Tensor Products and Quotient Rings which are Finite Commutative Principal Ideal Rings

Jilyana Cazaran*

*Louisiana State University

Copyright ©1999 by the authors. Mathematical Journal of Okayama University is produced by The Berkeley Electronic Press (bepress). http://escholarship.lib.okayama-u.ac.jp/mjou
Tensor Products and Quotient Rings which are Finite Commutative Principal Ideal Rings

Jilyana Cazaran

Abstract

We give structure theorems for tensor products $R \oplus S$, and quotient rings $Q/I$ to be finite commutative principal ideal rings with identity, where $Q$ is a polynomial ring and $I$ is an ideal of $Q$ generated by univariate polynomials. We also show when $Q/I$ is a direct product of finite fields or Galois rings.

KEYWORDS: finite commutative rings, principal ideal rings, tensor products.
TENSOR PRODUCTS AND QUOTIENT RINGS WHICH ARE FINITE COMMUTATIVE PRINCIPAL IDEAL RINGS

JILYANA CAZARAN

Abstract. We give structure theorems for tensor products $R \otimes S$, and quotient rings $Q/I$ to be finite commutative principal ideal rings with identity, where $Q$ is a polynomial ring and $I$ is an ideal of $Q$ generated by univariate polynomials. We also show when $Q/I$ is a direct product of finite fields or Galois rings.

Finite commutative rings with identity are nice examples of Artinian rings, [5], and they have applications in combinatorics. A ring $R$ is called a principal ideal ring (abbreviated PIR) if, for any ideal $I$ of $R$, there exists $x \in I$ such that $I = Rx = xR$, [6]. We consider when a finite commutative ring with identity is a PIR. These PIRs are useful to define as error-correcting codes, [2], [3] and [10].

We give structure theorems for tensor products and quotient rings, and all rings considered are commutative with identity. Theorem 1.11 gives a necessary condition for a tensor product $R \otimes S$ to be a finite PIR, where $R$ and $S$ are not assumed to be PIRs. Let $Q = R[x_1, \ldots, x_n]$, where $R$ is a finite principal ideal ring and $I$ is an ideal of $Q$ generated by univariate polynomials. Theorem 2.1 gives conditions for $Q/I$ to be a finite principal ideal ring. Theorem 2.11 shows when $Q/I$ is a direct product of finite fields or Galois rings.

This paper is a continuation of the results given in [3] and [4].

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

$$R_p = \{ r \in R \mid p^k r = 0 \text{ for some positive integer } k \}.$$
If the ideals of a ring form a chain, then it is called a chain ring (see [8, p.184]). By Lemma 1.3, 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 1.1** ([4, Lemma 3]). A finite ring is a PIR if and only if its radical is a principal ideal.

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 $(\mathbb{Z}/(p^m))[x]/(f(x))$, where $p$ is a prime, $m$ an integer, and $f(x) \in \mathbb{Z}/(p^m)[x]$ is a monic polynomial of degree $r$ which is irreducible modulo $p$. If $R = GR(p^m, r) = (\mathbb{Z}/(p^m))[y]/(g(y)) \neq 0$ is a Galois ring which is not a field, then $m > 1$, because $(\mathbb{Z}/(p))[y]/(g(y))$ is a field, given that $g(y)$ is irreducible modulo $p$.

The ring $GR(p^n, r)$ is well defined independently of the monic polynomial of degree $r$ (see [12, §16]).

Notice that $GR(p^m, 1) \cong \mathbb{Z}/(p^m)$ and $GR(p, r) \cong GF(p^r)$, the finite field of order $p^r$. Lemma 1.2, first proved in [14], shows that a tensor product of Galois rings is a PIR.

**Lemma 1.2** ([12, Theorem 16.8]). Let $p$ be a prime, $k_1, k_2, r_1, r_2$ positive integers, and let $k = \min\{k_1, k_2\}$, $d = \gcd(r_1, r_2)$, $m = \text{lcm}(r_1, r_2)$.

