# On the Structure of Finite Completely Primary Rings

*

by

Chiteng'a John Chikunji

*Department of Mathematics & Statistics,*
*The University of Zambia, Lusaka.*

**Abstract**

Let $R$ be any finite Completely Primary Ring and let $b$ be an element of $R$ of multiplicative order $p^r - 1$, where $p$ is a prime and $r$ is a positive integer. Then in this paper we show that there exists a minimal $K_o$-basis for $R$, where $K_o =< b > \cup\{0\}$. We also show that each element of $R$ may be uniquely expressed as a linear combination of the basis elements, and further show that the maximal ideal $\mathcal{M}$ of $R$ has a distinguished $K_o$-basis.

## 1 Introduction

In this paper, all rings are finite, associative and have an identity. A completely primary ring is a ring $R$ in which the set $\mathcal{M}$ of all zero-divisors forms an ideal. Let $R$ be a completely primary ring with maximal ideal $\mathcal{M}$ and Galois subring $R_o$. In [3], Raghavendran showed that $R$ contains an element $b$ of order $p^r - 1$ such that $b + \mathcal{M}$ is a primitive element of $R/\mathcal{M}$. This element plays an important role in the theory of completely primary rings (e.g. see [1]).

In [4], Wilson developed a structure theory for $R_o$-bimodules and Raghavendran proved in [3] that if $V$ is a finite dimensional $(F, F)$-unital module, where $F$ is the Galois field $GF(p^r)$, then, $V$ possesses at least one distinguished basis over $F$ (Theorem 1). Also, in [5], Wirt proved that if $R$ is a completely primary ring and $R_o$ is a coefficient subring of $R$, then there exist $x_1$, ..., $x_k \in \mathcal{M}$ and $\sigma_1$, ..., $\sigma_k \in Aut(R_o)$ such that $R = R_o \oplus \sum_{i=1}^{k} R_o x_i$ and $x_i r = r^{\sigma_i} x_i$, $\forall r \in R_o$ and $\forall i = 1$, ..., $k$.

So in Section 2 of this paper, we collect some preliminary results on completely primary rings and give a slightly different treatment of the element $b$. In Section 3, we collect some facts on $R_o$-bimodules, develop some results on $R$-modules, and reprove Wirt's result using an easier method. In Section 4, we show that there exists a minimal $K_o$-basis for the maximal ideal of $R$, where $K_o =< b > \cup\{0\}$, and prove that every element of $R$ can be expressed uniquely as a linear combination of the basis elements with coefficients in $K_o$. Section 5 deals with more results on $R$-modules and finally extend the work of Raghavendran [3] to all finite completely primary rings by proving the existence of a distinguished $K_o$-basis for the maximal ideal $\mathcal{M}$ of $R$.

## 2 Preliminaries

Let $R$ be a completely primary ring with maximal ideal $\mathcal{M}$. The following results will be assumed (see [3]). Then $|R| = p^{nr}$, $|\mathcal{M}| = p^{(n-1)r}$, $R/\mathcal{M} \cong GF(p^r)$ the finite field of $p^r$ elements and $CharR = p^k$, where $1 \leq k \leq n$, for some prime $p$ and positive integers $n$, $r$, $k$. Moreover, $\mathcal{M}$ is nilpotent and has index of nilpotence $l$ for some $l \leq n$. Thus, $\mathcal{M}$ contains a chain of ideals $\mathcal{M} \supseteq \mathcal{M}^2 \supseteq \ldots \supseteq \mathcal{M}^{l-1} \supseteq \mathcal{M}^l = \{0\}$. If $k = n$, then $R = Z_{p^n}[b]$, where $b$ is an element of $R$ of multiplicative order $p^r - 1$, $\mathcal{M} = pR$ and $Aut(R) \cong Aut(R/\mathcal{M})$. Such a ring is called a *Galois ring* and is denoted by $GR(p^{nr}, p^n)$.

**Proposition 2.1** *Let $R$ be a completely primary ring with maximal ideal $\mathcal{M}$. Then, there exists an element $b \in R$ of multiplicative order $p^r - 1$ such that if $\psi : R \to R/\mathcal{M}$ is a canonical homomorphism, then $\psi(b)$ is a primitive element of $R/\mathcal{M}$ and $K_o =< b > \cup\{0\}$ forms a complete system of coset representatives of $\mathcal{M}$ in $R$. Further, if $\lambda$, $\mu \in K_o$ with $\lambda - \mu \in \mathcal{M}$, then $\lambda = \mu$.*

**Proof** Obviously, the group of units $G_R$ of $R$ is $R-\mathcal{M}$, and $\phi : R \to R/\mathcal{M}$ induces a surjective multiplicative group homomorphism

$$\theta : G_R \to (R/\mathcal{M})^*.$$

Since $Ker\phi = \mathcal{M}$, we have $Ker\theta = 1+\mathcal{M}$. In particular, $1+\mathcal{M}$ is a normal subgroup of $G_R$.

Let $<\beta>=(R/\mathcal{M})^*$ and let $b_o \in \theta^{-1}(\beta)$. Then, the multiplicative order of $b_o$ must be a multiple of $p^r-1$ and a divisor of

$$|R-\mathcal{M}| = p^{nr} - p^{(n-1)r} = p^{(n-1)r}(p^r-1);$$

hence, of the form $p^s(p^r-1)$. But then $b = b_o^{p^s}$ has multiplicative order $p^r-1$ and $\theta(b_o^{p^s}) = \beta^{p^s}$ which is a generator of $(R/\mathcal{M})^*$, since $p^s$ and $p^r-1$ are co-prime.

Further, $\phi(K_o) = R/\mathcal{M}$, and hence, $K_o$ is a complete set of coset representatives of $\mathcal{M}$ in $R$. Hence, $\lambda,\ \mu \in K_o$ with $\lambda-\mu \in \mathcal{M}$ implies that $\lambda = \mu$.

In what follows, $b$ shall be taken to be an element of $R$ satisfying the properties of Proposition 2.1.

