Artinian rings, finite principal ideal rings and algebraic error-correcting codes

by

Jilyana Cazaran

Bachelor of Science in Mathematics, University of Queensland, 1987
Master of Applied Science in Mathematics by research and thesis,
Queensland University of Technology, 1991

A thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy

in

Mathematics

by research and thesis

Department of Mathematics,
Faculty of Science,
University of Tasmania,
Australia

31st July 1998

Declaration

The work contained in this thesis is my own except where due reference is made, and includes the joint work with my supervisor Dr. Andrei V. Kelarev. To the best of my knowledge this thesis contains no material previously written by another person which is claimed to be my own work. No part of this thesis has been submitted for a degree, diploma or award in any University or other institution.

Jilyana Cazaran

Jilyana Cazaran

Authority of Access

I authorize this thesis to be immediately available worldwide to any person for loan and copying in accordance with the *Australian Copyright Act 1968.*

Jilyana Cazaran

Jilyana Cazaran

Abstract

This thesis contains structure theorems for several types of Artinian rings, in particular, finite rings, commutative Artinian rings containing an identity, finite commutative rings containing an identity, and semisimple Artinian semigroup-graded rings. Chapter 1 provides an introduction to Artinian rings, semigroup-graded rings and some algebraic coding theory. Except for a small percentage of lemmas which are referenced, all the theory contained in Chapters 2 to 5 is new. It is original work either by myself or in collaboration with my supervisor Andrei V. Kelarev. Some results obtained while conducting my Ph.D. research have appeared in [8] to [22].

Chapter 2 contains theorems about the generators and weights of some polynomial codes. A class of ideals in polynomial rings is considered which contains all generalized Reed-Muller codes. Necessary and sufficient conditions are given for such an ideal to have a single generator. A description is also given of all quotient rings $(\mathbb{Z}/m\mathbb{Z})[x_1, \ldots, x_n]/I$ which are commutative PIRs where I is generated by univariate polynomials. Formulas are given for the minimum Hamming weight of the radical and its powers in the algebra $F[x_1, \ldots, x_n]/(x_1^{a_1}(1 - x_1^{b_1}), \ldots, x_n^{a_n}(1 - x_n^{b_n}))$ for an arbitrary field F.

Chapter 3 contains theorems about the tensor products and quotient rings of finite commutative rings containing identity elements. For such rings R and S, necessary conditions are given for the tensor product $R \otimes_{\mathbb{Z}} S$ to be a PIR. These conditions are shown to be sufficient when R and S are PIRs. Conditions are given for the ring $R[x]/(f(x))$ to be a PIR when R is a PIR and $f(x)$ is a monic polynomial. For a polynomial ring $Q = R[x_1, \ldots, x_n]$, and an ideal $I \subset Q$ generated by univariate polynomials, conditions are given for Q/I to be a PIR when R is a PIR and Q/I is finite. Conditions are also given for Q/I to be a direct sum of finite fields or Galois rings.

Chapter 4 contains theorems about radicals of finite rings and PIRs. For a class $\mathcal{R}$ of finite rings, necessary and sufficient conditions are given for $\mathcal{R}$ to be a radical class and also a semisimple class. The hereditary radical classes are characterized. Conditions are given when several such classes consist of PIRs.

Chapter 5 contains structure theorems for Artinian semigroup-graded rings. Consider a semigroup S and an S-graded ring $R = \oplus_{s \in S} R_s$ with support $\mathrm{supp}(R)$. Some finiteness conditions are given on $\mathrm{supp}(R)$ when R is semisimple Artinian. Various necessary and sufficient conditions are given for R to be semisimple Artinian when S is a semilattice, a finite semilattice, an in-

verse semigroup and a Clifford semigroup. Semigroup identities are given for a semigroup variety $\mathcal{V}$ which ensures that a semigroup algebra FS is semisimple Artinian, where F is a arbitrary field and S is a finite semigroup.

Acknowledgements

I wish to express my appreciation for the support and advice given to me by my supervisor Dr. Andrei V. Kelarev. I am indebted to Andrei for his help. His mathematical capabilities and capacity to quickly produce clever proofs has continued to be an overwhelming inspiration to me.

I sincerely thank Professor Rudi Lidl for his generous financial support and for inviting me to Tasmania to do the Ph.D. degree. This financial support from the Australian Research Council, was awarded to Professor Lidl in the form of a large ARC research grant.

During the course of my Ph.D work I attended 17 conferences and presented talks at 10 conferences in Australia, Canada, France, Germany, Scotland and the USA, [8]-[17]. Immediately after the submission of this thesis I will be presenting talks at 2 further conferences, the ICM98 in Germany, [18], and a number theory conference [19], in Austria. I am most grateful for the financial support I received from several of the conference organizers for most of the conference and accommodation fees. While conducting my Ph.D. research, I have also visited several mathematicians, universities and mathematical institutes in Australia, North America and Europe. I sincerely thank all these mathematicians and institutions for their kind hospitality.

I visited Dr. Pieter Moree and other colleagues at the Department of Mathematics, MPCE, Macquarie University, Sydney from December 1994 to January 1995, and also from April to May 1995, and at the Max Planck Institut für Mathematik, Bonn, Germany from May to July 1997. I owe a special thanks to Pieter for being so kind to me and supporting me during these visits and several conferences.

Other short visits I am most grateful for were up to two weeks duration, at some of which I was able to give seminars. I thank Professor Henk van Tilborg's Discrete Mathematics group at the Department of Mathematics and Computer Science, Eindhoven University of Technology, Eindhoven, the Netherlands, for encouraging me to visit them for one week and to give a seminar in August

1995. I thank Dr. Michael Zieve for allowing me to visit him at the Department of Mathematics, University of California, Berkeley in August 1995. I thank Dr. Eric Liverance and other colleagues at the Department of Mathematics, University of Southern California, Los Angeles, USA, for my one week visit in September 1995.

I also thank several people with whom I have had mathematical conversations during my Ph.D enrolment including Dr. Barry Gardner, Dr. Rex Matthews and Dr. Patrick Solé.

I am extremely grateful to the Department of Mathematics, University of Tasmania for allowing me, for several semesters, to be a part-time temporary lecturer of the 3rd year undergraduate subjects in coding theory and cryptography, SMA315 and KMA315. I thank several other members of this department for miscellaneous support they have given to me. I especially thank Kym M. Hill, from whom I have been very fortunate to have received help with computers whenever I required it.

I feel honoured to have recently been elected a Fellow of the ICA. I thank the people of this international mathematical society, the Institute of Combinatorics and its Applications, for providing me with this opportunity.

This thesis, which has now reached its completion, precisely an integral number of years since my day of origination (birth), represents the fact that mathematics has been such an integral part of my life. So too have many treasured relatives and friends of indisputable integrity, which I am so fortunate to have. Hence, last but not least, in fact most of all, I thank all these people, whose integrated efforts have helped me get to where I am right now.

Contents

Glossary of Notation

Symbol	Definition	Pages
$\mathcal{B}$	$\mathcal{B} = \{ay^b \mid \text{where } 0 < a < p \text{ and } 0 \le b < r\} \subset R = GR(p^m, r)$, $m \ge 2$; if $r = 1$ then $\mathcal{B} = [0, p-1]$	20, 36
$\mathcal{B}[x]$	$\mathcal{B}[x] \subset R[x]$, $R = GR(p^m, r)$	20, 36
$\text{char}(R)$	the characteristic of a ring R	9
$d = d_f$	$d = d'$ is defined for $f \in \mathbb{Z}_{p^m}[x]$, $m \ge 2$, $d \in \mathcal{B}[x]$, $\mathcal{B} = [0, p-1] \subset \mathbb{Z}_{p^m}$, $\overline{d} = \text{sp}(\overline{f})$ hence $\overline{f} \in \mathbb{Z}_p[x]$, $d = \text{SP}(f)$	21
$\overline{f}$	the image in $R[x]/pR[x]$ of $f \in R[x]$, $R = GR(p^m, r)$	20, 29
f'	$f \in R[x]$, $f' \in \mathcal{B}[x]$, $\overline{f'} = \overline{f}$, $R = GR(p^m, r)$	20, 36
f''	$f \in R[x]$, $f'' \in \mathcal{B}[x]$, $f - f' - pf'' \in p^2R$, $R = GR(p^m, r)$	21, 36
$\widehat{f}$	$\widehat{f} = \overline{f'' + (f' - \text{SP}(f)\,\text{UP}(f))''} = \overline{f'' - (\text{SP}(f)\,\text{UP}(f))''}$ and $\widehat{f} \in (R/pR)[x] = GF(p^r)[x]$, $R = GR(p^m, r)$	21, 36
F	an arbitrary field	12
$F[S]$	or FS is a semigroup algebra	12
$gcd(r_1, r_2)$	the greatest common divisor of r_1 and r_2	30
$GF(p^r)$	$= F_q$, the finite field, or Galois field, of order $q = p^r$	13
$GR(p^m, r)$	the Galois ring of characteristic p^m and order p^{mr}	29
$lcm(r_1, r_2)$	the least common multiple of r_1 and r_2	30
$\mathcal{N}(R)$	the radical (nilradical or Jacobson radical) of an Artinian ring R	11
$\mathcal{N}_\pi$	a certain class of nilpotent rings	52
PIR	a principal ideal ring	10
ϱ	the mapping $\varrho : \mathcal{R} \to \mathcal{R}$ is a radical of a class of rings $\mathcal{R}$	48
$\varrho(R)$	the radical of a ring R	48
$\mathcal{R}, \mathcal{S}$	classes of rings	48, 49

$\oplus_{s\in S}R_s$	a semigroup-graded ring where S is a semigroup	12
R_s	a component of a semigroup-graded ring R.....	12
$\oplus_{g\in G}R_g$	$= R_G$ is a subring of a semigroup-graded ring R where G is a group	57
R_p	the $p-$component of a ring R.....	13
$\mathrm{sp}(f)$	the squarefree part of $f \in F[x]$, where F is a field.....	18, 36
$\mathrm{SP}(f)$	$\mathrm{SP}(f)$ is defined for $f \in GR(p^m, r)[x]$; if $m = 1$ then $\mathrm{SP}(f) = \mathrm{sp}(f)$; if $m \geq 2$, then $\mathrm{SP}(f) \in \mathcal{B}[x]$, $\mathcal{B}$ $\subset GR(p^m, r)$, $\overline{\mathrm{SP}(f)} = \mathrm{SP}(\overline{f})$ hence $\overline{f} \in GF(p^r)[x]$;...	36
$\mathrm{supp}(R)$	the support of the ring R.....	56
$\mathrm{UP}(f)$	$\mathrm{UP}(f)$ is defined for $f \in GR(p^m, r)[x]$, $m \geq 2$, $\mathrm{UP}(f)$ $\in \mathcal{B}[x]$, $\mathcal{B} \subset GR(p^m, r)$, $\overline{f} = \overline{\mathrm{SP}(f)\,\mathrm{UP}(f)}$;.....	36
$u = u_f$	$u = u'$ is defined for $f \in \mathbb{Z}_{p^m}[x]$, $m \geq 2$, $u \in \mathcal{B}[x]$, $\mathcal{B} = [0, p-1] \subset \mathbb{Z}_{p^m}$, $\overline{f} = \overline{d}\overline{u}$, $u =$ $\mathrm{UP}(f)$.....	21
$\mathcal{V}$	a variety of semigroups.....	65
$w_H(I)$	the minimum Hamming weight of an ideal I	25
$\mathbb{Z}_m$	or $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}/(m)$ is the ring of residues modulo m	13
$\otimes$	$= \otimes_{\mathbb{Z}}$, the tensor product over $\mathbb{Z}$.....	10
$I \lhd R$	I is an ideal of a ring R	10
$\lceil x \rceil$	$\lceil x \rceil = [x] + 1$, the smallest integer $\geq x$.....	26
$[x]$	the integer part of x, the largest integer $\leq x$	14
$a \mid b$	a divides b, b is divisible by a.....	24
$a \nmid b$	a does not divide b, b is not divisible by a.....	x

Index of Main Results

Theorem, Page — **Main statement of the theorem or lemma**

11, 18 The ring $R = F[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$, where the $f_i(x_i)$ are monic, is a PIR if and only if the number of nonsquarefree $f_i(x_i)$ is ≤ 1.

15, 21 The ring $R = \mathbb{Z}_{p^a}[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$, where the $f_i(x_i)$ are monic, is a PIR if and only if

(i) the number of 'nonsquarefree mod p $f_i(x_i)$' is ≤ 1;

(ii) if $f_i(x_i)$ is not squarefree mod p then $\gcd(\widehat{f}, \overline{u_f}) = 1$.

18, 25 Let $R = F[x_1, \ldots, x_n]/(x_1^{a_1}(1 - x_1^{b_1}), \ldots, x_n^{a_n}(1 - x_n^{b_n}))$ where $a_i \geq 0$, $b_i \geq 1$ for $1 \leq i \leq n$. If $\operatorname{char} F = 0$, then $w(I^h) = 2^\ell$ if $a_1 + \cdots + a_{\ell-1} - \ell + 1 < h \leq a_1 + \cdots + a_\ell - \ell$ and $w(I^h) = 0$ if $a_1 + \cdots + a_k - k \leq h$. If $\operatorname{char} F = p > 0$, then $w(I^h) = 2$ if $h < a_1 + \cdots + a_{n-z}$ and $w(I^h) = \min_{T \subseteq [1,n-z]} \{2^{|L|+|T|} w(h - a_L - a_T; S \backslash T)\}$ otherwise.

27, 32 The ring $R \otimes S$ is a PIR if and only if, for each prime p, R_p or S_p is a direct product of Galois rings, where R and S are finite commutative PIRs with identities.

31, 34 If $R \otimes S$ is a PIR then, for each prime p, R_p or S_p is a direct product of Galois rings, where R and S are finite commutative rings with identities.

33, 36 Let R be a finite commutative chain ring with $\operatorname{char}(R) = p^m$, and let $f_i(x_i)$ for $1 \leq i \leq n$ be monic polynomials over R, then $Q = R[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$ and all rings $R[x_i]/(f_i(x_i))$ are PIRs, if and only if one of the following conditions is true.

(i) R is a field and the number of nonsquarefree $f_i(x_i)$ is ≤ 1;

(ii) R is a Galois ring, the number of 'nonsquarefree mod p $f_i(x_i)$' is ≤ 1 and if $f_i(x_i)$ is not squarefree mod p then $\gcd(\widehat{f}, \overline{\operatorname{UP}(f)}) = 1$;

(iii) R is not a field or Galois ring, $n = 1$ and f_1 is squarefree mod p.

35, 37 The ring $Q = GR(p^m, r)[x]/(f(x))$ where $m \geq 2$ and $f(x)$ is monic and not squarefree mod p, is a PIR if and only if $\gcd(\widehat{f}, \overline{\operatorname{UP}(f)}) = 1$.

45, 44 Let R be a finite commutative chain ring with $\mathrm{char}(R) = p^m$, and let $f_i(x_i)$ for $1 \leq i \leq n$ be monic polynomials over R, then $Q = R[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$ satisfies

(i) Q is a direct product of finite fields if and only if R is a finite field and all the f_i are squarefree;

(ii) Q is a direct product of Galois rings if and only if R is a Galois ring and all the f_i are squarefree modulo p.

49, 48 A class of finite rings, or finite commutative rings, is a radical class if and only if it is closed for homomorphic images and ideal extensions.

50, 49 A class of finite rings, or finite commutative rings, is a semisimple class if and only if it is closed for ideals and ideal extensions.

52, 52 For a radical semisimple class, $\mathcal{R}$, of finite rings and a set π of primes, $\mathcal{N}_{\mathcal{R}} = \mathcal{N}_{\pi}$.

53, 53 $\mathcal{R}_{\pi,\mathcal{M}}$ is a radical semisimple class of finite rings. Conversely, every radical semisimple class of finite rings coincides with some class $\mathcal{R}_{\pi,\mathcal{M}}$.

55, 54 $\mathcal{R}_{\mathcal{K}}$ is a radical semisimple class where $\mathcal{K}$ is a class of finite simple rings. Conversely, every radical semisimple class coincides with some class $\mathcal{R}_{\mathcal{K}}$.

56, 54 A hereditary radical of finite rings consists of PIRs if and only if it is subidempotent.

57, 55 A semisimple class of finite rings consists of PIRs if and only if its radical is supernilpotent.

58, 55 The class of all finite commutative PIRs with identity is a radical class.

59, 57 If R is a semisimple Artinian S-graded ring then $\mathrm{supp}(R)$ intersects a finite number of maximal subgroups of S.

62, 58 For any semigroup S, the following conditions are equivalent.

(i) Every S-graded ring $R = \bigoplus_{s \in S} R_s$ with a finite number of idempotents in $\mathrm{supp}(R)$ is semisimple Artinian if and only if all subrings R_e are semisimple Artinian for all idempotents e of S;

(ii) S is a semilattice.

64, 60 For any semigroup S, the following conditions are equivalent.

(i) Every S-graded ring $R = \bigoplus_{s\in S} R_s$ with $\mathrm{supp}(R)$ intersecting a finite number of maximal subgroups is semisimple Artinian if and only if all subrings $R_G = \bigoplus_{g\in G} R_g$ are semisimple Artinian for all maximal subgroups G of S;

(ii) S is a Clifford semigroup.

65, 61 A special B-graded ring $R = \bigoplus_{b\in B} R_b$ is semisimple Artinian if and only if B is a finite semilattice and all components R_b are semisimple Artinian, where B is a band.

68, 62 Let S be an inverse semigroup, and let $R = \bigoplus_{s\in S} R_s$ be a faithful S-graded ring with a finite number of idempotents in $\mathrm{supp}(R)$. If R_G is semisimple Artinian for all maximal subgroups G of S, then R is semisimple Artinian.

69, 63 For any inverse semigroup S, the following conditions are equivalent.

(i) every S-graded ring $R = \bigoplus_{s\in S} R_s$ is semisimple Artinian if and only if R is semiprime and all subrings $R_G = \bigoplus_{g\in G} R_g$ are semisimple Artinian for all maximal subgroups G of S;

(ii) S has a finite number of idempotents.

70, 65 For any semigroup variety $\mathcal{V}$ and field F with $\mathrm{char}(F) = p \geq 0$, the following conditions are equivalent.

(i) FS is semisimple Artinian for every finite semigroup $S \in \mathcal{V}$;

(ii) all semigroups in $\mathcal{V}$ are semilattices of p'-groups;

(iii) $\mathcal{V}$ satisfies $x^{m+1} = x$, $(xy)^m = (yx)^m$, $m \in \mathbb{Z}$ and $p \nmid m$.

Chapter 1

Introduction

1.1 An overview of this thesis

An overview of this thesis is given here followed by a description of each chapter. This thesis contains structure theorems for Artinian rings. Each chapter concentrates on a different type of Artinian ring or class of Artinian rings, and each ring R may or may not be finite, commutative or contain an identity. Except for a small percentage of lemmas which are referenced, all the theory contained in Chapters 2 to 5 is new. It is original work either by myself or in collaboration with my supervisor Andrei V. Kelarev. Some results obtained while conducting my Ph.D. research have appeared in [8] to [22].

In Chapter 2, all quotient rings $R = S[x_1, \ldots, x_n]/I$ are described which are finite commutative PIRs, where $S = \mathbb{Z}/m\mathbb{Z}$ and I is an ideal generated by univariate polynomials. This is generalized in Chapter 3 with S being a finite commutative PIR. Chapter 2 also has a theorem containing conditions for $R = F[x_1, \ldots, x_n]/I$ to be a PIR where F is an arbitrary field. Formulas are then given for the minimum Hamming weight of the radical and its powers in the algebra $F[x_1, \ldots, x_n]/(x_1^{a_1}(1 - x_1^{b_1}), \ldots, x_n^{a_n}(1 - x_n^{b_n}))$. To achieve the generalization stated above in Chapter 3, conditions are given for the ring $R \otimes S$ to be a PIR when R and S are finite commutative PIRs. The necessary condition is then proved when R and S are not both PIRs. Conditions are also given for $R = S[x_1, \ldots, x_n]/I$ to be a direct sum of finite fields or Galois rings, when S is a finite commutative PIR.

Since these rings R are commutative Artinian rings with identities, then

R is a PIR if and only if the radical $\mathcal{N}(R)$ is a principal ideal. The investigation of radicals is continued in Chapter 4. There, the more general concept of a radical ϱ and a radical class of finite rings is studied. These rings are not necessarily commutative nor do they necessarily contain identities. Necessary and sufficient conditions are obtained for a class of finite rings to be a radical class, semisimple class and hence a radical semisimple class. Characterizations of radical semisimple classes are given, including classes consisting of PIRs.

The polynomial ring $R = F[x_1, \ldots, x_n]$ where F is an arbitrary field, is a simple example of a commutative semigroup-graded ring, see p.12. The study of this ring R from Chapter 2 is continued in Chapter 5, where some structure theorems for semisimple Artinian semigroup-graded rings are presented. Several semigroups are used, including semilattices, inverse semigroups and Clifford semigroups. The conditions given are for a semigroup-graded ring to be semisimple Artinian. The ring $R = F[x_1, \ldots, x_n]$ is also a semigroup algebra over the field F, see p.12. Chapter 5 concludes with a theorem giving semigroup identities which ensure that a semigroup algebra over a finite semigroup is semisimple Artinian.

Chapter 2 : Generators and weights of polynomial codes

In Chapter 2 necessary and sufficient conditions are given for certain rings R to be PIRs. Formulas are then given for the minimum Hamming weight of a certain ideal in a particular algebra. All rings considered are commutative Artinian rings with identities. Most of Chapter 2 appears in [20].

Let $R = S[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$ where S is either $\mathbb{Z}/m\mathbb{Z}$ or an arbitrary field F. Since R is an Artinian ring, it is a PIR if and only if $\mathcal{N}(R)$ is a principal ideal. Theorem 11 gives conditions for R to be a PIR when $S = F$.

11. The ring $R = F[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$, where the $f_i(x_i)$ are monic, is a PIR if and only if the number of nonsquarefree $f_i(x_i)$ is ≤ 1.

Corollary 13, the main result of [42], is an immediate corollary to Theorem 11. Generalized Reed-Muller codes, C, coincide with powers of the radical of the algebra, $A = F_q[x_1, \ldots, x_n]/(x_1^{q_1} - 1, \ldots, x_n^{q_n} - 1)$, where $p = \operatorname{char} F_q$, $q_i = p^{c_i}$ and $c_i \geq 1$ for $i = 1, \ldots, n$, [5], [24]. Corollary 14 gives conditions for the existence of a single generator polynomial for C. Theorem 15 gives conditions for R to be a PIR when $S = \mathbb{Z}/m\mathbb{Z}$ and R is finite.

15. The ring $R = \mathbb{Z}_{p^a}[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$, where the $f_i(x_i)$ are monic, is a PIR if and only if

(i) the number of 'nonsquarefree mod p $f_i(x_i)$' is ≤ 1;

(ii) if $f_i(x_i)$ is not squarefree mod p then $\gcd(\widehat{f}, \overline{u_f}) = 1$.

Theorem 18 provides formulas for the minimum Hamming weight $w(J)$, where $J = (\mathcal{N}(R))^h$ is any power of the radical $\mathcal{N}(R)$, of the algebra $R = F[x_1, \ldots, x_n]/(x_1^{a_1}(1 - x_1^{b_1}), \ldots, x_n^{a_n}(1 - x_n^{b_n}))$. The ideal J is a generalization of a generalized Reed-Muller code.

Chapter 3 : Finite commutative principal ideal rings with identities

In Chapter 3 every ring R is a finite commutative ring with an identity, with the exception of a polynomial ring such as $R[x_1, \ldots, x_n]$. For such rings R and S, conditions are given for the tensor product $R \otimes_{\mathbb{Z}} S$ to be a PIR. Sufficient conditions are then given for a certain quotient ring to be a PIR. Several parts of Chapter 3 appear in [22].

In the theory of finite commutative rings R with identities, the PIRs play a central role, see [71]. Every such ring R is a direct product of local rings, where each local ring is a homomorphic image of a polynomial ring over a PIR. A theorem is often proved for the special case of a PIR before attempting a local ring proof.

In Chapter 3 a series of lemmas give conditions for several rings of the form $R \otimes S$ to be PIRs. Lemma 25 proves that if R is a Galois ring, and S is a chain ring, then $R \otimes S$ is a PIR. Lemma 26 proves that if R and S are chain rings which are not Galois rings then $R \otimes S$ is not a PIR, unless $R \otimes S = 0$. Since a PIR is a direct product of local PIRs, Lemmas 25 and 26 form the basis of the proof of Theorem 27.

27. The ring $R \otimes S$ is a PIR if and only if, for each prime p, R_p or S_p is a direct product of Galois rings, where R and S are finite commutative PIRs with identities.

Lemma 29 proves that if R and S are finite local rings and S/pS is not a PIR then $R \otimes S$ is not a PIR. Lemma 30 proves that if R and S are finite

local rings which are not both PIRs and $R \otimes S \neq 0$ is a PIR then R is a Galois ring and S/pS is a finite chain ring which is not a Galois ring. Lemma 30 is used to prove Lemma 31, a partial generalization of Lemma 27.

31. If $R \otimes S$ is a PIR then, for each prime p, R_p or S_p is a direct product of Galois rings, where R and S are finite commutative rings with identities.

Theorem 27 is used to prove Theorem 33, that a certain ring of the form $Q = R[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$ is a PIR, since $Q \cong \otimes_{i=1}^{n} R[x_i]/(f_i(x_i))$. The main result needed to prove Theorem 33 is then Lemma 35.

35. The ring $Q = GR(p^m, r)[x]/(f(x))$ where $m \geq 2$ and $f(x)$ is monic and not squarefree mod p, is a PIR if and only if $\gcd(\widehat{f}, \overline{\mathrm{UP}(f)}) = 1$.

33. Let R be a finite commutative chain ring with $\mathrm{char}(R) = p^m$, and let $f_i(x_i)$ for $1 \leq i \leq n$ be monic polynomials over R, then $Q = R[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$ and all rings $R[x_i]/(f_i(x_i))$ are PIRs, if and only if one of the following conditions is true.