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 1.3** ([12, Theorem 17.5]). Let $R$ be a finite commutative ring which is not a field. Then the following conditions are equivalent:

1. $R$ is a chain ring;
2. $R$ is a local PIR;
3. 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 $R$, $t = n - (m - 1)s > 0$, $g(x) = x^n + ph(x)$, $\deg(h) < s$, and the constant term of $h(x)$ is a unit in $GR(p^m, r)$.}

http://escholarship.lib.okayama-u.ac.jp/mjou/vol41/iss1/3
Let $R$ be a chain ring as defined in Lemma 1.3(3). The characteristic of $R$ is $p^m$ and its residue field is $R/N(R) \cong GF(p^r)$. 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 1.4, $R$ is a Galois ring if and only if $s = 1$.

**Lemma 1.4** ([12, 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 1.5** ([4, Lemma 9]). If $R$ is a Galois ring, and $S$ is a chain ring, then $R \otimes S$ is a PIR.

**Lemma 1.6** ([4, Lemma 10]). Let $R$ and $S$ be chain rings which are not Galois rings, and let $\text{char}(R) = p^m$, $\text{char}(S) = p^n$, for a prime $p$ and positive integers $m, n$. Then $R \otimes S$ is not a PIR.

**Theorem 1.7** ([4, 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 $R_p$ or $S_p$ is a direct 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 1.2,

$$R_p \otimes S_p = \mathbb{Z}/(p) \otimes (GR(p^m, r)[x]/(x^s)) \cong (\mathbb{Z}/(p) \otimes GR(p^m, r))[x]/(x^s) \cong GF(p^r)[x]/(x^s) \cong S_p/pS_p.$$

By Lemma 1.3, $S_p$ 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 $r, s \geq 1$.

This provides motivation to prove Lemma 1.9, which relies on Lemma 1.8.

**Lemma 1.8** ([12, Theorem 17.1, p.337-338]). Let $R$ be a finite local ring satisfying $\text{char}(R) = p^m$ for a prime $p$ and positive integer $m$. If $N(R)$ 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 $R/N(R) \cong GF(q^r)$.

**Lemma 1.9.** Let $R$ and $S$ be finite local rings satisfying $\text{char}(R) = p^m$, $\text{char}(S) = p^n$, 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 $N(S)$ has a minimum of $k$ generators then by Lemma 1.8, $S \cong \mathbb{Z}/(p^n)[x_1, \ldots, x_k]/J$ 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 $$J' \cong J/pJ. \quad (R \otimes S)/p(R \otimes S) \to (R/pR) \otimes (S/pS) = \text{bar}.$$
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 1.7. Assume that $R$ and $S$ are not both PIRs. Since $R \otimes S$ is a PIR, 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 1.5 and 1.6, $R_p$ or $S_p$ must be a Galois ring. If $R_p$ and $S_p$ are not both PIRs, then by Lemma 1.10, $R_p$ 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 1.6. Thus at least one of the rings $R_p$ or $S_p$ is a direct product of Galois rings. □

Theorem 1.11 could only provide a necessary condition for $R \otimes S$ to be a finite commutative PIR. We give necessary and sufficient conditions for this to be true in Lemmas 1.13 and 1.14 in the special case when $R \otimes S$ is a direct product of either Galois rings or finite fields. Lemma 1.12 is required for Lemmas 1.13, 1.14 and Corollary 2.8. Lemma 1.5 follows from Lemma 1.12.

Lemma 1.12. Let $R$ be a direct product of Galois rings and $S$ be a PIR. Then $R \otimes S$ is a PIR. If $N(S) = gS$ for some generator $g \in S$, then $N(R \otimes S) = g(R \otimes S)$, the ideal generated by $g$ in $R \otimes S$.

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 $(g) = g(R \otimes S)$. Since $(g)$ is nilpotent, $(g) \subseteq N(R \otimes S)$. If $R$ is not a finite field, it follows from Lemma 7 of [4] that $p \in gS$, and so $p \in (g)$. Since $S/gS$ and $R/pR$ are direct products of finite fields, by Lemma 1.2, so is $(R \otimes S)/(g)$. Therefore $(g) = N(R \otimes S)$. By Lemma 1.1, $R \otimes S$ is a PIR.

Lemma 1.13. Let $R$ and $S$ be finite rings satisfying $\text{char}(R) = p^m$, $\text{char}(S) = q^n$, 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 immediate by Lemma 1.2, since tensor product distributes over direct products.

