Canad. Math. Bull. Vol. **19** (3), 1976

FULL IDEALS AND RING GROUPS IN $Z_n[x]$

BY
JOHN A. SUVAK

Introduction. If we add the operation of composition to the polynomial ring $R[x]$, where R is a commutative ring with identity, we get a tri-operational algebra $\mathcal{A}=(R[x],+,\cdot,\circ)$. A *full ideal* or *tri-operational ideal* of $\mathcal{A}$ is the kernel of a tri-operational homomorphism on $\mathcal{A}$. This is equivalent [4, pp. 73–74] to the following: A full ideal of $\mathcal{A}$ is a ring ideal A of $R[x]$ such that $f\circ g\in A$ for every $f\in A$ and $g\in R[x]$. For a full ideal A of $R[x]$ we can form the tri-operational algebra $(R[x]/A,+,\cdot,\circ)$ where $(R[x]/A,\circ)$ forms a monoid called the *ring semi-group* of $R[x]$ over A, denoted by $H_R(A)$. The group of units of $H_R(A)$ is called the *ring group* of $R[x]$ over A, denoted by $G_R(A)$.

For any ideal I of R, $(I)=I[x]$ and $\{I\}_R=\{f\in R[x]:f(a)\in I$ for every $a\in R\}$ are full ideals of $R[x]$. Dickson [2] characterized the full ideals $\{I\}_z$ where Z is the ring of integers, and Nöbauer [7] developed a general theory of ring groups and used these results to describe the ring groups $G_Z((I))$ and $G_Z(\{I\})$. It is natural to ask whether these results can be extended to the rings Z_n of integers modulo n. In this paper, then, we will first characterize the full ideals $\{I\}_{Z_n}$, which we will shorten to $\{I\}_n$, and secondly we will describe the ring groups $G_{Z_n}((I))$ and $G_{Z_n}(\{I\})$, which we will shorten to $G_n((I))$ and $G_n(\{I\})$, for every n and every ideal I of Z_n.

1. The full ideals $\{I\}_n$. Since Z_n is a principal ideal ring and, in fact, every ideal I of Z_n has a unique generator which is a divisor of n, our first problem is reduced to describing the ideals

$$\{\langle d\rangle\}_n=\{f\in Z_n[x]:f(a)\equiv 0 \bmod d \quad \text{for every} \quad a\in Z_n\}$$

for every n and every d that divides n. We begin by giving a characterization for the full ideals $\{0\}_n=\{\langle n\rangle\}_n$, where 0 is the zero (full) ideal of $Z_n[x]$, and then we will see how these results can be used to find $\{I\}_n$ for any ideal I.

In characterizing $\{0\}_n$ for arbitrary n we will make considerable use of results obtained by Dickson [2] for $Z[x]$. We thus consider the homomorphism $\phi:Z\to Z_n$ and the injective map $\psi:Z_n\to Z$, where ϕ is reduction modulo n, and the induced tri-operational homomorphism $\bar{\phi}:Z[x]\to Z_n[x]$ and injective map $\bar{\psi}:Z_n[x]\to Z[x]$, with $\phi\circ\psi$ and $\bar{\phi}\circ\bar{\psi}$ the identity maps on Z_n and $Z_n[x]$ respectively. In Chapter II of [2] Dickson gives a method for constructing a

Received by the editors August 26, 1975.

https://doi.org/10.4153/CMB-1976-050-6 Published online by Cambridge University Press

generating set for all *residual polynomials modulo n*; that is, all polynomials $f \in Z[x]$ with $f(a) \equiv 0 \bmod n$ for every $a \in Z$. The following lemma and theorem allow us to apply these results to solving our problem.

LEMMA 1. (1) *If* $f \in Z[x]$ *and* $a \in Z$, *then* $\phi(f(a)) = \bar{\phi}(f)(\phi(a))$.
(2) *If* $f \in Z_n[x]$ *and* $a \in Z_n$, *then* $\psi(f(a)) \equiv \bar{\psi}(f)(\psi(a)) \bmod n$.