Let $R$ be a completely primary ring, $|R/\mathcal{M}| = p^r$ and $CharR = p^k$. Then it can be deduced from the main theorem in [2] that $R$ has a coefficient subring $R_o$ of the form $GR(p^{kr},\ p^k)$ which is clearly a maximal Galois subring of $R$. Moreover, there exist $m_1, m_2, \ldots, m_h \in \mathcal{M}$ and $\sigma_1, \sigma_2, \ldots, \sigma_h \in Aut(R_o)$ such that

$$R = R_o \oplus \sum_{i=1}^{h} \oplus R_o m_i \ (\text{as } R_o - \text{modules}),\ m_i r = r^{\sigma_i} m_i,$$

for every $r \in R_o$ and any $i = 1, \ldots, h$. Moreover, $\sigma_1, \ldots, \sigma_h$ are uniquely determined by $R$ and $R_o$ (see 1.6 in [1]). If $S_o$ is another coefficient subring of $R$ then there exists an invertible element $x$ in $R$ such that $S_o = xR_ox^{-1}$ (see theorem 8 in [3]). Finally, let $R_o$ be a maximal Galois subring of $R$. Then $R_o = \mathbb{Z}_{p^k}[b]$. Let $K_o =< b > \cup\{0\}$. Then it is easy to show that every element of $R_o$ can be written uniquely as $\sum_{i=0}^{k-1} p^i\lambda_i$, where $\lambda_i \in K_o$.

Since $R = R_o \oplus \sum_{i=1}^{h} \oplus R_o m_i$, it is easy to see that $\mathcal{M} = pR_o \oplus \sum_{i=1}^{h} \oplus R_o m_i$.

**Corollary 2.2** *Let $R$ be a completely primary ring. Then every element of $R$ can be expressed uniquely in the form $\lambda + m$ with $\lambda \in K_o$ and $m \in \mathcal{M}$.*

**Proof** This follows easily from Proposition 2.1 since, $\lambda$ being a coset of $\mathcal{M}$ in $R$, the map $\psi : R \to R/\mathcal{M}$ implies that the elements of $R$ are of the form $\lambda + m$ and from the fact that $R = R_o \oplus \sum_{i=1}^{h} \oplus R_o m_i$, and elements of $R_o$ can be uniquely expressed in the form $\sum_{i=0}^{k-1} p^i\lambda_i$, where $\lambda_i \in K_o$.

# 3 Some Module theory over Galois rings

We start with the following:

**Proposition 3.1** *Let $R_o$ be the Galois ring $GR(p^{nr}, p^n)$ and let $M$ be a finite $R_o$-bimodule. Then, there exist $x_1,\ \ldots,\ x_k \in M$ such that*

$$M = R_o x_1 \oplus \ldots \oplus R_o x_k.$$

*Moreover, if $M = R_o y_1 \oplus \ldots \oplus R_o y_l$ is another such decomposition of $M$, then $l = k$ and the order ideals of the $y_j$ are (after possible reindexing) the order ideals of the $x_i$.*

This is essentially Corollary 2 of proposition 1.1 in [4].

**Proposition 3.2** *Let $R_o$ be the Galois ring $GR(p^{nr}, p^n)$ and let $M$ be a finite $R_o$-bimodule. Then,*

$$M = M_1 \oplus M_2 \oplus \ldots \oplus M_r \quad (as\ R_o - modules),$$

*where for each $i$, $1 \le i \le r$, there exist $\sigma_i \in Aut(R_o)$ such that $mr_o = r_o^{\sigma_i} m$, $\forall m \in M_i$ and $\forall r_o \in R_o$.*

**Proof** Let $f \in \mathbb{Z}_{p^n}[X]$ be monic, of degree $r$ and irreducible modulo $p$. Then $f$ splits into $f = (X - \alpha_1)(X - \alpha_2)...(X - \alpha_r)$, where $\alpha_1, ..., \alpha_r \in R_o$. Since $f$ modulo $p$ has distinct roots in $R_o/pR_o$, we have that $\bar{\alpha}_i \neq \bar{\alpha}_j$ for $i \neq j$, in $R_o/pR_o$. Thus, $\alpha_i - \alpha_j$ is not in $pR_o$ and hence, is a unit in $R_o$. Now, for $i = 1, ..., r$, define

$$f_i = \prod_{j=1}^{r} (X - \alpha_j), \text{with } j \neq i.$$

Then,

$$f_i(\alpha_i) = (\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \cdots (\alpha_i - \alpha_r)$$

is a unit in $R_o$.

Let $g = \sum_{i=1}^{r} [f_i(\alpha_i)]^{-1} f_i - 1$. It is clear that $g$ is of degree $\leq r - 1$ and $\alpha_1, ..., \alpha_r$ are roots of $g$.

Consider the canonical homomorphism

$$\begin{array}{rccc} \psi: & R_o & \longrightarrow & R_o/pR_o \\ & r & \longmapsto & \bar{r} \end{array}$$

extended to

$$\begin{array}{rccc} \psi: & R_o[X] & \longrightarrow & (R_o/pR_o)[X] \\ & g & \longmapsto & \bar{g}. \end{array}$$

Then, $\bar{g}(\bar{\alpha}_i) = 0$. But degree of $\bar{g} \leq r - 1$; so $\bar{g} = 0$ because it has $r$ roots. Let $g = p^k g_o$ where $(p,\ g_o) = 1$ and $0 \leq k < n$. Then, $0 = g(\alpha_i) = p^k g_o(\alpha_i)$. Thus, $g_o(\alpha_i)$ is a zero-divisor and hence, $\bar{g}_o(\bar{\alpha}_i) = 0$; but $\bar{g}_o$ is of degree $< r$; so $\bar{g}_o = 0$. Thus, $g_o = 0$ and hence,

$$\sum_{i=1}^{r} [f_i(\alpha_i)]^{-1} f_i = 1.$$

Observe that if $\lambda \in R_o$, then

$$\begin{array}{rccc} \phi_\lambda: & M & \longrightarrow & M \\ & m & \longmapsto & \lambda m \end{array}$$

is a left $R_o$-homomorphism, and $\phi_\lambda \in End_{R_o}(M)$. Consider the map

$$\begin{array}{rccc} \phi: & R_o & \longrightarrow & End_{R_o}(M) \\ & \lambda & \longmapsto & \phi_\lambda. \end{array}$$

It is easy to see that $\phi$ is a ring-homomorphism and $\phi(R_o)$ is contained in the centre of the ring $End_{R_o}(M)$.