The ‘only if’ part. Since $R \otimes S$ is a PIR, by Theorem 1.11, either $R$ or $S$ is a direct product of Galois rings. Assume that $R$ is a direct product of Galois rings. If $S/pS$ is not a PIR, then by Lemma 1.9, neither is $R \otimes S$, so $S/pS$ must be a PIR.

Assume that $S$ is a PIR. Since $R \otimes S$ is a direct product of Galois rings, by Lemma 1.4, $N(R \otimes S) = p(R \otimes S)$ and $N(R) = pR$. If $N(S) = gS$ for some generator $g \in S$ then by Lemma 1.12, $N(R \otimes S) = g(R \otimes S)$. By Lemma 1.4, $g = p$, so $S$ must be a direct product of Galois rings.

Now assume that $S$ is not a PIR. By Lemma 1.10, $S/pS$ is a PIR such that, as a direct product of local rings, no factor of $S/pS$ is a Galois ring. By Lemma 1.3, each factor of $S/pS$ is of the form $GF(p^r)[x]/(x^{s_i})$
for some integers \( r \geq 1, s_i \geq 2 \). Since \( R/pR \) is a direct product of finite fields, \((R/pR) \otimes (S/pS)\) must contain a factor of the form \( T = GF(p^t) \otimes (GF(p^{em(t,r)})[x]/(x^{s_1})) \) by Lemma 1.2.

The class of finite direct products of Galois rings is closed for homomorphic images by Lemma 1.4. The same is true for a finite direct product of finite fields such as \((R \otimes S)/p(R \otimes S)\). Therefore since \((R/pR) \otimes (S/pS)\) is a homomorphic image of \((R \otimes S)/p(R \otimes S)\), it must be a finite direct product of finite fields. Since \( T \) is not a direct product of finite fields this contradiction implies that \( S \) must be a PIR. Therefore \( S \) must be a direct product of Galois rings.

**Lemma 1.14.** Let \( R \) and \( S \) be finite rings satisfying \( \text{char}(R) = p^m \), \( \text{char}(S) = p^n \), 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 immediate by Lemma 1.2, since tensor product distributes over direct products.

The ‘only if’ part. By Lemma 1.13, \( R \) and \( S \) are direct products of Galois rings. By Lemma 1.12, \( \mathcal{N}(R \otimes S) = g(R \otimes S) \), and \( \mathcal{N}(S) = gS \) for some generator \( g \in S \). Since \( R \otimes S \) is a direct product of finite fields, \( \mathcal{N}(R \otimes S) = 0 = \mathcal{N}(S) \), 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 1.2. This contradiction implies that \( R \) is a direct product of finite fields. \( \square \)

We now give a more general version of Lemma 1.1 for a local ring.

**Lemma 1.15.** If \( R \) is a local ring with maximal ideal \( m \), which is not necessarily Noetherian but satisfies \( \cap_n m^n = 0 \), then the following conditions on \( R \) are equivalent:

1. \( m \) is principal;
2. \( R \) is a PIR;
3. \( R \) is a chain ring, hence \( R \) is Noetherian.

**Proof.** (3)\( \implies \) (2) Let \( \pi \in m \setminus m^2 \). Since \( R \) is a chain ring, \( \pi \notin m^e \) for \( e > 1 \). So \( (\pi) \neq m^e \) for \( e > 1 \), and \( (\pi) = m \). Now since all ideals are of the form \( m^e = (\pi^e) \), \( R \) is a PIR.

(2)\( \implies \) (1) is immediate.

(1)\( \implies \) (3) This is similar to the proof of Theorem 31.5 in [13]. Let \( m = (\pi) \). Then \( m^e = (\pi^e) \) for all \( e \geq 1 \). Since \( \cap_n m^n = 0 \) and every ideal \( a \) satisfies \( a \subseteq m \), for some \( e \geq 1 \), \( a \subseteq m^e \) and \( a \nsubseteq m^{e+1} \). For ideals \( a, b, c \) of a ring \( R \), \( a \subseteq c \iff a : b \subseteq c : b \), \( a \nsubseteq (\pi^{e+1}) \) implies \( a : (\pi^e) \nsubseteq (\pi^{e+1}) : (\pi^e) = (\pi) \), hence \( a : (\pi^e) = R \). Since \( (a : b) = R \) implies \( b \subseteq a \), we see \( (\pi^e) \subseteq a \), and
hence \( a = (\pi^e) = \mathfrak{m}^e \). As every ideal of \( R \) is a power of \( \mathfrak{m} \), \( R \) is a chain ring.