(i) R is a field and the number of nonsquarefree $f_i(x_i)$ is ≤ 1;

(ii) R is a Galois ring, the number of 'nonsquarefree mod p $f_i(x_i)$' is ≤ 1 and if $f_i(x_i)$ is not squarefree mod p then $\gcd(\widehat{f}, \overline{\mathrm{UP}(f)}) = 1$;

(iii) R is not a field or Galois ring, $n = 1$ and f_1 is squarefree mod p.

Let R and S be finite local rings. Lemma 41 proves that $R \otimes S$ is a direct product of Galois rings if and only if so too are R and S. Lemma 42 proves the same statement with finite fields instead of Galois rings. Let $S = R[x]/(f(x))$ where R is a chain ring and f is monic. Lemma 43 proves that if S is a direct product of Galois rings then R is a Galois ring and f is squarefree modulo p. Lemma 44 proves that if S is a direct product of finite fields then R is a finite field and f is squarefree. These lemmas are used to prove Theorem 45.

45. Let R be a finite commutative chain ring with $\mathrm{char}(R) = p^m$, and let $f_i(x_i)$ for $1 \leq i \leq n$ be monic polynomials over R, then $Q = R[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$ satisfies

(i) Q is a direct product of finite fields if and only if R is a finite field and all the f_i are squarefree;

(ii) Q is a direct product of Galois rings if and only if R is a Galois ring and all the f_i are squarefree modulo p.

Chapter 4 : Radicals of finite rings and principal ideal rings

In Chapter 4 several necessary and sufficient conditions are given which characterize radical semisimple, radical and semisimple classes of finite rings. Further conditions are given for such classes to consist of PIRs. All rings considered are finite but it is not required that these rings are commutative or contain identity elements.

Radicals are basic structural tools of ring theory, see [38]. A radical class $\mathcal{R}$, consists of all rings $R \in \mathcal{R}$ which are ϱ-radical, hence satisfy $\varrho(R) = R$, for some radical mapping ϱ. A semisimple class $\mathcal{S}$, consists of all rings $S \in \mathcal{S}$ satisfying $\varphi(R) = 0$ for some radical mapping φ. A radical semisimple class satisfies both these conditions for some radical mappings ϱ and φ. Theorems 49 and 50 provide necessary and sufficient conditions to characterize these classes when they consist of finite rings. The same conditions are true for the subclass of finite commutative rings.

49. A class of finite rings, or finite commutative rings, is a radical class if and only if it is closed for homomorphic images and ideal extensions.

50. A class of finite rings, or finite commutative rings, is a semisimple class if and only if it is closed for ideals and ideal extensions.

Let $\mathcal{R}$ be a radical semisimple class of finite rings. In Theorem 52 the set $\mathcal{N}_{\mathcal{R}}$ of all nilpotent rings are shown to be of the form $\mathcal{N}_\pi$ for a set π of primes. Two characterizations are given for $\mathcal{R}$. Theorems 53 and 55 prove respectively, that $\mathcal{R}$ coincides with certain classes denoted by $\mathcal{R}_{\pi,\mathcal{M}}$ and $\mathcal{R}_{\mathcal{K}}$. Conditions are derived in Theorems 56 and 57 for two classes of rings to consist of PIRs.

56. A hereditary radical of finite rings consists of PIRs if and only if it is subidempotent.

57. A semisimple class of finite rings consists of PIRs if and only if its radical is supernilpotent.

Theorem 58 proves that the class of all finite commutative PIRs with

identity is a radical class.

Chapter 5 : Semisimple Artinian semigroup-graded rings

In [97], Zel'manov proved that if a nonzero semigroup ring KS is right Artinian, then the semigroup S is finite. In Chapter 5 several necessary and sufficient conditions are given for various S-graded rings $R = \oplus_{s\in S} R_s$ to be semisimple Artinian under certain finiteness conditions on $supp(R) \subset S$. All rings considered are Artinian but it is not required that these rings are commutative or contain identity elements. Most of Chapter 5 appears in [21].

Consider the two finiteness conditions on supp(R),

(i) supp(R) intersects a finite number of maximal subgroups of S,

(ii) supp(R) contains a finite number of idempotents.

Condition (i) is proved true for a semisimple Artinian S-graded ring in Theorem 59. Condition (ii) then follows for this ring by Corollary 60. Two theorems, 62 and 64, are then proved for all S-graded rings satisfying conditions (i) and (ii) respectively.

62. For any semigroup S, the following conditions are equivalent.

(i) Every S-graded ring $R = \bigoplus_{s\in S} R_s$ with a finite number of idempotents in supp(R) is semisimple Artinian if and only if all subrings R_e are semisimple Artinian for all idempotents e of S;

(ii) S is a semilattice.

64. For any semigroup S, the following conditions are equivalent.

(i) Every S-graded ring $R = \bigoplus_{s\in S} R_s$ with supp(R) intersecting a finite number of maximal subgroups is semisimple Artinian if and only if all subrings $R_G = \bigoplus_{g\in G} R_g$ are semisimple Artinian for all maximal subgroups G of S;

(ii) S is a Clifford semigroup.

Following from Theorem 62 is Corollary 63, the class of semisimple Artinian rings is S-closed if and only if S is a finite semilattice. Two theorems, 65 and 68, respectively give conditions for special B-graded rings, and faithful S-graded rings, to be semisimple Artinian rings.

65. A special B-graded ring $R = \bigoplus_{b \in B} R_b$ is semisimple Artinian if and only if B is a finite semilattice and all components R_b are semisimple Artinian, where B is a band.

68. Let S be an inverse semigroup, and let $R = \bigoplus_{s \in S} R_s$ be a faithful S-graded ring with a finite number of idempotents in $\mathrm{supp}(R)$. If R_G is semisimple Artinian for all maximal subgroups G of S, then R is semisimple Artinian.

Theorem 69 uses a third finiteness condition on S, that being, (iii) S has a finite number of idempotents.

69. For any inverse semigroup S, the following conditions are equivalent.

(i) every S-graded ring $R = \bigoplus_{s \in S} R_s$ is semisimple Artinian if and only if R is semiprime and all subrings $R_G = \bigoplus_{g \in G} R_g$ are semisimple Artinian for all maximal subgroups G of S;

(ii) S has a finite number of idempotents.

Finally Theorem 70 states equivalent conditions for a certain semigroup variety $\mathcal{V}$, involving semigroup identities, which ensure that a semigroup algebra FS is semisimple Artinian, where F is an arbitrary field and S is a finite semigroup.

1.2 Motivation for the theorems in this thesis and its connections with the mathematical literature

Chapter 2 considers certain commutative Artinian algebras and some error-correcting codes associated with them. Several authors have established that many interesting codes are ideals in certain algebras. Berman [5], in the case of characteristic two, and Charpin [24], in the general case, proved that all

generalized Reed-Muller codes coincide with powers of the radical of the algebra $A = F_q[x_1, \ldots, x_n]/(x_1^{q_1} - 1, \ldots, x_n^{q_n} - 1)$, where F_q is a finite field, $p = \operatorname{char} F_q > 0$ and $q_i = p^{c_i}$, for $i = 1, \ldots, n$, and gave formulas for their Hamming weights. These codes form an important class containing many codes of practical value. Code properties of ideals in algebras A have also been considered by Poli [81].

This approach helped to improve some parameters of the codes. For example, Berman [5] showed that in certain cases, abelian group codes, [6, §4.8], have better error-correcting properties than cyclic codes. Using the underlying algebraic structure, a new fast decoding algorithm for Reed-Muller codes was developed by Landrock and Manz in [66]. Since these radicals have such good code properties, Chapter 2 determines when these radicals possess a single generator polynomial. It also determines when more general commutative Artinian algebras are PIRs. If the radical, $\mathcal{N}(R)$, of a commutative Artinian algebra R, is a principal ideal, then the same is true of all its powers and R is then a PIR. Chapter 2 also gives formulas for the Hamming distance of the powers of $\mathcal{N}(R)$ when the coefficient ring is a field F in Theorem 18, a special case of which is given in [5] as Theorem 1.2.

The polynomial codes in Chapter 2 are Jacobson radicals of commutative Artinian rings. Jacobson radicals have been studied for several classes of rings, see [53]. We refer to the surveys of [52] and [56] for descriptions of the Jacobson radicals of commutative semigroup rings. For recent results on the Jacobson radical of graded rings we refer to [27], [63] and the surveys [48], [55] and [62].

The polynomial rings in Theorem 18 of Chapter 2 are commutative semigroup rings. Conditions for them to be PIRs are contained in Corollary 13. Commutative semigroup rings which are PIRs have been investigated in [49] and [51] and a complete description of commutative semigroup rings which are PIRs was obtained in [34]. All graded commutative PIRs were described in [33].

Chapter 3 considers tensor products and certain quotient rings of finite commutative rings and determines when they are PIRs. Finite commutative rings are interesting objects of ring theory and have many applications in combinatorics. Tensor products of Galois rings have been determined in [95]. If we want to use certain ring constructions in combinatorial applications of finite rings, then a natural question arises of when a ring construction is a PIR. This question has been considered in the literature for several ring constructions, as mentioned in the preceding paragraphs.

Chapter 4 considers radical classes and semisimple classes of finite rings and determines when radicals of finite commutative rings contain PIRs. Radicals are important structural tools of ring theory. This gives motivation for investigating radicals in the class of finite rings. First, we shall develop the radical theory of finite rings and prove several theorems which seriously differ from the corresponding facts obtained earlier in the class of all associative rings. In particular, we describe all radical semisimple classes of finite rings. This description is quite different from the description of radical semisimple classes of arbitrary rings due to Stewart and Gardner, see [39], [87].

As many interesting error-correcting codes are radicals in finite commutative rings, it makes sense to answer the following question. When does each ideal in every radical ring have a single generator polynomial? Second, we describe all radicals with this interesting property.

Chapter 5 determines several structural theorems for Artinian semigroup-graded rings. Zel'manov proved that if a nonzero semigroup ring KS is right Artinian, then the semigroup S is finite, see [97]. Several analogues of this theorem for graded rings have appeared in the literature recently, see [28], [50], [60]. The strongest result has been obtained in [60].

Many constructions of rings are examples of semigroup-graded rings. These include polynomial and skew polynomial rings, direct and semidirect products of rings, matrix and structural matrix rings, Rees matrix rings, Morita contexts and generalized matrix rings, group and semigroup rings, monomial rings, smash products and cross products and group-graded rings. More examples are given in [62].

Graded rings satisfying various important finiteness conditions have been considered in many papers, see [2], [7], [26], [28], [31], [32], [47], [50], [60], [58], [59], [61], [74], [75], [76], [92], [91]. Subrings of simple Artinian rings were considered in [37].

1.3 Some Preliminary Theory

Arbitrary rings

Let R be an arbitrary ring. If R has an identity then the *characteristic*, $\mathrm{char}(R)$, of R, is the smallest positive integer n such that $n1 = 0$. If such an

integer does not exist then $\text{char}(R) = 0$. We denote by $R \otimes S = R \otimes_{\mathbb{Z}} S$, the *tensor product* over $\mathbb{Z}$ of the rings R and S. The notation $I \lhd R$ means I is an ideal of a ring R. Define the quotient ring $S \cong R/I$ of R for some ideal $I \lhd R$. A *homomorphic image* of R is isomorphic to some quotient ring S of R. An *ideal extension* R, of I by S, is a ring R such that $R/I \cong S$ for some ideal $I \lhd R$ and ring S. An *idempotent* r of a semigroup or a ring R is an element $r \in R$ satisfying $r^2 = r$. If every ideal of a ring R has one generator, then R is called a *principal ideal ring*, PIR.

There are several algebraic structures involving the terminology *radical*, which are related to each other. These include the following.

- a *radical* ϱ, of a class $\mathcal{R}$ of rings;
- a ϱ-*radical* ring R;
- a radical class $\mathcal{R}$ of rings;
- a radical $\varrho(A)$ of a ring A with respect to a radical class of rings $\mathcal{R}$;
- the radical $rad(I)$, of an ideal $I \lhd R$ of a ring R;
- the radical $\mathcal{N}(R)$ of an Artinian ring R.

We now provide definitions of these structures and illustrate some relations between them.

Definition 1 A *nilpotent element* r, of a ring R, satisfies $r^n = 0$ for some positive integer n. A *nil ideal* I, of a ring R consists of nilpotent elements. A *nilpotent ideal* I, of a ring R satisfies $I^N = 0$ for some positive integer N. The *nilpotent index* or *index of nilpotency* of an ideal I is the smallest positive integer N satisfying $I^N = 0$. For a commutative ring R, with ideal I, define the radical of the ideal I as $rad(I) = \sqrt{I} = \{r \in R : \exists n > 0 \text{ with } r^n \in I\}$. The set, $rad((0))$, of all nilpotent elements of R, is the *nilradical* of R, [41] p.19.

Definition 2 Let $\mathcal{U}$ be a class of rings satisfying

(i) $A \in \mathcal{U}, A \cong B \Rightarrow B \in \mathcal{U}$;

(ii) $I \lhd A,\ A \in \mathcal{U} \Rightarrow I \in \mathcal{U}$;

(iii) $I \lhd A,\ A \in \mathcal{U} \Rightarrow A/I \in \mathcal{U}$

Let ϱ be a function which assigns an ideal $\varrho(R)$ to each $R \in \mathcal{U}$. Then ϱ is called a *radical* if it satisfies

(M1) $\varrho(R)/I \subseteq \varrho(R/I)$ for every ring R with ideal I;

(M2) $\varrho(R)$ is the largest ideal among all ideals I of R such that $\varrho(I) = I$;

(M3) $\varrho(R/\varrho(R)) = 0$ for each R.

A ring R is said to be *radical* or *ϱ-radical* if $\varrho(R) = R$. The class $\{R \in \mathcal{U} : \varrho(R) = R\}$ is called the *radical class* defined by ϱ. A ring R is said to be *semisimple* or *ϱ-semisimple* if $\varrho(R) = 0$. The class $\{R \in \mathcal{U} : \varrho(R) = 0\}$ is called the *semisimple class* defined by ϱ. Let $\mathcal{R}$ be a radical class of rings defined by ϱ. For any ring $A \in \mathcal{R}$ let $\varrho(A)$ be the largest ideal of A such that $\varrho(A) \in \mathcal{R}$ then $\varrho(A)$ is the *radical* of A with respect to $\mathcal{R}$, [38] p.13.

Definition 3 A ring R satisfies the descending chain condition if every descending chain of ideals in R is finite. A ring R is left Artinian (right Artinian) if it satisfies the descending chain condition on its left ideals (right ideals). The ring R is *Artinian* if it is left and right Artinian, [82] p.167.

It immediately follows that a finite ring is an Artinian ring. Almost all classes of rings considered in this thesis are Artinian rings. Since the Jacobson radical and nilradical $\mathcal{N}(R)$ of an Artinian ring R are identical, [1] p.89, we refer to this ideal as the *radical* of R. An equivalent definition is that the radical $\mathcal{N}(R)$ of an Artinian ring R is the unique maximal nil ideal of R, [82] p.200.

Consider the following example. Let $\mathcal{U}$ be the class of all rings and for each $R \in \mathcal{U}$, let $\varrho(R)$ be the largest nil ideal. Then ϱ is a radical, its radical class being the class of all nil rings. The semisimple class of ϱ is the class of rings with no nonzero nil ideals. If R is Artinian then $\varrho(R) = \mathcal{N}(R)$, the largest nilpotent ideal of R. In general, $\varrho(R)$ is not an Artinian ring if R is Artinian.

A major part of ring theory is concerned with describing how far a ring is from being a semisimple Artinian ring. As shown in [82] p.xvii, p.169, a *simple* Artinian ring is a matrix ring over a division ring and a *semisimple* Artinian ring is a finite direct product of simple Artinian rings.

Definition 4 Given some collection $\{A_i : i \in I\}$ of ideals of a ring R, R is a *subdirect product* of the rings $\{R/A_i : i \in I\}$ if the canonical homomorphism $\varphi : R \to \prod_{i\in I} R/A_i$ is an injection. A ring is *prime* if the product of any two nonzero ideals is nonzero. A *semiprime ring* is a subdirect product of prime rings, see [82] p.143, 164.

Definition 5 A *semigroup ring* $R[S]$, or RS, is the set of all functions $f : S \to R$ from a semigroup S to a ring R under the following standard definitions of addition and multiplication. For every $f, g \in R[S]$ and $s \in S$,

$$\begin{aligned} (f+g)(s) &= f(s)+g(s) \\ (fg)(s) &= \sum_{ab=s} f(a)g(b) \end{aligned}$$

Elements of $R[S]$ may be written as $f = \sum_{s\in S} f(s)s$. A *semigroup algebra* $F[S]$, or FS, is a semigroup ring which is also a vector space over some field F, [77] p.33. If S is a group G, then $R[G]$, or RG, is a *group ring* and $F[G]$, or FG, is a *group algebra.*

The term *algebra* is used throughout this thesis to denote a ring which is also a vector space over some field. An interesting example of a semigroup ring is the set of all arithmetical functions $f : G \to \mathbb{C}$ on an arithmetical semigroup G. Its corresponding semigroup algebra is the Dirichlet algebra Dir(G), which is a unique factorization domain, see [64] p.23. A simple example of a semigroup algebra is the polynomial ring $R = F[x_1, \ldots, x_n] = F[S]$ considered as an algebra over some field F. The semigroup is $S = \oplus_{i=1}^{n} \mathbb{Z}^+$ where $\mathbb{Z}^+$ is the additive semigroup of positive integers. An element of $F[S]$ is a mapping $f : S \to F$ assigning to any $s = (s_1, \ldots, s_n) \in S$ an element $f(s) = a_s \in F$, and this mapping is represented by the polynomial $f = \sum_{s\in S} a_s x_1^{s_1} \cdots x_n^{s_n}$.

Definition 6 Let S be a semigroup. A *semigroup-graded ring*, or S-graded ring, is an associative ring R with the decomposition $R = \bigoplus_{s\in S} R_s$ into a direct sum of Abelian groups such that for all $s, t \in S$, $R_s R_t \subseteq R_{st}$, [62].

A semigroup ring $R[S]$ is an example of a semigroup-graded ring where $R[S]$ is graded by S. A simple example of a semigroup-graded ring is the polynomial ring $R = F[x_1, \ldots, x_n]$ where F is an arbitrary field. Here $R = \bigoplus_{s\in S} R_s$ is graded by the commutative semigroup $S = \mathbb{Z}^+$, the additive semigroup of positive integers $s \geq 0$. For any integer $s \geq 0$, R_s is the additive Abelian

group of all linear combinations of monomials of total degree d, such a monomial being given by $f(x_1, \ldots, x_n) = a \prod_{i=1}^{n} x_i^{b_i}$ where $\sum_{i=1}^{n} b_i = d$ and $a \in F$. Commutative rings graded by $\mathbb{Z}^+$ are used widely throughout commutative algebra, [73] p.21, and algebraic geometry, [43] p.9, 426, where they are known as *graded rings*. The terminology graded rings refers more generally to the rings given in Definition 6.

Let F be an arbitrary field and $f = \prod_{i \in I} a_i \in F[x]$ be squarefree. By the chinese remainder theorem for ideals, [35], Exercise.2.6 p.80, $F[x]/(f(x)) \cong \prod_{i \in I} F[x]/(a_i(x))$, a finite direct product of fields. Since $F[x]$ is a Euclidean ring, it is a PIR. As any homomorphic image of a PIR is a PIR, then $F[x]/I$ is a PIR for any ideal $I \lhd F[x]$. In particular this applies when F is a finite field F_q. But $R[x]$ is not a Euclidean ring when R is not a field and the determination of ideals I which make $R[x]/I$ a PIR is an interesting problem.

Finite commutative rings with identity

The Galois field $GF(p^r) = F_q$ is the finite field with $q = p^r$ elements. The ring $\mathbb{Z}/m\mathbb{Z}$ of residues modulo m is written as $\mathbb{Z}_m$ here to shorten the notation, since the p-adic integers are not mentioned in this thesis. The Galois ring $GR(p^m, r)$ of characteristic p^m and order p^{mr} satisfies $GR(p^1, r) \cong GF(p^r)$ and $GR(p^m, 1) \cong \mathbb{Z}/p^m\mathbb{Z}$, see p.29 of this thesis and [71, §16].

A *local ring* is a ring containing only one maximal ideal $\mathfrak{m}$. Let R be a finite commutative ring with identity. The structure of R is given in [71]. The ring R is a direct product of local rings. Each such local ring is isomorphic to a homomorphic image of a polynomial ring of the form $GR(p^m, q)[x_1, \ldots, x_k]$, see Lemma 28. If R is a PIR then it is a direct product of local PIRs. These local rings are called *finite chain rings* since the ideal lattice of each chain ring is a chain, $0 = \mathfrak{m}^N \subset \mathfrak{m}^{N-1} \subset \cdots \subset \mathfrak{m}$, where N is the nilpotent index of the chain ring. The radical of a finite chain ring R satisfies $\mathcal{N}(R) = \mathfrak{m}$, where R has maximal ideal $\mathfrak{m}$.

For any ring R and prime p, the $p-$component of R is defined by

$$R_p = \{r \in R \mid p^k r = 0 \text{ for some positive integer } k\}.$$

Let R be a finite commutative ring with identity. It may be decomposed as $R = \prod_{p \in P} R_p$, a direct product of its $p-$components R_p, where P is a finite set. Each ring R_p is a direct product of finite chain rings, $R_p = \prod_{i \in I} C_i$, such that $\text{char}(C_i) = p^{i_j}$ for some integers $i, i_j \geq 1$, where I is a finite set.

Algebraic coding theory

This section contains a few standard definitions of coding theory which are needed in Chapter 2.

Definition 7 A code C is a subset of the vector space $(F_q)^n$. A codeword $\underline{c} \in C$ has Hamming weight $w(\underline{c})$ if it has $w(\underline{c})$ nonzero co-ordinates. An (n, k, d) *linear code* C is a subspace of dimension k of $(F_q)^n$, with length n, Hamming distance d =minimum$\{w(\underline{c}) : \underline{c} \in C\}$ and can correct $t = [(d-1)/2]$ errors per codeword. A *polynomial code* C over F_q is an ideal of the ring $R = F_q[x_1, \ldots, x_m]/I$ for some ideal I. Since R is an algebra over F_q, C is a linear code. The generators of this ideal are the generators of the code. A *cyclic code* of length n is an ideal of $F_q[x]/(x^n - 1)$ such that $(n, q) = 1$. A *nonlinear code* is a code which is not isomorphic to a linear code. A *binary code* has co-ordinates in the field $F_2 = GF(2)$. See [70].

Definition 8 ([70, Ch.13 §3].) Given two binary codes C_1 and C_2 with the same length n define the binary code C_3 as

$$C_3 = C_1 * C_2 = \{(\underline{u}|\underline{u}+\underline{v}) \ : \ \underline{u} \in C_1, \underline{v} \in C_2\}$$

where $(\underline{a}|\underline{b})$ is the concatenation of the vectors $\underline{a}$ and $\underline{b}$. Define the binary $r-$th order *Reed-Muller code* $C(r, m)$ as follows. For any positive integers m and r where $0 \leq r \leq m$, $C(r, m)$ has codewords of length 2^m,

$$\begin{aligned} C(0,m) &= \{\underline{0}, \underline{1}\}, \text{ where } \underline{0} = (00\ldots0) \text{ and } \underline{1} = (11\ldots1); \\ C(m,m) &= (GF(2))^{2^m}; \quad C(r+1, m+1) = C(r+1, m) * C(r, m). \end{aligned}$$

$C(r, m)$ is a linear $(2^m, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r})$ code, which is not usually cyclic but it is an extended cyclic code. The first order binary Reed-Muller code $C(1, m)$ is a $(2^m, m+1, 2^{m-1})$ linear code and all codewords except $\underline{0}$ and $\underline{1}$ have weight $n/2 = 2^{m-1}$.

Example 9 C(0,1)={ 00, 11 } C(1,1)={ 00, 10, 01 ,11 }
C(0,2)={0000, 1111 }
C(1,2)=C(1,1)*C(0,1)={ 0000, 0011, 1010, 1001, 0101, 0110, 1111, 1100 }
C(1,3)=C(1,2) * C(0,2)={ 00000000, 00001111, 00110011, 00111100,
10101010, 10100101, 10011001, 10010110, 01010101, 01011010,
01100110, 01101001, 11111111, 11110000, 11001100, 11000011}
$C(1, 2)$ is a cyclic even weight $(4, 3, 2)$ code. $C(1, 5)$ is a $(32, 6, 16)$ linear code with 64 codewords and $t = 7$.

NASA uses error-correcting codes to correct errors introduced into their transmission channels, when sending pictures of the various planets to earth via their space probes. In 1972, the Mariner 9 space probe transmitted black and white pictures of Mars to Earth using $C(1,5)$, see [89] p.4.

A description of *generalized Reed-Muller codes* is given in [6, §1.10] and their connection with the codes of Berman [5], is given in [6, §4.8].

Chapter 2

Generators and weights of polynomial codes

This chapter is devoted to two ring constructions and one theorem on the Hamming weight $w((\mathcal{N}(R))^h)$ for a certain algebra R. The rings considered are Artinian and of the form $R = S[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$ where S is either $\mathbb{Z}/m\mathbb{Z}$ or an arbitrary field F. Only the case when R is finite is considered when $S = \mathbb{Z}/m\mathbb{Z}$. Necessary and sufficient conditions are given for R to be a PIR for each of the two rings R. Formulas are then given for the minimum Hamming weight $w(J)$ where $J = \mathcal{N}(R))^h$ is any power of the radical $\mathcal{N}(R)$ of the algebra $R = F[x_1, \ldots, x_n]/(x_1^{a_1}(1 - x_1^{b_1}), \ldots, x_n^{a_n}(1 - x_n^{b_n}))$. Since most of this chapter appears in [20] the notation is the same for both, yet has some slight differences to that used in Chapter 3.

2.1 Generators of polynomial codes

Several authors have established that many linear codes are ideals in certain algebras. Berman [5], in the case of characteristic two, and Charpin [24], in the general case, proved that all generalized Reed-Muller codes coincide with powers of the radical of the algebra $A = F_q[x_1, \ldots, x_n]/(x_1^{q_1} - 1, \ldots, x_n^{q_n} - 1)$, where F_q is a finite field, $p = \operatorname{char} F_q > 0$ and $q_i = p^{c_i}$, for $i = 1, \ldots, n$. We determine when this radical and more general radicals have a single generator polynomial.

