine Geometry
Enrico Bombieri, Walter Gubler

Free Ideal Rings and Localization in General Rings

P. M. COHN
Department of Mathematics
University College London

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314-321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi - 110025, India

103 Penang Road, #05-06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9780521853378

First published 2006

A catalogue record for this publication is available from the British Library

ISBN 978-0-521-85337-8 Hardback

To my granddaughters Chasya and Ayala

Contents

Preface

It is not your duty to complete the work,
But neither are you free to desist from it.

R. Tarphon, Sayings of the Fathers.

One of the questions that intrigued me in the 1950s was to find conditions for an embedding of a non-commutative ring in a skew field to be possible. I felt that such an embedding should exist for a free product of skew fields, but there seemed no obvious route. My search eventually led to the notion of a *free ideal ring, fir* for short, and I was able to prove (i) the free product of skew fields (amalgamating a skew subfield) is a fir and (ii) every fir is embeddable in a skew field. Firs may be regarded as the natural generalization (in the non-commutative case) of principal domains, to which they reduce when commutativity is imposed. The proof of (i) involved an algorithm, which when stated in simple terms, resembled the Euclidean algorithm but depended on a condition of linear dependence. In this form it could be used to characterize free associative algebras, and this ‘weak’ algorithm enables one to develop a theory of free algebras similar to that of a polynomial ring in one variable. Of course free algebras are a special case of firs, and other facts about firs came to light, which were set forth in my book *Free Rings and their Relations* (a pun and a paradox). It appeared in 1971 and in a second edition in 1985. A Russian translation appeared in 1975.

More recently there has been a surprising increase of interest, in many fields of mathematics, in non-commutative theories. In functional analysis there has been a greater emphasis on non-commutative function algebras and quantum groups have been introduced in the study of non-commutative geometry, while quantum physics uses non-commutative probability theory, in which even free associative algebras have made their appearance. The localization developed in *Free Rings* has also found a use by topologists. All this, and the fact that many proofs have been simplified, has encouraged me to write a book based on the earlier work, but addressed to a wider audience. Since skew fields play a prominent role, the prefix 'skew' will often be left out, so fields are generally assumed to be not necessarily commutative.

The central part is Chapter 7, in which non-commutative localization is studied. For any ring R the various homomorphisms into fields are described by their singular kernels, the matrices with a singular image, which form a resemblance to prime ideals and so are called *prime matrix ideals*. Various classes of rings, such as firs and semifirs, are shown to be embeddable in fields, and an explicit criterion is given for such an embedding of a general ring to be possible, as well as conditions for a universal field of fractions to exist. This is the case for firs, while for free algebras the universal field of fractions can be shown to be 'free'. The existence of the localization now has a simpler and more direct proof, which is described in Sections 7.1–7.4. It makes only occasional reference to earlier chapters (mainly parts of Chapter 0) and so can be read at any stage.

In the remaining chapters the theory of firs is developed. Their similarity to principal ideal domains is stressed; the theory of the latter is recalled in Chapter 1, while Chapter 0 brings essential facts about presentations of modules over general rings, particularly projective modules, facts that are perhaps not as well known as they should be. Chapter 2 introduces firs and semifirs and deals with the most important example, a ring possessing a generalized form of the division algorithm called the *weak algorithm*. The unique factorization property of principal ideal domains has an analogue in firs, which applies to square matrices as well; this result and its consequences for modules are discussed in Chapter 3. It turns out that the factors of any element form a modular lattice (as in principal ideal domains), which in the case of free algebras is even distributive; this result is the subject of Chapter 4. In Chapter 5 the module theory of firs and semifirs is studied; this leads to a wider class of rings, the Sylvester domains (characterized by Sylvester's law of nullity), which share with semifirs the property of possessing a universal field of fractions. Chapter 6 examines centres, centralizers and subalgebras of firs and semifirs.

Results from lattice theory, homological algebra and logic that are used in the book are recalled in an Appendix. Thus the only prerequisites needed are a basic knowledge of algebra: rings and fields, up to about degree level. Although much of the work already occurs in *Free Rings*, the whole text has been reorganized to form a better motivated introduction and there have been many improvements that allow a smoother development. On the other hand, the theory of skew field extensions has been omitted as a fuller account is now available in my book on skew fields (SF; see p. xv). The rather technical section on the work of

Gerasimov, leading to information on the localization of n-firs, has also been omitted.