\[ \square \]

2. Quotient rings of polynomial rings

For a finite commutative ring \( R \), \( Q = R[x_1, \ldots, x_n] \) is a polynomial ring over \( R \). The following theorem describes 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 [9]. Theorem 1.7 is used in the proof of Theorem 2.1. Ideals of the form \( (f_1(x_1), \ldots, f_n(x_n)) \) are called elementary ideals (see [11, Definition 1.14]). Some definitions are needed before we can state these results.

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

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

\[ B = \{ a y^b \mid \text{where } 0 < a < p \text{ and } 0 \leq b < r \} \]

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

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

Recall the definition of \( \overline{f} \) which follows Lemma 1.1. For any \( f \in R[x] \), there exists a unique basic polynomial \( \text{SP}(f) \in R[x] \) such that \( \overline{\text{SP}(f)} = \text{SP}(\overline{f}) \). Therefore there exists a unique basic polynomial \( \text{UP}(f) \in R[x] \) such that \( \overline{\text{SP}(f) \text{UP}(f)} \) or, equivalently, \( f' - \text{SP}(f) \text{UP}(f) \in pR[x] \). Since \( f' \) is basic, \( (f')'' = 0 \) for any \( f \), and so \( (f' - \text{SP}(f) \text{UP}(f))'' = -(\text{SP}(f) \text{UP}(f))'' \). So we introduce the following notation

\[ \hat{f} = f'' + (f' - \text{SP}(f) \text{UP}(f))'' = \overline{f'' - (\text{SP}(f) \text{UP}(f))''}. \]

For any \( f, g \in GR(p^m, r)[x] \), 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 [12, 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 our theorems hold for regular polynomials \( f(x) \). However, for simplicity, we assume that these polynomials are monic.

A finite direct product of rings is a PIR if and only if all its components are PIRs (see [15, Theorem 33]). Every finite PIR is a direct product.
of chain rings (see [12, §6]). 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. From [12, Theorem 13.2(c)] , \( Q \) is finite if and only if all the \( f_i(x_i) \) are regular. Theorem 2.1 gives necessary and sufficient conditions for \( Q \) to be a PIR. The sufficient conditions were proved in [4, Theorem 2].

**Theorem 2.1.** 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 \( R_i = R[x_i]/(f_i(x_i)) \) for \( 1 \leq i \leq n \) are PIRs, if and only if one of the following conditions is satisfied:

1. \( R \) is a field and the number of polynomials \( f_i \) which are not squarefree does not exceed one;
2. \( R \) 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 \( \hat{f} \) is coprime with \( \overline{\text{UP}(f)} \);
3. \( R \) 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 2.2** ([4, 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 \( p \).

**Lemma 2.3.** 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 \( \overline{\text{UP}(f)} \) is coprime with \( \hat{f} \).

**Proof.** When \( \hat{f} \) is not squarefree, we get \( \overline{\text{UP}(f)} \neq 0 \) and \( \text{SP}(f) \neq 0 \).

Suppose that \( \hat{f} \) is coprime with \( \overline{\text{UP}(f)} \). Denote by \( h \) a basic polynomial in \( R[x] \) such that \( \hat{h} \) is the product of all irreducible divisors of \( \hat{f} \) which do not divide \( \hat{f} \). Let \( g = \text{SP}(f) + ph \in R[x] \). It is proved in [4, Lemma 12] that the radical \( \mathcal{N}(Q) \) is equal to the ideal \( I \) generated in \( Q \) by \( g \).

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

Since \( (\overline{g}) = (\overline{\text{SP}(f)}) = \mathcal{N}(\mathbb{Z}/(q)[x]/(\overline{f})) \), we get \( \overline{g} = t\overline{\text{SP}(f)} + e\overline{f} \) for some \( t = t' \in R \) and \( e(x) \in R[x] \). There exists an integer \( s = s' \in R \) such that \( ts \equiv 1 \mod p \). Since \( s(g - ef) = st\overline{\text{SP}(f)} = \overline{\text{SP}(f)} = \overline{\text{SP}(f)} \) and
Given \( p \in \mathcal{N}(Q) \), we get \( p = vf + wg \) for some \( v, w \in R[x] \). Since 
\[ (vf + wg)' = (vf' + w'g)' = 0, \]
It follows that 
\[ w' = -w' UP(f), \]
whence 
\[ w' = -w' UP(f) + pz \]
for some \( z = z' \in R[x] \).