Let $\sigma : M \longrightarrow M$ be defined by $\sigma(m) = m\alpha_1$; then, it is trivial to check that $\sigma \in End_{R_o}(M)$. Since $\phi(R_o)$ is contained in the centre of $End_{R_o}(M)$, there exists a ring-homomorphism

$$\begin{array}{rccc} \tilde{\phi}: & R_o[X] & \longrightarrow & End_{R_o}(M) \\ & \sum \lambda_i X^i & \longmapsto & \sum \phi(\lambda_i)\sigma^i. \end{array}$$

Hence,

$$\tilde{\phi}(\sum [f_i(\alpha_i)]^{-1} f_i) = id_M \in End_{R_o}(M).$$

Let $f = X^r + a_1 X^{r-1} + ... + a_r$, where $a_i \in Z_{p^n}$. Then,

$$\begin{aligned} \tilde{\phi}(f)(m) &= (\sigma^r + \phi(a_1)\sigma^{r-1} + ... + \phi(a_r))(m) \\ &= m\alpha_1^r + a_1 m\alpha_1^{r-1} + ... + a_r m \\ &= mf(\alpha_1) \\ &= 0. \end{aligned}$$

Let

$$M_i = \tilde{\phi}([f_i(\alpha_i)]^{-1} f_i)M,\ 1 \leq i \leq r.$$

Then, since $id_M = \tilde{\phi}(\sum[f_i(\alpha_i)]^{-1}f_i)$,

$$M = M_1 + M_2 + ... + M_r. \quad *$$

To show that this sum is direct, suppose, without loss of generality, that $m \in M_1 \cap (M_2 + ... + M_r)$. Now, $m \in M_1$ implies that $m = \tilde{\phi}([f_1(\alpha_1)]^{-1}f_1)(m_1)$, for some $m_1 \in M$. Now,

$$\begin{aligned}(\sigma - \phi(\alpha_1))(m) &= (\sigma - \phi(\alpha_1))\tilde{\phi}([f_1(\alpha_1)]^{-1}f_1)(m_1)\\ &= \phi([f_1(\alpha_1)]^{-1})\tilde{\phi}(f)(m_1)\\ &= 0.\end{aligned}$$

On the other hand, since $m \in M_2 + ... + M_r$,

$$m = \sum_{i=2}^{r} \tilde{\phi}([f_i(\alpha_i)]^{-1}f_i)(m_i),$$

for some $m_2, ..., m_r$ in $M$. Thus,
$(\sigma - \phi(\alpha_2))(\sigma - \phi(\alpha_3)) \cdots (\sigma - \phi(\alpha_r))(m)$

$$\begin{aligned}. &= [\prod_{j=2}^{r}(\sigma - \phi(\alpha_j))]\sum_i \tilde{\phi}([f_i(\alpha_i)]^{-1}f_i)(m_i)\\ &= \prod_{j=3}^{r}(\sigma - \phi(\alpha_j))\phi([f_2(\alpha_2)]^{-1})(\sigma - \phi(\alpha_2))\tilde{\phi}(f_2)(m_2)\\ &\quad + ... + \prod_{j=2}^{r-1}(\sigma - \phi(\alpha_j))\phi([f_r(\alpha_r)]^{-1})(\sigma - \phi(\alpha_r))\tilde{\phi}(f_r)(m_r)\\ &= 0.\end{aligned}$$

This implies that $m = \sum_{i=2}^{r} \tilde{\phi}([f_i(\alpha_i)]^{-1}f_i)m_i = 0$ . Therefore, the sum is direct.

Now, for each $m$ in $M_i$, $m = \tilde{\phi}([f_i(\alpha_i)]^{-1}f_i)(m_i)$ for some $m_i$ in $M$, and

$$\begin{aligned}(\sigma - \phi(\alpha_i))(m) &= (\sigma - \phi(\alpha_i))\phi([f_i(\alpha_i)]^{-1})\tilde{\phi}(f_i)(m_i)\\ &= \phi([f_i(\alpha_i)]^{-1})(\sigma - \phi(\alpha_i))\tilde{\phi}(f)(m_i)\\ &= 0.\end{aligned}$$

Thus, $\sigma(m) = \alpha_i m$; but $\sigma(m) = m\alpha_1$. Consequently, for $m$ in $M_i$, $m\alpha_1 = \alpha_i m$.

Since $\alpha_1$ and $\alpha_i$ are roots of $f$ in $R_o$, there exists an automorphism $\sigma_i$ of $R_o$ such that $\alpha_1^{\sigma_i} = \alpha_i$ (since $Aut(R_o)$ is cyclic and isomorphic to $Aut(R_o/pR)$). That is, for each $m \in M_i$, $m\alpha_1 = \alpha_1^{\sigma_i}m$. But every element of $R_o$ can be written in the form $\sum_{j=0}^{r-1}\lambda_j\alpha_1^j$, where $\lambda_j \in Z_{p^n}$ and $\alpha_1^j \in < b >$. Thus, for any $m$ in $M_i$ and $\forall r_o \in R_o$,

$$mr_o = m\sum\lambda_j\alpha_1^j = \sum\lambda_j m\alpha_1^j = \sum\lambda_j(\alpha_1^j)^{\sigma_i}m = (\sum\lambda_j\alpha_1^j)^{\sigma_i}m = r_o^{\sigma_i}m.$$

**Corollary 3.3** *Let $M$ be a finite $R_o$-bimodule, where $R_o$ is the Galois ring $GR(p^{nr}, p^n)$. Then, there exist $x_1$, ..., $x_k \in M$ and $\sigma_1, ..., \sigma_k \in Aut(R_o)$ such that*

$$M = R_o x_1 \oplus ... \oplus R_o x_k \quad \text{and} \quad x_i r = r^{\sigma_i}x_i, \quad \forall r \in R_o.$$

This is the direct consequence of Propositions 3.1 and 3.2.