I have had the help of many correspondents in improving this edition, and would like to express my appreciation. Foremost among them is G. M. Bergman, who in 1999–2000 ran a seminar at the University of California at Berkeley on the second edition of *Free Rings*, and provided me with over 300 pages of comments, correcting mistakes, outlining further developments and raising interesting questions. As a result the text has been greatly improved. I am also indebted to V. O. Ferreira for his comments on *Free Rings*.

My thanks go also to the staff of the Cambridge University Press for the efficient way they have carried out their task.

University College London
October 2005 P. M. Cohn

Note to the reader

Chapter 0 consists of background material from ring theory that may not be entirely standard, whereas the Appendix gives a summary of results from lattice theory, homological algebra and logic, with reference to proofs, or in many cases, sketch proofs. Chapter 1 deals with principal ideal domains, and so may well be familiar to the reader, but it is included as a preparation for what is to follow. The main subject matter of the book is introduced in Chapter 2 and the reader may wish to start here, referring back to Chapters 1 or 0 only when necessary. In any case Chapter 2 as well as Chapter 3 are used throughout the book (at least the earlier parts, Sections 2.1–2.7 and 3.1–3.4), as is Chapter 5, while Chapters 4 and 6 are largely independent of the rest. The first half of Chapter 7 (Sections 7.1–7.5) is quite independent of the preceding chapters, except for some applications in Section 7.5, and it can also be read at any stage.

All theorems, propositions, lemmas and corollaries are numbered consecutively in a single series in each section, thus Theorem 4.2.5 is followed by Corollary 4.2.6, and this is followed by Lemma 4.2.7, in Section 4.2, and in that section they are referred to as Theorem 2.5, Corollary 2.6, Lemma 2.7 (except in the enunciation). The end or absence of a proof is indicated by ■. A few theorems are quoted without proof. They are distinguished by letters, e.g. Theorem 7.8.A. There are exercises at the end of each section; the harder ones are marked * and open-ended (or open) problems are marked $^\circ$, though sometimes this may refer only to the last part; the meaning will usually be clear.

References to the bibliography are by author's name and the year of publication, though 19 is omitted for publications between 1920 and 1999. Publications by the same author in a given year are distinguished by letters. The following books by the author, which are frequently referred to, are indicated by abbreviations:

CA. *Classic Algebra*. John Wiley & Sons, Chichester 2000.
BA. *Basic Algebra, Groups, Rings and Fields*. Springer-Verlag, London 2002.
FA. *Further Algebra and Applications*. Springer-Verlag, London 2003.
SF. *Skew Fields, Theory of General Division Rings*. Encyclopedia of Mathematics and its Applications, 57. Cambridge University Press, Cambridge 1995.
UA. *Universal Algebra*, rev. edn. Mathematics and its Applications, Vol. 6. D. Reidel, Publ. Co., Dordrecht 1981.
IRT. *Introduction to Ring Theory*. Springer Undergraduate Mathematics Series. Springer-Verlag, London 2000.
FR.1. *Free Rings and their Relations*. London Math. Soc. Monographs No. 2. Academic Press, New York 1971.
FR.2. *Free Rings and their Relations*, 2nd edn. London Math. Soc. Monographs No. 19. Academic Press, New York 1985.

Terminology, notation and conventions used

For any set X, the number of its elements, or more generally, its cardinality is denoted by $|X|$. If a condition holds for all elements of X except a finite number, we say that the condition holds for *almost all* members of X.

All rings occurring are associative, but not generally commutative (in fact, much of the book reduces to well-known facts in the commutative case). Every ring has a unit-element or one, denoted by 1, which is inherited by subrings, preserved by homomorphisms and acts as the identity operator on modules. The same convention applies to monoids (i.e. semigroups with one). A ring may consist of 0 alone; this is so precisely when $1 = 0$ and R is then called the *zero ring*. Given any ring R, the opposite ring R^o is defined as having the same additive group as R and multiplication $a.b = ba$ $(a, b \in R)$. With any property of a ring we associate its left–right dual, which is the corresponding property of the opposite ring. Left–right duals of theorems, etc. will not usually be stated explicitly.

