Canad. Math. Bull. Vol. 27 (1), 1984

THE FIXED SUBRING OF SOME GROUPS OF RING AUTOMORPHISMS

BY

MARY DOWLEN

ABSTRACT. Let Z_m denote the ring of integers modulo an integer $m>1$ and let $G(Z_m)$ be the group under composition of all Z_m-automorphisms of $Z_m[X]$. In this paper we determine $Z_m[X]^{G(Z_m)}$, the subring of $Z_m[X]$ left fixed by elements of $G(Z_m)$.

1. **Introduction.** Let R be a commutative ring with identity and let $R[X]$ be the polynomial ring in one variable over R. A ring automorphism σ of $R[X]$ is said to be an R-automorphism of $R[X]$ if $\sigma(r)=r$ for each $r\in R$. The set $G(R)$ of all R-automorphisms of $R[X]$ is a group under composition. If H is a subgroup of $G(R)$, then we denote by $R[X]^H$ the fixed subring of H—that is,

$$R[X]^H=\{f\in R[X] \mid \sigma(f)=f \text{ for each } \sigma\in H\}.$$

In this paper we determine the ring $R[X]^{G(R)}$, where $R=Z_m$ is the ring of integers modulo an integer $m>1$. Using the standard direct sum decomposition of Z_m, most of our work goes into the case where $m=p^k$ is a prime power (this case is considered in Section 2). If $k=1$, Z_p is a field, and little work is required because of results that are known. To wit, if R is an integral domain, then standard results from Galois theory show that if H is infinite then $R[X]^H=R$, whereas a result of Samuel [2] shows that if H is finite then $R[X]^H=R[f]$, where $f=\prod_{\sigma\in H}\sigma(X)$.

Before proceeding it is necessary to consider the elements of $G(R)$ more closely and to establish some notation. It is well known that an R-endomorphism of $R[X]$ is determined by $\sigma(X)$—that is, if $\sigma(X)=h$, then $\sigma(f(X))=f(h)$ for each $f(X)\in R[X]$; we denote this endomorphism by σ_h. Moreover, in [1] Gilmer gave the following characterization of the elements of $G(R)$: If $h=\sum_{i=0}^n h_iX^i\in R[X]$, then σ_h is an R-automorphism of $R[X]$ if and only if h_1 is a unit of R and h_i is nilpotent for $i\geq 2$. From this characterization we see that $G(Z_m)$ is an infinite group if Z_m contains a nonzero nilpotent element. However, it turns out that $Z_m[X]^{G(Z_m)}$ is a finite ring extension of Z_m properly containing Z_m. In the case where m is a prime p, we show in Section 2 using Samuel's result for integral domains that $Z_p[X]^{G(Z_p)}=Z_p[(X^p-X)^{p-1}]$.

Received by the editors Novermber 30, 1982 and, in revised form, March 22, 1983.
AMS Subject Classification: 13B10.

https://doi.org/10.4153/CMB-1984-016-8 Published online by Cambridge University Press

In the case where m is not prime, we determine in Sections 2 and 3 a set of generators for $Z_m[X]^{G(Z_m)}$ as a finite ring extension of Z_m.

2. **A prime power modulus.** In this section we determine a finite set $\{g_i\}_{i=1}^t$ of polynomials in $Z_m[X]$ such that $Z_m[X]^{G(Z_m)} = Z_m[g_1, \ldots, g_t]$, where $m = p^k$ is a prime power. For any positive integer j, define $v(j)$ as the highest power of p that divides j. That is, $p^{v(j)} \mid j$, but $p^{v(j)+1} \nmid j$. Furthermore, let

$$g_i(X) = p^{k-1-v(i)}(X^p - X)^{(p-1)i} \quad \text{for all} \quad 1 \le i \le p^{k-1}.$$

LEMMA 1. $Z_p[X]^{G(Z_p)} = Z_p[(X^p - X)^{p-1}]$.

