ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 22, Number 3, Summer 1992

# ON THE POWER POLYNOMIAL $x^d$ OVER GALOIS RINGS

JAVIER GOMEZ-CALDERON

ABSTRACT. Let $p$ denote a prime. Let $\mathrm{GR}(p^n, m)$ denote the Galois ring of order $p^{nm}$. Let $P_d(x)$ denote the power polynomial $P_d(x) = x^d$ over the ring $\mathrm{GR}(p^n, m)$. In this paper we determine two cardinalities: the cardinality of the value set $\{P_d(x) : x \in \mathrm{GR}(p^n, m)\}$, and the cardinality of the preimage $P_d^{-1}(P_d(x))$ for each $x$ in $\mathrm{GR}(p^n, m)$.

**1. Introduction.** For a prime $p$, let $\mathrm{GR}(p^n, m)$ denote the Galois ring of order $p^{nm}$ which can be obtained as a Galois extension of $Z_{p^n}$ of degree $m$. Thus $\mathrm{GR}(p^n, 1) = Z_{p^n}$ and $\mathrm{GR}(p, m) = K_{p^m}$, the finite field of order $p^m$. The reader can find further details concerning Galois rings in the excellent reference [**1**].

Now, for $d \geq 1$, let $P_d(x) = x^d$ denote the power polynomial of degree $d$ over $\mathrm{GR}(p^n, m)$. Then it is easy to check that the cardinality of the value set of $P_d(x)$ over the field $\mathrm{GR}(p, m) = K_p m = K_q$ depends only upon $(d, q-1)$, the greatest common divisor of $d$ and $q-1$. To be more specific,

$$|\{P_d(x) : x \in \mathrm{GR}(p, m) = K_q\}| = \frac{q-1}{(q-1, d)} + 1$$

where $q = p^m$.

In this paper we not only determine the cardinality of the value set $\{P_d(x) : x \in \mathrm{GR}(p^n, m)\}$ for $n \geq 1$, but if $x_0 \in \mathrm{GR}(p^n, m)$, we also determine the cardinality of the preimage of $P_d(x_0)$.

**2. p odd.** Throughout this section we assume that $p$ is odd. Let $\mathrm{GR}^*(p^n, m)$ denote the group of units of $\mathrm{GR}(p^n, m)$. Then, see [**1**, Theorem XVI.9], $\mathrm{GR}^*(p^n, m)$ is a direct product of two groups $G_1$ and

Received by the editors on September 8, 1989 and in revised form on June 15, 1990.