We shall adopt the convention of writing (as far as practicable) homomorphisms of left modules on the right and vice versa. Mappings will be composed accordingly, although we shall usually give preference to writing mappings on the right, so that fg means 'first f, then g'. If R is any ring, then for any left R-module M, its *dual* is $M^* = \mathrm{Hom}_R(M, R)$, a right R-module; similarly on the other side. The space of $m \times n$ matrices over M is written ${}^mM^n$, and we shall also write ${}^mM$ for ${}^mM^1$ (column vectors) and M^n for ${}^1M^n$ (row vectors). A similar notation is used for rings.

In any ring R the set of non-zero elements is denoted by $R^\times$, but this notation is mostly used for integral domains, where $R^\times$ contains 1 and is closed under multiplication. Thus an integral domain need not be commutative. If $R^\times$ is a group under multiplication, R is called a *field*; occasionally the prefix 'skew' is used, to emphasize the fact that our fields need not be commutative. An element u in a ring or monoid is *invertible* or a *unit* if it has an *inverse* u^{-1} satisfying

$uu^{-1} = u^{-1}u = 1$. Such an inverse is unique if it exists at all. The units of a ring (or monoid) R form a group, denoted by $U(R)$. The ring of all $n \times n$ matrices over R is written $\mathfrak{M}_n(R)$ or R_n. The set of all square matrices over R is denoted by $\mathfrak{M}(R)$. Instead of $U(R_n)$ we also write $GL_n(R)$, the general linear group. The matrix with (i, j)-entry 1 and the rest zero is denoted by e_{ij} and is called a *matrix unit* (see Section 0.2). An *elementary* matrix is a matrix of the form $B_{ij}(a) = \mathrm{I} + ae_{ij}$, where $i \neq j$; these matrices generate a subgroup $E_n(R)$ of $GL_n(R)$, the *elementary group*. By a *permutation matrix* we understand the matrix obtained by applying a permutation to the columns of the unit matrix. It is a member of the *extended* elementary group $E_n^*(R)$, the group generated by $E_n(R)$ and the matrix $\mathrm{I} - 2e_{11}$. If in a permutation matrix the sign of one column is changed whenever the permutation applied was odd, we obtain a *signed* permutation matrix; these matrices generate a subgroup $P_n(R)$ of $E_n(R)$.

An element u of a ring is called a *left zero-divisor* if $u \neq 0$ and $uv = 0$ for some $v \neq 0$; of u is neither 0 nor a left zero-divisor, it is called *right regular*. Thus u is right regular whenever $uv = 0$ implies $v = 0$. Corresponding definitions hold with left and right interchanged. A left or right zero-divisor is called a *zero-divisor*, and an element that is neither 0 nor a zero-divisor is called *regular*. These terms are also used for matrices, not necessarily square. Over a field a square matrix that is a zero-divisor or 0 is also called *singular*, but this term will not be used for general rings.

An element u of a monoid is called *regular* if it can be cancelled, i.e. if $ua = ub$ or $au = bu$ implies $a = b$. If every element of a monoid S can be cancelled, S is called a *cancellation monoid*. A monoid is called *conical* if $ab = 1$ implies $a = 1$ (and so also $b = 1$).

An element of a ring is called an *atom* if it is a regular non-unit and cannot be written as a product of two non-units. A factorization is called *proper* if all its factors are non-units; if all its factors are atoms, it is called a *complete* factorization. An integral domain is said to be *atomic* if every element other than zero or a unit has a complete factorization. If a, b are elements of a commutative monoid, we say that *a divides b* and write $a|b$ if $b = ac$ for some element c.

The maximum condition or ascending chain condition on a module or the left or right ideals of a ring or a monoid is abbreviated as ACC. If a module satisfies ACC on submodules on at most n generators, we shall say that it satisfies ACC_n. In particular, left (right) ACC_n for a ring R is the ACC on a n-generator left (right) ideals of R. A module (or ring) satisfying ACC_n for all n is said to satisfy pan-ACC. Similar definitions apply to the minimum condition or descending chain condition. DCC for short.