Lemma 10 *An Artinian ring R is a PIR if and only if its radical $\mathcal{N}(R)$ is a principal ideal.*

Proof. The 'only if' part is trivial. An Artinian ring is a direct product of local rings ([1], Proposition 8.7). If the radical of a local Artinian ring is a principal ideal, then all ideals are principal by Lemma 32 or [1], Proposition 8.8. □

Thus since A is an Artinian ring, the question of when the radical is a principal ideal is crucial for all other ideals to have a single generator. For example, it is well known that cyclic codes are ideals in the algebra $A = F_q[X]/(X^k - 1)$, and each ideal in A is generated by one polynomial, see p.13. This property is convenient both for representing the code and for developing encoding and decoding algorithms. Similar questions have been considered in several papers. For example, Charpin [23] described extended Reed-Solomon codes which are principal ideals.

Theorem 11 answers this question for even more general algebras

$$F[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n)),$$

where $f_1, \ldots, f_n$ are arbitrary univariate polynomials and F is an arbitrary field. As an immediate corollary (see Corollary 13), we get the main result of [42].

A few authors have considered codes over the ring $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ of residues modulo m. A new motivation for the study of these codes has been provided recently by [44] where it is shown that many important nonlinear codes can be viewed as binary images of linear codes over $\mathbb{Z}_4$. Thus, introducing codes over $\mathbb{Z}_m$ makes it possible to apply to nonlinear codes the techniques developed earlier for linear codes, or in particular polynomial codes.

Theorem 15 describes all finite rings

$$\mathbb{Z}_m[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$$

which have radicals that are principal ideals. It turns out that in this case the description is essentially more complicated, and does not follow from our first theorem.

After that, we give formulas for the minimum Hamming weight of the radical and its powers in the algebra

$$F[x_1, \ldots, x_n]/(x_1^{a_1}(1 - x_1^{b_1}), \ldots, x_n^{a_n}(1 - x_n^{b_n})).$$

If $f = g_1^{m_1} \cdots g_k^{m_k}$, where $f \in F[x]$ and $g_1, \ldots, g_k$ are irreducible polynomials over F, then by $\mathrm{sp}(f)$ we denote the squarefree part $g_1 \cdots g_k$ of f. We assume that $\mathrm{sp}(0) = 0$ and regard 0 as a squarefree polynomial. Since the Jacobson radical and nilradical $\mathcal{N}(R)$ of an Artinian ring R are identical, [1] p.89, we refer to this as the *radical* of R.

Theorem 11 *Let $f_1(x_1), \ldots, f_n(x_n)$ be univariate polynomials over an arbitrary field F, and let $R = F[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$. Then the radical $\mathcal{N}(R)$ is a principal ideal of R if and only if the number of polynomials $f_1, \ldots, f_n$ which are not squarefree does not exceed one.*

We shall use the following description of the radical.

Lemma 12 ([3, §8.2]). *The radical $\mathcal{N}(R)$, of*

$$R = F[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$$

is equal to the ideal generated by the squarefree parts of all polynomials $f_1, \ldots, f_n$.

Proof of Theorem 11. The 'if' part immediately follows from Lemma 12. Indeed, if all $f_1, \ldots, f_n$ are squarefree, then $\mathcal{N}(R) = 0$. If f_i is not squarefree, and all the other polynomials are squarefree, then $\mathcal{N}(R)$ is generated by the squarefree part of $f_i(x_i)$.

The 'only if' part: Suppose to the contrary that the radical of R is a principal ideal, but two polynomials, say $f_1(x_1)$ and $f_2(x_2)$, are not squarefree.

Assume that $f_1, \ldots, f_k \neq 0$ and $f_{k+1}, \ldots, f_n = 0$. Then it follows from Lemma 12 that the radical $\mathcal{N}(R)$ is equal to

$$\mathcal{N}\{F[x_1, \ldots, x_k]/(f_1(x_1), \ldots, f_k(x_k))\}[x_{k+1}, \ldots, x_n].$$

To simplify the notation we may assume that $k = n$, i.e. all $f_1, \ldots, f_n$ are nonzero.

Then R has finite dimension as a vector space. Therefore it is a direct sum of local rings ([1], Proposition 8.7). If the radical of a local Artinian ring is a principal ideal, then all ideals are principal by [1], Proposition 8.8. Thus R is a PIR.

Since $R/(x_3, \ldots, x_n)$ is a homomorphic image of R, it is also a PIR. Hence we may assume that $n = 2$. Let $f_1(x_1) = g_1^{\alpha_1}(x_1) \ldots g_k^{\alpha_k}(x_1)$ where $g_1(x_1), \ldots, g_k(x_1)$ are irreducible over F and $\alpha_1 > 1$. Since $(g_1^{\alpha_1}, f_2) \supset (f_1, f_2)$, the ring $F[x_1, x_2]/(g_1^2(x_1), f_2(x_2))$ is a homomorphic image of R and so it is a PIR too. Therefore we may assume that from the very beginning $f_1(x_1) = g_1^2(x_1)$. Given that $g_1(x_1)$ is irreducible, we see that $Q = F[x_1]/(g_1(x_1))$ is a field. If we regard $f_2(x_2) \in F[x_2] \subseteq Q[x_2]$ as a polynomial over Q it is not squarefree. Consider the factorization $f_2(x_2) = h_1^{\beta_1}(x_2) \ldots h_m^{\beta_m}(x_2)$ where all $h_i(x_2) \in Q[x_2]$ are irreducible and $\beta_1 > 1$. Clearly, $Q[x_2] = (F[x_1]/(g_1(x_1)))[x_2]$ $= F[x_1, x_2]/(g_1(x_1))$ is a homomorphic image of $F[x_1, x_2]$. Denote by $h(x_1, x_2)$ a polynomial in $F[x_1, x_2]$ whose image in $Q[x_2]$ equals $h_1(x_2)$. Consider the ideal I generated by $g_1(x_1)$ and $h(x_1, x_2)$ in $F[x_1, x_2]$. We see that

$$\begin{aligned} F[x_1, x_2]/I &\cong \{F[x_1, x_2]/(g_1(x_1))\}/\{(g_1(x_1), h(x_1, x_2))/(g_1(x_1))\} \\ &\cong Q[x_2]/h_1(x_2) \end{aligned}$$

is a field, because $h_1(x_2)$ is irreducible over Q. Therefore I is a maximal ideal. By [41], Proposition 38.4(b), the ring $F[x_1, x_2]$ must not have ideals which lie strictly between I and I^2. However, $(g_1(x_1), h^2(x_1, x_2), g_1(x_1)h(x_1, x_2))$ strictly contains I^2 and is contained in I. This contradiction shows that at most one of the polynomials $f_1, \ldots, f_n$ can be squarefree. □

Theorem 11 immediately gives the main result of [42].

Corollary 13 ([42]) *Let F be a field, $m \leq n$, $a_1, \ldots, a_m$ nonnegative integers, $b_1, \ldots, b_m$ positive integers, and let*

$$R = F[x_1, \ldots, x_n]/(x_1^{a_1}(1 - x_1^{b_1}), \ldots, x_m^{a_m}(1 - x_m^{b_m})).$$

If $\operatorname{char} F = 0$, *then the radical of R is a principal ideal if and only if at most one of the $a_1, \ldots, a_m$ is greater than* 1.

If $\operatorname{char} F = p > 0$, *then R is a PIR if and only if one of the following conditions is satisfied:*

(1) $a_1, \ldots, a_m \leq 1$ and p divides at most one number among $b_1, \ldots, b_m$;

(2) exactly one of $a_1, \ldots, a_m$, say a_1, is greater than 1 *and p does not divide each of $b_2, \ldots, b_m$.*

Proof of Corollary 13. Consider the polynomial $f = x^a(1 - x^b)$. By [3], Lemma 2.85, a polynomial is squarefree if and only if it is coprime with its derivative. If $\operatorname{char} F = 0$, then we see that f is squarefree if and only if $a = 1$. If however $\operatorname{char} F = p > 0$, then f is squarefree if and only if $a = 1$ and p does not divide b. Thus Theorem 11 completes the proof. □

A second corollary to Theorem 11, Corollary 14, shows that the generalized Reed-Muller codes which contain only one generator polynomial are defined using polynomials $x_i^{p^{c_i}} - 1$ with $c_i > 1$ for at most one i, $i = 1 \ldots, n$.

Corollary 14 *Let* $A = F_q[x_1, \ldots, x_n]/(x_1^{q_1} - 1, \ldots, x_n^{q_n} - 1)$, *where* F_q *is a finite field,* $p = \operatorname{char} F_q$, $q_i = p^{c_i}$ *and* $c_i \geq 1$ *for* $i = 1, \ldots, n$. *Let* $C_h = (\mathcal{N}(R))^h$ *be a generalized Reed-Muller code, where* $1 \leq h < N$, *and* N *is the nilpotent index of* A. *Then* C_h *has only one generator polynomial if and only if* $n = 1$ *or* $c_i > 1$ *for at most one* i.

Proof. For $i = 1, \ldots, n$, the polynomial $x_i^{q_i} - 1 = (x^p - 1)^{c_i} \in F_q[x]$ is squarefree if and only if $c_i = 1$. □

Let $m = p_1^{a_1} \cdots p_k^{a_k}$ be a positive integer, where $p_1 < \cdots < p_k$ are primes. Suppose that we want to describe all finite rings

$$R = \mathbb{Z}_m[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$$

which have radicals that are principal ideals. Since $\mathbb{Z}_m$ is isomorphic to the direct product $\prod_{i=1}^k \mathbb{Z}/p_i^{a_i}\mathbb{Z}$, and the radical of a finite direct product is a principal ideal if and only if the radicals of all direct components are principal, it easily follows that we need only to consider the case where $m = p^a$ for a prime p.

Let $m = p^a$. Any element of $\mathbb{Z}_m$ is uniquely represented by an element of the integer interval $[0, m-1] = \{0, 1, \ldots, m-1\} \subseteq \mathbb{Z}$. Denote by $\mathcal{B}[x]$ the set of all polynomials $f \in \mathbb{Z}_m[x]$ such that all coefficients of f are represented by elements of $\mathcal{B} = [0, p-1]$. Let $f \longmapsto \overline{f}$ denote the natural homomorphism of $\mathbb{Z}_m[x]$ onto $\mathbb{Z}_p[x]$ (i.e., reduction of coefficients modulo p).

For any polynomial $g \in \mathbb{Z}_p[x]$ there exists a unique polynomial $g' \in \mathcal{B}[x]$ such that $\overline{g'} = g$. Hence, for any polynomial $f \in \mathbb{Z}_m[x]$ there exists a unique polynomial $f' \in \mathcal{B}[x]$ such that $\overline{f'} = \overline{f}$. Evidently, $\overline{f} = \overline{g}$ if and only if $f' = g'$.

Similarly, if $a > 1$, then there exists a unique polynomial $f'' \in \mathcal{B}[x]$ such that $f - f' - pf'' \in p^2\mathbb{Z}_m$. For $a = 1$, we put $f'' = 0$.

Using this terminology, for any $f \in \mathbb{Z}_m[x]$, we define unique polynomials $d = d_f, u = u_f \in \mathcal{B}[x]$ and $\widehat{f} \in \mathbb{Z}_p[x]$ by the following conditions, $d = d'$, $u = u'$, $\overline{d} = \mathrm{sp}(\overline{f})$, $\overline{f} = \overline{d}\overline{u}$ and $\widehat{f} = \overline{f'' - (ud)''}$. It follows that $f' - ud \in p\mathbb{Z}_m[x]$. Since $f' \in \mathcal{B}[x]$ then $(f')'' = 0$ for any f and we also get $\widehat{f} = \overline{f'' + (f' - ud)''}$.

A polynomial $f \in \mathbb{Z}_{p^a}[x]$ is *regular* if it is not a zero divisor. It follows from [71], Theorem 13.2, that p divides f if and only if f is a zero divisor. Therefore if f is a zero divisor then $f = p^r e$ for some integer $1 \leq r \leq a - 1$ and monic polynomial $e(x) \in R[x]$. By [71], Theorem 13.6, if $f(x)$ is regular then there exists a unit $u \in R$ and monic polynomial $e(x) \in R[x]$ such that $f = ue$.

Let R be defined as in Theorem 15, with the $f_i(x_i)$ being univariate polynomials. It follows from [71], Theorem 13.2(c), that R is finite if and only if all the $f_i(x_i)$ are regular. Theorem 15 and Corollary 16 are true when the $f_i(x_i)$ are regular polynomials but for simplicity we assume they are monic.

Theorem 15 *Let $m = p^a$, where p is a prime and a is a positive integer. The radical $\mathcal{N}(R)$ of the ring*

$$R = \mathbb{Z}_m[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$$

where $f_1(x_1), \ldots, f_n(x_n)$ are monic, is a principal ideal if and only if the following conditions are satisfied:

(i) the number of polynomials $f_1, \ldots, f_n$ which are not squarefree modulo p does not exceed one;

(ii) if $a > 1$ and $f = f_i$ is not squarefree modulo p, then $\widehat{f}$ is coprime with $\overline{u_f}$.

Proof of Theorem 15. If $a = 1$, then $\mathbb{Z}/p^a\mathbb{Z}$ is a field, and the assertion follows from Theorem 11. Further, we assume that $a \geq 2$.

The radical $\mathcal{N}(R)$ contains the ideal pR, because $(pR)^a = 0$. If all polynomials $\overline{f}_1(x_1), \ldots, \overline{f}_n(x_n)$ are squarefree over $\mathbb{Z}_p$, then

$$R/pR \cong \mathbb{Z}_p[x_1, \ldots, x_n]/(\overline{f}_1(x_1), \ldots, \overline{f}_n(x_n))$$

is semisimple by Lemma 12, and so $\mathcal{N}(R) = pR$ is a principal ideal.

Suppose that exactly one polynomial, say $f = f_1$, is not squarefree. Let u, d be polynomials in $\mathbb{Z}_m[x]$ as defined above then it follows from Lemma 12 that

$$\mathcal{N}(R) = (d_f, p) = \{\mathcal{N}(\mathbb{Z}_m[x_1]/(f_1))\}[x_2, \ldots, x_n]/(f_2, \ldots, f_n).$$

Therefore $\mathcal{N}(R)$ is a principal ideal if and only if $\mathcal{N}(\mathbb{Z}_m[x_1]/(f_1))$ is principal. So we may assume that $n = 1$, $x = x_1$, and $R = \mathbb{Z}_m[x]/(f(x))$.

Suppose that $\widehat{f}$ is coprime with $\overline{u_f} = \overline{u}$. Denote by h a polynomial in $\mathbb{Z}_m[x]$ such that $h = h'$ and $\overline{h}$ is the product of all irreducible divisors of $\overline{f}$ which do not divide $\widehat{f}$. Put $g = d + ph \in \mathbb{Z}_m[x]$. We claim that the radical $\mathcal{N}(R)$ is equal to the ideal I generated in R by g.

It follows from Lemma 12 that $\mathcal{N}(R) = (p, d)$. hence $g \in \mathcal{N}(R)$ so $I \subseteq \mathcal{N}(R)$. Therefore it remains to show that $p, d \in (g) = I$.

The choice of h ensures that $\widehat{f} - \overline{hu}$ is not divisible by any irreducible factor of $\overline{f}$ which does not divide $\widehat{f}$. If we look at an irreducible factor of $\overline{f}$ which divides $\widehat{f}$, then it does not divide $\overline{h}$, and so it does not divide $\overline{hu}$, because $\overline{u}$ is coprime with $\widehat{f}$. Thus $\widehat{f} - \overline{hu}$ and $\overline{d}$ are coprime.

Hence there exist $A, B \in \mathbb{Z}_m[x]$ such that $A = A'$, $B = B'$ and $\overline{1} = \overline{A}(\widehat{f} - \overline{hu}) + \overline{B}\overline{d}$. Notice that $f' - ud = p[(f' - ud)''] + p^2 w$ for some $w \in \mathbb{Z}_m[x]$, because $(f' - ud)' = 0$. There exists a unique polynomial $f^* = (f^*)' \in \mathbb{Z}_m[x]$ satisfying $\overline{f^*} = \widehat{f}$. Since p^a is the characteristic of $\mathbb{Z}_m$ then $p^a w = 0$ for all $w \in \mathbb{Z}_m[x]$. We can lift the equation from $\mathbb{Z}_m[x]/p\mathbb{Z}_m[x] \cong \mathbb{Z}_p[x]$ to $\mathbb{Z}_m[x]$ and multiply by p^{a-1} to get the following.

$$\begin{aligned}
p^{a-1} &= p^{a-1}[A(f^* - hu) + Bd] \\
&= p^{a-1}[A\{f'' + (f' - ud)'' - hu\} + Bd] \\
&= p^{a-2}[A\{pf'' + (f' - ud) - phu\} + pBd] \\
&= p^{a-2}[A(f' + pf'') - Au(d + ph) + pBd] \\
&= p^{a-2}[Af - (Au - pB)g].
\end{aligned}$$

Therefore $p^{a-1} \in (g, f) \subset \mathbb{Z}_m[x]$, and so $p^{a-1} \in I$.

Since p^{a-1} belongs to both I and $\mathcal{N}(\mathbb{Z}_{p^a})$, we can factor out the ideal generated by p^{a-1} in R and consider the ideal $I/p^{a-1}I$ in $R/p^{a-1}R$. Also clearly $\mathbb{Z}_{p^a}/p^{a-1}\mathbb{Z}_{p^a} \cong \mathbb{Z}_{p^{a-1}}$. We identify $f, g \in \mathbb{Z}_{p^a}[x]$ with their images in $f, g \in \mathbb{Z}_{p^{a-1}}[x]$. We can now lift the equation from $\mathbb{Z}_p[x]$ to $\mathbb{Z}_{p^{a-1}}[x]$

and multiply by p^{a-2} and repeat the argument above with $p^{a-1}w = 0$ for all $w \in \mathbb{Z}_{p^{a-1}}[x]$ to get $p^{a-2} \in (g, f) \subset \mathbb{Z}_{p^{a-1}}[x]$. Identifying $p^{a-2} \in \mathbb{Z}_{p^a}[x]$ with its image $p^{a-2} \in \mathbb{Z}_{p^{a-1}}[x]$ then $p^{a-2} \in I/p^{a-1}I$ so $p^{a-2} \in I$. Repeating this argument $a-3$ times we get $p \in I$.

Next we prove that $d \in I$. Since $g, p \in I$ then $d = g - ph \in I$. Thus $I = \mathcal{N}(R)$. This means that $\mathcal{N}(R)$ is a principal ideal.

Conversely, suppose that the radical is a principal ideal generated by some polynomial $g \in \mathbb{Z}_m[x]$.

Since $(\overline{g}) = (\overline{d}) = \mathcal{N}(\mathbb{Z}_p[x]/(\overline{f}))$, we get $\overline{g} = \overline{t}\overline{d} + \overline{e}\overline{f}$ for some $t = t' \in \mathbb{Z}_m$ and $e(x) \in \mathbb{Z}_m[x]$. There exists an integer $s = s' \in \mathbb{Z}_m$ such that $ts \equiv 1 (\bmod p)$. Since $\overline{s(g - ef)} = \overline{std} = \overline{d}$ and $(\overline{g}) = (\overline{d})$ then g generates the same ideal as $s(g - ef)$ in $R = \mathbb{Z}_m[x]/(f)$, so we can replace g by $s(g - ef)$. To simplify the notation we assume that $\overline{g} = \overline{d}$, and so $g' = d$.

Given that $p \in \mathcal{N}(R)$, we get $p = Af + Bg$ for some $A, B \in \mathbb{Z}_m[x]$. Since $(Af + Bg)' = (A'f' + B'g')' = 0$, it follows that $\overline{A'f'} + \overline{B'g'} = 0$. Therefore $\overline{B'} = -\overline{A'}\overline{u}$ whence $B' = -A'u + pz$ for some $z = z' \in \mathbb{Z}_m[x]$.

Further, $p = (A' + pA'')(f' + pf'') + (B' + pB'')(g' + pg'') + p^2w$, for some $w \in \mathbb{Z}_m[x]$. Notice that $f' = (ug')'$ because $\overline{f'} = \overline{f} = \overline{ug'}$. Since $u = u'$ and $g = g'$ then $ug' = (ug')' + p(ug')'' = f' + p(ug')''$. It follows that $f' - ug' = -p(ug')''$. Therefore we get

$$\begin{aligned} p^{a-1} &= p^{a-2}[(A' + pA'')(f' + pf'') + (-A'u + pz + pB'')(g' + pg'')] \\ &= p^{a-2}[A'(f' - ug' + pf'') - A'upg'' + pA''f' + pg'(z + B'')] \\ &= p^{a-1}[A'(-(ug')'' + f'') - uA'g'' + A''(ug')' + g'(z + B'')], \end{aligned}$$

Given that $p^a = 0$, then $p^{a-1}v = p^{a-1}w$ if and only if $\overline{v} = \overline{w}$ where $v, w \in \mathbb{Z}_m[x]$. Hence

$$\begin{aligned} \overline{1} &= \overline{A'}(\overline{-(ug')'' + f''}) - \overline{u}(\overline{A'g''}) + \overline{A''}(\overline{(ug')'}) + \overline{g'}(\overline{z + B''}) \\ &= \overline{A'}\widehat{f} - \overline{u}(\overline{A'g''}) + \overline{A''}\overline{ug'} + \overline{g'}(\overline{z + B''}). \end{aligned}$$

Since all irreducible factors of $\overline{u}$ divide $\overline{g'} = \overline{d}$, they also divide the polynomial $-\overline{u}(\overline{A'g''}) + \overline{A''}\overline{ug'} + \overline{g'}(\overline{z + B''})$, and we see that $\overline{u}$ must be coprime with $\widehat{f}$. This completes the proof. □

When $n = 1$ Theorem 15 becomes Corollary 16.

Corollary 16 *Let $f(x) \in \mathbb{Z}_m[x]$ be a monic polynomial which is not square-free modulo p, where $m = p^a$, p is prime and $a \geq 2$ is a positive integer. Define $R = \mathbb{Z}_m[x]/(f(x))$ then R is a PIR if and only if $\overline{u}_f$ is coprime with $\widehat{f}$.*

The proof of Theorem 15 shows that if $R = \mathbb{Z}_m[x]/(f(x))$ is a PIR then $\mathcal{N}(R)$ is generated by $g = d + ph \in \mathbb{Z}_m[x]$ where h satisfies $h = h'$ and $\overline{h}$ is the product of all irreducible divisors of $\overline{f}$ not dividing $\widehat{f}$.

Example 17 Define $R = \mathbb{Z}_{27}[x]/(f(x))$ where $f(x) = x^7+4x^6+18x^5+11x^4+9x^3+6x^2+7x+8 \in \mathbb{Z}_{27}[x]$. The set $\mathcal{B} = [0, 1, 2]$ defines the set of polynomials $\mathcal{B}[x]$. The notation f', f'' may be continued to define f''', f'''' etc. but only the polynomials f' and f'' actually need to be calculated. So $f = f' + 3f'' + 3^2 f'''$ where $f' = x^7+x^6+2x^4+x+2$, $f'' = 19x^6+24x^5+21x^4+21x^3+20x^2+26x+5$, $f''' = x+2 \in \mathbb{Z}_{27}[x]$. Since $\overline{f}(x) = x^7+x^6+2x^4+x+2 = (x+1)^3(x^2+x+2)(x^2+1) \in \mathbb{Z}_3[x]$, where $(x+1), (x^2+x+2)$ and (x^2+1) are irreducible over $\mathbb{Z}_3$, then $\overline{d}(x) = \text{sp}(\overline{f}) = (x+1)(x^2+x+2)(x^2+1) = x^5+2x^4+x^3+x^2+2 \in \mathbb{Z}_3[x]$ and since $\overline{f} = \overline{d}\overline{u}$ then $\overline{u}(x) = (x+1)^2 = x^2+2x+1 \in \mathbb{Z}_3[x]$. Since $d = d', u = u' \in \mathcal{B}[x] \subset \mathbb{Z}_{27}[x]$ are the same polynomials as $\overline{d}, \overline{u} \in \mathbb{Z}_3[x]$ then $d = x^5 + 2x^4 + x^3 + x^2 + 2$, $u = x^2 + 2x + 1$ and
$ud = x^7 + 4x^6 + 6x^5 + 5x^4 + 3x^3 + 3x^2 + 4x + 2 \in \mathbb{Z}_{27}[x]$.
So $f' - ud = 3(8x^6 + 7x^5 + 8x^4 + 8x^3 + 8x^2 + 8x) = 3(f' - ud)''$ and

$$\begin{aligned}
\hat{f} &= \overline{(f' - ud)'' + f''} \\
&= \overline{(8x^6 + 7x^5 + 8x^4 + 8x^3 + 8x^2 + 8x)} \\
&\quad \overline{+(19x^6 + 24x^5 + 21x^4 + 21x^3 + 20x^2 + 26x + 5)} \\
&= \overline{4x^5 + 2x^4 + 2x^3 + x^2 + 7x + 5} = x^5 + 2x^4 + 2x^3 + x^2 + x + 2 \\
&= (x+2)(x^2+1)^2 \in \mathbb{Z}_3[x].
\end{aligned}$$

The ideal $\mathcal{N}(R)$ is principal since $\gcd(\hat{f}, \overline{u}) = 1$. As $(x^2+1)|\hat{f}$ then $\overline{d} = \overline{h}(x^2+1)$, $\overline{h} = (x+1)(x^2+x+2) = x^3+2x^2+2 \in \mathbb{Z}_3[x]$ and $h = h' = x^3+2x^2+2 \in \mathbb{Z}_{27}[x]$. $\mathcal{N}(R)$ is generated by $g = d + 3h = (x^5+2x^4+x^3+x^2+2) + 3(x^3+2x^2+2) = x^5+2x^4+4x^3+7x^2+8$. Calculations for this example were done using the software [69].