**Proposition 3.4** *Let $M$ be a finite $R_o$-bimodule, where $R_o$ is the Galois ring $GR(p^{nr}, p^n)$. Let $m \in M$ and $p^t$ be the additive order of $m$. Then, $|R_o m| = p^{tr}$.*

**Proof** Consider the map

$$\begin{array}{rccc} * & \phi: & R_o & \longrightarrow & R_o m \\ & & r & \longmapsto & rm. \end{array}$$

Then, it is easy to see that $\phi$ is an $R_o$-homomorphism and $Ker\phi = p^t R_o$. Therefore, $R_o m \cong R_o/p^t R_o$ and hence, $|R_o m| = p^{tr}$.

We now state and reprove the following result of Wirt [5] in a simpler manner:

**Proposition 3.5** *Let $R$ be a completely primary ring of order $p^{nr}$, $|R/\mathcal{M}| = p^r$, $CharR = p^k$, and let $R_o$ be a maximal Galois subring of $R$. Then, there exist $x_1$, ..., $x_h \in \mathcal{M}$ and $\sigma_1$, ..., $\sigma_h \in Aut(R_o)$ such that*

$$R = R_o \oplus R_o x_1 \oplus \ldots \oplus R_o x_h \text{ and } x_i r = r^{\sigma_i} x_i, \ \forall r \in R_o \text{ and } \forall i = 1, \ldots, h.$$

**Proof** Consider $\mathcal{M}/pR_o$. This is clearly an $R_o$-bimodule. Hence, by Corollary 3.3, $\exists m_1 + pR_o$, ..., $m_h + pR_o \in \mathcal{M}/pR_o$ and $\sigma_1$, ..., $\sigma_h \in Aut(R_o)$ such that $\mathcal{M}/pR_o = \oplus \sum_{i=1}^{h} R_o(m_i + pR_o)$ and $(m_i + pR_o)r = r^{\sigma_i}(m_i + pR_o)$, $\forall r \in R_o$ and $\forall i = 1, \ldots, h$. Suppose that $p^{n_1}$, ..., $p^{n_h}$ are the additive orders of $m_1 + pR_o$, ..., $m_h + pR_o$, respectively.

Let $R_o = \mathbb{Z}_{p^k}[b]$, where $b$ is as above, and let $m_i b = b^{\sigma_i} m_i + r_i$, where $r_i \in pR_o$. If $\sigma_i \neq id_{R_o}$, put $s_i = (b^{\sigma_i} - b)^{-1} r_i$, where $(b^{\sigma_i} - b)$ is a unit in $R_o$ (because its image under the canonical homomorphism $R_o \longrightarrow R_o/pR_o$ is not zero), and put $x_i = m_i + s_i$. Then,

$$\begin{aligned} x_i b &= (m_i + s_i)b \\ &= m_i b + s_i b \\ &= b^{\sigma_i} m_i + r_i + s_i b \\ &= b^{\sigma_i} m_i + (b^{\sigma_i} - b)s_i + s_i b \\ &= b^{\sigma_i} m_i + b^{\sigma_i} s_i \\ &= b^{\sigma_i} x_i. \end{aligned}$$

Next, since $p^{n_i}$ is the additive order of $m_i + pR_o$, $p^{n_i} x_i \in pR$ and hence $p^{n_i} b x_i = p^{n_i} x_i b$. But $p^{n_i} x_i b = p^{n_i} b^{\sigma_i} x_i$; so $p^{n_i} b x_i = p^{n_i} b^{\sigma_i} x_i$. This implies that $p^{n_i}(b - b^{\sigma_i})x_i = 0$ and hence, if $p^{n_i} x_i \neq 0$, then $b = b^{\sigma_i}$, a contradiction, because $\sigma_i \neq id_{R_o}$. Therefore, $p^{n_i} x_i = 0$.

If $\sigma_i = id_{R_o}$, then

$$\begin{aligned} m_i &= m_i b^{p^r - 1} = m_i b b^{p^r - 2} = (b m_i + r_i) b^{p^r - 2} = (b m_i b + r_i b) b^{p^r - 3} \\ &= (b^2 m_i + r_i b + r_i b) b^{p^r - 3} = \\ &\quad \ldots\ldots \\ &= b^{p^r - 1} m_i + (p^r - 1) r_i b^{p^r - 2} = m_i + (p^r - 1) r_i b^{p^r - 2}; \end{aligned}$$

and hence, $(p^r - 1)r_i = 0$, which implies that $r_i = 0$, since $p^r - 1$ is a unit. Hence, $m_i b = b m_i$.

Let $p^{n_i} m_i = p^{t_i} u_i$, where $u_i$ is a unit in $R_o$. If $n_i \geq t_i$, then, $p^{t_i}(p^{n_i - t_i} m_i - u_i) = 0$ and hence, $p^{n_i - t_i} m_i - u_i$ is a zero-divisor in $R$; a contradiction. Hence, $n_i < t_i$. Put $x_i = m_i - p^{t_i - n_i} u_i$. In this case, it is clear that the additive order of $x_i$ is $p^{n_i}$.

Thus, the additive orders of $x_1$, ..., $x_h$ are $p^{n_1}$, ..., $p^{n_h}$, respectively.

Now, clearly,

$$\mathcal{M} = pR_o + \sum_{i=1}^{h} R_o x_i.$$

But, by Proposition 3.4,

$$|R_o x_i| = |R_o(m_i + pR_o)|.$$

Now, by comparing orders, we deduce that

$$\mathcal{M} = pR_o \oplus R_o x_1 \oplus \ldots \oplus R_o x_h$$

and hence,

$$R = R_o \oplus R_o x_1 \oplus \ldots \oplus R_o x_h.$$

Also, $x_i b = b^{\sigma_i} x_i$.

