Acta Math. Univ. Comenianae
Vol. LXVIII, 1(1999), pp. 77–84

ON FINITE PRINCIPAL IDEAL RINGS

J. CAZARAN AND A. V. KELAREV

ABSTRACT. We find new conditions sufficient for a tensor product $R \otimes S$ and a quotient ring Q/I to be a finite commutative principal ideal ring, where Q is a polynomial ring and I is an ideal of Q generated by univariate polynomials.

1. Main Results

Finite commutative rings are interesting objects of ring theory and have many applications in combinatorics. For these applications it is often important to know when a ring is a principal ideal ring. Let us give only one example. Many classical error-correcting codes are ideals in finite commutative rings. The existence of single generators in ideals is important for computer storage as well as for encoding and decoding algorithms (see [**9**]).

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 principal ideal ring. This question has been considered in the literature for several ring constructions. For example, a complete description of commutative semigroup rings which are PIR's was obtained in [**5**]. All graded commutative principal ideal rings were described in [**4**].

This paper is devoted to two ring constructions which are important, general and lead to interesting results.

All rings considered are commutative and have identity elements. We write $\otimes$ for $\otimes_{\mathbb{Z}}$.

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.

Received May 21, 1998.
1980 *Mathematics Subject Classification* (1991 *Revision*). Primary 13F10, 13F20.
The authors were supported by two grants of Australian Research Council.

Theorem 1. *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 and S_p is a direct product of Galois rings.*

Let R be a finite ring, $Q = R[x_1, \dots, x_n]$ a polynomial ring. Our second main theorem describes all rings of the form

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

which are finite principal ideal rings. This gives a generalization of the main result of [**7**]. Theorem 1 is used in the proof of Theorem 2. Ideals of the form $(f_1(x_1), \dots, f_n(x_n))$ are called **elementary ideals** (see [**8**, 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 $g_1, \dots, g_k$ 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. Then $m > 1$, because $(\mathbb{Z}/p\mathbb{Z})[y]/(g(y))$ is a field, given that $g(y)$ is irreducible modulo p. 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

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

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

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

If the ideals of a ring form a chain, then it is called a **chain ring** (see [**6**, p. 184]). By Lemma , every finite local principal ideal ring and every field is a chain ring. A finite direct product is a PIR if and only if all its components are PIRs (see [**12**, Theorem 33]). Since every finite PIR is a direct product of chain rings (see [**10**, §6]), the general problem of describing all polynomial rings

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

which are finite PIRs reduces to the case where R is a chain ring. It follows from [**10**, Theorem 13.2(c)], that Q is finite if and only if all the $f_i(x_i)$ are regular and then we can assume that all the $f_i(x_i)$ are monic by [**10**, Theorem 13.6]. The following theorem gives new conditions sufficient for Q to be a PIR.

Theorem 2. *Let R be a finite commutative chain ring, and let $f_1, \dots, f_n$ be univariate monic polynomials over R. Then*

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

is a principal ideal ring and all rings $R[x_i]/(f_i(x_i))$ are PIRs, 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, the number of polynomials $f_1, \dots, f_n$ 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.*

2. Proofs

The radical of a finite ring R is the largest nilpotent ideal $\mathcal{N}(R)$.

Lemma 3. *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 [**1**, Proposition 8.8]. □

Lemma 4. *Let F be a finite field, $P = F[x_1, \dots, x_n]$, and let I be the ideal generated by $f_1(x_1), \dots, f_n(x_n)$. Then the radical of P/I is equal to the ideal generated by the squarefree parts of all polynomials $f_1, \dots, f_n$.*

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 [**2**, §8.2]. □

The ring $GR(p^n, r)$ is well defined independently of the monic polynomial of degree r (see [**10**, §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. For any $f, g \in GR(p^n, r)[x]$, it is clear that $\overline{f} = \overline{g}$ if and only if $f' = g'$. The following lemma shows that a tensor product of Galois rings is a PIR.

Lemma 5. ([**10**, Theorem 16.8]) *Let p be a prime, k_1, k_2, r_1, r_2 positive integers, and let $k = \min\{k_1, k_2\}$, $d = \gcd(r_1, r_2)$, $m = \mathrm{lcm}\,(r_1, r_2)$. 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 6. ([**10**, 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 principal ideal ring;*
(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 $GR(p^m, r)$.

Also, the characteristic of R is p^m and its residue field is $R/\mathcal{N}(R) \cong GF(p^r)$. The polynomial $g(x)$ which occurs in Lemma 6 is called an **Eisenstein polynomial**.

Lemma 7. *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 8. ([**10**, 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 9. *If R is a Galois ring, and S is a chain ring, then $R \otimes S$ is a PIR.*

Proof. Let $\operatorname{char}(R) = p^m$, $\operatorname{char}(S) = q^n$, 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 $(g) \subseteq \mathcal{N}(R \otimes S)$. It is noted in the proof of Lemma 7 that $p \in gS$, and so $p \in (g)$. Since $S/gS \cong GF(p^u)$ and $R/pR \cong GF(p^v)$, for some u, v, we get $(R \otimes S)/(g) \cong GF(p^u) \otimes GF(p^v) \cong \prod_1^d GF(p^w)$ where $w = \operatorname{lcm}\{u, v\}$ and $d = \gcd\{u, v\}$, by Lemma 5. Therefore $(g) = \mathcal{N}(R \otimes S)$. By Lemma 3, $R \otimes S$ is a PIR. □