2.2 Hamming weights of polynomial codes

Let F be a field, $a_1, \ldots, a_n$ nonnegative integers, $b_1, \ldots, b_n$ positive integers, and let

$$R = F[x_1, \ldots, x_n]/(x_1^{a_1}(1 - x_1^{b_1}), \ldots, x_n^{a_n}(1 - x_n^{b_n})).$$

Formulas are given here for the minimum Hamming weight of the radical and its powers in the algebra R. Ideals of the form $(x_1^{a_1}(1-x_1^{b_1}),\ldots,x_n^{a_n}(1-x_n^{b_n}))$ are called periodic ideals, see [65], Definition 6.16, p.2817. Denote by I the radical $\mathcal{N}(R)$ of R. Lemma 12 tells us that I is generated by the squarefree parts of the polynomials $x_1^{a_1}(1-x_1^{b_1})$. The *Hamming distance* or *minimum Hamming weight* $w_H(I)$ of I in the basis $B=\{x_1^{e_1}\cdots x_n^{e_n}|0\le e_i<a_i+b_i \text{ for } 1\le i\le n\}$ is the minimum number of nonzero coordinates in B of nonzero vectors in I. It is an important characteristic, and in particular determines the number of errors the code I can detect or correct (see [68]). Clearly, $w_H(\{0\})=0$. Formulas are given for the Hamming weight of powers of I with respect to the basis B.

Let $w(r)$ be the Hamming weight of $r\in R$ and let $w(J)$ be the minimum Hamming weight of an ideal $J\subset R$ with respect to B. For positive integers $b_1,\ldots,b_n$ write $b_i=p^{c_i}d_i$ where p does not divide d_i and $i=1,\ldots,n$. We may assume that $c=c_1\ge c_2\ge\ldots\ge c_n\ge 0$. Denote by $z\ge 0$ the number of elements $c_1,\ldots,c_n$ which are equal to 0 or, in other words, the number of elements $b_1,\ldots,b_n$ not divisible by p. Let $[1,n]=\{1,2,\ldots,n\}$. Denote by L the set of all i such that $a_i>p^{c_i}$. Let $S=[1,n]\backslash L$. For any $T\subseteq[1,n]$, put $a_T=\sum_{i\in T}a_i-|T|$.

Theorem 18 *Let F be a field, $a_1,\ldots,a_n$ nonnegative integers, $b_1,\ldots,b_n$ positive integers, and with $I=\mathcal{N}(R)$, let*

$$R=F[x_1,\ldots,x_n]/(x_1^{a_1}(1-x_1^{b_1}),\ldots,x_n^{a_n}(1-x_n^{b_n})).$$

If $\operatorname{char}F=0$, *then*

$$w(I^h)=\begin{cases}2^\ell & \text{if } a_1+\cdots+a_{\ell-1}-\ell+1<h\le a_1+\cdots+a_\ell-\ell\\ 0 & \text{if } a_1+\cdots+a_k-k\le h.\end{cases}$$

If $\operatorname{char}F=p>0$, *then*

$$w(I^h)=\begin{cases}2 & \text{if } h<a_1+\cdots+a_{n-z}\\ \min\limits_{T\subseteq[1,n-z]}\{2^{|L|+|T|}w(h-a_L-a_T;S\backslash T)\} & \text{otherwise.}\end{cases}$$

Proof. Suppose that F has zero characteristic. We may assume that $a_1\ge\ldots\ge a_k>1$ and $a_{k+1},\ldots,a_n\le 1$. Then the radical I is generated by all polynomials $x_i(1-x_i^{b_i})$, for $i=1,\ldots,k$. It follows that I is also generated

by all polynomials $g_i = x_i(1 - x_i^{b_i+a_i(b_i-1)})$, for $i = 1, \ldots, k$. Since $g_i^{a_i} = 0$ and $g_i^j = x_i^j(1 - x_i^{b_i+a_i(b_i-1)})$ modulo $x_i^{a_i}(1 - x_i^{b_i})$, we see that the linear span of all powers g_i^j has Hamming weight 2, for $j = 1, \ldots, a_i - 1$. Therefore, the theorem in Section 2 of [90] gives us the following formula for the Hamming weight $w(I^h)$ of I^h:

$$w(I^h) = \begin{cases} 2^\ell & \text{if } a_1 + \cdots + a_{\ell-1} - \ell + 1 < h \leq a_1 + \cdots + a_\ell - \ell \\ 0 & \text{if } a_1 + \cdots + a_k - k \leq h. \end{cases}$$

Let F be a field of characteristic $p > 0$. First, we consider the case where $a_1 = \cdots = a_n = 0$. By the definitions of z and the d_i, the radical I is generated by all elements $f_i = 1 - x^{d_i}$, for $i = 1, \ldots, n - z$.

Following Berman [5], for $a \geq 0$, denote by ℓ_a the number of exponents c_i such that $c_i > a$. In particular, $\ell_0 = n - z$ and $\ell_c = 0$. Put $m_a = \ell_a(p-1)p^a$.

The nilpotency index of I is $N = p^{m_0+m_1+\cdots+m_c}$. Suppose that $h < N$. Then there exists b such that $\sum_{a=b+1}^{c} m_a \leq h < \sum_{a=b}^{c} m_a$. We can find t such that $h = \sum_{a=b+1}^{c} m_a + t(p-1)p^b + s$ and $t(p-1)p^b \leq h - \sum_{a=b+1}^{c} m_a < (t+1)(p-1)p^b$. Then $w(I^h)$ is equal to the following number (see [5], [24] or [90])

$$w(h; c_1, \ldots, c_n) = \begin{cases} 0 & \text{if } h \geq p^{m_0+m_1+\cdots+m_c} \\ p^{\ell_{b+1}+\ell_{b+2}+\cdots+\ell_c+t}(1 + \lceil sp^{-b} \rceil) & \text{otherwise.} \end{cases}$$

where $\lceil x \rceil$ is the smallest integer $\geq x$.

Next, consider the case where $n = 1$. Put $a = a_1, b = b_1, c = c_1, d = d_1$. Then $R = F[x]/(x^a(1-x^b))$ and $b = p^c d$. It is routine to verify that the radical of R is generated by $g = x(1 - x^{b+a(b-1)})$ and $f = x^a(1 - x^d)$. Since $x^{a-1}g = 0$, the linear span V of $g, xg, \ldots, x^{a-2}g$ annihilates f. Hence $I = V + (f)$. For any $v \in V$ and $y \in (f)$ it is clear that $w(v + y) \leq w(y)$. Exactly as in the case of characteristic zero, $w(V) = w(V^2) = \cdots = w(V)^{a-1} = 2$. For $h \geq a$, we get $I^h = (f)^h$. Thus we have the following formula

$$w(I^h) = \begin{cases} 2 & \text{if } h < a \\ w(h; c) & \text{otherwise.} \end{cases}$$

In the general case, the algebra R is a tensor product of algebras

$$R_i = F[x_i]/(x^{a_i}(1 - x^{b_i})),$$

where $i = 1, \ldots, n$. The radical of R is generated by all $g_i = x_i(1 - x_i^{b_i + a_i(b_i-1)})$ and $f_i = x_i^a(1 - x^{d_i})$. As we have seen, the weight of the radical I_i of every R_i is equal to the weight of an element of the form g_i^k or f_i^k. It follows from the theorem in Section 2 of [90] that the weight of I^h is equal to the weight of some element of the form $q_1^{k_1}(x_1) \cdots q_n^{k_n}(x_n)$, where $q_i \in \{f_i, g_i\}$ and $k_1 + \cdots + k_n \geq n$. Therefore,

$$w(I^h) = \min \left\{ \prod w(I_i^{k_i}) \mid k_1 + \cdots + k_n \geq n; \text{ all } k_i \geq 0 \right\}.$$

Combining the formula above with the formulas for the weights of I_i^h, we get the following

$$w(I^h) = \begin{cases} 2 & \text{if } h < a_1 + \cdots + a_{n-z} \\ \min\limits_{T \subseteq [1, n-z]} \{2^{|L|+|T|} w(h - a_L - a_T; S \backslash T)\} & \text{otherwise.} \end{cases}$$

□

A special case of Theorem 18 is given in [5] as Theorem 1.2.

We conclude this chapter with a discussion of some semigroup algebras and error-correcting codes. Let $a \geq 0$ and $b \geq 1$ be integers. Define C_b as the cyclic group of order b. Let $S_{a,b}$ be the finite cyclic semigroup such that each $s \in S$ satisfies $s^{a+b} = s^a$. A finite Abelian group G is a direct product of cyclic groups, and similarly a finite commutative semigroup S is a union of groups and finite cyclic semigroups. We now consider tensor products of semigroup algebras over finite cyclic semigroups. The ring $F[x]/(1 - x^b)$ is a group algebra FC_b. Similarly the ring $F[x]/(x^a(1 - x^b))$ is a semigroup algebra $FS_{a,b}$. Lemma 19 is proved in the special case when S is a finite group $S = \prod_{i=1}^2 C_{b_i}$, as the example on p.165 of [80]. This proof can be modified to prove Lemma 19.

Lemma 19 *The ring $\otimes_{i=1}^n FS_{a_i,b_i}$ is isomorphic to the semigroup algebra FS where $S = \prod_{i=1}^n S_{a_i,b_i}$.*

Define the group $G = \prod_{i=1}^n C_{b_i}$ and semigroup $S = \prod_{i=1}^n S_{a_i,b_i}$. By Lemma 19,

$$F[x_1, \ldots, x_n]/(1 - x_1^{b_1}, \ldots, 1 - x_n^{b_n}) \cong \otimes_{i=1}^n F[x]/(1 - x^{b_i}) \cong FG,$$

$$F[x_1, \ldots, x_n]/(x_1^{a_1}(1 - x_1^{b_1}), \ldots, x_n^{a_n}(1 - x_n^{b_n})) \cong \otimes_{i=1}^n F[x]/(x^{a_i}(1 - x^{b_i}) \cong FS.$$

These identities provide the motivation for the following definitions of codes. Let F_q be the finite field with $\text{char}(F_q) = p \geq 2$. A *cyclic code* of length b is an ideal of the group algebra $F_q[x]/(x^b - 1) \cong F_q C_b$ where $(b, p) = 1$. An *Abelian group code* is an ideal in an Abelian group algebra, see [6] p.227. Analogously we can define a *semicyclic code* as an ideal of the semigroup algebra $F_q[x]/(x^a(1 - x^b)) \cong F_q S_{a,b}$, where $(b, p) = 1$. More generally, we can define a *multivariate semicyclic code* as any ideal of the semigroup algebra $R = F_q[x_1, \ldots, x_n]/\ (x_1^{a_1}(1 - x_1^{b_1}), \ldots, x_n^{a_n}(1 - x_n^{b_n})) = F_q S$, where $S = \prod_{i=1}^{n} S_{a_i,b_i}$ and $n \geq 2$. We can also define a *commutative semigroup code* as an ideal in a commutative semigroup algebra.

Let $R = F_q[x_1, \ldots, x_n]/(x_1^{a_1}(1 - x_1^{b_1}), \ldots, x_n^{a_n}(1 - x_n^{b_n}))$ have nilpotent index N. Consider the codes $C_h = \mathcal{N}(R)^h$ for $1 \leq h \leq N - 1$, the distinct powers of the radical $\mathcal{N}(R)$. The minimum Hamming distance $d = d(C_h) = w(\mathcal{N}(R)^h)$ is given in Theorem 18 with $\text{char}(F_q) = p \geq 2$. By Theorem 11 and Corollary 13, the code C_h is a principal ideal if and only if R is a PIR if and only if at most one of the polynomials $f(x_i) = x_i^{a_i}(1 - x_i^{b_i})$, for $1 \leq i \leq n$, is not squarefree. Let $\text{sp}(f)$ denote the squarefree part of a polynomial $f(x) \in F_q[x]$. Consider the case when R is a PIR and $f_1(x_1)$ is a nonsquarefree polynomial, hence $f_2, \ldots, f_n$ are squarefree. By Lemma 12, $\mathcal{N}(R)$ is equal to the ideal generated by the squarefree parts of all polynomials $f_1, \ldots, f_n$. By Corollary 40, since R is a PIR then $\mathcal{N}(R) = (\text{sp}(f_1))$. Hence the code C_h has a single generator polynomial $g = \text{sp}(f_1)^h$.

Chapter 3

Finite commutative principal ideal rings with identities

This chapter is devoted to two ring constructions and all rings considered are commutative and have identity elements. Conditions are given for the tensor product $R \otimes_{\mathbb{Z}} S$ to be a finite commutative PIR. Conditions are then given for a quotient ring Q/I to be a finite commutative PIR, where $Q = R[x_1, \ldots, x_n]$, R is a PIR and I is an ideal of Q generated by univariate polynomials. Several parts of this chapter appear in [22].

3.1 Tensor products of rings

The tensor product over $\mathbb{Z}$ is written as $\otimes$. For any ring R and prime p, the $p-$component of R is defined by

$$R_p = \{r \in R \mid p^k r = 0 \text{ for some positive integer } k\}.$$

Let R be an arbitrary ring, p a prime, and let $f \in R[x]$. Denote by $\overline{f}$ the image of f in $R[x]/pR[x]$. We say that f is *squarefree (irreducible) modulo* p if $\overline{f}$ is squarefree (respectively, irreducible). A *Galois ring* $GR(p^m, r)$ is a ring of the form $(\mathbb{Z}/p^m\mathbb{Z})[x]/(f(x))$, where p is a prime, m an integer, and $f(x) \in \mathbb{Z}/p^m\mathbb{Z}[x]$ is a monic polynomial of degree r which is irreducible modulo p. If $R = GR(p^m, r) = (\mathbb{Z}/p^m\mathbb{Z})[y]/(g(y)) \neq 0$ is a Galois ring which is not a field then $m > 1$, because $(\mathbb{Z}/p\mathbb{Z})[y]/(g(y))$ is a field, given that $g(y)$ is irreducible modulo p.

If the ideals of a ring form a chain, then it is called a *chain ring* (see [41] p.184). By Lemma 22, every finite local PIR and every field is a chain ring. The radical of a finite ring R is the largest nilpotent ideal $\mathcal{N}(R)$.

Lemma 20 *A finite ring is a PIR if and only if its radical is a principal ideal.*

Proof. The 'only if' part is trivial. If R is finite, then it is an Artinian ring. Therefore it is a direct product of local rings ([1], Proposition 8.7). If the radical of a local Artinian ring is a principal ideal, then all ideals are principal by Lemma 32 or [1], Proposition 8.8. □

The ring $GR(p^n, r)$ is well defined independently of the monic polynomial of degree r (see [71, §16]). Notice that $GR(p^m, 1) \cong \mathbb{Z}/p^m\mathbb{Z}$ and $GR(p, r) \cong GF(p^r)$, the finite field of order p^r. Lemma 21, first proved in [95], shows that a tensor product of Galois rings is a PIR.

Lemma 21 ([71], Theorem 16.8). *Let p be a prime, k_1, k_2, r_1, r_2 positive integers, and let $k = \min\{k_1, k_2\}$, $d = \gcd(r_1, r_2)$, $m = \operatorname{lcm}(r_1, r_2)$. Then*

$$GR(p^{k_1}, r_1) \otimes GR(p^{k_2}, r_2) \cong \prod_1^d GR(p^k, m).$$

In particular,

$$GF(p^{r_1}) \otimes GF(p^{r_2}) \cong \prod_1^d GF(p^m).$$

Lemma 22 ([71], Theorem 17.5). *Let R be a finite commutative ring which is not a field. Then the following conditions are equivalent:*

(i) *R is a chain ring;*

(ii) *R is a local PIR;*

(iii) *there exist a prime p and integers m, r, n, s, t such that*

$$R \cong GR(p^m, r)[x]/(g(x), p^{m-1}x^t),$$

where n is the index of nilpotency of the radical of R, $t = n-(m-1)s > 0$, $g(x) = x^s + ph(x)$, $\deg(h) < s$, and the constant term of $h(x)$ is a unit in $GR(p^m, r)$.

Let R be a chain ring as defined in Lemma 22(iii). The characteristic of R is p^m and its residue field is $R/\mathcal{N}(R) \cong GF(p^r)$. The polynomial $g(x)$ is called an *Eisenstein polynomial.* Since $GR(p^m, r)/pGR(p^m, r) \cong GF(p^r)$, we get $R/pR \cong GF(p^r)[x]/(x^s)$. By Lemma 24, R is a Galois ring if and only if $s = 1$.

Lemma 23 *Let $R = GR(p^m, r)[x]/(g(x), p^{m-1}x^t)$ be a chain ring, and let $s \geq 2$. Then the radical of R is generated by x.*

Proof. Clearly, p is a nilpotent element of R. Therefore (x) is a nilpotent ideal, because $g(x) = x^s + ph(x)$. Hence $(x) \subseteq \mathcal{N}(R)$. Given that $g(x) = x^s + ph(x)$ and the constant term of $h(x)$ is a unit in $GR(p^m, r)$, it follows that $p \in (x)$. Since $R/(x) \cong GF(p^r)$ is a semisimple ring, we get $(x) = \mathcal{N}(R)$. □

Lemma 24 ([71], Exercise 16.9). *A chain ring of characteristic p^m is a Galois ring if and only if its radical is generated by p. A PIR of characteristic p^m is a direct product of Galois rings if and only if its radical is generated by p.*

Lemma 25 *If R is a Galois ring, and S is a chain ring, then $R \otimes S$ is a PIR.*

Proof. Let $\text{char}\,(R) = p^m$, $\text{char}\,(S) = q^n$, for primes p, q and positive integers m, n. If $p \neq q$, then $R \otimes S = 0$ is a PIR.

Suppose that $p = q$. Let g be the generator of the radical of S. Denote by (g) the ideal generated by g in $R \otimes S$. Clearly, (g) is nilpotent, and so $(g) \subseteq \mathcal{N}(R \otimes S)$.

If R is a finite field, let $R = GF(p^v)$. If R is not a finite field, it is noted in the proof of Lemma 23 that $p \in gS$, and so $p \in (g)$. In either case, since $S/gS \cong GF(p^u)$ and $R/pR \cong GF(p^v)$, for some integers $u, v \geq 1$, we get $(R \otimes S)/(g) \cong GF(p^u) \otimes GF(p^v) \cong \prod_1^d GF(p^w)$ where $w = \text{lcm}\,\{u, v\}$ and $d = \gcd\{u, v\}$, by Lemma 21. Therefore $(g) = \mathcal{N}(R \otimes S)$. By Lemma 20, $R \otimes S$ is a PIR. □

Lemma 26 *Let R and S be chain rings which are not Galois rings, and let* $\mathrm{char}\,(R) = p^m$, $\mathrm{char}\,(S) = p^n$, *for a prime p and positive integers m, n. Then $R \otimes S$ is not a PIR.*

Proof. Suppose to the contrary that $P = R \otimes S$ is a PIR. Then P/pP is a PIR, too. By Lemma 22, $R \cong GR(p^u, q)[x]/(x^s + ph(x), p^{u-1}x^t)$. Since $GR(p^u, q)/pGR(p^u, q) \cong GF(p^q)$, we get $R/pR \cong GF(p^q)[x]/(x^s)$. If $s = 1$, then $R = GR(p^u, q)$ is a Galois ring. Therefore $s \geq 2$. Similarly, $S/pS \cong GF(p^r)[x]/(x^t)$, for some $t \geq 2$. It follows that $H = GF(p^q)[x]/(x^2) \otimes GF(p^r)[y]/(y^2)$ is a homomorphic image of P/pP, and so H is a PIR. Further, $H = (GF(p^q) \otimes GF(p^r))[x, y]/(x^2, y^2)$. By Lemma 21, $GF(p^q) \otimes GF(p^r)$ is a direct product of finite fields. Denote by F one of these fields. Then $F[x, y]/(x^2, y^2)$ is a homomorphic image of H, and so it is a PIR. However, if we set $I = (x, y)$, then I is a maximal ideal, and $I^2 \subset (x^2, xy) \subset I$. This is impossible by [41], Proposition 38.4(b). This contradiction completes the proof. □

Theorem 27 *A tensor product $R \otimes S$ of two finite commutative PIRs is a PIR if and only if, for each prime p, at least one of the rings R_p or S_p is a direct product of Galois rings.*

Proof. The 'if' part. Take any prime p. Suppose that R_p is a direct product of Galois rings, and S_p is a PIR. Hence S_p is a direct product of chain rings. Since tensor product distributes over direct products, Lemma 25 shows that $R_p \otimes S_p$ is a PIR. Hence $R \otimes S$ is a PIR, because it is a direct product of a finite number of rings $R_p \otimes S_p$, for some p.

The 'only if' part. Given that R and S are PIRs, obviously R_p and S_p are PIRs, for every p. Consider the decompositions of R_p and S_p into direct products of chain rings. If both of these decompositions contain chain rings which are not Galois rings, then we get a contradiction to Lemma 26. Thus at least one of the rings R_p or S_p must be a product of Galois rings. □

For rings R_p and S_p, which are p components , it is false that $R_p \otimes S_p \neq 0$ being a PIR implies that both R_p and S_p are PIRs. For example let $R_p = \mathbb{Z}_p$ and $S_p = GR(p^m, r)[x]/(x^s)$ then by Lemma 21,

$$\begin{aligned} R_p \otimes S_p &= \mathbb{Z}_p \otimes (GR(p^m, r)[x]/(x^s)) \cong (\mathbb{Z}_p \otimes GR(p^m, r))[x]/(x^s) \\ &\cong GF(p^r)[x]/(x^s) \cong S/pS. \end{aligned}$$

By Lemma 22, S_p cannot be a PIR when $m \geq 2$ and $s \geq 2$, yet $R_p \otimes S_p \cong GF(p^r)[x]/(x^s)$ is a PIR since $GF(p^r)[x]$ is a PIR for all integers $r, s \geq 1$, see p.13. This provides motivation to prove Lemma 29, which relies on Lemma 28.

Lemma 28 ([71], Theorem 17.1 p.337-338.) *Let R be a finite local ring satisfying* $\mathrm{char}\,(R) = p^m$ *for a prime p and positive integer m. If $\mathcal{N}(R)$ has a minimum of k generators then $R \cong GR(p^m, q)[x_1, \ldots, x_k]/J$ for some primary ideal J, $GR(p^m, q)$ is the largest Galois extension of $\mathbb{Z}/(p^m)$ in R, and $R/\mathcal{N}(R) \cong GF(p^q)$.*

Lemma 29 *Let R and S be finite local rings satisfying* $\mathrm{char}\,(R) = p^m$, $\mathrm{char}\,(S) = p^n$, *for a prime p and positive integers $m, n \geq 1$. If S/pS is not a PIR then $R \otimes S$ is not a PIR.*

Proof. If $\mathcal{N}(S)$ has a minimum of k generators then by Lemma 28, $S \cong \mathbb{Z}/(p^n)[x_1, \ldots, x_k]/J$ for some primary ideal J. Since S is not a PIR, $k \geq 2$. Let $R = \mathbb{Z}/(p^m)$ and consider the following sequence of homomorphic images, with $J' \cong J/pJ$. $(R \otimes S)/p(R \otimes S) \rightarrow (R/pR) \otimes (S/pS) = \mathbb{Z}/(p) \otimes (\mathbb{Z}/(p)[x_1, \ldots, x_k]/J') \cong \mathbb{Z}/(p)[x_1, \ldots, x_k]/J' = S/pS$. Since a homomorphic image of a PIR is a PIR and S/pS is not a PIR then $\mathbb{Z}/(p^m) \otimes S$ is not a PIR. Now let $\mathcal{N}(R)$ have a minimum of l generators then by Lemma 28, $R \cong \mathbb{Z}/(p^m)[x_1, \ldots, x_l]/I$ for some primary ideal I and $l \geq 1$. Let $R \rightarrow \mathbb{Z}/(p^m)$ be the canonical homomorphism. This induces the homomorphism $R \otimes S \rightarrow \mathbb{Z}/(p^m) \otimes S$. Since $\mathbb{Z}/(p^m) \otimes S$ is not a PIR then $R \otimes S$ is not a PIR. □

Lemma 30 *Let R and S be finite local rings which are not both PIRs, satisfying* $\mathrm{char}\,(R) = p^m$, $\mathrm{char}\,(S) = q^n$, *for primes p, q and positive integers m, n. If $R \otimes S$ is a PIR then (i) or (ii) is satisfied.*

(i) $p \neq q$ or $R = 0$ or $S = 0$ in which case $R \otimes S = 0$;

(ii) $p = q$, $R \neq 0 \neq S$, R is a Galois ring and S/pS is a finite chain ring which is not a Galois ring, or R and S may be interchanged.

Proof. Condition (ii). Let $R \otimes S$ and R be PIRs and S be a ring which is not a PIR.

By Lemma 29, S/pS is a PIR. Since $\mathrm{char}\,(S/pS) = p$, S/pS can only be a Galois ring if it is a finite field F_q where $\mathrm{char}\,(F_q) = p$. Since S is a local ring, $S/pS \cong F_q$ implies $(p) = \mathcal{N}(S)$ is a maximal ideal of S. By [71], Exercise 16.9, if S is a local ring, then $\mathcal{N}(S) = (p)$ if and only if S is a Galois ring. Since S is not a PIR, it is false that $S/pS \cong F_q$. Therefore S/pS is a chain ring which is not a Galois ring.

Assume R is not a Galois ring. It follows that $R \otimes S$ is a PIR, and both R and S/pS are chain rings which are not Galois rings. The conditions appearing in the proof of Lemma 26 are that $R \otimes S$ is a PIR, and both R and S are chain rings which are not Galois rings. This condition on S implies the same condition on S/pS. Therefore we can follow the proof of Lemma 26 exactly to arrive at a contradiction. Hence R is a Galois ring, so (ii) is satisfied. □

In general, if S/pS is a finite local PIR then by Lemma 22, $S/pS \cong GF(p^r)[x]/(x^s)$ for some integers $r, s \geq 1$. Therefore $S \cong GR(p^m, r)[x_1, \ldots, x_k]/(I + pJ)$ where $I = (x_1^s + pa)$, for some integer $m \geq 1$ and polynomial $a(x_1, \ldots, x_k)$ and ideal J. If S/pS is not a Galois ring then $s \geq 2$.

The converse of Lemma 30 is false. For example, if $R = \mathbb{Z}_{p^m}$ and $S = GR(p^m, r)[x]/(x^s)$ where $s \geq 2$ then $R \otimes S = \mathbb{Z}_{p^m} \otimes GR(p^m, r)[x]/(x^s) \cong (\mathbb{Z}_{p^m} \otimes GR(p^m, r))[x]/(x^s) \cong GR(p^m, r)[x]/(x^s) = S$ is not a PIR by Lemma 22, yet $S/pS \cong GF(p^r)[x]/(x^s)$ is a PIR which is not a Galois ring. Therefore as proved in Theorem 31, only the necessary condition of Theorem 27 is true when R and S are not both PIRs.