Proof.
(1) If $f = \sum c_i x^i \in Z[x]$ and $a \in Z$, then $\phi(f(a)) = \phi(\sum c_i a^i) = \sum \phi(c_i)[\phi(a)]^i = \bar{\phi}(f)(\phi(a))$.
(2) For $f \in Z_n[x]$ and $a \in Z_n$ we have, using (1) and the fact that $\phi \circ \psi$ and $\bar{\phi} \circ \bar{\psi}$ are identity maps, that $\phi(\psi(f(a))) = f(a)$ and also $\phi(\bar{\psi}(f)(\psi(a))) = \bar{\phi}(\bar{\psi}(f))(\phi(\psi(a))) = f(a)$. Thus $\psi(f(a)) \equiv \bar{\psi}(f)(\psi(a)) \bmod n$.

THEOREM 2. *Let* $\bar{\phi}$ *and* $\bar{\psi}$ *be defined as above. Then,*
(1) *If f is a residual polynomial modulo n, then* $\bar{\phi}(f) \in \{0\}_n$.
(2) *If* $f \in \{0\}_n$, *then* $\bar{\psi}(f)$ *is a residual polynomial modulo n.*

Proof.
(1) If f is a residual polynomial modulo n and $a \in Z$, then $f(a) \equiv 0 \bmod n$ and $\phi(f(a)) = 0$. So $\bar{\phi}(f)(\phi(a)) = 0$ by Lemma 1, and since ϕ is surjective we have $\bar{\phi}(f)(b) = 0$ for every $b \in Z_n$ and thus $\bar{\phi}(f) \in \{0\}_n$.
(2) Let $f \in \{0\}_n$ and $a \in Z$. Then $\psi(\phi(a)) \equiv a \bmod n$. So by Lemma 1, $\bar{\psi}(f)(a) \equiv \bar{\psi}(f)(\psi(\phi(a))) \equiv \psi(f(\phi(a))) \bmod n$. But $f(\phi(a)) = 0$ since $f \in \{0\}_n$. Thus $\bar{\psi}(f)(a) \equiv 0 \bmod n$.

This theorem together with results of Dickson [2] in characterizing residual polynomials can be applied in a simple way to our case to get the following results describing $\{0\}_n$. If p is a prime and $t \le p$, then Theorem 27 of [2] gives,

$$\{0\}_{p^t} = \langle p^{t-1}(x^p - x), p^{t-2}(x^p - x)^2, \ldots, p(x^p - x)^{t-1}, (x^p - x)^t \rangle.$$

Note that taking $t = 1$ we get the principal ideal $\{0\}_p = \langle x^p - x \rangle$. If we now define a map $\pi: Z^+ \to Z[x]$ by $\pi(k) = x(x-1)(x-2) \cdots (x-k+1)$ and identify $\bar{\phi}(\pi(k))$ with $\pi(k)$, then Theorem 2 above and equation (32) of [2] give that each $f \in \{0\}_n$ of degree m can be expressed in the form $f = a_2\pi(2) + a_3\pi(3) + \cdots + a_m\pi(m)$ where $k!\, a_k = 0$ for $k = 2, 3, \ldots, m$. Moreover we are able to give a method for constructing a generating set for $\{0\}_n$. For m a positive integer let $\mu(m)$ denote the least positive integer such that $\mu(m)!$ is divisible by m. Now for a given n, partition the divisors $d > 1$ of n into sets by the equivalence relation that identifies divisors with the same μ value. Choose as a representative of each class the largest d of that class and let $d_1, d_2, \ldots, d_s$ denote these representatives. Then Theorem 2 together with equation (27) and Theorem 28 of [2] give us, COROLLARY 3. *Let n be arbitrary and $d_1, d_2, \ldots, d_s$ be the divisors of n selected above. Then*

$$\{0\}_n = \left\langle \frac{n}{d_1}\pi(\mu(d_1)), \frac{n}{d_2}\pi(\mu(d_2)), \ldots, \frac{n}{d_s}\pi(\mu(d_s)) \right\rangle.$$

As an example the reader can verify that $\{0\}_{30} = \langle 15\pi(2), 5\pi(3), \pi(5)\rangle$.