Two elements a, b of a ring (or monoid) R (or matrices) are *associated* if $a = ubv$ for some $u, v \in U(R)$. If $u = 1$ ($v = 1$), they are *right* (*left*) associated; if $u = v^{-1}$, they are *conjugate* under $U(R)$. A polynomial in one variable (over any ring) is said to be *monic* if the coefficient of the highest power is 1. Two elements a, b of a ring R are *left coprime* if they have no common left factor apart from units; they are *right comaximal* if $aR + bR = R$. Clearly two right comaximal elements are left coprime, but not necessarily conversely. Two elements a, b are said to be *right commensurable* if there exist a', b' such that $ab' = ba' \neq 0$. Again, corresponding definitions apply on the other side. A row $(a_1, \ldots, a_n)$ of elements in R is said to be *unimodular* if the right ideal generated by the a_i is R; thus a pair is unimodular precisely when it is right comaximal. Similarly, a column is unimodular if the left ideal generated by its components is R.

Let A be a commutative ring; by an A-*algebra* we understand a ring R which is an A-module such that the multiplication is bilinear. Sometimes we shall want a non-commutative coefficient ring A; this means that our ring R is an A-bimodule such that $x(yz) = (xy)z$ for any x, y, z from R or A; this will be called an A-*ring*. To rephrase the definitions, a A-ring is a ring R with a homomorphism $\alpha \mapsto \alpha.1$ of A into R, while an A-algebra is a ring R with a homomorphism of A into the centre of R. Moreover, the use of the term 'A-algebra' implies that A is commutative. Frequently our coefficient ring will be a skew field, usually written K, or also k when it is assumed to be commutative.

Let R be an A-ring. A family (u_i) of elements of R is *right linearly dependent* over A or *right A-dependent* if there exist $\lambda_i \in A$ almost all but not all zero, such that $\sum u_i\lambda_i = 0$. In the contrary case (u_i) is *right A-independent*. Occasionally we speak of *a set* being linearly dependent; this is to be understood as a family indexed by itself. For example, two elements of an integral domain R are *right commensurable* if and only if they are right linearly R-dependent and both non-zero.

If A, B are matrices, we write $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ as $A \oplus B$ or $\mathrm{diag}(A, B)$. We shall also sometimes write columns as rows, with a superscript T to indicate transposition (reflexion in the main diagonal). In such cases the blocks are to be transposed as a whole, thus $(A, B)^{\mathrm{T}}$ means $\begin{pmatrix} A \\ B \end{pmatrix}$, not $\begin{pmatrix} A^{\mathrm{T}} \\ B^{\mathrm{T}} \end{pmatrix}$. For any $m \times n$ matrix A its *index* $i(A)$ is defined as $n - m$, and $m \times n$, or n in case $m = n$, is described as its *size* or *order*.

The letters $\mathbb{N}, \mathbb{N}_{>0}, \mathbb{Z}, \mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ stand as usual for the set (respectively ring) of non-negative integers, all positive integers, all integers, all integers mod p, rational, real and complex numbers, respectively. If $T \subseteq S$, the complement of T in S is written $S \backslash T$.

In a few places in Chapter 7 and the Appendix some terms from logic are used. We recall that a *formula* is a statement involving elements of a ring or group. Formulae can be combined by forming a *conjunction* $P \wedge Q$ (P and Q), a *disjunction* $P \vee Q$ (P or Q) or a *negation* $\neg P$ (not P). A formula that is not formed by conjunction, disjunction or negation from others is called *atomic*.

List of special notation

(Notation that is either standard or only used locally has not always been included.)

$\|I\|$	cardinality of the set I, xvi
$R^{\times}$	set of non-zero elements in a ring R, xvi
$U(R)$	group of units in a ring R, xvii
R°	opposite ring, xvi
$\mathfrak{M}_n(R)$, R_n	ring of all $n \times n$ matrices over R, xvii
M^n	set of all n-component row vectors over a module M, xvi, 7
M^I	direct power of M indexed by a set I, 1
$M^{(I)}$	direct sum of $\|I\|$ copies of M, 1
${}^mM$	set of all m-component column vectors over M, xvi, 7
${}^mM^n$	set of all $m \times n$ matrices over M, xvi, 7
$i(A)$	index of a matrix A, xviii
M^*	dual of M, xvi, 2
$\rho(A)$	inner rank of a matrix A, 3
$\rho^*(A)$	stable rank of A, 5
$V_{m,n}$	canonical non-IBN ring, 7
e_{ij}	matrix unit, xvii, 8
e_i, e_i^T	row, resp. column vector, 9f.
Rg, Rg_n	category of rings, $n \times n$ matrix rings, 9
I_0	0×0 matrix, 9
$\mathfrak{W}_n$	n-matrix reduction functor, 11
${}_R\text{Mod}$	category of left R-modules
${}_R\text{proj}$	category of finitely generated projective left R-modules, 14
$\boldsymbol{S}(R)$	monoid of finitely generated projective left R-modules, 14
$K_0(R)$	Grothendieck group, 14
$J(R)$	Jacobson radical of R, 15