Theorem 31 *If a tensor product $R \otimes S$ of two finite commutative rings is a PIR then, for each prime p, at least one of the rings R_p or S_p is a direct product of Galois rings.*

Proof. If R and S are both PIRs then the theorem follows from Theorem 27. Assume R and S are not both PIRs. Since $R \otimes S$ is a PIR then for each prime p, $R_p \otimes S_p$ is a PIR. Consider the case when R_p and S_p are local rings. If R_p and S_p are both PIRs then by Lemmas 25 and 26, R_p or S_p must be a Galois ring. If R_p and S_p are not both PIRs then by Lemma 30, R_p or S_p must be a Galois ring. Now consider the case when R_p and S_p decompose into direct products of local rings. Since tensor product distributes over direct products, if both decompositions contain rings which are not Galois rings then $R_p \otimes S_p$ will contain a factor in its representation as a direct product, which is a tensor product of two rings, where neither ring is a Galois ring. Such a

factor is not a PIR by Lemma 26. Thus at least one of the rings R_p or S_p is a direct product of Galois rings. □

We now give a more general version of Lemmas 10 and 20 for a local ring.

Lemma 32 *If R is a local ring with maximal ideal $\mathfrak{m}$, which is not necessarily Noetherian but satisfies $\cap_n \mathfrak{m}^n = 0$ then the following conditions on R are equivalent:*

(i) $\mathfrak{m}$ *is principal;*

(ii) *R is a PIR;*

(iii) *R is a chain ring, hence R is Noetherian.*

Proof. (iii)$\Longrightarrow$(ii) Let $\pi \in \mathfrak{m}\backslash\mathfrak{m}^2$ then since R is a chain ring, $\pi \notin \mathfrak{m}^e$ for $e > 1$, so $(\pi) \neq \mathfrak{m}^e$ for $e > 1$ hence $(\pi) = \mathfrak{m}$. Now since all ideals are of the form $\mathfrak{m}^e = (\pi^e)$ then R is a PIR. (ii)$\Longrightarrow$(i) is immediate.
(i)$\Longrightarrow$(iii) This is similar to the proof of Theorem 31.5 in [73]. Let $\mathfrak{m} = (\pi)$ then $\mathfrak{m}^e = (\pi^e)$ for all $e \geq 1$. Since $\cap_n \mathfrak{m}^n = 0$ and every ideal $\mathfrak{a}$ satisfies $\mathfrak{a} \subseteq \mathfrak{m}$ then for some $e \geq 1$, $\mathfrak{a} \subseteq \mathfrak{m}^e$ and $\mathfrak{a} \not\subset \mathfrak{m}^{e+1}$. As ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ in a ring R satisfy $\mathfrak{a} \subseteq \mathfrak{c} \iff \mathfrak{a} : \mathfrak{b} \subseteq \mathfrak{c} : \mathfrak{b}$ then $\mathfrak{a} \not\subset (\pi^{e+1})$ implies $\mathfrak{a} : (\pi^e) \not\subset (\pi^{e+1}) : (\pi^e) = (\pi)$, hence $\mathfrak{a} : (\pi^e) = R$. Now since $(\mathfrak{a} : \mathfrak{b}) = R \Rightarrow \mathfrak{b} \subseteq \mathfrak{a}$, then $(\pi^e) \subseteq \mathfrak{a}$, hence $\mathfrak{a} = (\pi^e) = \mathfrak{m}^e$. So every ideal of R is a power of $\mathfrak{m}$, hence R is a chain ring. □

3.2 Quotient rings of polynomial rings

Let R be a finite ring, $Q = R[x_1, \ldots, x_n]$ a polynomial ring. Theorem 33 describes all rings of the form

$$R[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$$

which are finite PIRs. This gives a generalization of the main result of [42]. Theorem 27 is used in the proof of Theorem 33. Ideals of the form $(f_1(x_1), \ldots, f_n(x_n))$ are called *elementary ideals* (see [65], Definition 1.14). A few definitions are needed before we can state these results.

If F is a field, and $f = g_1^{m_1} \cdots g_k^{m_k}$, where $f \in F[x]$ and $g_1, \ldots, g_k$ are irreducible polynomials over F, then by $\mathrm{SP}(f)$ we denote the squarefree part $g_1 \cdots g_k$ of f. We assume that $\mathrm{SP}(0) = 0$.

Let $R = GR(p^m, r) = (\mathbb{Z}/p^m\mathbb{Z})[y]/(g(y)) \neq 0$ be a Galois ring which is not a field hence $m \geq 2$. We say that a polynomial $f(x) \in R[x]$ is *basic* if all nonzero coefficients of $f(x)$ belong to the subset

$$\mathcal{B} = \{ay^b \mid \text{where } 0 < a < p \text{ and } 0 \leq b < r\}$$

of the Galois ring R, where r is the degree of $g(y)$. Clearly, for every $f \in R[x]$, there exist unique basic polynomials

$$f', f'' \in \mathcal{B}[x] \subseteq R[x] \text{ such that } f - f' - pf'' \in p^2R[x].$$

For any $f \in R[x]$, there exists a unique basic polynomial $\mathrm{SP}(f) \in R[x]$ such that $\overline{\mathrm{SP}(f)} = \mathrm{SP}(\overline{f})$. Therefore there exists a unique basic polynomial $\mathrm{UP}(f) \in R[x]$ such that $\overline{f} = \overline{\mathrm{SP}(f)\,\mathrm{UP}(f)}$ or, equivalently, $f' - \mathrm{SP}(f)\,\mathrm{UP}(f) \in pR[x]$. Since f' is basic, $(f')'' = 0$ for any f, and so $(f' - \mathrm{SP}(f)\,\mathrm{UP}(f))'' = -(\mathrm{SP}(f)\,\mathrm{UP}(f))''$. We introduce the following notation

$$\widehat{f} = \overline{f'' + (f' - \mathrm{SP}(f)\,\mathrm{UP}(f))''} = \overline{f'' - (\mathrm{SP}(f)\,\mathrm{UP}(f))''}.$$

For any $f, g \in GR(p^n, r)[x]$, it is clear that $\overline{f} = \overline{g}$ if and only if $f' = g'$.

Let R be a finite commutative local ring. A polynomial $f(x) \in R[x]$ is *regular* if it is not a zero divisor. By [71], Theorem 13.6, if $f(x)$ is regular then there exists a unit $u \in R$ and monic polynomial $e(x) \in R[x]$ such that $f = ue$. All the theorems in Chapter 3 are true for regular polynomials $f(x)$ but for simplicity we assume that these polynomials are monic.

A finite direct product is a PIR if and only if all its components are PIRs (see [96], Theorem 33) and every finite PIR is a direct product of chain rings (see [71, §6]). By taking Lemmas 46 and 47 into consideration, the main case of describing all polynomial rings

$$Q = R[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$$

which are finite PIRs is the case where R is a finite chain ring. It follows from [71], Theorem 13.2(c), that Q is finite if and only if all the $f_i(x_i)$ are regular. The following theorem gives new conditions for Q to be a PIR.

Theorem 33 *Let R be a finite commutative chain ring, and let $f_1, \ldots, f_n$ be univariate monic polynomials over R. Then*

$$Q = R[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$$

is a PIR and all rings $R[x_i]/(f_i(x_i))$ are PIRs, if and only if one of the following conditions is satisfied:

(i) *R is a field and the number of polynomials f_i which are not squarefree does not exceed one;*

(ii) *R is a Galois ring of characteristic p^m, for a prime p, and a positive integer $m \geq 2$, the number of polynomials $f_1, \ldots, f_n$ which are not squarefree modulo p does not exceed one, and if $f = f_i$ is not squarefree modulo p, then $\widehat{f}$ is coprime with $\overline{\mathrm{UP}(f)}$;*

(iii) *R is a chain ring, which is not a Galois ring, R has characteristic p^m, for a prime p, $n = 1$ and f_1 is squarefree modulo p.*

Lemma 34 *Let R be a Galois ring of characteristic p^m, $f(x)$ a monic polynomial over R, and let $Q = R[x]/(f(x))$. Then Q is a direct product of Galois rings if and only if $f(x)$ is squarefree modulo p.*

Proof. Lemma 38 shows that $f(x)$ is squarefree modulo p if and only if Q/pQ is semisimple, i.e., $\mathcal{N}(Q) = pQ$. By Lemma 24, this is equivalent to Q being a direct product of Galois rings. □

Lemma 35 *Let $R = GR(p^m, r)$ be a Galois ring, where $m \geq 2$, let $f(x) \in R[x]$ be a monic polynomial which is not squarefree modulo p, and let $Q = R[x]/(f(x))$. Then Q is a PIR if and only if $\overline{\mathrm{UP}(f)}$ is coprime with $\widehat{f}$.*

Proof. Given that $\overline{f}$ is not squarefree, we get $\mathrm{UP}(f) \neq 0$ and $\mathrm{SP}(f) \neq 0$.

Suppose that $\widehat{f}$ is coprime with $\overline{\mathrm{UP}(f)}$. Denote by h a basic polynomial in $R[x]$ such that $\overline{h}$ is the product of all irreducible divisors of $\overline{f}$ which do not divide $\widehat{f}$. Let $g = \mathrm{SP}(f) + ph \in R[x]$. We claim that the radical $\mathcal{N}(Q)$ is equal to the ideal I generated in Q by g.

It follows from Lemma 38 that $\mathcal{N}(Q) = (\mathrm{SP}(f), p)$. Hence $g \in \mathcal{N}(Q)$, so $I \subseteq \mathcal{N}(Q)$. Therefore it remains to show that p, $\mathrm{SP}(f) \in I$.

First, we prove that $p^{m-1} \in I$. It suffices to show that $p^{m-1} \in \underline{(g, f)}$ in $R[x]$, because $I \subseteq Q = R[x]/(f)$. The choice of h implies that $\widehat{f} - \overline{h\,\mathrm{UP}(f)}$

is not divisible by any irreducible factor of $\overline{f}$ which does not divide $\widehat{f}$. If an irreducible factor of $\overline{f}$ divides $\widehat{f}$, then it does not divide $\overline{h}$, and so it does not divide $\overline{h\,\mathrm{UP}(f)}$, because $\overline{\mathrm{UP}(f)}$ is coprime with $\widehat{f}$. Thus $\widehat{f} - \overline{h\,\mathrm{UP}(f)}$ and $\mathrm{SP}(\overline{f})$ are coprime. Hence there exist basic polynomials $v, w \in R[x]$ such that $\overline{1} = \overline{v}(\widehat{f} - \overline{h\,\mathrm{UP}(f)}) + \overline{w\,\mathrm{SP}(f)}$. There exists a unique basic polynomial $f^* \in R[x]$ satisfying $\overline{f^*} = \widehat{f}$. Since p^m is the characteristic of R, $p^m u = 0$ for all $u \in R[x]$. Therefore $\overline{A} = \overline{B}$ is equivalent to $p^{m-1}A = p^{m-1}B$ for all $A, B \in R[x]$. We can lift the equation $\overline{1} = \overline{v}(\widehat{f} - \overline{h\,\mathrm{UP}(f)}) + \overline{w\,\mathrm{SP}(f)}$ from $R[x]/pR[x] \cong GF(p^r)[x]$ to $R[x]$ and multiply by p^{m-1} to get the following.

$$\begin{aligned}
p^{m-1} &= p^{m-1}[v(f^* - h\,\mathrm{UP}(f)) + w\,\mathrm{SP}(f)] \\
&= p^{m-1}[v\{f'' + (f' - \mathrm{UP}(f)\,\mathrm{SP}(f))'' - h\,\mathrm{UP}(f)\} + w\,\mathrm{SP}(f)] \\
&= p^{m-2}[v\{pf'' + (f' - \mathrm{UP}(f)\,\mathrm{SP}(f)) - ph\,\mathrm{UP}(f)\} + pw\,\mathrm{SP}(f)] \\
&= p^{m-2}[v(f' + pf'') - v\,\mathrm{UP}(f)(\mathrm{SP}(f) + ph) + pw\,\mathrm{SP}(f)] \\
&= p^{m-2}[vf - (v\,\mathrm{UP}(f) - pw)g] \in R[x].
\end{aligned}$$

We have used the fact that $f' - \mathrm{UP}(f)\,\mathrm{SP}(f) = p[(f' - \mathrm{UP}(f)\,\mathrm{SP}(f))''] + p^2 u$ for some $u \in R[x]$, because $(f' - \mathrm{UP}(f)\,\mathrm{SP}(f))' = 0$. Thus $p^{m-1} \in (g, f) \subset R[x]$, and so $p^{m-1} \in I$.

Since p^{m-1} belongs to both I and $\mathcal{N}(Q)$, we can factor out the ideal generated by p^{m-1} in Q and consider the ideal $I/p^{m-1}I$ in $Q/p^{m-1}Q$. Also clearly $R/p^{m-1}R \cong GR(p^{m-1}, r)$. We identify $f, g \in R[x]$ with their images in $(R/p^{m-1}R)[x]$. We can now lift the equation $\overline{1} = \overline{v}(\widehat{f} - \overline{h\,\mathrm{UP}(f)}) + \overline{w\,\mathrm{SP}(f)}$ from $(R/pR)[x]$ to $(R/p^{m-1}R)[x]$ and multiply by p^{m-2} and repeat the argument from the preceding paragraph taking into account that $p^{m-1}u = 0$ for all $u \in (R/p^{m-1}R)[x]$. Then we deduce $p^{m-2} \in (g, f) \subset (R/p^{m-1}R)[x]$. Identifying $p^{m-2} \in R[x]$ with its image $p^{m-2} \in (R/p^{m-1}R)[x]$, we get $p^{m-2} \in I/p^{m-1}I$. Given that $p^{m-1} \in I$, it follows that $p^{m-2} \in I$.

Repeating this reduction $m - 3$ times we get $p \in I$.

Next we prove that $\mathrm{SP}(f) \in I$. Since $g, p \in I$, then $\mathrm{SP}(f) = g - ph \in I$. Thus $I = \mathcal{N}(Q)$, because $\mathcal{N}(Q) = (p, \mathrm{SP}(f))$. This means that $\mathcal{N}(Q)$ is a principal ideal, and so Q is a PIR.

Conversely, suppose that the radical is a principal ideal generated by some polynomial $g \in R[x]$.

Since $(\overline{g}) = (\mathrm{SP}(\overline{f})) = \mathcal{N}(Z\!\!Z/(q)[x]/(\overline{f}))$, we get $\overline{g} = \overline{t}\,\mathrm{SP}(\overline{f}) + \overline{e}\overline{f}$ for some $t = t' \in R$ and $e(x) \in R[x]$. There exists an integer $s = s' \in R$ such that $ts \equiv 1 (\mathrm{mod}\, p)$. Since $\overline{s(g - ef)} = \overline{st\,\mathrm{SP}(f)} = \overline{\mathrm{SP}(f)} = \mathrm{SP}(\overline{f})$ and

$(\overline{g}) = (\overline{\mathrm{SP}(f)})$ then g generates the same ideal as $s(g - ef)$ in $Q = R[x]/(f)$, so we can replace g by $s(g - ef)$. To simplify the notation we assume that $\overline{g} = \overline{\mathrm{SP}(f)}$, and so $g' = \mathrm{SP}(f)$.

Given that $p \in \mathcal{N}(Q)$, we get $p = vf + wg$ for some $v, w \in R[x]$. Since $(vf + wg)' = (v'f' + w'g')' = 0$, it follows that $\overline{v'f'} + \overline{w'g'} = 0$. Therefore $\overline{w'} = -\overline{v'}\,\overline{\mathrm{UP}(f)}$ whence $w' = -v'\,\mathrm{UP}(f) + pz$ for some $z = z' \in R[x]$.

Further, $p = (v' + pv'')(f' + pf'') + (w' + pw'')(g' + pg'') + p^2u$, for some $u \in R[x]$. Notice that $f' = (\,\mathrm{UP}(f)g')'$ because $\overline{f'} = \overline{f} = \overline{\mathrm{UP}(f)g'}$. Since $\mathrm{UP}(f)$ and g' are basic, $\mathrm{UP}(f)g' = (\,\mathrm{UP}(f)g')' + p(\,\mathrm{UP}(f)g')'' = f' + p(\,\mathrm{UP}(f)g')''$. It follows that $f' - \,\mathrm{UP}(f)g' = -p(\,\mathrm{UP}(f)g')''$. Therefore we get

$$\begin{aligned} p^{m-1} &= p^{m-2}[(v' + pv'')(f' + pf'') + (-v'\,\mathrm{UP}(f) + pz + pw'')(g' + pg'')] \\ &= p^{m-2}[v'(f' - \,\mathrm{UP}(f)g' + pf'') - v'\,\mathrm{UP}(f)pg'' + pv''f' + pg'(z + w'')] \\ &= p^{m-1}[v'(-(\,\mathrm{UP}(f)g')'' + f'') - \,\mathrm{UP}(f)v'g'' + v''(\,\mathrm{UP}(f)g')' + g'(z + w'')], \end{aligned}$$

Given that $p^m = 0$, then $p^{m-1}A = p^{m-1}B$ if and only if $\overline{A} = \overline{B}$ where $A, B \in R[x]$. Hence

$$\begin{aligned} \overline{1} &= \overline{v'}(\overline{-(\,\mathrm{UP}(f)g')'' + f''}) - \overline{\mathrm{UP}(f)}(\overline{v'g''}) + \overline{v''}(\overline{(\,\mathrm{UP}(f)g')'}) + \overline{g'}(\overline{z + w''}) \\ &= \overline{v'}\,\widehat{f} - \overline{\mathrm{UP}(f)}(\overline{v'g''}) + \overline{v''}\,\overline{\mathrm{UP}(f)}\,\overline{g'} + \overline{g'}(\overline{z + w''}). \end{aligned}$$

Since all irreducible factors of $\overline{\mathrm{UP}(f)}$ divide $\overline{g'} = \overline{\mathrm{SP}(f)}$, they also divide the polynomial $\overline{\mathrm{UP}(f)}(\overline{v'g''}) + \overline{v''}\,\overline{\mathrm{UP}(f)}\,\overline{g'} + \overline{g'}(\overline{z + w''})$, and we see that $\overline{\mathrm{UP}(f)}$ must be coprime with $\widehat{f}$. This completes the proof. □

Example 36 We demonstrate Lemma 35 in the case when Q is a finite local ring. Let $R = GR(p^m, r)$ then $R/(\mathcal{N}(R)) \cong GF(p^r)$. For $c \in GF(p^r)[x]$ define $c_b \in R[x]$ as the unique basic polynomial satisfying $\overline{c_b} = c$, then c_b and c have the same coefficients identified under the canonical injective mapping of sets $\mathcal{B} \to GF(p^r)$. Notice that $\mathcal{B}$ is not the isomorphic copy of $GF(p^r)$ contained in R. For example if $R = \mathbb{Z}/(3^2)$ then as sets $\mathcal{B} = \{0, 1, 2\} \subset \{0, 1, 2, \ldots, 8\} = R$, $R/(\mathcal{N}(R)) \cong GF(3) = \{0, 1, 2\}$ yet $F = \{0, 3, 6\}$ is the isomorphic copy of $GF(3)$ contained in R.

Let $R = GR(p^m, r)$ and let $e \in R[x]$ be a monic irreducible polynomial, [71] p.254, $f = e^n$ for some integer $n \geq 1$ and $Q = R[x]/(f)$. By [71], Theorem 13.7(b), $\overline{e} = c^\ell$ for some monic irreducible $c \in GF(p^r)[x]$ and integer $\ell \geq 1$. Therefore $\overline{\mathrm{SP}(f)} = \mathrm{SP}(\overline{f}) = c$ and $\mathrm{SP}(f) = c_b$. Now because $c^{\ell n} = \overline{f} = \overline{\mathrm{SP}(f)\,\mathrm{UP}(f)} = c\,\overline{\mathrm{UP}(f)}$ then $\overline{\mathrm{UP}(f)} = c^{\ell n - 1}$ and $\mathrm{UP}(f) =$

$(c^{\ell n-1})_b$. Evidently $\widehat{f} = \overline{(e^n)'' - (c_b(c^{\ell n-1})_b)''}$. It follows from Lemma 38 that $\mathcal{N}(Q) = (p, c_b)$. Therefore since $(\overline{f}) = (c^{\ell n}) \subseteq (d) \subset F_{p^r}[x]$ then $Q/\mathcal{N}(Q) = (GR(p^m, r)[x]/(f))/(p, c_b) \cong GF(p^r)[x]/(c) \cong GF(p^{r\ degree(c)})$. Hence Q is a finite local ring. Therefore by the chinese remainder theorem for ideals, [35], Exercise.2.6 p.80, for an arbitrary monic polynomial f, the ring $R[x]/(f)$ is a finite local ring if and only if $f = e^n$ where e is a monic irreducible polynomial and $n \geq 1$. By [71], Theorem 13.6, this is also true when f and hence e are regular but not monic. We see that for such a local ring Q which is not a Galois ring, it is a PIR if and only if c does not divide $\widehat{f}$.

Lemma 37 *Let R be a chain ring of characteristic p^m which is not a Galois ring, let $f(x)$ be a monic polynomial over R, and let $Q = R[x]/(f(x))$. Then Q is a PIR if and only if f is squarefree modulo p.*

Proof. By Lemma 22, $R \cong GR(p^m, r)[y]/(y^s + ph(y), p^{m-1}y^t)$. Since R is not a Galois ring, evidently $s \geq 2$. Lemma 23 implies that $p \in yR$.

The 'if' part. Suppose that f is squarefree modulo p. Then $Q/yQ \cong GF(p^r)[x]/(\overline{f})$ is semisimple by Lemma 38. Thus $\mathcal{N}(Q)$ is a principal ideal. Lemma 20 tells us that Q is a PIR.

The 'only if' part. Suppose that Q is a PIR then the ring $Q/pQ \cong GF(p^r)[x, y]/(y^s, \overline{f(x)})$ is a PIR. This ring is isomorphic to the tensor product of $GF(p^r)[y]/(y^s)$ and $GF(p^r)[x]/(\overline{f(x)})$. Both of these rings are PIRs. Lemma 24 and Lemma 34 both imply that $GF(p^r)[y]/(y^s)$ is not a direct product of Galois rings. By Lemma 24, $GF(p^r)[x]/(\overline{f(x)})$ must be a direct product of Galois rings. Lemma 34 completes the proof. □

Lemma 38 *Let F be a finite field, $P = F[x_1, \ldots, x_n]$, and let I be the ideal generated by $f_1(x_1), \ldots, f_n(x_n)$. Then the radical of P/I is equal to the ideal generated by the squarefree parts of all polynomials $f_1, \ldots, f_n$.*

Proof. Since every finite field is perfect, and any set of univariate polynomials in pairwise distinct variables forms a Gröbner basis of the ideal it generates, this lemma is a special case of more general results of [3, §8.2]. □

Proof of Theorem 33. The ring Q is isomorphic to the tensor product of the rings $R[x_i]/(f_i(x_i))$, for $i = 1, \ldots, n$. Since $\mathrm{char}\,(R) = p^m$ where $m = 1$ if R is a field, then $R_i = (R_i)_p$ for $i = 1, \ldots, n$ and $Q = Q_p$.

(i): Suppose that R is a field of characteristic p. Then all the $R[x_i]/(f_i(x_i))$ are PIRs. Theorem 27 tells us that Q is a PIR if and only if at least $n-1$ of the rings $R[x_i]/(f_i(x_i))$ are direct products of Galois rings. By Lemma 34, this is equivalent to the fact that at most one of the polynomials $f_i(x_i)$ is not squarefree.

(ii): Suppose that R is a Galois ring. By Lemma 35, all $R[x_i]/(f_i(x_i))$ are PIRs if and only if, for each polynomial $f_i(x_i)$ which is not squarefree modulo p, $\overline{\mathrm{UP}(f_i)}$ is coprime with $\widehat{f_i}$. Further, suppose that this condition is satisfied. As in case (i), we see that Q is a PIR if and only if at most one of the polynomials $f_i(x_i)$ is not squarefree modulo p.

(iii): Suppose that R is a chain ring which is not a Galois ring. Since the class of finite direct products of Galois rings is closed for homomorphic images by Lemma 24, we see that each $R[x_i]/(f_i(x_i))$ is not a direct product of Galois rings. Theorem 27 shows that $n = 1$. By Lemma 37, Q is a PIR if and only if $f_1(x_1)$ is squarefree modulo p. □

For finite rings, our Theorem 33 immediately gives the following Theorem 1 of [42].

Corollary 39 ([42]) *Let F be a field of characteristic $p > 0$, $a_1, \ldots, a_n$ non-negative integers, $b_1, \ldots, b_n$ positive integers, and let*

$$R = F[x_1, \ldots, x_n]/(x_1^{a_1}(1 - x_1^{b_1}), \ldots, x_n^{a_n}(1 - x_n^{b_n})).$$

then R is a PIR if and only if one of the following conditions is satisfied:

(1) $a_1, \ldots, a_n \leq 1$ and p divides at most one number among $b_1, \ldots, b_n$;

(2) exactly one of $a_1, \ldots, a_n$, say a_1, is greater than 1 and p does not divide each of $b_2, \ldots, b_n$.

Proof. Consider the polynomial $f = x^a(1 - x^b)$. By [3], Lemma 2.85, a polynomial is squarefree if and only if it is coprime with its derivative. Since $\mathrm{char}\,(F) = p > 0$, then f is squarefree if and only if $a = 1$ and p does not divide b. Thus Theorem 33 completes the proof. □

In our second Corollary to Theorem 33, we give an explicit generator g for the radical of Q when Q is a PIR.

Corollary 40 *Let $R = GR(p^m, r)$ be a Galois ring, where $m \geq 1$, let $f_1, \ldots, f_n$ be univariate monic polynomials over R with $f_1(x_1)$ not squarefree modulo p and let*

$$Q = R[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$$

be a PIR. Let $\mathcal{N}(S_1) = gS_1$ where $S_1 = R[x_1]/(f_1(x_1))$, then $\mathcal{N}(Q) = gQ$ where gQ is the ideal generated by $g = g(x_1)$ in Q.