Since every element of $R_o$ can be written uniquely as $\sum_{j=0}^{k-1} p^j \lambda_j$ where $\lambda_j \in K_o =< b > \cup\{0\}$, then $\forall r \in R_o$,

$$\begin{aligned} x_i r &= x_i[\sum_{j=0}^{k-1} p^j \lambda_j] = \sum_{j=0}^{k-1} p^j x_i \lambda_j \\ &= [\sum_{j=0}^{k-1} p^j \lambda_j^{\sigma_i}] x_i = [\sum_{j=0}^{k-1} p^j \lambda_j]^{\sigma_i} x_i \\ &= r^{\sigma_i} x_i. \end{aligned}$$

**Proposition 3.6** *Let $R$ be a completely primary ring of order $p^{nr}$, $|R/\mathcal{M}| = p^r$, $CharR = p^k$, and let $R_o$ be a maximal Galois subring of $R$. Let $\sigma_1, ..., \sigma_h \in Aut(R_o)$ be as defined in Proposition 3.5. Then, $\sigma_1, ..., \sigma_h$ are uniquely determined by $R$ and $R_o$.*

**Proof** Let $R_o = \mathbb{Z}_{p^k}[b]$, with $b$ as above and suppose that

$$R = R_o \oplus R_o x_1 \oplus \ldots \oplus R_o x_h = R_o \oplus R_o y_1 \oplus \ldots \oplus R_o y_h,$$

such that $x_i r = r^{\sigma_i} x_i$; $y_i r = r^{\theta_i} y_i$, $\forall r \in R_o$ and $\forall i = 1, ..., h$; where $x_i, y_i \in \mathcal{M}$ and $\sigma_i, \theta_i \in Aut(R_o)$. Also, assume that $\sigma_i$ and $\theta_i$ occur with multiplicity $n_i$ and $n_i'$, respectively. We want to prove (after possible reindexing) that $\{\sigma_1, ..., \sigma_h\} = \{\theta_1, ..., \theta_h\}$ and $n_i = n_i'$, $\forall i = 1, ..., h$.

Since $\forall i = 1, ..., h$; $y_i \in \mathcal{M} = pR_o \oplus R_o x_1 \oplus \ldots \oplus R_o x_h$ and $y_i \notin pR_o$, $y_i = pr_i + \sum_j r_{ij} x_j$, where $r_{ij} x_j \neq 0$ for at least one $j$. Now,

$$\begin{aligned} pb^{\theta_i} r_i + \sum_j b^{\theta_i} r_{ij} x_j &= b^{\theta_i} y_i = y_i b = pr_i b + \sum_j r_{ij} x_j b \\ &= pbr_i + \sum_j b^{\sigma_j} r_{ij} x_j. \end{aligned} \tag{14}$$

Since the sums are direct, it follows, for all j, that

$$b^{\theta_i} r_{ij} x_j = b^{\sigma_j} r_{ij} x_j, \text{and hence } (b^{\theta_i} - b^{\sigma_j}) r_{ij} x_j = 0.$$

If now $r_{ij} x_j \neq 0$, then $b^{\theta_i} - b^{\sigma_j} = 0$ and so $\theta_i = \sigma_j$. This shows two things. On the one hand, since $r_{ij} x_j \neq 0$ for at least one $j$, it follows that $\theta_i \in \{\sigma_1, ..., \sigma_h\}$ and by symmetry $\{\sigma_1, ..., \sigma_h\} = \{\theta_1, ..., \theta_h\}$. On the other hand, if $\sigma_j \neq \theta_i$ then $r_{ij} x_j = 0$ and so

$$y_i = pr_i + \sum_{\sigma_j = \theta_i} r_{ij} x_j \in pR_o \oplus \overset{\oplus}{\sum_{\sigma_j = \theta_i}} R_o x_j.$$

Hence, $R_o \oplus \sum^{\oplus}_{\theta_\lambda = \theta_i} R_o y_\lambda \subset R_o \oplus \sum^{\oplus}_{\sigma_j = \theta_i} R_o x_j$.

By symmetry $R_o \oplus \sum^{\oplus}_{\theta_\lambda = \theta_i} R_o y_\lambda = R_o \oplus \sum^{\oplus}_{\sigma_j = \theta_i} R_o x_j$. By Proposition 3.1, the number of summands is the same. Hence, if $\sigma_j = \theta_i$ the multiplicities of $\sigma_j$ and $\theta_i$ are the same.

**Definition** We shall call $\sigma_1$, ..., $\sigma_h$ defined above, the *associated automorphisms* of $R$ with respect to $R_o$.

Let $B = \{x_1, \ldots, x_h\}$ be as above and let $\tau \in Aut(R_o)$. Put

$$B_\tau = \{x \in B : xb = b^\tau x\}$$

and let $\mathcal{M}_\tau = \sum_{x_i \in B_\tau}^{\oplus} R_o x_i$.

Then, obviously, $\mathcal{M}_\tau$ is an $R_o$-submodule of $\mathcal{M}$.

**Corollary 3.7** *Let $R$ be a finite completely primary ring with maximal ideal $\mathcal{M}$. Then, $\mathcal{M} = pR_o \oplus \sum_{\tau \in Aut R_o}^{\oplus} \mathcal{M}_\tau$ as $R_o$ – modules.*

## 4 Existence of a Minimal Basis for $R$

In this section, we show that there exists a Minimal Basis for $R$ and that every element of $R$ can be expressed uniquely as a linear combination of a Minimal Basis for $R$ with coefficients in $K_o$.

Let $R$ be a finite completely primary ring with maximal ideal $\mathcal{M}$. We know that $\mathcal{M}$ is nilpotent and has index of nilpotence $l$ for some $l \leq n$. Thus, $\mathcal{M}$ contains a chain of ideals $\mathcal{M} \supseteq \mathcal{M}^2 \supseteq \ldots \supseteq \mathcal{M}^{l-1} \supseteq \mathcal{M}^l = (0)$ (see Section 2).