We now use the above results to characterize the full ideals $\{I\}_n$ for arbitrary n and any ideal I of Z_n. Let $\{I\}_n = \{\langle d\rangle\}_n$ where d divides n. Then the maps $\alpha: Z_n \to Z_d$ and $\bar{\alpha}: Z_n[x] \to Z_d[x]$, which are reduction modulo n, are ring epimorphisms, and, as in Lemma 1, for any $f \in Z_n[x]$ and $a \in Z_n$ we have $\alpha(f(a)) = \bar{\alpha}(f)(\alpha(a))$. We also have the obvious injection maps $\beta: Z_d \to Z_n$ and $\bar{\beta}: Z_d[x] \to Z_n[x]$ and these are such that $\alpha \circ \beta$ and $\bar{\alpha} \circ \bar{\beta}$ are identity maps. We first show,

LEMMA 4. *Let $\bar{\alpha}$ be as given above and let $f \in Z_n[x]$. Then $f \in \{\langle d\rangle\}_n$ if and only if $\bar{\alpha}(f) \in \{0\}_d$.*

Proof. If $f \in \{\langle d\rangle\}_n$, then $f(a) \equiv 0 \bmod d$ for every $a \in Z_n$ and hence $\alpha(f(a)) = \bar{\alpha}(f)(\alpha(a)) = 0$. Since α is surjective we have $\bar{\alpha}(f)(b) = 0$ for every $b \in Z_d$ and $\bar{\alpha}(f) \in \{0\}_d$. Conversely, if $\bar{\alpha}(f) \in \{0\}_d$, then for any $a \in Z_n$ we have $0 = \bar{\alpha}(f)(\alpha(a)) = \alpha(f(a))$. So $f(a) \equiv 0 \bmod d$ and $f \in \{\langle d\rangle\}_n$.

With this we can prove our desired result.

THEOREM. *If $\{0\}_d = \langle f_1, f_2, \ldots, f_k\rangle$ and d divides n, then $\{\langle d\rangle\}_n = \langle \bar{\beta}(f_1), \bar{\beta}(f_2), \ldots, \bar{\beta}(f_k), d\rangle$ where d is the constant polynomial $f = d$ in $Z_n[x]$.*

Proof. Suppose $f \in \langle \bar{\beta}(f_1), \bar{\beta}(f_2), \ldots, \bar{\beta}(f_k), d\rangle$, so $f = dg + \sum_{i=1}^k \bar{\beta}(f_i)g_i$ with g, $g_i \in Z_n[x]$, $i = 1, 2, \ldots, k$. Since $\bar{\alpha}$ is a ring homomorphism and $\bar{\alpha} \circ \bar{\beta}$ is the identity map on $Z_d[x]$ we get $\bar{\alpha}(f) = \sum_{i=1}^k f_i \bar{\alpha}(g_i) \in \{0\}_d$, and so by Lemma 4 we have $f \in \{\langle d\rangle\}_n$. Conversely, suppose $f \in \{\langle d\rangle\}_n$. Then $\bar{\alpha}(f) \in \{0\}_d$ by Lemma 4 and we can write $\bar{\alpha}(f) = \sum_{i=1}^k f_i g_i$ for some $g_i \in Z_d[x]$. Now consider the polynomial $h = \sum_{i=1}^k \bar{\beta}(f_i)\bar{\beta}(g_i)$. Then $\bar{\alpha}(h) = \sum_{i=1}^k f_i g_i$ and $\bar{\alpha}(f) = \bar{\alpha}(h)$ or $\bar{\alpha}(f-h) = 0$. Hence $f - h = dg$ for some $g \in Z_n[x]$ and so

$$f = dg + h = dg + \sum_{i=1}^{k} \bar{\beta}(f_i)\bar{\beta}(g_i)$$

and $f \in \langle \bar{\beta}(f_1), \bar{\beta}(f_2), \ldots, \bar{\beta}(f_k), d\rangle$ and the theorem is proved.