Cambridge University Press
978-0-521-85337-8 — Free Ideal Rings and Localization in General Rings
P. M. Cohn
Frontmatter
More Information

$GL_n(R)$	general linear group of $n \times n$ invertible matrices over R, xvii
$E_n(R)$	subgroup generated by the elementary matrices, xvii, 117
$E_n{}^*(R)$	extended elementary group, xvii, 147
$P_n(R)$	subgroup of signed permutation matrices, xvii, 159
$Tr_n(R)$	subgroup of upper unitriangular matrices, 159
$\chi(M)$	characteristic of a module with a finite-free resolution of finite length, 26
$I(-)$	idealizer, 33
$E(-)$	eigenring, 33
M_t	submodule of torsion elements, 48
$\Gamma_{\geq 0}$	set of all elements ≥ 0 in an ordered additive group Γ, 337
$\Gamma_{>0}$	set of all elements > 0 in Γ
$a\|b$	a divides b, 52
$l(c)$ or $\|c\|$	length of an element c of a UF-monoid, 56
$a \parallel b$	a is a total divisor of b, 79
$A_1(k)$	Weyl algebra over k, 64
$R_{(n)}$	component of a filtered ring, 125
$R_{\lceil n \rceil}$	component of an inversely filtered ring, 157
$k\langle X\rangle$	free k-algebra on X, 135
$D_K\langle X\rangle$	free tensor D-ring centralizing K, 136
$k\langle\langle X\rangle\rangle$	formal power series ring on X over k, 161
$k\langle\langle X\rangle\rangle_{\text{rat}}$	subring of all rational power series, 167
$k\langle\langle X\rangle\rangle_{\text{alg}}$	subring of all algebraic power series, 167
c^*	bound of an element c (in a PID), 342
$\iota(c)$	inner automorphism defined by c
$d(f)$	degree of a polynomial f, 60f.
$o(f)$	order of a power series f, 88
$L(cR, R)$	lattice of principal right ideals containing cR, 116
$H(X), H(R : k)$	Hilbert series, 142
Tor	category of torsion modules (over a semifir), 193
$Tr(-)$	transpose of a module, 269
Pos, Neg	category of positive, negative modules over a semifir (in Section 4.4 $\mathcal{Pos}$ is also used for the category of all finite partially ordered sets), 273
M_b	bound component of a module M, 264f.
$B(\Sigma)$	set of displays, 437
Inv(R)	set of all invariant elements of R, 57, 333
X^*	free monoid on an alphabet X, 358
$\|f\|$	length of a word f, 358
f^λ, A^λ	terms of highest degree in f, A, 312

$\mathfrak{M}(R)$	set of all square matrices over R, 411
Ker φ	singular kernel of homomorphism φ, 423
$A \nabla B$	determinantal sum of A and B, 429
$\sqrt{\mathcal{A}}$	radical of a matrix ideal $\mathcal{A}$, 434
$\mathcal{F}_R$	category of all R-fields and specializations, 420
ε_R	full subcategory of epic R-fields, 421
$\mathcal{Z}$ ($\mathcal{Z}_0$)	least matrix (pre-)ideal, 444
$\mathcal{N} = \sqrt{\mathcal{Z}}$	matrix nilradical, 444
$o(A)$	order of an admissible matrix A, 414
$X(R)$	field spectrum of R, 442
$\mathcal{D}(A)$	singularity support of the matrix A, 442
$\Phi(R)$	set of all full matrices over R, 447
$K_1(U)$	Whitehead group of a field U, 495
G^{ab}	universal abelianization of a group G, 494
$D(R)$	divisor group of R, 497