Further, 
\[ (v' + pv'')(f' + pf'') + (w' + pw'')(g' + pg'') = 0. \]
So we see
\[ T = v'(-v' UP(f)g')' + f'' + UP(f)(v'g'') + \bar{v}''(v''(UP(f)g')' + g'(z + w'')). \]

Since all irreducible factors of \( UP(f) \) divide \( g' = SP(f) \), they also divide the polynomial 
\[ UP(f)(v'g'') + v''UP(f)g' + g'(z + w''). \]
So we see that \( UP(f) \) must be coprime with \( \hat{f} \). This completes the proof.

**Example 2.4.** We demonstrate Lemma 2.3 in the case \( Q \) is a finite local ring. Let \( R = GR(p^n, r) \). 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 \( B \to GF(p^r) \).

Notice that \( B \) is not the isomorphic copy of \( GF(p^r) \) contained in \( R \). For example, if \( R = \mathbb{Z}/(3^2) \), then \( B = \{0, 1, 2\} \subset \{0, 1, 2, \ldots, 8\} = R, R/(\mathcal{N}(R)) \cong GF(3) = \{0, 1, 2\}, \) yet \( F = \{0, 3, 6\} \) is the isomorphic copy of \( GF(3) \) contained in \( R \).

Let \( R = GR(p^n, r) \) and let \( e \in R[x] \) be a monic irreducible polynomial \( (12, p.254) \). Let \( f = e^n \) for some integer \( n \geq 1 \) and \( Q = R[x]/(f) \). By [12, Theorem 13.7(b)], \( c \in GF(p^r)[x] \) and an integer \( \ell \geq 1 \). Therefore 
\[ \bar{SP}(f) = SP(f) = c, \]
and \( \bar{SP}(f) = c_b \).

Now as \( c^{\ell n} = \bar{f} = \bar{SP}(f) \bar{UP}(f) = c \bar{UP}(f) \), \( \bar{UP}(f) = c^{\ell n - 1} \) and \( \bar{UP}(f) = c^{\ell n - 1} \).

Evidently \( \bar{f} = (e^n)'' + (c^{\ell n - 1})b'' \). It follows from Lemma 2.6 that \( \mathcal{N}(Q) = (c, c_b) \).

Since \( \bar{f} = (e^n) \subseteq (d) \subset F_p^r[x] \), \( Q/\mathcal{N}(Q) = (GR(p^n, r)[x]/(f))/(p, c_b) \cong GF(p^r)[x]/(c) \cong GF(p^r \text{ degree}(c)) \).

Hence \( Q \) is a finite local ring. Therefore, by the Chinese Remainder Theorem for
ideals ([7, 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 [12, 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 \( b \).

**Lemma 2.5 ([4, Lemma 13]).** 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 \( p \).

**Lemma 2.6 ([4, Lemma 4]).** Let \( F \) be a finite field, \( P = F[x_1, \ldots, x_n] \), and let \( I \) be the ideal generated by \( f_1(x_1), \ldots, f_n(x_n) \) in \( P \). 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 of Theorem 2.1.** The ring \( Q \) is isomorphic to the tensor product of the rings \( R_i = R[x_i]/(f_i(x_i)) \), for \( i = 1, \ldots, n \). Since \( \text{char}(R) = p^m \) where \( m = 1 \), if \( R \) is a field, \( R_i = (R_i)_p \) for \( i = 1, \ldots, n \) and \( Q = Q_p \).

(1): Suppose that \( R \) is a field of characteristic \( p \). Then all the \( R_i \) are PIRs. Theorem 1.7 tells us that \( Q \) is a PIR if and only if at least \( n - 1 \) of the rings \( R_i \) are direct products of Galois rings. By Lemma 2.2, this is equivalent to the fact that at most one of the polynomials \( f_i(x_i) \) is not squarefree.