Proof. By Samuel's result [2] it suffices to show that $\prod_{\sigma \in G(Z_p)} \sigma(X) = (X^p - X)^{p-1}$. Let $\sigma \in G(Z_p)$. Then by the characterization of elements of $G(Z_p)$ [1] we have $\sigma(X) = a + bX$, where $a, b \in Z_p$ and $b \ne 0$. Hence,

$$\begin{aligned}
\prod_{\sigma \in G(Z_p)} \sigma(X) &= \prod_{a \in Z_p} \prod_{b \in Z_p/\{0\}} (a + bX) \\
&= \prod_{a \in Z_p} \prod_{b \in Z_p/\{0\}} b(ab^{-1} + X) \\
&= \prod_{c \in Z_p} \prod_{b \in Z_p/\{0\}} b(c + X) \\
&= \prod_{b \in Z_p/\{0\}} b \prod_{c \in Z_p} (c + X) \\
&= \prod_{b \in Z_p/\{0\}} b\,(X^p - X) \\
&= (X^p - X)^{p-1}
\end{aligned}$$

LEMMA 2. *Let n be a positive integer. Then* $p^{v(n)+1} \,\Big|\, \binom{n}{i} p^i$ *for all* $1 \le i \le n$.

Proof. It suffices to show that $p^{v(n)+1-i} \,\Big|\, \binom{n}{i}$ for $1 \le i \le v(n)+1$. Let $n = p^{v(n)} \cdot r$ and $i = p^{v(i)} \cdot s$. Then

$$\binom{n}{i} = (n/i)\binom{n-1}{i-1} = p^{v(n)-v(i)}(r/s)\binom{n-1}{i-1}.$$

since $\binom{n}{i}$ is an integer and s is relatively prime to p, then $(r/s)\binom{n-1}{i-1}$ is an integer. Hence, it suffices to show that $p^{v(n)+1-i} \mid p^{v(n)-v(i)}$ for $1 \le i \le v(n)+1$. But this is trivially true since $i \ge v(i)+1$ for all positive integers i. Thus, $p^{v(n)+1} \,\Big|\, \binom{n}{i} p^i$ for $1 \le i \le n$.

LEMMA 3. *Let* $f(X) = \sum_{i=0}^n f_i X^i \in Z_{p^k}[X]^{G(Z_{p^k})}$. *Then* $p(p-1) \mid n$.

https://doi.org/10.4153/CMB-1984-016-8 Published online by Cambridge University Press

Proof. Let $\sigma_{1+X} \in G(Z_{p^k})$. Then $\sigma_{1+X}(f) = f$ or $\sigma_{1+X}(f) - f = 0$. If we equate the coefficients of X^{n-1}, we obtain $f_{n-1} + nf_n - f_{n-1} = 0$ or $nf_n = 0$. Since $f_n \neq 0$, then $n \in (p)$ so $p \mid n$.

Next choose an element b of Z_{p^k} such that $b + (p)$ is a $(p-1)^{\text{st}}$-primitive root of unity in $Z_{p^k}/(p)$. Since $b \notin (p)$, then b is a unit in Z_{p^k}. Also, if $(p-1) \nmid i$, then $b^i - 1 \notin (p)$. Now $\sigma_{bX}(f) = f$ because $\sigma_{bX} \in G(Z_{p^k})$. If we equate the coefficients of X^n in this equation, we have $b^n f_n = f_n$ or $f_n(b^n - 1) = 0$. Since $f_n \neq 0$, then $b^n - 1 \in (p)$ so $(p-1) \mid n$. Thus, $p(p-1) \mid n$.

THEOREM 1. $Z_{p^k}[X]^{G(Z_{p^k})} = Z_{p^k}[\{g_i(X)\}_{i=1}^{p^{k-1}}]$.

