دانشگاه صنعتی اصفهان

دانشکده علوم ریاضی

# تجزیه چندجمله‌ای‌ها روی حلقه‌های گالوا و ٹکدهای دوری و منفی‌ـدوری

پایان‌نامه کارشناسی ارشد ریاضی محض

**عارف ارفع‌نژاد**

استاد راهنما

**دکتر بیژن طائری**

۱۳۸۵

# فهرست مطالب

## چکیده:

فرض کنید $R$ یک حلقه موضعی متناهی با ایدال ماکسیمال $M$ باشد. تمام عناصر $M$ پوچ‌توان هستند و عناصر $R\backslash M$ یکه هستند. میدان $K := R/M$ را میدان مانده‌ای $R$ گوییم. تصویر $c \in R$ تحت همریختی کانونی $\mu$ از $R$ به $K$را با $\overline{c}$ نشان می‌دهیم. این همریختی به طور طبیعی به همریختی کانونی از $R[x]$ به $K[x]$ توسعه می‌یابد. چندجمله‌ای $f \in R[x]$ را تحویل‌ناپذیر اساسی گوییم اگر $\overline{f}(x)$ در $K[x]$ تحویل‌ناپذیر باشد. اگر $f(x) \in \mathbb{Z}_{p^n}[x]$ و $f(x)$ یک چندجمله‌ای تکین تحویل‌ناپذیر اساسی از درجه‌ی $r$ باشد حلقه‌ی رده‌های مانده‌ای $\frac{\mathbb{Z}_{p^n}[x]}{\langle f(x)\rangle}$ را حلقه‌ی گالوا می‌نامیم. این حلقه را با $GR(p^n, r)$ نشان می‌دهیم. در این پایان‌نامه تجزیه چندجمله‌ای‌های ابتدایی به عوامل تحویل‌ناپذیر روی حلقه‌های گالوا از مشخصه $p^2$ را بررسی می‌کنیم و یک الگوریتم برای تجزیه این چندجمله‌ای‌ها ارایه می‌دهیم. همچنین فرم کلی ایدال‌های حلقه‌های $\mathcal{R} = \frac{R[x]}{\langle x^n-1\rangle}$ و $\mathcal{S} = \frac{R[x]}{\langle x^n+1\rangle}$ را تعیین می‌کنیم. ایدال‌های $\mathcal{R}$ را کدهای دوری از طول $n$ و ایدال‌های $\mathcal{S}$ کدهای منفی ـدوری از طول $n$ می‌نامیم. در آخر کدهای دوری از طول $2^s$ روی $\mathbb{Z}_4$ و کدهای منفی ـدوری از طول $2^s$ را روی حلقه‌های گالوا به‌دست می‌آوریم.