(2): Suppose that \( R \) is a Galois ring. By Lemma 2.3, all \( R_i \) are PIRs if and only if, for each polynomial \( f_i(x_i) \) which is not squarefree modulo \( p \), \( \text{UP}(f_i) \) is coprime with \( \hat{f}_i \). Further, suppose that this condition is satisfied. As in case (1), 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 \( p \).

(3): 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 1.4, we see that each \( R_i \) is not a direct product of Galois rings. Theorem 1.7 shows that \( n = 1 \). By Lemma 2.5, \( Q \) is a PIR if and only if \( f_1(x_1) \) is squarefree modulo \( p \).

Our Theorem 2.1 immediately gives the following Theorem 1 of [9] for finite rings.

**Corollary 2.7 ([9, Theorem 1]).** Let \( F \) be a field of characteristic \( p > 0 \), \( a_1, \ldots, a_n \) nonnegative integers, \( b_1, \ldots, b_n \) positive integers, and let

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

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 [1, Lemma 2.85], a polynomial is squarefree if and only if it is coprime with its derivative. Since \(\text{char}(F) = p > 0\), then \(f\) is squarefree if and only if \(a = 1\) and \(p\) does not divide \(b\). Thus Theorem 2.1 completes the proof. \(\square\)

In our second Corollary to Theorem 2.1, we give an explicit generator \(g\) for the radical of \(Q\) when \(Q\) is a PIR.

**Corollary 2.8.** 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 \(N(S_1) = gS_1\) where \(S_1 = R[x_1]/(f_1(x_1))\). Then \(N(Q) = gQ\) where \(gQ\) is the ideal generated by \(g = g(x_1)\) in \(Q\).

Proof. By Theorem 2.1, \(Q\) is a PIR and \(f_1(x_1)\) is not squarefree modulo \(p\), so the rings \(R_i = R[x_i]/(f_i)\) for \(2 \leq i \leq n\) are Galois rings. By Lemma 1.12, \(S_2 \cong R_2 \otimes S_1\) is a PIR and \(N(S_2) = gS_2\). Repeating this argument with \(S_{i+1} \cong R_{i+1} \otimes S_i\) for \(2 \leq i \leq n - 1\), we get \(N(Q) = gQ\). \(\square\)

Let \(Q\) be the PIR defined in Corollary 2.8. Let \(R\) be a Galois ring which is not a finite field. From the proof of Lemma 2.3, using the ring \(S_1 = R[x_1]/(f(x_1))\), one may choose \(g = \text{SP}(f(x_1)) + ph(x_1)\). Also, if \(f_i(x_i)\) for \(1 \leq i \leq n\) are squarefree modulo \(p\), then either by Lemma 1.2 and Lemma 1.4, or by the same proof as Corollary 2.8, \(N(Q) = pQ\). If \(R\) is a finite field, then \(g = sp(f_1)\), the squarefree part of \(f_1\), generates \(N(Q)\).

Theorem 2.1 provides conditions for the ring \(Q\) to be a PIR. Theorem 2.11 provides similar conditions for \(Q\) to be a special type of PIR. To prove it, Lemmas 1.13, 1.14 and the following two lemmas are required.

**Lemma 2.9.** Let us assume that \(S = R[x]/(f(x))\) is 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 2.2 and 2.5, \(f\) is squarefree modulo \(p\). Assume that \(R\) is not a Galois ring. By Lemma 1.3, \(R \cong GR(p^m, r)[y]/(y^s + ph(y), p^{m-1}y^r)\) for suitable \(h(y)\) and integers \(m, r, t\) where \(s \geq 2\). It follows that \(S/pS \cong GF(p^s)[x, y]/(\overline{f(x)}, h^s) \cong GF(p^s)[x]/(\overline{f(x)}) \otimes GF(p^s)[y]/(y^s)\). Since \(s \geq 2\), \(GF(p^s)[y]/(y^s)\) is a finite chain ring which is not a finite field,
yet $GF(p^r)[x]/(f(x))$ is a direct product of finite fields since $f(x)$ is squarefree. Consider the following ring. For some integer $q \geq 2$, by Lemma 1.2, $GF(p^q) \otimes (GF(p^r)[y]/(y^s)) \cong \prod_{i=1}^{d}(GF(p^i)[y]/(y^s))$, where $d = \gcd(q, r)$ and $l = \text{lcm}(q, r)$. Since this ring is not a direct product of finite fields, neither is $(GF(p^r)[x]/(f(x))) \otimes GF(p^r)[y]/(y^s)) = S/pS$. This is a contradiction, by Lemma 1.4, since $S$ is a direct product of Galois rings. Therefore $R$ must be a Galois ring.