Lemma 10. *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 6 $R \cong GR(p^u, q)[x]/(x^s + ph(x), p^{u-1}x^t)$. 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 5 $GF(p^q) \otimes GF(p^r)$ 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 [**6**, Proposition 38.4(b)]. This contradiction completes the proof. □

Proof of Theorem 1. 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 9 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 10. Thus at least one of the rings R_p and S_p must be a product of Galois rings. □

Lemma 11. *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 4 shows that $f(x)$ is squarefree modulo p if and only if Q/pQ is semisimple, i.e., $\mathcal{N}(Q) = pQ$. By Lemma 8 this is equivalent to Q being a direct product of Galois rings. □

Lemma 12. *Let $R = GR(p^m, r)$ be a Galois ring, where $m > 1$, let $f(x)$ be a monic polynomial over R which is not squarefree modulo p, and let $Q = R[x]/(f(x))$. Then Q is a PIR 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 4 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 $p^{m-1} \in \overline{(g,f)}$ 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 $f' - \mathrm{UP}\,(f)\,\mathrm{SP}\,(f) = p[(f' - \mathrm{UP}\,(f)\,\mathrm{SP}\,(f))''] + p^2u$ 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. □

Lemma 13. *Let R be a chain ring 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 6 $R \cong GR(p^m, r)[y]/(y^s + ph(y), p^{m-1}y^t)$. Since R is not a Galois ring, evidently $s \geq 2$. Lemma 7 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 4. Thus $\mathcal{N}(Q)$ is a principal ideal. Lemma 3 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 11 and Lemma 8 both imply that $GF(p^r)[y]/(y^s)$ is not a direct product of Galois rings. By Lemma 8 $GF(p^r)[x]/(\overline{f(x)})$ must be a direct product of Galois rings. Lemma 11 completes the proof. □

Proof of Theorem 2. The ring Q is isomorphic to the tensor product of the rings $R[x_i]/(f_i(x_i))$, for $i = 1, \dots, n$.

(i): Suppose that R is a field of characteristic p. Then all the $R[x_i]/(f_i(x_i))$ are PIRs. Theorem 1 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 11 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 12 all $R[x_i]/(f_i(x_i))$ are PIRs 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 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 8, we see that each $R[x_i]/(f_i(x_i))$ is not a direct product of Galois rings. Theorem 1 shows that $n = 1$. By Lemma 13 Q is a PIR if and only if $f_1(x_1)$ is squarefree modulo p. □

For finite rings, our Theorem 2 immediately gives the following Theorem 1 of [**7**].

Corollary 14. ([**7**]) *Let F be a field of characteristic $p > 0$, $a_1, \dots, a_n$ non-negative integers, $b_1, \dots, b_n$ positive integers, and let*

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

then R is a principal ideal ring if and only if one of the following conditions is satisfied:

(1) *$a_1, \dots, a_n \le 1$ and p divides at most one number among $b_1, \dots, b_n$;*
(2) *exactly one of $a_1, \dots, a_n$, say a_1, is greater than 1 and p does not divide each of $b_2, \dots, b_n$.*

Proof. Consider the polynomial $f = x^a(1 - x^b)$. By [**2**, Lemma 2.85], a polynomial is squarefree if and only if it is coprime with its derivative. Since char $F = p > 0$, then f is squarefree if and only if $a = 1$ and p does not divide b. Thus Theorem 2 completes the proof. □

References

1. Atiyah M. and McDonald I., *Introduction to Commutative Algebra*, Addison-Wesley Pub. Co., 1969.

2. Becker T. and Weispfenning V., *Gröbner Bases. A Computational Approach to Commutative Algebra*, Springer-Verlag, 1993.

3. Cazaran J. and Kelarev A. V., *Generators and weights of polynomial codes*, Archiv Math. (Basel) **69** (1997), 479–486.

4. Decruyenaere F. and Jespers E., *Graded Commutative Principal Ideal Rings*, Bull. Belg. Math. Soc. Ser. B **43** (1991), 143–150.

5. Decruyenaere F., Jespers E. and Wauters P., *On Commutative Principal Ideal Semigroup Rings*, Semigroup Forum **43** (1991), 367–377.

6. Gilmer R., *Multiplicative Ideal Theory*, Marcel Dekker Inc., New York, 1972.

7. Glastad B. and Hopkins G., *Commutative semigroup rings which are principal ideal rings*, Comment. Math. Univ. Carolinae **21** (1980), 371–377.

8. Kurakin V. L., Kuzmin A. S., Mikhalev A. V. and Nechaev A. A., *Linear recurring sequences over rings and modules*, Journal of Mathematical Sciences **76(6)** (1995), 2793–2915.

9. Landrock P. and Manz O., *Classical codes as ideals in group algebras*, Des. Codes Cryptogr. **2(3)** (1992), 273–285.

10. McDonald B. R., *Finite Rings with Identity*, Marcel Dekker, New York, 1974.

11. Nagata M., *Local rings*, John Wiley & Sons, New York, 1962.

12. Zariski O. and Samuel P., *Commutative Algebra*, Van Nostrand, Princeton, New Jersey, 1958.

J. Cazaran, Department of Mathematics, University of Tasmania, G.P.O. Box 252-37, Hobart, Tasmania 7001, Australia; *e-mail*: cazaran@hilbert.maths.utas.edu.au

A. V. Kelarev, Department of Mathematics, University of Tasmania, G.P.O. Box 252-37, Hobart, Tasmania 7001, Australia; *e-mail*: kelarev@hilbert.maths.utas.edu.au