Proof. Let $\sigma_h \in G(Z_{p^k})$, where $h = h_0 + h_1 X + \cdots + h_m X^m$, and fix $1 \leq i \leq p^{k-1}$. Then we show that $\sigma_h(g_i(X)) = g_i(X)$. We can write $h = h_0 + h_1 X + ph*(X)$, since h_j is nilpotent for $2 \leq j \leq m$. Moreover, by Fermat's theorem we know that $h_i^p = h_i + pr_{hi}$ for $i = 0, 1$. Then using these facts we can simplify

$$\sigma_h(X^p - X) = h(X)^p - h(X) = h_1 X^p - h_1 X + pm(X),$$

where

$$m(X) = r_{h1} X^p + r_{h0} - h^*(X) + \sum_{j=1}^{p} \binom{p}{j} p^{j-1} h^*(X)^j (h_0 + h_1 X)^{p-j}$$
$$+ \sum_{j=1}^{p-1} \left[\binom{p}{j} \Big/ p \right] h_0^j h_1^{p-j} X^{p-j}.$$

Hence,

$$\sigma_h(g_i(X)) = p^{k-1-v(i)}(h_1 X^p - h_1 X + pm(X))^{(p-1)i}$$
$$= p^{k-1-v(i)}(h_1 X^p - h_1 X)^{(p-1)i}$$
$$+ \sum_{j=1}^{(p-1)i} p^{k-1-v(i)} \binom{(p-1)i}{j} p^j m(X)^j (h_1 X^p - h_1 X)^{(p-1)i-j}$$

By Lemma 2, we know that $p^k \mid p^{k-1-v(i)} \binom{(p-1)i}{j} p^j$ for all $1 \leq i \leq (p-1)i$. Hence,

$$\sigma_h(g_i(X)) = p^{k-1-v(i)} h_1^{(p-1)i} (X^p - X)^{(p-1)i}$$

Again using Lemma 2 and writing $h_1^{p-1} = 1 + pr_{h1} h_1^{-1}$, we get $p^{k-1-v(i)} h_1^{(p-1)i} = p^{k-1-v(i)}(1 + pr_{h1} h_1^{-1})^i = p^{k-1-v(i)}$. So finally,

$$\sigma_h(g_i(X)) = p^{k-1-v(i)}(X^p - X)^{(p-1)i} = g_i(X).$$

Thus, $Z_{p^k}[\{g_i(X)\}_{i=1}^{p^{k-1}}] \subseteq Z_{p^k}[X]^{G(Z_{p^k})}$.

Let $f = \sum_{i=0}^{n} f_i X^i \in Z_{p^k}[X]^{G(Z_{p^k})}$, then by Lemma 3 we know $n = p(p-1)r$. we use induction on n. If $n = 0$, then $f = f_0 \in Z_{p^k} \subseteq Z_{p^k}[\{g_i(X)\}_{i=1}^{p^{k-1}}]$. We assume the hypothesis is true for all polynomials of degree less than n. Let $r = p^{k-1}s + t$, where $0 \leq t < p^{k-1}$. We note that $v(r) = v(t)$ because $t < p^{k-1}$. From the proof

https://doi.org/10.4153/CMB-1984-016-8 Published online by Cambridge University Press

of Lemma 3 we know that $f_n \in (p^{k-1-v(t)})$, so we write $f_n = p^{k-1-v(t)}c$. We consider
$$f^*(X) = f(X) - c[g_{p^{k-1}}(X)]^s[g_t(X)].$$

Clearly, $f^*(X) \in Z_{p^k}[X]^{G(Z_{p^k})}$ and $\deg f^*(X) < n$ so $f^*(X) \in Z_{p^k}[\{g_i(X)\}_{i=1}^{p^{k-1}}]$ by the induction hypothesis. Hence $f(X)$ is also in $Z_{p^k}[\{g_i(X)\}_{i=1}^{p^{k-1}}]$. This completes the proof that $Z_{p^k}[X]^{G(Z_{p^k})} = Z_{p^k}[\{g_i(X)\}_{i=1}^{p^{k-1}}]$.