Lemma 2.10. Let us assume that $S = R[x]/(f(x))$ is 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 Lemma 2.9, $f$ is squarefree modulo $p$, and $R \cong GR(p^m, r)$ where $m, r \geq 1$ are integers. Assume that $R$ is not a finite field ($m \geq 2$). Since $f$ is squarefree modulo $p$, $S = R[x]/(f(x))$ is a direct product of Galois rings of characteristic $p^m > p$, which is a contradiction. Therefore $m = 1$. So $R$ is a finite field and $f$ is squarefree.

Theorem 2.11. Let $R$ be a finite commutative chain ring satisfying 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

1. $Q$ is a direct product of finite fields if and only if $R$ is a finite field and all the $f_i$ are squarefree;
2. $Q$ 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 $R_i = R[x_i]/(f_i(x_i))$ for $i = 1, \ldots, n$. Then $Q \cong \otimes_{i=1}^{n} R_i$. Since $R = R_p$, $Q = Q_p$, where $R_p$ is the $p$–component of $R$.

(1) The ‘if’ part. If $R$ is a finite field and $f$ is squarefree, then by the chinese remainder theorem for ideals ([7, Exercise 2.6, p.80]), $R[x]/(f(x))$ is a direct product of finite fields. By Lemma 1.2, a tensor product of finite fields is a direct product of finite fields, so tensor product distributes over direct products. Then $Q$ is a direct product of finite fields.

The ‘only if’ part. By Lemma 1.14, if $R_1 \otimes R_2$ is a direct product of finite fields, then so too are $R_1$ and $R_2$. By iterating this argument, if $Q \cong \otimes_{i=1}^{n} R_i$ is a direct product of finite fields, then so is each $R_i$. By Lemma 2.10, $R$ is a finite field and all the $f_i$ are squarefree.

(2) The ‘if’ part. If $R$ is a Galois ring and $f$ is squarefree modulo $p$, then by Lemma 2.2, $R[x]/(f(x))$ is a direct product of Galois rings. The proof is now identical to (1) replacing ‘finite field’ by ‘Galois ring’, ‘squarefree’ by ‘squarefree modulo $p$’ and using Lemmas 1.13 and 2.9.

Finally, let us consider the case when the ideal $I \triangleleft R[x]$ contains several univariate polynomials $I = (f_1(x), \ldots, f_r(x))$. Let $R$ be a finite local ring.
We say that \( g \in R[x] \) is primary if \((g)\) is a primary ideal in \( R[x] \) (see [12, p.254]). Lemma 2.12 follows from [12], Theorem 13.11.

**Lemma 2.12.** 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, \((g_{i}) = (h_{i}) \triangleleft R[x]\).

For a finite local ring \( R \), 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 \( f_{2} \), for some integer \( s \geq 1 \). Then by Lemma 2.12, \( \gcd(f_{1}, f_{2}) \) is well-defined and is unique up to associates. Similarly \( \gcd(f_{1}, \ldots, f_{r}) \) is defined for \( f_{1}, \ldots, f_{r} \in R[x] \). Then we see that \((\gcd(f_{1}, \ldots, f_{r})) = (f_{1}, \ldots, f_{r}) \). Therefore, the theorems in this paper which are stated for rings of the form \( Q = R[x]/(f_{1}(x)) \) hold for rings of the form \( Q = R[x]/(f_{1}(x), \ldots, f_{r}(x)) \), where the \( f_{i} \) are monic, or more generally, are regular polynomials.

**References**


JILYANA CAZARAN
DEPARTMENT OF MATHEMATICS
LOUISIANA STATE UNIVERSITY
BATON ROUGE, LOUISIANA, 70803-4918, USA

e-mail address: cazaran@math.lsu.edu

(Received March 18, 1999)
(Revised January 24, 2000)