Proof. By Theorem 33, since Q is a PIR and $f_1(x_1)$ is not squarefree modulo p then the rings $R_i = R[x_i]/(f_i)$ for $2 \leq i \leq n$ are Galois rings. Since tensor product distributes over direct products, in Lemma 25 we can replace the phrase 'S is a chain ring' by 'S is a direct product of chain rings', hence 'S is a PIR'. Then in the proof of Lemma 25, $\mathcal{N}(R \otimes S) = g(R \otimes S)$ where S is a PIR, R is a Galois ring and g is defined by $\mathcal{N}(S) = gS$. Using this Lemma with g defined by $\mathcal{N}(S_1) = gS_1$, R_2 a Galois ring, then both S_1 and $S_2 \cong R_2 \otimes S_1$ are PIR's and it follows that $\mathcal{N}(S_2) = gS_2$. Repeating this argument with $S_{i+1} \cong R_{i+1} \otimes S_i$ for $2 \leq i \leq n-1$ gives $\mathcal{N}(Q) = gQ$. □

Let Q be the PIR defined in Corollary 40. Let R be a Galois ring which is not a finite field. From the proof of Lemma 35 using the ring $S_1 = R[x_1]/(f(x_1))$ one may choose $g = \mathrm{SP}(f(x_1)) + ph(x_1)$. Also if $f_i(x_i)$ for $1 \leq i \leq n$ are squarefree modulo p then either by Lemma 21 and Lemma 24, or by the same proof as Corollary 40, $\mathcal{N}(Q) = pQ$. If R is a finite field then $g = \mathrm{sp}(f_1)$, the squarefree part of f_1, generates $\mathcal{N}(Q)$.

Theorem 33 provides conditions for the ring Q to be a PIR. Theorem 45 provides similar conditions for Q to be a special type of PIR, its proof requiring Lemmas 41 to 44.

Lemma 41 *Let R and S be finite local rings satisfying* $\mathrm{char}\,(R) = p^m$, $\mathrm{char}\,(S) = p^n$, *for a prime p and positive integers $m, n \geq 1$. The ring $R \otimes S$ is a direct product of Galois rings if and only if so too are R and S.*

Proof. The 'if' part. This is true by Lemma 21, since tensor product distributes over direct products.

The 'only if' part. Since $R \otimes S$ is a PIR then by Theorem 31, either R or S is a direct product of Galois rings. Assume R is a direct product of Galois rings. Since $R \otimes S$ is a direct product of Galois rings, then by Lemma 24,

$\mathcal{N}(R \otimes S) = p(R \otimes S)$ and $\mathcal{N}(R) = pR$. Here pR is the ideal generated by p in R. Let g be the generator of $\mathcal{N}(S)$ in S, $\mathcal{N}(S) = gS$, and denote by $g(S \otimes R)$ the ideal generated by g in $R \otimes S$. Since tensor product distributes over direct products, in Lemma 25 we can replace the phrase 'S is a chain ring' by 'S is a direct product of chain rings', hence 'S is a PIR'. Then from the proof of Lemma 25, $\mathcal{N}(R \otimes S) = g(R \otimes S)$ where S is a PIR and R is a direct product of Galois rings. By Lemma 24, only p can generate the radical of $R \otimes S$, hence $g = p$. Therefore by Lemma 24, S must be a direct product of Galois rings. □

Lemma 42 *Let R and S be finite local rings satisfying* $\mathrm{char}\,(R) = p^m$, $\mathrm{char}\,(S) = p^n$, *for a prime p and positive integers $m, n \geq 1$. The ring $R \otimes S$ is a direct product of finite fields if and only if so too are R and S.*

Proof. The 'if' part. This is true by Lemma 21, since tensor product distributes over direct products.

The 'only if' part. Since $R \otimes S$ is a direct product of finite fields then $\mathcal{N}(R \otimes S) = 0$. The proof is identical to the 'only if' part of Lemma 41 until it shows $\mathcal{N}(R \otimes S) = g(R \otimes S)$. Then $g = 0$, so S is a direct product of finite fields. If R is a direct product of Galois rings which are not all finite fields then so too must be $R \otimes S$, by Lemma 21. This contradiction implies R is a direct product of finite fields. □

Lemma 43 *Let $S = R[x]/(f(x))$ be a direct product of Galois rings where R is a chain ring and f is monic. Then R is a Galois ring and f is squarefree modulo p.*

Proof. By Lemmas 34 and 37, f is squarefree modulo p. Assume R is not a Galois ring then by Lemma 22, $R \cong GR(p^m, r)[y]/(y^s + ph(y), p^{m-1}y^t)$ where $s \geq 2$. It follows that $S/pS \cong GF(p^r)[x,y]/(\overline{f(x)}, y^s) \cong GF(p^r)[x]/(\overline{f(x)}) \otimes GF(p^r)[y]/(y^s)$. Since $s \geq 2$ then $GF(p^r)[y]/(y^s)$ is a finite chain ring which is not a finite field, yet $GF(p^r)[x]/(\overline{f(x)})$ is a direct product of finite fields since $\overline{f(x)}$ is squarefree. Consider the following ring. For some integer $q \geq 2$, by Lemma 21, $GF(p^q) \otimes (GF(p^r)[y]/(y^s)) \cong \prod_1^d (GF(p^l)[y]/(y^s))$, where $d = gcd(q,r)$ and $l = lcm(q,r)$. Since this ring is not a direct product of finite fields then neither is $(GF(p^r)[x]/(\overline{f(x)}) \otimes GF(p^r)[y]/(y^s)) = S/pS$. This is a contradiction, by Lemma 24, since S is a direct product of Galois rings.

Therefore R must be a Galois ring. □

Lemma 44 *Let $S = R[x]/(f(x))$ be a direct product of finite fields where R is a chain ring and f is monic. Then R is a finite field and f is squarefree.*

Proof. By Lemmas 34 and 37, f is squarefree modulo p. Assume R is not a finite field then by Lemma 22, $R \cong GR(p^m, r)[y]/(y^s + ph(y), p^{m-1}y^t)$ where $m \geq 2$ or $s \geq 2$. It follows that $S/pS \cong GF(p^r)[x,y]/\ (\overline{f(x)}, y^s)$ $\cong GF(p^r)[x]/(\overline{f(x)}) \otimes GF(p^r)[y]/(y^s)$. Let $s \geq 2$ then $GF(p^r)[y]/(y^s)$ is a finite chain ring which is not a finite field, yet $GF(p^r)[x]/(\overline{f(x)})$ is a direct product of finite fields since $\overline{f(x)}$ is squarefree. Consider the following ring. For some integer $q \geq 2$, by Lemma 21, $GF(p^q) \otimes (GF(p^r)[y]/(y^s)) \cong \prod_1^d (GF(p^l)[y]/(y^s))$, where $d = gcd(q,r)$ and $l = lcm(q,r)$. Since this ring is not a direct product of finite fields then neither is $(GF(p^r)[x]/(\overline{f(x)}) \otimes GF(p^r)[y]/(y^s)) = S/pS$. This is a contradiction since S being a direct product of finite fields implies $S/pS = S$. Let $m \geq 2$ and $s = 1$ then by the comment following Lemma 22, $R = GR(p^m, r)$. Since f is squarefree modulo p then $S = R[x]/(f(x))$ is a direct product of Galois rings of characteristic $p^m > p$, which is a contradiction. Therefore $s = 1$ and $m = 1$ so R is a finite field, and f being squarefree modulo p implies f is squarefree. □

Theorem 45 *Let R be a finite commutative chain ring satisfying* $\mathrm{char}\,(R) = p^m$, *and $Q = R[x_1, \ldots, x_n]/(f_1(x_1), \ldots, f_n(x_n))$ where $f_1 \ldots, f_n$ are monic polynomials, then*

(i) Q is a direct product of finite fields if and only if R is a finite field and all the f_i are squarefree;

(ii) Q is a direct product of Galois rings if and only if R is a Galois ring and all the f_i are squarefree modulo p.

Proof. Define $S_i = R[x_i]/(f_i(x_i))$ for $i = 1, \ldots, n$, then $Q \cong \otimes_{i=1}^n S_i$. Since $R = R_p$ then $Q = Q_p$ where R_p is the $p-$component of R.

(i) The 'if' part. If R is a finite field and f is squarefree then by the chinese remainder theorem for ideals, [35], Exercise.2.6 p.80, $R[x]/(f(x))$ is a direct product of finite fields. By Lemma 21, a tensor product of finite fields

is a direct product of finite fields, and since tensor product distributes over direct products, then Q is a direct product of finite fields.

The 'only if' part. By Lemma 42, if $S_1 \otimes S_2$ is a direct product of finite fields then so too are S_1 and S_2. By iterating this argument, if $Q \cong \otimes_{i=1}^{n} S_i$ is a direct product of finite fields then so is each S_i. By Lemma 44, R is a finite field and all the f_i are squarefree.

(ii) The 'if' part. If R is a Galois ring and f is squarefree modulo p then by Lemma 34, $R[x]/(f(x))$ is a direct product of Galois rings. By Lemma 21, a tensor product of Galois rings is a direct product of Galois rings, and since tensor product distributes over direct products, then Q is a direct product of Galois rings.

The 'only if' part. By Lemma 41, if $S_1 \otimes S_2$ is a direct product of Galois rings then so too are S_1 and S_2. By iterating this argument, if $Q \cong \otimes_{i=1}^{n} S_i$ is a direct product of Galois rings then so is each S_i. By Lemma 43, R is a Galois ring and all the f_i are squarefree modulo p. □

The case now considered is when R is a finite local ring which is not necessarily a PIR. Lemma 46 follows immediately from Lemmas 34 and 37. Lemma 47 is close to being a converse to Lemma 46.

Lemma 46 *Let R be a local ring satisfying* $\mathrm{char}\,(R) = p^m$ *and $f \in R[x]$ is a monic polynomial. If R is a chain ring and f is squarefree modulo p then $S = R[x]/(f(x))$ is a finite commutative chain ring.*

Lemma 47 *Let R be a local ring satisfying* $\mathrm{char}\,(R) = p^m$ *and $f \in R[x]$ is a monic polynomial. If $S = R[x]/(f(x))$ is a finite commutative chain ring then R/pR is a chain ring.*

Proof. Assume R is a local ring which is not a chain ring. By Lemma 28, $R \cong GR(p^m, q)[y_1, \ldots, y_k]/J$ for some primary ideal J, and integers $p, m, q \geq 1$, $k \geq 2$. Since S is a PIR then so too is $S/pS \cong GF(p^q)[y_1, \ldots, y_k, x]/(\overline{J}, \overline{f(x)}) \cong A \otimes B$, where $\overline{J} = J/pJ$, $A = GF(p^q)[y_1, \ldots, y_k]/\overline{J}$ and $B = GF(p^q)[x]/(\overline{f(x)})$. The ring B is a PIR since it is a homomorphic image of the PIR, $GF(p^q)[x]$. By Lemma 29, if $A = A/pA$ is not a PIR then $A \otimes B \cong S/pS$ is not a PIR which is a contradiction. Hence $A = R/pR$ is a chain ring. □

It has not been proved in this thesis that 'if $S = R[x]/(f(x))$ is a finite commutative chain ring then R is not a chain ring'. Therefore Theorems 33 and 45 are only proved for the case when R is a chain ring.

Consider the case when the ideal $I \lhd R[x]$ contains several univariate polynomials $I = (f_1(x), \ldots, f_r(x))$. Let R be a finite local ring then $g \in R[x]$ is *primary* if (g) is a primary ideal in $R[x]$, see [71] p.254. Lemma 48 follows from [71], Theorem 13.11.

Lemma 48 *Let R be a finite local ring. Let $f \in R[x]$ be a monic polynomial then $f = \prod_{i=1}^{s} g_i$ where the g_i are monic primary coprime polynomials, for some integer $s \geq 1$. This factorization of f is unique up to associates. That is, if $f = \prod_{i=1}^{t} h_i$ then $s = t$ and after renumbering, $(g_i) = (h_i) \lhd R[x]$.*

For R a finite local ring, we may now define a *greatest common divisor* of two monic polynomials $f_1, f_2 \in R[x]$. For $j = 1, 2$, let $f_j = \prod_{i=1}^{s^{(j)}} g_i^{(j)}$ where the $g_i^{(j)}$ are monic primary coprime polynomials. Define $gcd(f_1, f_2) = \prod_{i=1}^{s} g_i^{(j)}$ where $g_i^{(j)}$ divides both f_1 and f_2. Then by Lemma 48, $gcd(f_1, f_2)$ is well-defined and is unique up to associates. Similarly $gcd(f_1, \ldots, f_r)$ is defined for $f_1, \ldots, f_r \in R[x]$. It is then true that $(gcd(f_1, \ldots, f_r)) = (f_1, \ldots, f_r)$. Therefore the theorems in Chapters 2 and 3 of this thesis which are true for rings of the form $Q = R[x]/(f_1(x))$ are also true for rings of the form $Q = R[x]/(f_1(x), \ldots, f_r(x))$ where the f_i are monic.

Chapter 4

Radicals of finite rings and principal ideal rings

This chapter is devoted to several constructions of classes of rings. All rings considered are finite but it is not required that these rings are commutative or contain identity elements. For a class $\mathcal{R}$ of finite rings, necessary and sufficient conditions are given for $\mathcal{R}$ to be a radical class and also a semisimple class. The radical semisimple classes $\mathcal{R}$ of finite rings are characterized along with their subsets $\mathcal{N}_{\mathcal{R}}$ of nilpotent rings. Classes consisting of PIRs are characterized, namely the hereditary and semisimple classes, and the class of all finite commutative PIRs with identity.

4.1 Radical classes and semisimple classes of finite rings

We describe radical semisimple classes of finite rings, and describe all radical classes consisting of finite PIRs. All rings considered in this chapter are finite but do not necessarily contain identity elements.

Theorem 49 is a special case of results in [94]. Theorem 50 and Corollary 54 are special cases of results in [83] and [84]. See also [67] and [93]. For the convenience of the reader we provide proofs of Theorem 49, Theorem 50 and Corollary 54 in the special case of a finite ring. The remaining results are new results.

For every finite ring R, let $\varrho(R)$ be a certain ideal of R. The mapping ϱ is called a *radical* if it satisfies the following properties:

(M1) $\varrho(R)/I \subseteq \varrho(R/I)$ for every finite ring R with ideal I;

(M2) $\varrho(R)$ is the largest ideal among all ideals I of R such that $\varrho(I) = I$;

(M3) $\varrho(R/\varrho(R)) = 0$ for each R.

A ring R is said to be *radical* or *ϱ-radical* if $\varrho(R) = R$. The class of all ϱ-radical rings is called the *radical class* of ϱ.

Theorem 49 *A class $\mathcal{R}$ of finite rings, or finite commutative rings, is a radical class if and only if it satisfies the following properties:*

(R1) *$\mathcal{R}$ is closed for homomorphic images;*

(R2) *$\mathcal{R}$ is closed for ideal extensions.*

Proof. We consider only classes of finite rings since the case of finite commutative rings is similar. The 'if' part. Suppose that a class $\mathcal{R}$ of finite rings satisfies properties (R1) and (R2).

For any ring R, denote by $\varrho(R)$ the sum of all $\mathcal{R}$-ideals of R.

Consider an ideal I of R which is a sum of two ideals $A, B \in \mathcal{R}$. The ring $(A+B)/B \cong A/(A \cap B)$ is a homomorphic image of A, and so it belongs to $\mathcal{R}$ by condition (R1). Since $A + B$ is an ideal extension of B by $A + B/B$, it follows that $A + B$ is in $\mathcal{R}$ by condition (R2).

Given that R is finite, easy induction shows that all sums of $\mathcal{R}$-ideals in R belong to $\mathcal{R}$. In particular, $\varrho(R)$ is a largest $\mathcal{R}$-ideal of R. Thus condition (M2) is satisfied.

Let I be an ideal of R such that $I \supset \varrho(R)$ and $I/\varrho(R) = \varrho(R/\varrho(R))$. As we have just proved, both rings $\varrho(R)$ and $\varrho(R/\varrho(R))$ belong to $\mathcal{R}$. Since I is an ideal extension of $\varrho(R)$ by $\varrho(R/\varrho(R))$, it follows that $I \in \mathcal{R}$. By the definition of $\varrho(R)$ we get $I \subseteq \varrho(R)$. Hence $I = \varrho(R)$, and so $\varrho(R/\varrho(R)) = 0$. Thus condition (M3) holds.

Consider a ring R with ideal I. Since $\varrho(R)/I \in \mathcal{R}$, it follows that $\varrho(R)/I \subseteq \varrho(R/I)$, i.e., condition (M1) holds.

Conditions (M1), (M2) and (M3) show that ϱ is a radical, hence $\mathcal{R}$ is the radical class of ϱ.

The 'only if' part. Let $\mathcal{R}$ be the radical class of a radical ϱ.

Take any ring R in $\mathcal{R}$, and let I be an ideal of R. Condition (M1) tells us that $R/I = \varrho(R)/I \subseteq \varrho(R/I)$. Hence $R/I \in \mathcal{R}$, and so condition (R1) holds.

Consider a ring R with ideal I such that $I, R/I \in \mathcal{R}$. Condition (M2) implies that $I \subseteq \varrho(R)$. Hence $R/\varrho(R) \cong (R/I)/(\varrho(R)/I)$ is in $\mathcal{R}$, i.e., $\varrho(R/\varrho(R)) = R/\varrho(R)$. However, condition (M3) tells us that $\varrho(R/\varrho(R)) = 0$. Therefore $R/\varrho(R) = 0$, and so $R = \varrho(R)$. Thus condition (R2) is satisfied. □

A ring R is said to be *semisimple* or *ϱ-semisimple* if $\varrho(R) = 0$. The class of all ϱ-semisimple rings is called the *semisimple class* of ϱ.

Theorem 50 *A class $\mathcal{S}$ of finite rings, or finite commutative rings, is a semisimple class if and only if it satisfies the following properties:*

(S1) *$\mathcal{S}$ is closed for ideals;*

(S2) *$\mathcal{S}$ is closed for ideal extensions.*

Note that for arbitrary rings, in contrast to the finite case, a class closed for ideals and ideal extensions need not be a semisimple class (see [38]). Thus the exact analog of Theorem 50 is not true for arbitrary rings.

Lemma 51 *Every class closed for ideals and ideal extensions is also closed for finite subdirect products.*

Proof. Let $\mathcal{S}$ be a class of rings closed for ideals and ideal extensions. It suffices to consider the case where a ring R is a subdirect product of two rings $R/A, R/B \in \mathcal{S}$, where A, B are ideals of R such that $A \cap B = 0$.

Since $(A+B)/B$ is an ideal of $R/B \in \mathcal{S}$ and the class $\mathcal{S}$ is closed for ideals, we see that $(A+B)/B \in \mathcal{S}$. Clearly, $A \cong A/0 = A/(A \cap B) \cong (A+B)/B \in \mathcal{S}$.

Given that $\mathcal{S}$ is closed for ideal extensions and $A, R/A \in \mathcal{S}$, it follows that $R \in \mathcal{S}$. This completes the proof. □

Radical classes of arbitrary associative rings closed for finite subdirect products were investigated in [40].

Proof of Theorem 50. We consider only classes of finite rings since the case of finite commutative rings is similar. The 'if' part. Suppose that $\mathcal{S}$ satisfies the properties (S1) and (S2).

For any ring R, denote by $\varrho(R)$ the intersection of all ideals I of R such that $R/I \in \mathcal{S}$.

Consider ideals A, B of R such that $R/A, R/B \in \mathcal{S}$. Clearly, $R/(A \cap B)$ is a subdirect product of R/A and R/B. Hence $R/(A \cap B) \in \mathcal{S}$ in view of Lemma 51.

Given that R is finite, easy induction shows that $R/\varrho(R) \in \mathcal{S}$.

Clearly, $R/\varrho(R) \in \mathcal{S}$ implies $\varrho(R/\varrho(R)) = 0$, and so ϱ satisfies (M3).

Denote by $\mathcal{R}$ the class of all rings without nonzero homomorphic images in $\mathcal{S}$.

If $R \in \mathcal{R}$ and I is an ideal of R, then $R/I \in \mathcal{R}$, because all homomorphic images of R/I are also homomorphic images of R. Thus $\mathcal{R}$ satisfies condition (R1).

Let R be a ring with ideal $I \in \mathcal{R}$ such that $R/I \in \mathcal{R}$. Suppose that a homomorphic image R/J is in $\mathcal{S}$. Given that $\mathcal{S}$ is closed for ideals and I/J is an ideal in R/J, we get $I/J \in \mathcal{S}$. By the choice of I it follows that $I/J = 0$. Hence R/J is a homomorphic image of $R/I \in \mathcal{S}$, and so $R/J = 0$. Therefore $\mathcal{R}$ satisfies condition (R2).

Thus $\mathcal{R}$ is a radical class by Theorem 49.

Denote by $\varphi(R)$ the largest $\mathcal{R}$-ideal of R. By the proof of Theorem 49 the mapping φ is a radical. We shall show that $\varphi = \varrho$.

Take any ring R and put $K = \varrho(\varrho(R))$.

Look at any element $r \in R$. Clearly, $rK\varrho(R) \subseteq rK$ and $\varrho(R)rK \subseteq \varrho(R)K \subseteq K$. Hence $(rK + K)/K$ is an ideal of $\varrho(R)/K$. Given that $\mathcal{S}$ is closed for ideals and $\varrho(R)/K \in \mathcal{S}$, we get $(rK + K)/K \in \mathcal{S}$.

Consider the mapping $\alpha : K \to (rK + K)/K$ defined by $\alpha(x) = rx + K$. We get $\alpha(xy) = rxy + K \subseteq RKK + K \subseteq \varrho(K)K + K \subseteq K$ and $\alpha(x)\alpha(y) = rxry + K \subseteq RKRK + K \subseteq \varrho(R)K + K \subseteq K$. Hence α is an epimorphism. Let Z be the kernel of α. For any $x \in Z$, $a \in \varrho(R)$, we get $rax \in \varrho(R)K \subseteq K$ and $rxa \in K\varrho(R) \subseteq K$. Hence Z is an ideal of K. Clearly, $K/Z \cong (rK + K)/K \in \mathcal{S}$ and $\varrho(R)/K \in \mathcal{S}$ imply that $\varrho(R)/Z \in \mathcal{S}$. By the definition of K it follows that $K = Z$. Hence $rK \subseteq K$.

Similarly, $Kr \subseteq K$. Thus K is an ideal of R.

Given that $\mathcal{S}$ is closed for ideal extensions, $R/\varrho(R), \varrho(R)/K \in \mathcal{S}$ yield $R/K \in \mathcal{S}$. The definition of $\varrho(R)$ shows that $\varrho(R) = K$.

Thus $\varrho(\varrho(R)) = \varrho(R)$. This means that $\varrho(R) \in \mathcal{R}$. Therefore $\varrho(R) \subseteq \varphi(R)$.

Given that $\mathcal{S}$ is closed for ideals, since $\varphi(R)/\varrho(R)$ is an ideal of $R/\varrho(R) \in \mathcal{S}$, we get $\varphi(R)/\varrho(R) \in \mathcal{S}$. The definition of the class $\mathcal{R}$ implies that $\varphi(R)/\varrho(R) = 0$. Hence $\varrho(R) \supseteq \varphi(R)$.

Thus $\varrho(R) = \varphi(R)$. Therefore ϱ is a radical. Evidently, $\mathcal{S}$ is the semisimple class of ϱ.

The 'only if' part. Let $\mathcal{S}$ be the semisimple class of a radical ϱ. Denote by $\mathcal{R}$ the radical class of ϱ.

Consider a ring R with ideal I such that $I, R/I \in \mathcal{S}$. Then $\varrho(R)/I \subseteq \varrho(R/I) = 0$ in view of condition (M1), and so $\varrho(R) \subseteq I$. Since $\varrho(\varrho(R)) = \varrho(R)$, the condition (M2) yields that $\varrho(R) \subseteq \varrho(I) = 0$. Thus $R \in \mathcal{S}$, i.e. condition (S2) holds.

Consider a ring $R \in \mathcal{S}$ with ideal I. Suppose to the contrary that $\varrho(I) = J \neq 0$.

For any $x \in R$, it is easily seen that J is an ideal in $J + xJ$, and the quotient ring $(J + xJ)/J$ is a homomorphic image of J. By Theorem 49 we get $J + xJ \in \mathcal{R}$.

Similarly, for any $x, y \in R$, $J + xJ$ is an ideal of $J + xJ + Jy$ and the quotient ring $(J+xJ+Jy)/(J+xJ)$ is a homomorphic image of $J+xJ$. Hence $J + xJ + Jy \in \mathcal{R}$.

It follows from the proof of Theorem 49 that $\varrho(R)$ is the largest $\mathcal{R}$-ideal of R. Hence $A = \sum_{x,y\in R}(J + xJ + Jy) \in \mathcal{R}$. Clearly, A is an $\mathcal{R}$-ideal of R. Therefore $\varrho(R) \supseteq A \supseteq J \neq 0$. This contradiction shows that $\mathcal{S}$ satisfies condition (S1), which completes the proof. □

Lower and upper radicals of finite rings were considered in [36], but there is no overlap with our results.

For any nonempty set π of primes, denote by $\mathcal{N}_\pi$ the class of all nilpotent rings whose characteristics are products of primes in π. If $\mathcal{R}$ is a radical class, then by $\mathcal{N}_\mathcal{R}$ we denote the set of all nilpotent rings in $\mathcal{R}$.

For any ring R and prime p, put

$$R_p = \{r \in R \mid p^m r = 0 \text{ for some } m > 0\}.$$

Theorem 52 *Let $\mathcal{R}$ be a radical semisimple class of finite rings. Then $\mathcal{N}_\mathcal{R} = \mathcal{N}_\pi$ for some set π of primes.*

Proof. Let π be the set of all primes p such that $\mathcal{R}$ has a nonzero nilpotent ring whose additive group is a p-group.

Let $A \in \mathcal{N}_\mathcal{R}$. Then $A = \bigoplus_{p\in\pi} A_p$. Hence all $A_p \in \mathcal{R}$ by Theorem 49. Therefore $A \in \mathcal{N}_\pi$, and so $\mathcal{N}_\mathcal{R} \subseteq \mathcal{N}_\pi$.