Now, consider any quotient $\mathcal{M}^i/\mathcal{M}^{i+1}$. This becomes a vector-space over the field $R/\mathcal{M}$ on defining

$$(r + \mathcal{M})(m + \mathcal{M}^{i+1}) = r \cdot m + \mathcal{M}^{i+1}$$

for any $r \in R$, $m \in \mathcal{M}^i$.

Thus, $\mathcal{M}/\mathcal{M}^2$, $\mathcal{M}^2/\mathcal{M}^3$, ..., $\mathcal{M}^{l-1}/\mathcal{M}^l (\cong \mathcal{M}^{l-1})$ may all be considered as $R/\mathcal{M}$-vector spaces, all of finite dimension.

Let $c_i$ denote the dimension of the vector space $\mathcal{M}^{i-1}/\mathcal{M}^i$ over $R/\mathcal{M}$, for $i = 2, 3, \ldots, l$, and let

$$x_{c_1+\ldots+c_{i-1}+1} + \mathcal{M}^i, x_{c_1+\ldots+c_{i-1}+2} + \mathcal{M}^i, \ldots, x_{c_1+\ldots+c_{i-1}+c_i} + \mathcal{M}^i$$

be a basis for $\mathcal{M}^{i-1}/\mathcal{M}^i$ for each $i = 2, \ldots, l$, where $c_1 = 0$. Consider the set $\{x_1, \ldots, x_{c_2}, x_{c_2+1}, \ldots, x_{c_2+c_3+\ldots+c_l}\}$ of elements of $\mathcal{M}$. Note that, since

$$|\mathcal{M}| = |\mathcal{M}/\mathcal{M}^2| \cdot |\mathcal{M}^2/\mathcal{M}^3| \cdot \ldots \cdot |\mathcal{M}^{l-1}/\mathcal{M}^l|,$$

we have

$$p^{(n-1)r} = p^{rc_2} \cdot p^{rc_3} \cdot \ldots \cdot p^{rc_l} = p^{r(c_2+\ldots+c_l)},$$

and therefore, $n - 1 = (c_2 + \ldots + c_l)$. Thus, we can write this set of elements of $\mathcal{M}$ as $\{x_1, x_2, \ldots, x_{n-1}\}$.

Suppose $0 \neq x \in \mathcal{M}$. Then $x + \mathcal{M}^2 \in \mathcal{M}/\mathcal{M}^2$, and therefore there are elements $\lambda_i + \mathcal{M}$ with $\lambda_i \in K_o$ such that

$$x + \mathcal{M}^2 = (\lambda_1 + \mathcal{M})(x_1 + \mathcal{M}^2) + \ldots + (\lambda_{c_2} + \mathcal{M})(x_{c_2} + \mathcal{M}^2) = \sum_{i=1}^{c_2} \lambda_i x_i + \mathcal{M}^2.$$

Hence,

$$x = \sum_{i=1}^{c_2} \lambda_i x_i + y, \text{where } y \in \mathcal{M}^2.$$

But then, $y + \mathcal{M}^3 \in \mathcal{M}^2/\mathcal{M}^3$, and therefore, we can find elements $\lambda_j + \mathcal{M}$ with $\lambda_j \in K_o$ such that

$$y = \sum_{j=c_2+1}^{c_2+c_3} \lambda_j x_j + z, \text{where } z \in \mathcal{M}^3.$$

Thus,

$$x = \sum_{i=1}^{c_2+c_3} \lambda_i x_i + z.$$

Continuing this process inductively, we find that there are elements $\lambda_i \in K_o$ such that

$$x = \sum_{i=1}^{n-1} \lambda_i x_i + w, \text{where } w \in \mathcal{M}^l = (0).$$

Hence,

$$x = \sum_{i=1}^{n-1} \lambda_i x_i,$$

and therefore the elements $x_1,\ x_2,\ \ldots,\ x_{n-1}$ may be said to "span" $\mathcal{M}$ over $K_o$. Furthermore, every element of $\mathcal{M}$ may be expressed uniquely as a "linear combination" of $x_1,\ x_2,\ \ldots,\ x_{n-1}$ with coefficients in $K_o$, for there are at most $(p^r)^{n-1}$ such combinations.

These results lead us to the following:

**Definition** Let $R$ be any completely primary ring with maximal ideal $\mathcal{M}$ of index of nilpotence $l$, and consider the $R/\mathcal{M}$-vector spaces

$$\mathcal{M}/\mathcal{M}^2,\ \mathcal{M}^2/\mathcal{M}^3,\ \ldots,\ \mathcal{M}^{l-1}/\mathcal{M}^l.$$

Consider any set $\{x_1,\ x_2,\ \ldots,\ x_{n-1}\}$ of elements of $\mathcal{M}$ such that $x_1+\mathcal{M}^2,\ x_2+\mathcal{M}^2,\ \ldots,\ x_{c_2}+\mathcal{M}^2$ is a basis for $\mathcal{M}/\mathcal{M}^2$, $x_{c_2+1}+\mathcal{M}^3,\ \ldots,\ x_{c_2+c_3}+\mathcal{M}^3$ is a basis for $\mathcal{M}^2/\mathcal{M}^3$, ..., and $x_{c_2+\ldots+c_{l-1}+1}+\mathcal{M}^l,\ \ldots,\ x_{n-1}+\mathcal{M}^l$ is a basis for $\mathcal{M}^{l-1}/\mathcal{M}^l$. Then, we shall call the set $\{x_1,\ x_2,\ \ldots,\ x_{n-1}\}$ a *Minimal Basis (M.B.)* of $\mathcal{M}$.

From what we have shown above, any *M.B.* of $\mathcal{M}$ has the property that any element of $\mathcal{M}$ may be expressed uniquely as a linear combination $\sum_{i=1}^{n-1} \lambda_i x_i$ with $\lambda_i \in K_o$.