3. **The general case.** In order to extend Theorem 1 to the case of modulus m, we use the standard direct sum decomposition of Z_m. If m is written as a product of distinct powers
$$m = p_1^{k_1} \cdots p_r^{k_r},$$
then the ring Z_m can be represented as a direct sum of rings
$$Z_m \overset{\phi}{\cong} Z_{p_1^k} \oplus \cdots \oplus Z_{p_r^k}.$$
The isomorphism ϕ is defined using the Chinese Remainder Theorem.

(1) $\qquad \phi(a) = (a_1, \ldots, a_r), \quad \text{where} \quad a = a_j (\text{mod } p_j^{k_j}) \qquad j = 1, 2, \ldots, r.$

The isomorphism ϕ extends to the polynomial ring $Z_m[X]$ and induces an isomorphism ϕ^* between $Z_m[X]$ and $Z_{p_1^{k_1}}[X] \oplus \cdots \oplus Z_{p_r^{k_r}}[X]$ defined by

(2) $\qquad \phi^*(f_0 + f_1X + \cdots + f_nX^n) = (f_{10} + \cdots + f_{1n}X^n, \ldots, f_{r0} + \cdots + f_{rn}X^n),$
$$\text{where} \quad \phi(f_i) = (f_{1i}, f_{2i}, \ldots, f_{ri}) \quad i = 1, \ldots, n.$$

Moreover, it can be verified that ϕ^* restricted to the subring $Z_m[X]^{G(Z_m)}$ maps $Z_m[X]^{G(Z_m)}$ onto the subring $Z_{p_1^{k_1}}[X]^{G(Z_{p_1^{k_1}})} \oplus \cdots \oplus Z_{p_r^{k_r}}[X]^{G(Z_{p_r^{k_r}})}$, yielding the following theorem.

THEOREM 2. *Let $m \in Z^+$ be such that $m = p_1^{k_1} \cdots p_r^{k_r}$, where $p_1, \ldots, p_r$ are primes and $k_i > 0$ for all $1 \le i \le r$. Let ϕ and ϕ^* be defined as in* (1) *and* (2). *For all $1 \le i \le r$ and $1 \le j \le p_i^{k_i - 1}$ define $g_{ij}^* = (h_{i1}, \ldots, h_{ir})$, where $h_{im} = 0$ for $i \ne m$ and*
$$h_{ii} = g_j.$$
Then $Z_m[X]^{G(Z_m)} = Z_m[f_{11}, \ldots, f_{1p_1^{k_1-1}}, \ldots, f_{r1}, \ldots, f_{rp_r^{k_r-1}}]$, *where* $f_{ij} = [(\phi^*)^{-1}(g_{ij}^*)]$.

EXAMPLE. $M = 12$. Let $Z_{12} \cong Z_4 \oplus Z_3$. We have seen that $Z_3[X]^{G(Z_3)} = Z_3[(X^3 - X)^2]$ and that $Z_4[X]^{G(Z_4)} = Z_4[2(X^2 - X), (X^2 - X)^2]$. By Theorem 2 we see that $Z_{12}[X]^{G(Z_{12})} = Z_{12}[6(X^2 - X), 9(X^2 - X)^2, 4(X^3 - X)^2]$.

REFERENCES

1. R. Gilmer, *R-automorphisms of R[X]*, Proc. London Math. Soc. (3) **18** (1968), 328–336.
2. P. Samuel, *Groupes finis d'automorphismes des anneaux de séries formelles*, Bull. Sc. Math., 2e série, 90, 1966, 97–101.

MATHEMATICS DEPARTMENT
FLORIDA STATE UNIVERSITY
TALLAHASSEE, FL 32306

https://doi.org/10.4153/CMB-1984-016-8 Published online by Cambridge University Press