For any $p \in \pi$, $\mathcal{R}$ contains a nonzero nilpotent ring $B = B_p$. Hence $0 \neq B/B^2 \in \mathcal{R}$. Choose a nonzero $x \in B/B^2$ with $px = 0$. Then the zero ring $\langle x \rangle$ is in $\mathcal{R}$, because it is an ideal of B/B^2. Every abelian p-group has a chain of normal subgroups with all factors of the chain being groups of order p. Therefore if we take any zero ring on a p-group, then it has a chain of ideals with all factors isomorphic to $\langle x \rangle$. Given that $\mathcal{R}$ is closed for ideal extensions, we see that $\mathcal{R}$ contains all zero rings on p-groups.

Look at $R = R_p \in \mathcal{N}_\pi$. Let $R^n = 0$ and $R^{n-1} \neq 0$. Then $(R^{n-1})^2 = 0$, and so we have $R^{n-1}, R/R^{n-1} \in \mathcal{R}$. Hence $R \in \mathcal{R}$. Thus $\mathcal{R}$ contains all nilpotent rings whose additive groups are p-groups.

Now take any $A \in \mathcal{N}_\pi$. Then $A = \bigoplus_{p\in\pi} A_p$ is a sum of nilpotent rings $A_p \in \mathcal{R}$. Therefore $\mathcal{N}_\mathcal{R} \supseteq \mathcal{N}_\pi$. This completes the proof. □

Theorem 53 *Let $\mathcal{R}$ be a radical semisimple class of finite rings. Denote by π the set of primes dividing nonzero characteristics of nilpotent rings in $\mathcal{R}$. Let $\mathcal{M}$ be the set of all matrix rings M over finite fields such that $M \in \mathcal{R}$. Denote by $\mathcal{R}_{\pi,\mathcal{M}}$ the class of all rings R which have an ideal $I \in \mathcal{N}_\pi$ such that R/I is a finite direct product of matrix rings in $\mathcal{M}$. Then*

$$\mathcal{R} = \mathcal{R}_{\pi,\mathcal{M}}.$$

Conversely, for every set π of primes and every set $\mathcal{M}$ of matrix rings over finite fields, the class $\mathcal{R}_{\pi,\mathcal{M}}$ is a radical semisimple class.

Proof. Take any $B \in \mathcal{R}$. As $\mathcal{R}$ is closed for ideals, the largest nilpotent ideal $N(B)$ of B is in $\mathcal{R}$. Therefore $N(B) \in \mathcal{N}_\pi$. Every finite Jacobson semisimple ring is a direct product of finite matrix rings. Therefore $B/N(B)$ is a direct product of matrix rings in $\mathcal{M}$. Thus $\mathcal{R} \subseteq \mathcal{R}_{\pi,\mathcal{M}}$. The reversed inclusion is obvious.

It is routine to verify that $\mathcal{R}_{\pi,\mathcal{M}}$ is closed for ideals, homomorphic images and ideal extensions, and so it is a radical semisimple class by Theorems 49 and 50. □

A radical ϱ is said to be *hereditary* if $\varrho(I) = I \cap \varrho(R)$ for every ring R with ideal I. It is easily seen that a radical is hereditary if and only if its radical class is closed for ideals. Therefore we get the following corollary.

Corollary 54 *All hereditary radical classes are precisely radical semisimple classes.*

Note that this corollary is not true in the case of arbitrary associative rings. In arbitrary rings radical semisimple classes are precisely the varieties generated by finite sets of finite fields (see [39], [87]). In particular, such radical classes do not contain nonzero nilpotent rings. We see that the situation in the finite ring case is quite different.

Theorem 55 *Let $\mathcal{K}$ be a class of finite simple rings. Denote by $\mathcal{R}_\mathcal{K}$ the class of all finite rings which have ideal chains with all factors in $\mathcal{K}$. Then $\mathcal{R}_\mathcal{K}$ is a radical semisimple class. Conversely, every radical semisimple class coincides with $\mathcal{R}_\mathcal{K}$ for some class $\mathcal{K}$ of finite simple rings.*

Proof. Given that $\mathcal{K}$ consists of simple rings, it is routine to verify that $\mathcal{R}_\mathcal{K}$ is closed for ideals, homomorphic images and ideal extensions. Therefore it is a radical semisimple class by Theorems 49 and 50.

Conversely, let $\mathcal{R}$ be a radical semisimple class. Denote by $\mathcal{K}$ the class of all simple rings in $\mathcal{R}$. Every finite ring in $\mathcal{R}$ has an ideal chain with simple factors, and by Theorem 49 all these factors are in $\mathcal{R}$, and so they belong to $\mathcal{K}$. Hence $\mathcal{R} \subseteq \mathcal{R}_\mathcal{K}$. Clearly, $\mathcal{R}_\mathcal{K} \subseteq \mathcal{R}$ by Theorem 49. Thus $\mathcal{R} = \mathcal{R}_\mathcal{K}$. □

4.2 Classes of principal ideal rings

If every ideal of a ring R has one generator, then R is called a *principal ideal ring*, PIR. A radical is *subidempotent* if its radical class does not contain any nonzero rings with zero multiplication. A radical is subidempotent if and only if its radical class does not contain any nilpotent rings.

Theorem 56 *A hereditary radical of finite rings consists of PIRs if and only if it is subidempotent.*

Proof. If a radical is subidempotent and hereditary, then every radical ring is Jacobson semisimple, and so is isomorphic to a finite direct product of matrix rings over finite fields. Therefore all radical rings are PIRs.

Conversely, suppose that a radical is not subidempotent. Then its radical class $\mathcal{R}$ contains a nonzero ring R with zero multiplication. It is clear that $R \times R \in \mathcal{R}$. However, $R \times R$ is not a PIR. □

A radical class is *supernilpotent* if it contains all nilpotent rings. A radical is *supernilpotent* if its radical class is supernilpotent.

Theorem 57 *A semisimple class of finite rings consists of PIRs if and only if its radical is supernilpotent.*

Proof. Let $\mathcal{S}$ be the semisimple class of a supernilpotent radical. Take any ring $R \in \mathcal{S}$. Since all nilpotent rings are radical, it follows that R has only zero nilpotent ideals, and so R is a finite direct product of matrix rings over finite fields. Therefore R is a PIR.

Conversely, suppose that $\mathcal{S}$ is a semisimple class of a radical which is not supernilpotent. Then there exists a ring $R \in \mathcal{S}$ with zero multiplication. As above, $R \times R$ belongs to $\mathcal{S}$ but is not a PIR. □

If in the definitions above we consider only finite *commutative* rings, then we get the concepts of a radical of finite commutative rings, and its radical and semisimple classes. The exact analogs of Theorems 49, 50 and Theorem 55 remain valid.

Theorem 58 *The class $\mathcal{R}$ of all finite commutative PIRs with identity is a radical class.*

Proof. If R has an ideal I with identity then R is isomorphic to the direct product $I \times (R/I)$. Therefore $\mathcal{R}$ is closed for ideal extensions. Theorem 33 of [96] tells us that every ring in $\mathcal{R}$ is a direct product of chain rings. A homomorphic image of a chain ring is a chain ring. Hence $\mathcal{R}$ is closed for homomorphic images. Theorem 49 completes the proof. □

Chapter 5

Semisimple Artinian semigroup-graded rings

This chapter is devoted to several structure theorems for Artinian semigroup-graded rings. All rings considered are Artinian but it is not required that these rings are commutative or contain identity elements. Consider a semigroup S and an S-graded ring $R = \oplus_{s \in S} R_s$ with support $\text{supp}(R)$. Two finiteness conditions are considered on $\text{supp}(R)$, (i) $\text{supp}(R)$ intersects a finite number of maximal subgroups of S and (ii) $\text{supp}(R)$ contains a finite number of idempotents. These conditions are used in giving several necessary and sufficient conditions for R to be semisimple Artinian when S is a semilattice, a finite semilattice, an inverse semigroup and a Clifford semigroup. Here R may be a special B-graded ring, or a faithful or arbitrary S-graded ring. Semigroup identities are given for a semigroup variety $\mathcal{V}$ which ensures that a semigroup algebra FS is semisimple Artinian, where F is a arbitrary field. Most of this chapter appears in [21].

5.1 Idempotents and supports

Let S be a semigroup. An associative ring $R = \bigoplus_{s \in S} R_s$ is said to be *S-graded* if $R_s R_t \subseteq R_{st}$ for all $s, t \in S$. The *support* of R is the set

$$\text{supp}(R) = \{s \in S \mid R_s \neq 0\}.$$

For a semigroup ring $R = KS$ we have $\text{supp}(R) = S$, so we are interested in finiteness conditions for supports of semigroup-graded rings. One condition of

this sort was obtained in [60], if S entirely consists of idempotents and R is right Artinian, then $\mathrm{supp}(S)$ is finite. (This theorem was generalized in [28] and in [50]).

We shall show that in general the support of a right Artinian semigroup-graded ring may contain infinitely many idempotents. However, if we require that R be a semisimple Artinian ring, then the number of idempotents in $\mathrm{supp}(R)$ is finite. In fact, we shall prove the following stronger theorem.

Theorem 59 *Let S be a semigroup. The support of a semisimple Artinian S-graded ring intersects a finite number of maximal subgroups of S.*

Proof. Suppose to the contrary that there exists a semisimple Artinian S-graded ring $R = \bigoplus_{s\in S} R_s$ such that the set M of all maximal subgroups intersecting $\mathrm{supp}(R)$ is infinite.

Consider the set P of all right ideals of the form $R_{GS^1} = \bigoplus_{s\in GS^1} R_s$, where $G \in M$. A semisimple Artinian ring is right Artinian and Noetherian, and so it contains only finite chains of right ideals. Hence P does not contain infinite chains. If P has an infinite set of pairwise incomparable elements $R_{G_1S^1}, R_{G_2S^1}, \ldots$, then it has an infinite ascending chain $R_{G_1S^1} \subset R_{G_1S^1} + R_{G_2S^1} \subset \cdots$, a contradiction. Therefore P has only finite sets of incomparable elements. The last exercise in [30, § 1.1] tells us that if every chain and every set of pairwise noncomparable elements in a partially ordered set P is finite, then P is finite. Hence there exists an infinite set $N \subseteq M$ such that $R_{GS^1} = R_{HS^1}$ for all $G, H \in N$.

Consider the set Q of all left ideals of the form $R_{S^1G} = \bigoplus_{s\in S^1G} R_s$, where G runs over N. Since a semisimple Artinian ring is left Artinian and Noetherian, the same argument as above shows that Q is a finite set. Therefore there exists an infinite set $L \subset N$ such that $R_{S^1G} = R_{S^1H}$ for all $G, H \in L$.

Take any $G, H \in L$. Given that G and H intersect $\mathrm{supp}(R)$, there exist $g \in G$, $h \in H$ such that $R_g \neq 0$, $R_h \neq 0$. Since $R_g \subseteq R_{GS^1} = R_{HS^1}$, we see that $g \in HS^1$, and so $gS^1 \subseteq HS^1$, whence $GS^1 = gGS^1 \subseteq HS^1$. Similarly, $GS^1 \supseteq HS^1$. Therefore $GS^1 = HS^1$. The same reasoning shows that $S^1G = S^1H$. Thus G and H generate the same left and right ideals in S, for all $G, H \in L$.

Thus L is contained in a single H-class of S. This H-class is a maximal subgroup of S by [46], Theorem 2.2.5. Therefore all subgroups in L coincide.

This contradiction completes the proof. □

Corollary 60 *The support of a semisimple Artinian semigroup-graded ring contains a finite number of idempotents.*

Example 61 Let F be field which is a twisted group ring of an infinite group G due to Passman [78]. Clearly, F is G-graded, $F = \bigoplus_{g\in G} F_g$. Consider the subring $R = Fe_{11} + Fe_{21}$ of the 2×2 matrix ring F_2, where e_{ij} denotes the standard matrix unit. It is easily seen that

$$R = \begin{bmatrix} F & 0 \\ F & 0 \end{bmatrix}$$

is a right Artinian ring. Denote by S the set

$$\{(g, i) \mid g \in G, i = 1, 2\}.$$

Introduce a multiplication on S putting

$$(g,1)(h,1) = (gh,1), \tag{5.1}$$
$$(g,2)(h,2) = (h,2), \tag{5.2}$$
$$(g,1)(h,2) = (h,2), \tag{5.3}$$
$$(g,2)(h,1) = (gh,2). \tag{5.4}$$

Then it is routine (although tedious) to verify that S is a semigroup and R is an S-graded ring, $R = \bigoplus_{s\in S} R_s$ with components $R_s = R_{(g,i)} = F_g e_{i1}$. The support of R is equal to S. Clearly, all elements $(g, 2)$, $g \in G$, are idempotents. Thus R is a right Artinian S-graded ring with infinitely many idempotents in the support.

Next, we obtain conditions sufficient for a graded ring with support intersecting a finite number of maximal subgroups or with finitely many idempotents in the support to be semisimple Artinian.

A semigroup entirely consisting of idempotents is called a *band*. A commutative band is called a *semilattice*. Semilattice-graded rings were considered in [25], [45], [54], [88] and other papers.

Theorem 62 *For any semigroup S, the following conditions are equivalent:*

(i) every S-graded ring $R = \bigoplus_{s\in S} R_s$ with a finite number of idempotents in the support is semisimple Artinian if and only if all subrings R_e are semisimple Artinian for all idempotents e of S;

(ii) S is a semilattice.

Proof. $(i) \Rightarrow (ii)$: First, we'll show that S is a band. Suppose to the contrary that S has an element x such that $x \neq x^2$. Denote by R any nonzero ring with zero multiplication. Let $R_x = R$, and for $x \neq s \in S$ put $R_s = 0$. Then $R = \bigoplus_{s\in S} R_s$ is an S-graded ring, and $R_e = 0$ for all idempotents $e \in S$. Therefore condition (i) implies that R is semisimple Artinian. This contradiction shows that S is a band.

If S is not commutative, then it follows from [46], Theorem 4.4.1, that S contains a nontrivial left or right zero band. Assume that S has a left zero subband $L = \{\ell, m\}$. Take any field F and consider the semigroup ring $R = FL$. Let $R_\ell = F\ell$, $R_m = Fm$, and for $s \in S\backslash L$ put $R_s = 0$. Then $R = \bigoplus_{s\in S} R_s$ is an S-graded ring, and for any idempotent $e \in S$ either $R_e = 0$ or $R_e \cong F$. Therefore condition (i) tells us that R is a semisimple Artinian ring. However, R has a nilpotent ideal $\{f\ell - fm \mid f \in F\}$. This contradiction shows that S is a semilattice.

$(ii) \Rightarrow (i)$: Suppose that S is a semilattice. Consider an S-graded ring $R = \bigoplus_{s\in S} R_s$ with a finite number of idempotents in the support.

Suppose that R is semisimple Artinian. Pick any idempotent e in S. Then the ideal $R_{eS} = \bigoplus_{s\in eS} R_s$ of R is semisimple Artinian, too. It is easily seen that R_e is isomorphic to the quotient ring $R_{eS}/R_{eS\backslash\{e\}}$. Therefore R_e is semisimple Artinian, as well.

Conversely, suppose that all rings R_e are semisimple Artinian for all idempotents $e \in S$. Recall that every semilattice is a partially ordered set with respect to the order defined by $x \leq y \Leftrightarrow xy = x$. Let $|\operatorname{supp}(R)| = n$. By induction we define idempotents $e_1, \ldots, e_n$. Choose a minimal element e_1 in S with the property that $R_{e_1} \neq 0$. Suppose that idempotents $e_1, \ldots, e_k$ have already been defined for some $1 \leq k \leq n$. Put $S_k = \{e_1, \ldots, e_k\}$. Choose a minimal idempotent in $\operatorname{supp}(R)\backslash S_k$. It is routine to verify that R has an ideal chain

$$R_{e_1} = R_{S_1} \subset R_{S_2} \subseteq \ldots \subseteq R_{S_n} = R,$$

and each factor $R_{S_k}/R_{S_{k-1}}$ is isomorphic to R_{e_k} for $k = 2, \ldots, n$. Since the class of semisimple Artinian rings is closed for ideal extensions, it follows that

R is semisimple Artinian, as required. □

A class $\mathcal{K}$ of rings is said to be *S-closed* if every S-graded ring R is in $\mathcal{K}$ provided that all subrings R_e are in $\mathcal{K}$ for all idempotents e of S (see [58]). Corollary 60 and Theorem 62 immediately give us the following

Corollary 63 *The class of semisimple Artinian rings is S-closed if and only if S is a finite semilattice.*

5.2 Inverse semigroups

A semigroup S is said to be *inverse* if, for every $s \in S$, there exists a unique $s^{-1} \in S$ such that $ss^{-1}s = s$ and $s^{-1}ss^{-1} = s^{-1}$. Inverse semigroups form an important class arising in many interesting situations (see [79]). Rings graded by inverse semigroups were considered in [61] and [91]. A semigroup is said to be *completely regular* if it is a union of groups. A *Clifford* semigroup is an inverse completely regular semigroup. Rings graded by Clifford semigroups have been considered in [4].

Let B be a semilattice. A semigroup S is a *semilattice B of subsemigroups* S_b, where $b \in B$, if $S = \cup_{b\in B} S_b$ is a disjoint union of the subsemigroups S_b, and $S_a S_b \subseteq S_{ab}$ for all $a, b \in B$. Theorem 4.2.1 of [46] tells us that every Clifford semigroup is a semilattice of groups.

Theorem 64 *For any semigroup S, the following conditions are equivalent:*

(i) every S-graded ring $R = \bigoplus_{s\in S} R_s$ with support intersecting a finite number of maximal subgroups is semisimple Artinian if and only if all subrings $R_G = \bigoplus_{g\in G} R_g$ are semisimple Artinian for all maximal subgroups G of S;

(ii) S is a Clifford semigroup.

Proof. $(i) \Rightarrow (ii)$: First, we claim that S is a completely regular semigroup. Suppose to the contrary that S has an element x which does not belong to any subgroup of S. Take any ring $R \neq 0$ with zero multiplication.

Put $R_x = R$, and for $x \neq s \in S$ put $R_s = 0$. Then $R = \bigoplus_{s \in S} R_s$ is an S-graded ring, and $R_G = 0$ for all subgroups G of S. This contradicts condition (i) and shows that S is completely regular.

If S is not inverse, then it follows from [46], Theorem 5.1.1 (3) and Proposition 2.3.3, that S contains a nontrivial left or right zero band. Assume that S has a left zero subband $L = \{\ell, m\}$. As in the proof of Theorem 62 the semigroup ring $R = FL$ gives us an example of an S-graded ring contradicting condition (i). Therefore S is inverse. Thus S is a Clifford semigroup.

$(ii) \Rightarrow (i)$: Suppose that S is a Clifford semigroup. Consider an S-graded ring $R = \bigoplus_{s \in S} R_s$ with support intersecting a finite number of maximal subgroups of S. Then Theorem 4.2.1 of [46] tells us that S is a semilattice Y of groups G_y, $y \in Y$. Clearly, $R = \bigoplus_{y \in Y} R_{G_y}$ is a semilattice-graded ring. Theorem 62 shows that R is semisimple Artinian if and only if all the rings R_{G_y} are semisimple Artinian for all $y \in Y$. □

We shall describe special band-graded rings which are semisimple Artinian rings. The concept of a special band-graded ring was introduced by Munn [72]. Let B be a band, and let $R = \bigoplus_{b \in B} R_b$ be a B-graded ring. If each ring R_b has identity 1_b, and $1_a 1_b = 1_{ab}$, for all a, b, then the ring R is called a *special band-graded ring* or a *special B-graded ring*. If B is a *semilattice*, then all special B-graded rings are strong semilattice sums of rings (see [25] for a definition).

Theorem 65 *Let B be a band, and let $R = \bigoplus_{b \in B} R_b$ be a special B-graded ring. Then R is semisimple Artinian if and only if B is a finite semilattice and all components R_b, $b \in B$, are semisimple Artinian.*

We need two lemmas from [57]. Recall that a *rectangular* band is a band satisfying the identity $xyx = x$.

Lemma 66 ([57], Lemma 2) *Let a band B be a semilattice S of rectangular bands H_s, $R = \bigoplus_{b \in B} R_b$ a special band-graded ring, 1_b the identity of R_b. For each $s \in S$ choose an element h_s in H_s and set*

$$Q_s = \bigoplus_{b \in H_s} R_b, I_s = \{x \in Q_s \mid 1_{h_s} x 1_{h_s} = 0\}, I = \bigoplus_{s \in S} I_s.$$

Then I is a locally nilpotent ideal of R. The quotient ring R/I is a special S-graded ring $R/I = \bigoplus_{s \in S} F_s$, where $F_s \cong R_{h_s}$. The ideal I and rings F_s do not depend on the choice of the elements h_s. Besides, $I_s^3 = 0$ for every $s \in S$.

Lemma 67 ([57], Lemma 4) *Let S be a finite semilattice and $R = \bigoplus_{s\in S} R_s$ a special semilattice-graded ring. Then R is isomorphic to the direct product $\prod_{s\in S} R_s$.*

Proof of Theorem 65. If B is not a semilattice, then R contains a nonzero locally nilpotent ideal I by Lemma 66. Hence B is a semilattice. Theorem 4 of [57] tells us that B is finite. Lemma 67 says that R is isomorphic to the direct product $\prod_{b\in B} R_b$. Therefore R is semisimple Artinian if and only if all the R_b are semisimple Artinian. □

A *Brandt semigroup* is an inverse completely 0-simple semigroup. (A semigroup is *completely 0-simple* if it has no proper nonzero ideals). Wauters and Jespers [91] proved that, for every Brandt semigroup S with a finite number of idempotents, an S-graded ring R is semisimple Artinian if and only if R is semiprime and all group-graded subrings R_G are semisimple Artinian for all maximal subgroups G of S ([91], Theorem 3.5). We describe all inverse semigroups S satisfying this property.

We say that the grading is *faithful* if, for any $s, t \in S$ and $r \in R_s$, each of the equalities $rR_t = 0$ and $R_t r = 0$ implies that $r = 0$, (see [29] and [61]).

Theorem 68 *Let S be an inverse semigroup, and let $R = \bigoplus_{s\in S} R_s$ be a faithfully S-graded ring with a finite number of idempotents in the support. If R_G is semisimple Artinian for all maximal subgroups G of S, then R is semisimple Artinian.*

Proof. Given that S is inverse, the main theorem of [61] tells us that if all the R_G are semisimple, then R is semisimple.

We proceed by induction on the number n of idempotents in the support of R.

Suppose that $n = 0$. If $R_s \neq 0$ for some $s \in S$, then the equality $ss^{-1}s = s$ implies $R_s R_{s^{-1}} R_s = R_s$, because R is faithfully graded. Hence $R_{s^{-1}} R_s \neq 0$, and therefore $R_{s^{-1}s} \neq 0$. This contradicts the fact that $s^{-1}s$ is an idempotent. Therefore $R = 0$, and the assertion is trivial.

Next, assume that $n \geq 1$. Take a ring $R = \bigoplus_{s\in S} R_s$ such that the number of idempotents in $\mathrm{supp}(R)$ equals n.

Choose an element $m \in \text{supp}(R)$ such that the ideal $M = S^1mS^1$ is minimal. Denote by N the set of all nongenerating elements of M. Clearly, $R_N = 0$ by the minimality of m, and so we may factor out N in S and assume that from the very beginning $N = 0$. Then $M = M/N$ is a 0-simple semigroup by [46], Proposition 3.1.5.

For any idempotent $0 \neq e \in M$, there exist elements $a, b \in M$ such that $aeb = m$. Hence $R_aR_eR_b = R_m$, and so $R_e \neq 0$, i.e., $e \in \text{supp}(R)$. Therefore M has a finite number of idempotents; whence it has a primitive idempotent and is a completely 0-simple semigroup by [46], Theorem 3.3.3 (4). Thus M is a Brandt semigroup by [46], Theorem 5.1.8.

For any $0 \neq s \in M$, there exist $a, b \in M$ such that $m = asb$. Hence $0 \neq R_m = R_aR_sR_b$, because R is faithfully graded. Therefore $R_s \neq 0$ for all $s \in M$. It follows that M has a finite number of idempotents.

Given that R_G is semisimple Artinian for all maximal subgroups G of M, it follows from [91], Theorem 3.5, that R_M is semisimple Artinian.

Clearly, R_M is an ideal of R, and R/R_M is an S-graded ring with $\text{supp}(R/R_M) \subseteq \text{supp}(R)\backslash M$. Therefore R/R_M has fewer than n idempotents in the support. By the induction assumption R/R_M is semisimple Artinian. Since the class of semisimple Artinian rings is closed under ideal extensions, it follows that R is semisimple Artinian, too. This completes the proof. □

Theorem 69 *For any inverse semigroup S, the following conditions are equivalent:*

(i) every S-graded ring $R = \bigoplus_{s\in S} R_s$ is semisimple Artinian if and only if R is semiprime and all subrings $R_G = \bigoplus_{g\in G} R_g$ are semisimple Artinian for all maximal subgroups G of S;

(ii) S has a finite number of idempotents.

Proof. $(i) \Rightarrow (ii)$: Suppose that every S-graded ring R is semisimple Artinian if and only if R is semiprime and all subrings R_G are semisimple Artinian for all maximal subgroups G of S. We'll show that S has a finite number of idempotents.

Denote by E the set of all idempotents of S. Let F be a field, and let $R = \prod_{e\in E} R_e$ be a direct product of isomorphic copies R_e of F. For all

$s \in S \backslash E$, put $R_s = 0$. Then it is easily seen that $R = \bigoplus_{s \in S} R_s$ is an S-graded ring. Clearly, R is semiprime. If G is a maximal subgroup of S with identity e, then $R_G = R_e \cong F$ is semisimple Artinian. Hence R is semisimple Artinian by condition (i). It follows that R is a finite direct product of the fields R_e. Therefore the set E is finite.

$(ii) \Rightarrow (i)$: Let S be an inverse semigroup with a finite number, say n, of idempotents. Fix an S-graded ring $R = \bigoplus_{s \in S} R_s$. We must verify that R is semisimple Artinian if and only if it is semiprime and all subrings $R_G = \bigoplus_{g \in G} R_g$ are semisimple Artinian for all maximal subgroups G of S. We proceed by induction on n.