Thus we can obtain a set of generators for $\{\langle d\rangle\}_n$ by sort of lifting the generators of $\{0\}_d$, which we can construct from Corollary 3, to $Z_n[x]$ and throwing in the constant polynomial $f = d$.

2. The ring groups $G_n((I))$. Nöbauer [7] obtained results concerning the ring groups $G_z((I))$. The following theorem and corollary allow us to apply these results to our problem.

THEOREM 6. *Let $I=\langle n\rangle$, n a positive integer, be an ideal of Z. Then $G_Z((I))\simeq G_n((0))$.*

Proof. Since $H_n((0))$ is the semi-group $(Z_n[x], \circ)$, we first define $\theta: H_Z((I))\to H_n((0))$ by $\theta(f+(I))=\bar{\phi}(f)$. Now θ is well-defined, for if $f+(I)=g+(I)$ then $f-g\in(I)$ and $\bar{\phi}(f-g)=0$, and so $\bar{\phi}(f)=\bar{\phi}(g)$. Clearly θ is an epimorphism since $\bar{\phi}$ is a tri-operational epimorphism. Also $\bar{\phi}(f)=\bar{\phi}(g)$ implies $\bar{\phi}(f-g)=0$ and $f-g\in(I)$ and so θ is a semi-group isomorphism. Since θ takes the identity of $H_Z((I))$ onto the identity of $H_n((0))$, the restriction of θ to $G_Z((I))$ is an isomorphism onto $G_n((0))$.

It immediately follows by factoring that,

COROLLARY 7. *Let $I=\langle m\rangle$ be an ideal of Z_n where m divides n. Then $G_n((I))\cong G_m((0))$.*

Thus we see that we will have the structure of $G_n((I))$ for every n and every ideal I of Z_n if we can only obtain the structure of $G_n((0))$ for every n.

The case of $n=p$, a prime, is particularly interesting since it can be generalized to obtaining the structure of $G_D((0))$, the group of units of $D[x]$ under composition, for any integral domain D. Let D^+ be the additive group of D and $U(D)$ be the group of multiplicative units of D. It is well known that

$$G_D((0))=\{a+bx\in D[x]: b\in U(D)\}.$$

We can now express $G_D((0))$ as a semi-direct product. If we let

$$B=\{a+x: a\in D\} \quad \text{and} \quad H=\{bx: b\in U(D)\},$$

then B is a normal subgroup of $G_d((0))$, H is a subgroup of $G_D((0))$, $B\cap H=\{x\}$, and $BH=G_D(q0))$. Thus $G_D((0))$ is a semi-direct product of B and H, and in fact

$$G_D((0))\simeq BX_\theta H$$

where $\theta: H\to \mathrm{Aut}(B)$ is given by $\theta(bx)(a+x)=ba+x$. Of course $B\simeq D^+$ and $H\simeq U(D)$ and we can also express

$$G_D((0))\simeq D^+X_\theta U(D)$$

where $\theta: U(D)\to \mathrm{Aut}(D^+)$ by $\theta(d)(a)=da$.

Thus we have characterized $G_D((0))$ as a semi-direct product for any integral domain D. Returning to the case of Z_p, a field, we get: Let p be a prime. Then $f\in Z_p[x]$ belongs to $G_p((0))$ if and only if f has the form $f=a+bx$, $b\neq 0$, and

$$G_p((0))\simeq Z_p^+X_\theta Z_p^*$$

where Z_p^* is the multiplicative group of non-zero elements of Z_p and $\theta: Z_p^*\to$

$\leftarrow \mathrm{Aut}(Z_p^+)$ is given by $\theta(a)(c)=ac$ for $a\in Z_p^*$ and $c\in Z_p^+$.

https://doi.org/10.4153/CMB-1976-050-6 Published online by Cambridge University Press