Now, let $\psi : R \longrightarrow R/\mathcal{M}$ be the canonical homomorphism, and let $\mathcal{P}$ be the set of primitive elements of $R/\mathcal{M}$. Define a set

$$S = \{x_o \in \psi^{-1}(\mathcal{P}) : o(x_o) = p^r - 1\},$$

where $o(x_o)$ denotes the order of the element $x_o$.

Then, any $x_o \in S$ behaves exactly as the element $b$, and therefore, we can find an *M.B.* of $\mathcal{M}$ "over" $< x_o > \cup\{0\}$. In fact, the element $x_o$ is interchangeable with $b$ in all that has preceded.

**Definition** The set $\{x_o,\ x_1,\ x_2,\ \ldots,\ x_{n-1}\}$ will be called an *M.B.* of $R$ if and only if $x_o \in S$ and $\{x_1,\ x_2,\ \ldots,\ x_{n-1}\}$ is an *M.B.* of $\mathcal{M}$.

**Proposition 4.1** *Let $R$ be a finite completely primary ring. Then, every element of $R$ can be expressed uniquely as a linear combination of the M.B. $\{x_o,\ x_1,\ x_2,\ \ldots,\ x_{n-1}\}$ with coefficients in $< x_o > \cup\{0\}$.*

**Proof** Let $r \in R$. Then, by Corollary 3.6, there exists $\lambda \in < x_o > \cup\{0\}$, $m \in \mathcal{M}$, such that $r = \lambda + m$.

But since $\{x_1,\ x_2,\ \ldots,\ x_{n-1}\}$ is an *M.B.* of $\mathcal{M}$, we have that there exist $\lambda_i \in < x_o > \cup\{0\}$ such that

$$m = \sum_{i=1}^{n-1} \lambda_i x_i.$$

Hence,

$$r = \lambda + \sum_{i=1}^{n-1} \lambda_i x_i = (\lambda x_o^{-1})x_o + \sum_{i=1}^{n-1} \lambda_i x_i,$$

which is the required form.

*

The uniqueness of expression follows from the fact that there are at most $(p^r)^n$ linear combinations, and $|R| = p^{nr}$.

## 5 Some Module theory over finite completely primary rings

In this section, we will be concerned with collecting a number of results and constructions concerning modules over finite completely primary rings.

Let $R$ be a finite completely primary ring of order $p^{nr}$, residue order $p^r$ and characteristic $p^k$, with maximal ideal $\mathcal{M}$ of index of nilpotence $l$. Let $K_o$ and $b$ be as in Proposition 2.1. Let $R_o = \mathbb{Z}_{p^k}[b]$ be a maximal Galois subring of $R$, $\mathcal{M}_o = pR_o = \mathcal{M} \cap R_o$, its maximal ideal and $R_o/\mathcal{M}_o \cong K$, where $K = R/\mathcal{M}$. Let $M$ be an $R$-module. Then, we have the following:

**Definitions**
(i) A *$K_o$-basis* of $M$ is a subset $\{m_1, m_2, ..., m_l\}$ of $M$ such that every element of $M$ is uniquely expressible as $\lambda_1 m_1 + .... + \lambda_l m_l$, $\lambda_i \in K_o$;
(ii) An *$R_o$-basis* of $M$ is a subset $\{m_1, m_2, ..., m_h\}$ of $M$ such that

$$M = R_o m_1 \oplus \ldots \oplus R_o m_h.$$

We now state and prove the following:

**Proposition 5.1** *Let $M$ be an $R_o$-module and $\{m_1, m_2, ..., m_h\} \in M$. Then, the following are equivalent:*
*(i) $\{m_1, m_2, ..., m_h\}$ is an $R_o$-basis of $M$;*
*(ii) the non-zero elements of $\{p^i m_j : i = 0, 1, ..., k-1; j = 1, ..., h\}$ form a $K_o$-basis of $M$.*

**Proof**
We first show that (i) implies (ii).
Notice that for every $\nu = 0, 1, ..., k-1$, the non-zero elements of

$$\mathcal{B}_\nu = \{p^\nu m_j + p^{\nu+1} M : j = 1, ..., h\}$$

are linearly indépendent over $K$. For let

$$\sum_{j=1}^{h} (\lambda_j + \mathcal{M}_o)(p^\nu m_j + p^{\nu+1} M) = p^{\nu+1} M,$$

with $\lambda_j \in K_o$. Then,

$$\sum_{j=1}^{h} \lambda_j p^\nu m_j \in p^{\nu+1} M$$

and so,

$$\sum_{j=1}^{h} \lambda_j p^\nu m_j = p^{\nu+1} \sum_{j=1}^{h} r_j m_j,$$

with $r_j \in R_o$, where $\sum_{j=1}^{h} r_j m_j = m$, for some $m \in M$. Hence,

$$\sum_{j=1}^{h} (\lambda_j - p r_j) p^\nu m_j = 0,$$

and since

$$M = R_o m_1 \oplus ..... \oplus R_o m_h,$$

$(\lambda_j - p r_j) p^\nu m_j = 0$, for every $j = 1, ..., h$.

Now, if $\lambda_j \neq 0$, then $(\lambda_j - pr_j)$ is invertible in $R_o$ and hence, $p^\nu m_j = 0$. But then $p^\nu m_j \neq 0$ implies $\lambda_j = 0$. Hence, the non-zero elements of $\mathcal{B}_\nu$ are linearly independent over $K$.

*

It is obvious that the set $C = \{p^i m_j \ : \ i = 0,\ 1,\ ...,\ k-1;\ j = 1,\ 2,\ ...,\ h\}$ generates $M$ over $K_o$, since

$$M = R_o m_1 \oplus ..... \oplus R_o m_h$$

and $\{1,\ p,\ p^2,\ ....,\ p^{k-1}\}$ is a $K_o$-basis of $R_o$.