If $n = 1$, then S is a group and condition (i) holds.

Suppose that $n > 1$. Note that if S is a completely 0-simple semigroup, then S is a Brandt semigroup by [46], Theorem 5.1.8; whence any S-graded ring is a generalized matrix ring, and so condition (i) follows from [91], Theorem 3.5. So we assume that S is not completely 0-simple. Consider two possible cases.

Case 1. S is a semigroup with zero. Every ideal of an inverse semigroup is generated by idempotents in view of [46], Theorem 5.1.1. Given that S has only a finite number of idempotents, it has a minimal nonzero ideal M. Since M has a finite number of idempotents, it follows from [46, § 3.2] that M is a completely 0-simple semigroup. Therefore M is a proper ideal of S. Hence the induction assumption applies to M and to S/M. Note that R/R_M is an S/M-graded ring.

Suppose that R is semisimple Artinian then R is semiprime. Take any maximal subgroup G of S. First, consider the case where G is a subgroup of M. Since R_M is an ideal of R, it is also semisimple Artinian, and by the induction assumption R_G is semisimple Artinian. Second, consider the case where G does not belong to M. Then G is a maximal subgroup of S/M. Since R/R_M is a semisimple Artinian S/M-graded ring, the induction assumption implies that R_G is semisimple Artinian, again.

Conversely, suppose that R is semiprime and all R_G are semisimple Artinian for all maximal subgroups G of S. Since R_M is an ideal of R, it is also semiprime by [38], Example 2.5(ii). By the induction assumption R_M is a semisimple Artinian ring. Since R_M has an identity, R is isomorphic to a direct product of R_M and R/R_M. Hence R/R_M is semiprime, too. All maximal subgroups of S/M are maximal subgroups of S. Therefore the induction assumption yields that R/R_M is semisimple Artinian. Since the class

of semisimple Artinian rings is closed for ideal extensions, R is semisimple Artinian, as required.

Case 2. S has no zero. Denote by K the kernel of S. It follows from [46], Proposition 3.1.4, that K is a simple semigroup. Since it has a finite number of idempotents, it is a completely simple semigroup. Given that K is inverse, [46], Theorem 5.1.1(3), implies that K is a group.

Suppose that R is semisimple Artinian. Then R is semiprime. Take any maximal subgroup G of S. If $G = K$, then R_G is semisimple Artinian, because it is an ideal in R. If $G \neq K$, then G is a maximal subgroup of S/K. Since S/K is a semigroup with zero, and so is covered by Case 1, and R/R_K is an S/K-graded semisimple Artinian ring, it follows that R_G is semisimple Artinian.

Conversely, suppose that R is semiprime and all R_G are semisimple Artinian for all maximal subgroups G of S. Since K is a maximal subgroup of S, R_K is semisimple Artinian, and so it has an identity. Hence R is isomorphic to the direct product of R_K and R/R_K. In view of Case 1, since S/K is a semigroup with zero and R/R_K is an S/K-graded ring, we see that R/R_K is semisimple Artinian. Therefore R is semisimple Artinian, too. This completes the proof. □

If p is a positive integer, then a group is called a *p'-group* if it has no elements of order p. For convenience, we shall call all groups $0'$-groups.

A class of all semigroups satisfying a certain set of identities is called a *variety*. The investigation of semigroup varieties is one of the most important directions of semigroup theory (see [85], [86]). Therefore it is interesting to determine whether it is possible to find semigroup identities which ensure that a semigroup algebra is semisimple Artinian. This is accomplished in the following theorem.

Theorem 70 *Let $\mathcal{V}$ be a semigroup variety, and let F be a field of characteristic $p \geq 0$. Then the following conditions are equivalent:*

(i) for every finite semigroup $S \in \mathcal{V}$, the semigroup algebra FS is semisimple Artinian;

(ii) all semigroups in $\mathcal{V}$ are semilattices of p'-groups;

(iii) $\mathcal{V}$ *satisfies the identities* $x^{m+1} = x$ *and* $(xy)^m = (yx)^m$, *where* m *is an integer not divisible by* p.

Proof. We shall prove implications $(i) \Rightarrow (ii)$ and $(i) \Rightarrow (iii)$ simultaneously.

Take the free semigroup F_1 of rank one in $\mathcal{V}$. Let x be the free generator of F_1. If $x \notin xF_1$, then $\mathcal{V}$ contains the two-element semigroup $Z_2 = F_1/xF_1$ with zero multiplication. The semigroup algebra FZ_2 is not semisimple: its radical contains $x - x^2$. This contradiction shows that $x \in xF_1$. Hence there exists a positive integer m such that $x^{m+1} = x$. Therefore F_1 is a group of order m. If m is divisible by p, then the radical of the group algebra FF_1 contains $x + x^2 + \cdots + x^m$, a contradiction. Therefore m is not divisible by p, and $\mathcal{V}$ satisfies the identity $x^{m+1} = x$.

If $L = \{a, b\}$ is a left or right zero band, then the semigroup algebra FL is not semisimple: its radical contains $a - b$. Therefore $\mathcal{V}$ does not contain nontrivial left and right zero bands. Theorem 4.1.3 of [46] tells us that S is a semilattice of completely simple semigroups. Every completely simple semigroup is a rectangular band of groups. If a completely simple semigroup is not a group, then it follows from [46], Exercise 2.6.3, that it contains a nontrivial left or right zero band. This contradiction shows that S is a semilattice of groups. Since these groups satisfy the identity $x^{m+1} = x$ where m is not divisible by p, it follows that they are p'-groups. Therefore S is a union of p'-groups. Thus condition (ii) holds.

Consider the free semigroup F_2 of rank two in $\mathcal{V}$. Let x, y be the free generators of F_2. Given that F_2 is a semilattice of groups, it is clear that xy and yx belong to the same maximal subgroup G of F_2. By the identity $x^{m+1} = x$ the elements $(xy)^m$ and $(yx)^m$ are both equal to the identity of G. Hence $(xy)^m = (yx)^m$, and so $\mathcal{V}$ satisfies the identity $(xy)^m = (yx)^m$. Thus condition (iii) holds.

$(iii) \Rightarrow (ii)$: Suppose that $\mathcal{V}$ satisfies the identities $x^{m+1} = x$ and $(xy)^m = (yx)^m$ for a positive integer m not divisible by p. Take any semigroup S in $\mathcal{V}$. The identity $x^{m+1} = x$ shows that S is a union of p'-groups. Therefore S is a semilattice of completely simple semigroups. The identity $(xy)^m = (yx)^m$ implies that S does not contain nontrivial left or right zero bands. As above, all completely simple semigroups without nontrivial left and right zero bands are groups. Therefore S is a semilattice of p'-groups.

$(ii) \Rightarrow (i)$: Take a finite semigroup S in $\mathcal{V}$. Let S be a semilattice Y of p'-

groups G_y, where $y \in Y$. Then $FS = \bigoplus_{y \in Y} FG_y$ is graded by the semilattice Y. By Maschke's theorem the group algebras FG_y are semisimple. Therefore FS is semisimple by [88], Theorem 1. Every semisimple finite dimensional algebra is semisimple Artinian. This completes our proof. □

Bibliography

[1] M. ATIYAH and I. MCDONALD, "Introduction to Commutative Algebra", Addison-Wesley, 1969. Math.Rev.39#4129

[2] M. BEATTIE, S. DASCALESCU and C. NASTASESCU, *A note on semilocal graded rings*, Rev. Roumaine Math. Pures Appl. **40** (1995), no.3-4, 253-258. Math.Rev.97e:16085

[3] T. BECKER and V. WEISPFENNING, "Gröbner Bases. A Computational Approach to Commutative Algebra", Graduate Texts in Mathematics **141**, Springer-Verlag, 1993. Math.Rev.95e:13018

[4] A.D. BELL, *Prime ideals and radicals in rings graded by Clifford semigroups*, Comm. Algebra **25** (1997), no.5, 1595–1608. Math.Rev.98e:16022

[5] S.D. BERMAN, *On the theory of group codes*, Kibernetika **3** (1967), no.1, 31–39; *translated as* Cibernetics **3** (1967), no.1, 25–31. Math.Rev.42#5702

[6] I.F. BLAKE and R.C. MULLIN, "The Mathematical Theory of Coding", Academic Press Inc. 1975. Math.Rev.52#16845

[7] D. BULACU, S. DASCALESCU and L. GRUNENFELDER, *Modules graded by G-sets : duality and finiteness conditions*, J. Algebra **195** (1997), no.2, 624–633. Curr.Math.Publ.98 01

[8] J. CAZARAN, *Mappings over finite rings*, abstract of a talk, CANT95 - 'Computational Algebra and Number Theory' conference, Macquarie University, Sydney, Australia, 12-14 Apr. 1995.

[9] J. CAZARAN, *A class of permutation polynomial vectors and their applications in cryptography*, pre-proceedings of the 'Cryptographic Policy and Algorithms Conference', Queensland University of Technology, Brisbane, Australia, 3-5 July 1995, 460–470.

[10] J. CAZARAN, *A class of permutation polynomial vectors over a finite ring*, abstract of a talk, F_q3 - '3rd International Conference on Finite Fields and their Applications', University of Glasgow, Scotland, 11-14 July 1995.

[11] J. CAZARAN and A.V. KELAREV, *On finite commutative principal ideal rings and error-correcting codes*, abstract of a talk, AGCT6 - 'Algebraic Geometry and Coding Theory' conference, CIRM, Marseille-Luminy, France, 23-27 June 1997.

[12] J. CAZARAN and A.V. KELAREV, *Polynomial codes and principal ideal rings*, proceedings of the '1997 IEEE International Symposium on Information Theory', Ulm, Germany, 29 June - 4 July 1997, 502–502.

[13] J. CAZARAN and A.V. KELAREV, *On finite commutative principal ideal rings and error-correcting codes*, abstract of a talk, 'Topics in Number Theory' conference, Penn State University, Pennsylvania, USA, 30 July - 3 Aug. 1997.

[14] J. CAZARAN and A.V. KELAREV, *On finite commutative principal ideal rings and multivariate polynomial codes over F_q*, abstract of a talk, F_q4 - '4th International Conference on Finite Fields and their Applications', University of Waterloo, Ontario, Canada, 12-15 Aug. 1997.

[15] J. CAZARAN, *Classes of polynomials which are closed under composition and represent injective mappings over a finite commutative ring and their application to public-key cryptosystems*, abstract of a rump session talk, Crypto97 - '17th International Cryptography Conference', University of California at Santa Barbara, California, USA, 17-22 Aug. 1997.

[16] J. CAZARAN and P. MOREE, *On a result in the first letter of Ramanujan to Hardy*, abstract of a talk, 'Conference to Commemorate the 50th Anniversary of the Death of G.H. Hardy', University of Sydney, Australia, 1-2 Dec. 1997

[17] J. CAZARAN and A.V. KELAREV, *A class of error-correcting codes based on finite commutative principal ideal rings*, abstract of a talk, CANT97 - 'Computational Algebra and Number Theory '97 - Number Theory and Cryptography Conference', University of Sydney, Australia, 3-5 Dec. 1997.

[18] J. CAZARAN and A.V. KELAREV, *Sufficient conditions for finite commutative rings to be principal ideal rings and an application to error-correcting codes*, abstract of a talk, ICM98 - 'International Congress of Mathematicians', Technical University, Berlin, Germany, 18-27 Aug. 1998.

[19] J. CAZARAN, P. MOREE and P. STEVENHAGEN, *On the permutational power of polynomials*, abstract of a talk, 'Algebraic Number Theory and Diophantine Analysis' conference, Graz, Austria, 31 Aug. - 4 Sept. 1998.

[20] J. CAZARAN and A.V. KELAREV, *Generators and weights of polynomial codes*, Arch. Math. **69** (1997), 479–486. Curr.Math.Publ.98 04

[21] J. CAZARAN and A.V. KELAREV, *Semisimple Artinian graded rings*, Comm. Algebra, to appear.

[22] J. CAZARAN and A.V. KELAREV, *On finite principal ideal rings*, submitted.

[23] P. CHARPIN, *The extended Reed-Solomon codes considered as ideals of a modular algebra*, Annals Discrete Math. **17** (North-Holland Math. Stud., **75**) (1983), 171–176. Math.Rev.87e:94038

[24] P. CHARPIN, *Une generalisation de la construction de Berman des codes de Reed et Muller p-aires*, Comm. Algebra **16** (1988), no.11, 2231–2246. Math.Rev.89m:94013

[25] H.L. CHICK and B.J. GARDNER, *The preservation of some ring properties by semilattice sums*, Comm. Algebra **15** (1987), no.5, 1017–1038. Math.Rev.88a:16015

[26] M.V. CLASE and E. JESPERS, *Perfectness of rings graded by finite semigroups*, Bull. Soc. Math. Belg. Ser. A **45** (1993), no.1-2, 93–102. Math.Rev.96b:16043

[27] M.V. CLASE and E. JESPERS, *On the Jacobson radical of semigroup graded rings*, J. Algebra **169** (1994), no.1, 79–97. Math.Rev.95m:16036

[28] M.V. CLASE, E. JESPERS, A.V. KELAREV and J. OKNIŃSKI, *Artinian semigroup-graded rings*, Bull. London Math. Soc. **27** (1995), no.5, 441–446. Math.Rev.96f:16051

[29] M. COHEN and S. MONTGOMERY, *Group-graded rings, smash products, and group actions*, Trans. Amer. Math. Soc. **282** (1984), no.1, 237–258. Math.Rev.85i:16002; Addendum Math.Rev.88a:16002

[30] P. CRAWLEY and R.P. DILWORTH, "Algebraic Theory of Lattices", Prentice Hall, New Jersey, 1973.

[31] S. DASCALESCU, *Graded semiperfect rings*, Bull. Math. Soc. Sci. Math. Roumanie, **36**(84)(1992), no.3-4, 247–254. Math.Rev.96b:16044

[32] S. DASCALESCU, *Graded $T-$rings with finite support*, Comm. Algebra, **21** (1993), no.10, 3619–3636. Math.Rev.94h:16076

[33] F. DECRUYENAERE and E. JESPERS, *Graded commutative principal ideal rings*, Bull. Belg. Math. Soc. Ser. B **43** (1991), no.2, 143–150. Math.Rev.95j:13017

[34] F. DECRUYENAERE, E. JESPERS and P. WAUTERS, *On commutative principal ideal semigroup rings*, Semigroup Forum, **43** (1991), no.3, 367–377. Math.Rev.92i:20070

[35] D. EISENBUD "Commutative Algebra. With a view toward algebraic geometry.", Graduate Texts in Mathematics **150**, Springer-Verlag, New York, 1995. Math.Rev.97a:13001

[36] J.L. FISHER, *Radicals for finite rings*, preprint.

[37] P.R. FUCHS and L. VAN WYK, *On subrings of simple Artinian rings*, Results Math. **24** (1993), no.1-2, 49–65. Math.Rev.94g:16039

[38] B.J. GARDNER, "Radical Theory", Pitman Research Notes in Math. **198**, Wiley, New york, 1989. Math.Rev.90h:16019

[39] B.J. GARDNER and P.N. STEWART, *On semi-simple radical classes*, Bull. Austral. Math. Soc. **13** (1975), no.3, 349–353. Math.Rev.53#505

[40] B.J. GARDNER and P.N. STEWART, *The closure of radical classes under finite subdirect products*, Compositio Math. **46** (1982), no.2, 145–158. Math.Rev.84a:16010

[41] R. GILMER, "Multiplicative Ideal Theory", Pure and Applied Mathematics **12**, Marcel Dekker Inc., New York, 1972. Math.Rev.55#323

[42] B. GLASTAD and G. HOPKINS, *Commutative semigroup rings which are principal ideal rings*, Comment. Math. Univ. Carolinae **21** (1980), no.2, 371–377. Math.Rev.81i:20099

[43] R. HARTSHORNE, "Algebraic Geometry", Graduate Texts in Mathematics **12**, Springer-Verlag, New York, 1977. Math.Rev.57#3116.

[44] A.R. HAMMONS JR., P.V. KUMAR, A.R. CALDERBANK, N.J.A. SLOANE and P. SOLÉ, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Information Theory **40** (1994), no.2, 301–319. Math.Rev.95k:94030

[45] YUE-CHAN-P HO, *The preservation of the semiprime Goldie property by strong semilattice sums*, Proc. Amer. Math. Soc. **114** (1992), no.3, 613–616. Math.Rev.92f:16029

[46] J.M. HOWIE, "Fundamentals of Semigroup Theory", London Mathematical Society Monographs. New Series **12**, Clarendon Press, Oxford University Press, New York, 1995. Math.Rev.98e:20059

[47] E. JESPERS, *Chain conditions and semigroup graded rings*, J. Austral. Math. Soc. Ser. A **45** (1988), no.3, 372-380. Math.Rev.89j:16024

[48] E. JESPERS, *Radicals of graded rings*, Colloq. Math. Soc. Janos Bolyai **61** : Theory of radicals (Szekszard, 1991), North-Holland, Amsterdam (1993), 109–130. Math.Rev.95d:16025

[49] E. JESPERS and J. OKNIŃSKI, *Semigroup algebras that are principal ideal rings*, J. Algebra **183** (1996), no.3, 837–863. Math.Rev.97g:20078

[50] E. JESPERS and J. OKNIŃSKI, *Descending chain conditions and graded rings*, J. Algebra **178** (1995), no.2, 458–479. Math.Rev.96i:16060

[51] E. JESPERS and P. WAUTERS, *Principal ideal semigroup algebras*, Comm. Alg. **23** (1995), no.13, 5057–5076. Math.Rev.96m:20110

[52] E. JESPERS and P. WAUTERS, *A description of the Jacobson radical of semigroup rings of commutative semigroups*, North-Holland Math. Stud. **126** (1986), 43–89. Math.Rev.87k:20105

[53] G. KARPILOVSKY, "The Jacobson Radical of Classical Rings", Pitman Monographs and Surveys in Pure and Applied Mathematics **53**, John Wiley & Sons, New York, 1991. Math.Rev.93a:16001

[54] A.V. KELAREV, *Radicals and semilattice sums of rings revisited*, Comm. Algebra **20** (1992), no.3, 701–709. Math.Rev.93e:16031

[55] A.V. KELAREV, *A general approach to the structure of radicals in some ring constructions*, Colloq. Math. Soc. Janos Bolyai **61** : Theory of radicals (Szekszard, 1991), North-Holland, Amsterdam (1993), 131–144. Math.Rev.94k:16036

[56] A.V. KELAREV, *Radicals of semigroup rings of commutative semigroups*, Semigroup Forum **48** (1994), no.1, 1–17. Math.Rev.94m:20131

[57] A.V. KELAREV, *Finiteness conditions for special band-graded rings*, Demonstratio Math. **27** (1994), no.1, 171–178. Math.Rev.95e:16040

[58] A.V. KELAREV, *Applications of epigroups to graded ring theory*, Semigroup Forum **50** (1995), no.3, 327–350. Math.Rev.96a:16044

[59] A.V. KELAREV, *On groupoid graded rings*, *J. Algebra*, **178** (1995), no.2, 391-399. Math.Rev.96i:16063

[60] A.V. KELAREV, *Artinian band sums of rings*, J. Austral. Math. Soc. Series A **58** (1995), no.1, 66–72. Math.Rev.96c:16054

[61] A.V. KELAREV, *Semisimple rings graded by inverse semigroups*, *J. Algebra*, **205** (1998), no.2, 451–459.

[62] A.V. KELAREV, *Recent results and open questions on radicals of semigroup-graded rings*, Fund. Appl. Math. **4** (1998), no.2, to appear.

[63] A.V. KELAREV and J. OKNIŃSKI, *The Jacobson radical of graded PI−rings and related classes of rings*, J. Algebra **186** (1996), no.3, 818–830. Math.Rev.97j:16032

[64] J. KNOPFMACHER, "Abstract Analytic Number Theory", North-Holland Mathematical library **12**, North-Holland Publ. Co., 1975. Math.Rev.54#7404

[65] V.L. KURAKIN, A.S. KUZMIN, A.V. MIKHALEV and A.A. NECHAEV, *Linear recurring sequences over rings and modules*, J. of Math. Sci. **76** (1995), no.6, 2793–2915. Math.Rev.97a:11201

[66] P. LANDROCK and O. MANZ, *Classical codes as ideals in group algebras*, Des. Codes Cryptogr. **2** (1992), no.3, 273–285. Math.Rev.93i:94017

[67] L.C.A. VAN LEEUWEN, *Complements of radicals in the class of hereditarily artinian rings*, Acta Sci. Math. (Szeged) **39** (1977), no.3-4, 313–318. Math.Rev.58#10990

[68] R. LIDL and G. PILZ, "Applied Abstract Algebra", Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1984. Math.Rev.86d:00002

[69] R.LIDL, R.W. MATTHEWS and R. WELLS, "Galois Algebra Package", Department of Mathematics, University of Tasmania, G.P.O. Box 252-37, Hobart, Tasmania, 7001, Australia, Copyright 1987.

[70] F.J. MACWILLIAMS and N.J.A. SLOANE, "The Theory of Error-Correcting Codes", North-Holland Mathematical Library **16**, North-Holland, Amsterdam, 1977. Math.Rev.57#5408ab

[71] B.R. MCDONALD "Finite Rings with Identity", Pure and Applied Mathematics **28**, Marcel Dekker Inc., New York, 1974. Math.Rev.50#7245

[72] W.D. MUNN, *A class of band-graded rings*, J. London Math. Soc. **45** (1992), no.1, 1–16. Math.Rev.93d:16059

[73] M. NAGATA "Local Rings", Interscience Tracts in Pure and Applied Mathematics **13**, John Wiley & Sons, New York, 1962. Math.Rev.27#5790

[74] C. NASTASESCU and F. VAN OYSTAEYAN, "Graded and filtered rings and modules", Lecture Notes in Mathematics **758**, Springer, Berlin, 1979. Math.Rev.80k:16002

[75] C. NASTASESCU, *Strongly graded rings of finite groups*, Comm. Algebra, **11**, (1983), no.10, 1033–1071. Math.Rev.84k:16004

[76] C. NASTASESCU and S. DASCALESCU, *Graded $T-$rings*, Comm. Algebra, **17** (1989), no.12, 3033–3042. Math.Rev.91a:16028

[77] J. OKNIŃSKI, "Semigroup Algebras", Monographs and Textbooks in Pure and Applied Mathematics, **138**, Marcel Dekker, New York, 1991. Math.Rev.92f:20076

[78] D.S. PASSMAN, *Radicals of twisted group rings II*, Proc. London Math. Soc. **22** (1971), no.3, 633–651. Math.Rev.45#2041

[79] M. PETRICH, "Inverse Semigroups", Pure and Applied Mathematics, John Wiley & Sons Inc., New York, 1984. Math.Rev.85k:20001

[80] R.S. PIERCE, "Associative Algebras", Graduate Texts in Mathematics **88**, Springer-Verlag, New York, 1982. Math.Rev.84c:16001

[81] A. POLI, *Important algebraic calculations for n-variables polynomial codes*, Discrete Math. **56** (1985), no.2-3, 255–263. Math.Rev.87f:94041

[82] L. ROWEN, "Ring Theory v.I", Pure and Applied Mathematics **127**, Academic Press, Inc., Boston, MA, 1988. Math.Rev. 89h:16001

[83] A.D. SANDS, *Strong upper radicals*, Quart. J. Math. Oxford (2)**27** (1976), no.105, 21–24. Math.Rev.53#509

[84] A.D. SANDS, *A characterisation of semisimple classes*, Proceedings of the Edinburgh Mathematical Society **24** (1981), no.1, 5–7. Math.Rev.83b:16006

[85] L.N. SHEVRIN and E.V. SUKHANOV, *Structural aspects of the theory of varieties of semigroups*, Izv. VUZ. Matematika (1989) no.6, 3–39; Soviet Math. Izv. VUZ **33** (1990), no.6, 1–34. Math.Rev.91a:20071

[86] L.N. SHEVRIN and M.V. VOLKOV, *Identities of semigroups*, Izv. VUZ. Matematika (1985) no.11, 3–47; Soviet Math. Izv. VUZ **29** (1985), no.11, 1–64. Math.Rev.87f:20094

[87] P.N. STEWART, *Semi-simple radical classes*, Pacific J. Math. **32** (1970), 249–254. Math.Rev.41#254

[88] M.L. TEPLY, E.G. TURMAN and A. QUESADA, *On semisimple semigroup rings*, Proc. Amer. Math. Soc. **79** (1980), no.2, 157–163. Math.Rev.81f:20094

[89] S.A. VANSTONE and P.C. VAN OORSCHOT, "An Introduction of Error Correcting Codes with Applications", The Kluwer International Series in Pure and Applied Mathematics, Kluwer Academic Publishers, Boston, 1989.

[90] H.N. WARD, *Visible codes*, Arch. Math. **54** (1990), no.3, 307–312. Math.Rev.90m:94042

[91] P. WAUTERS and E. JESPERS, *Rings graded by an inverse semigroup with finitely many idempotents*, Houston J. Math. **15** (1989), no.2, 291–304. Math.Rev.91a:16029

[92] P. WAUTERS, *Rings graded by a semilattice—applications to semigroup rings*, "Groups and semigroup rings", North-Holland Math. Stud., **126**, (1986), 253–267 Math.Rev.87k:20106

[93] A. WIDIGER and R. WIEGANDT, *Theory of radicals for hereditarily Artinian rings*, Acta Sci. Math. (Szeged) **39** (1977), no.3-4, 303–312. Math.Rev.58#16748

[94] R. WIEGANDT, *Radical theory of rings*, The Mathematics Student **51** (1983), no.1-4, 145–185. Math.Rev.90m:16013

[95] R.S. WILSON, *On the structure of finite rings*, Compositio Math. **26** (1973), no.1, 79–93. Math.Rev.47#8606

[96] O. ZARISKI and P. SAMUEL, "Commutative Algebra v.I", Van Nostrand, Princeton, New Jersey, 1958. Math.Rev.19#833, *reprinted in* Graduate Texts in Mathematics **28**, Springer-Verlag, 1975.

[97] E.I. ZEL'MANOV, *Semigroup algebras with identities*, Siberian Math. J. **18** (1977), no.4, 787-798. Math.Rev.58#6022

Index