Observe that $|G_p((0))| = p(p-1)$, and since $Z_p^+ \simeq \sigma(p)$ and $Z_p^* \simeq \sigma(p-1)$ we also have $G_p((0))$ expressed as a semi-direct product of cyclic groups. Furthermore, in this case we can identify these semi-direct products $G_p((0))$ as known groups. For any three positive integers m, n and k the *metacyclic group* $M(m, n, k)$ is defined [3, p. 462] as the group generated by two elements a and b satisfying $a^m = 1$, $b^n = 1$ and $bab^{-1} = a^k$ where $k^n \equiv 1 \bmod m$. We then have,

THEOREM 8. *Let p be a prime and n a primitive root of p. Then $G_p((0)) \simeq M(p, p-1, n)$.*

Proof. If we let $f = 1 + x$ and $g = nx$, then $f, g \in G_p((0))$ with $f^p = x$, $g^{p-1} = x$ and $g \circ f \circ g^{-1} = n + x = f^n$ with $n^{p-1} \equiv 1 \bmod p$. Also it is easily seen that f and g generate $G_p((0))$ since $f^\alpha g^\beta = \alpha + n^\beta x$ and n is a primitive root of p.

To describe $G_n((0))$ for composite n we use Theorem 6 to apply results Nöbauer [7] obtained for the ring groups $G_z((I))$. If n is a power of a prime then we can use equations (11) and (12) of [7] and Theorem 6 to determine which elements of $Z_{p^t}[x]$ belong to $G_{p^t}((0))$. Specifically, if p is a prime and $t > 0$, then $f \in G_{p^t}((0))$ if and only if it can be expressed in the form

$$f = a + bx + px^2\alpha(x)$$

with $b \in U(Z_{p^t})$, so $b \not\equiv 0 \bmod p$, and $\alpha(x) \in Z_{p^t}[x]$. Thus we have a structural representation for $G_{p^t}((0))$ to the extent that elements of $Z_{p^t}[x]$ are identifiable as elements of $G_{p^t}((0))$ or not.

Finally, for n arbitrary, $n = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r}$, $p_i \neq p_j$ for $i \neq j$, we can use Theorem 6 to apply a result of Nöbauer [7, p. 257] to get

$$G_n((0)) \simeq G_{p_1}t_1((0)) X G_{p_2}t_2((0)) X \cdots X G_{p_r}t_r((0)).$$

From this we get the result,

THEOREM 9. *$G_n((0))$ is finite if and only if n is square free.*

Proof. If $n = p_1 p_2 \cdots p_r$ is square free, then $|G_n((0))| = \prod_{i=1}^r p_i(p_i - 1)$ and hence is finite, and if n is not square free then $G_n((0))$ is not finite since $G_{p^i}((0))$ is not finite for $i > 1$.

3. The ring groups $G_n(\{I\})$. This problem is again reduced to describing $G_n(\{\langle d \rangle\})$ for every n and every d that divides n. The following theorem and corollary give us a further reduction and allow us to apply the results of Nöbauer [5, 6, 7] to this case.

THEOREM 10. *Let $I = \langle n \rangle$, n a positive integer, be an ideal of Z. Then $G_Z(\{I\}) \simeq G_n(\{0\})$.*

Proof. We first define $\theta : H_Z(\{I\}) \to H_n(\{0\})$ by $\theta(f + \{I\}) = \bar{\phi}(f) + \{0\}_n$. Now θ is well-defined, for if $f + \{I\} = g + \{I\}$ then $f - g \in \{I\}$ and by Theorem 2 we have

https://doi.org/10.4153/CMB-1976-050-6 Published online by Cambridge University Press

$\bar{\phi}(f-g)=\bar{\phi}(f)-\bar{\phi}(g)\in\{0\}_n$. Also θ is an epimorphism since ϕ is a tri-operational epimorphism. Furthermore θ is injective, for if $\phi(f)+\{0\}_n=\bar{\phi}(g)+\{0\}_n$ then $\bar{\phi}(f-g)\in\{0\}_n$ and $f-g\in\{I\}$, and so $f+\{I\}=g+\{I\}$. Thus θ is a semi-group isomorphism. Since θ takes the identity of $H_Z(\{I\})$ onto the identity of $H_n(\{0\})$, the restriction of θ to $G_Z(\{I\})$ is an isomorphism onto $G_n(\{0\})$.