It remains to show that every element of $M$ can be written *uniquely* as a $K_o$-linear combination of the non-zero elements of $C$. So, let

$$\sum_{j=1}^{h}\sum_{i=0}^{k-1} \lambda_{ij} p^i m_j = \sum_{j=1}^{h}\sum_{i=0}^{k-1} \mu_{ij} p^i m_j, \tag{15}$$

$\lambda_{ij}, \mu_{ij} \in K_o$. Then,

$$\sum_{j=1}^{h} (\lambda_{0j} + \mathcal{M}_o)(m_j + pM) = \sum_{j=1}^{h} (\mu_{0j} + \mathcal{M}_o)(m_j + pM).$$

Since $\mathcal{B}_o$ is $K$-independent, we have

$$\lambda_{0j} + \mathcal{M}_o = \mu_{0j} + \mathcal{M}_o,$$

for every $j = 1,\ ...,\ h$. Since $\lambda_{0j}, \mu_{0j} \in K_o$, by Remark 1.1, $\lambda_{0j} = \mu_{0j}$, for every $j = 1,\ ...,\ h$. Now, (2) gives

$$\sum_{j=1}^{h} (\lambda_{1j} + \mathcal{M}_o)(pm_j + p^2 M) = \sum_{j=1}^{h} (\mu_{1j} + \mathcal{M}_o)(pm_j + p^2 M);$$

and since $\mathcal{B}_1$ is $K$-independent, we have

$$\lambda_{1j} = \mu_{1j},$$

for every $j = 1,\ ...,\ h$. Continuing the process,we see that $\lambda_{ij} = \mu_{ij}$, for every $i = 0,\ 1,\ ...,\ k-1$ and every $j = 1,\ ...,\ h$ and this establishes our claim that every element of $M$ can be written uniquely as a $K_o$-linear combination of the non-zero elements of $C$. This establishes that (i) implies (ii).

We now show that (ii) implies (i).
Since $\{1,\ p,\ ...,\ p^{k-1}\}$ is a $K_o$-basis of $R_o$, for every $m \in M$, we have

$$m = \sum_{i=0}^{k-1}\sum_{j=1}^{h} \lambda_{ij} p^i m_j = \sum_{j=1}^{h}(\sum_{i=0}^{k-1} \lambda_{ij} p^i) m_j,$$

with $\lambda_{ij} \in K_o$, $\sum_{i=0}^{k-1} \lambda_{ij} p^i \in R_o$; hence, $M = R_o m_1 + .... + R_o m_h$.

To show the sum is direct, let $\sum_{j=1}^{h} r_j m_j = 0$, with $r_j \in R_o$. Then,

$$r_j = \sum_{i=0}^{k-1} \lambda_{ij} p^i,$$

and, hence,

$$\sum_{i=0}^{k-1}\sum_{j=1}^{h} \lambda_{ij} p^i m_j = 0,$$

with $\lambda_{ij} \in K_o$; which implies $\lambda_{ij} = 0$, for every $i = 0,\ 1,\ ...,\ k-1$ and every $j = 1,\ ...,\ h$; provided $p^i m_j \neq 0$. But then

$$\sum_{i=0}^{k-1} \lambda_{ij} p^i m_j = 0,$$

for every $j = 1,\ ...,\ h$.

**Corollary 5.2** *Let $M$ be a finite $R$-module, where $R$ is a finite completely primary ring, with maximal Galois subring $R_o$. Then $M$ has an $R_o$-basis (and hence, also a $K_o$-basis).*

**Proof** Clearly, $M$ is also a finite $R_o$-module and since $R_o$ is commutative $M$ can be considered as an $R_o$-bimodule. Then, by Corollary 3.3, $M$ has an $R_o$ basis (and by the previous Proposition, it has a $K_o$-basis).

**Corollary 5.3** *Any finite completely primary ring has a $R_o$-basis (and hence a $K_o$- basis).*

We complete this section by proving that the maximal ideal $\mathcal{M}$ of a completely primary ring $R$ has a distinguished $K_o$-basis, considered as an $R_o$-submodule of $R$.

We first introduce some notation which will be convenient for this purpose.

Let $K = R/\mathcal{M}$ and let $\sigma \in Aut(K)$. Then $\sigma$ is given by $\sigma(x) = x^{p^\nu}$ for some $\nu \in \{1, 2, ..., r\}$, and we can consider the function

$$\begin{array}{rccc} \theta: & K_o & \longrightarrow & K_o \\ & \lambda & \longmapsto & \lambda^{p^\nu} \end{array}$$

which defines an automorphism on $R_o$ by

$$\sum \alpha_i b^i \longmapsto \sum \alpha_i b^{ip^\nu}.$$

We shall write $\lambda^\sigma$ for $\lambda^{p^\nu}$ and $(\sum \alpha_i b^i)^\sigma$ for $\sum \alpha_i b^{ip^\nu}$.

**Definition.** Let $M$ be an $R_o$-submodule of $R$, and let $\{m_1, ...., m_h\}$ be an $R_o$- or a $K_o$-basis of $M$. We say that $\{m_1, ...., m_h\}$ is *distinguished* if there exist $\sigma_1, ...., \sigma_h \in Aut(K)$ such that for $i = 1, ..., h$,

$$m_i b = b^{\sigma_i} m_i.$$

We now state the following proposition which extends the work of Raghavendran to all completely primary rings:

**Proposition 5.4** *Let $R$ be a finite completely primary ring with maximal ideal $\mathcal{M}$. Then, $\mathcal{M}$ has a distinguished $K_o$-basis.*

**Proof** This follows directly from Corollary 3.3, since $\mathcal{M}$ is, in a natural way, an $R_o$-bimodule.

## References

[1] **C. J. Chikunji**, On a Class of Finite Rings, Comm. Algebra, Vol. 27, No. 10 (1999), p.5049 - 5081.
[2] **E. W. Clark**, A coefficient ring for finite non-commutative rings, Proc. Amer. Math. Soc. 33 (1972), p.25 - 28.
[3] **R. Raghavendran**, Finite associative rings, Compositio Math. 21, Fasc. 2 (1969), p.195 - 229.
[4] **R. S. Wilson**, On the structure of finite rings, Compositio Math. 26, Fasc. 1 (1973), p. 79 - 93.
[5] **B. R. Wirt**, Finite non-commutative Local rings, Ph.D. Thesis, University of Oklahoma (1972).