Again by factoring we get,

COROLLARY 11. *Let $I=\langle m\rangle$ be an ideal of Z_n where m divides n. Then* $G_n(\{I\})\simeq G_m(\{0\})$.

Thus we reduce the problem to that of finding $G_n(\{0\})$ for arbitrary n.

The case of $n=p$, a prime, is taken care of by a more general result. If $F=GF(p^k)$ is the field of p^k elements, then using Satz 10 of [7] and Theorem 3 of [1] it is easy to see that

$$G_F(\{0\})\simeq S_{p^k}$$

where S_{p^k} is the symmetric group on p^k elements. Taking $k=1$ gives

$$G_p(\{0\})\simeq S_p.$$

The case of n composite can be solved by applying Theorem 10 to results of Nöbauer [5, 6]. First, we find the structure of $G_{p^t}(\{0\})$, p a prime, $t>1$. From Satz IV of [6] and Theorem 10 we know that all the elements of $G_{p^{t-1}}(\{0\})$ which have a representative of the form

$$f=a_0+a_1x+pa_2x^2+\cdots+p^{t-2}a_{t-1}x^{t-1}$$

form a subgroup of $G_{p^{t-1}}(\{0\})$. If we denote this subgroup by $B_{p^{t-1}}$ then Satz V of [6] gives us that $G_{p^t}(\{0\})$ is isomorphic to the complete monomial group of degree p of $B_{p^{t-1}}$. (See Ore [8] for a general study of monomial groups.) We can also obtain a formula for the order of $G_{p^t}(\{0\})$. Let $n=p^t$, p a prime, be given. For a positive integer i let $\varepsilon(i)$ denote the exponent of p in the prime factorization of $i!$, and let s be the largest integer for which $s+\varepsilon(s)<t$ and let $T=\sum_{i=0}^{s}(t-i-\varepsilon(i))$. Then equation (15) of [6] gives us that

$$|G_{p^t}(\{0\})|=p!\,(p-1)^p p^{(T-2)p}$$

Finally we can obtain $G_n(\{0\})$ for arbitrary n. If $n=p_1^{t_1}p_2^{t_2}\cdots p_r^{t_r}$ is any positive integer, then applying Theorem 10 to a result of Nöbauer [7, p. 257] we get

$$G_n(\{0\})\simeq G_{p_1}t_1(\{0\})XG_{p_2}t_2(\{0\})X\cdots XG_{p_r}t_r(\{0\}).$$

Thus we can find $G_n(\{I\})$ for any n and any ideal I of Z_n. Also, $G_n(\{I\})$ is finite for every n and I, and in fact we can obtain a formula for its order.

References

1. L. Carlitz, *A Note on Permutation Functions over a Finite Field*, Duke Math. Journal, **29** (1962), 325–332.

2. Leonard Eugene Dickson, *Introduction to the Theory of Numbers*, Dover Publications, Inc., New York, 1929.

3. Saunders MacLane and Garrett Birkhoff, *Algebra*, The MacMillan Company, New York, 1967.

4. Murray Mannos, *Ideals in Tri-operational Algebras* I, Reports Math. Colloquium, **7** (1946), 73–79.

5. Wilfred Nöbauer, *Über Gruppen von Restklassen nach Restpolynomidealen*, Sitsber. Akad. Wiss. Wien, Abt. II, **162** (1953), 207–233.

6. Wilfred Nöbauer, *Gruppen von Restpolynomidealrestklassen nach Primzahlpotenzen*, Monatsh. f. Math., **59** (1955), 194–202.

7. Wilfred Nöbauer, *Über die Operation des Einsetzen in Polynomringen*, Math. Ann., **134** (1958), 248–259.

8. Oystein Ore, *Theory of Monomial Groups*, Trans. Amer. Math. Soc., **51** (1942), 15–64.

4 Outerbridge Street,
St. John's,
Newfoundland, Canada,
A1E 3X5