



دانشگاه صنعتی اصفهان

دانشکده علوم ریاضی

تجزیه چند جمله‌ای‌ها روی حلقه‌های گالوا و گدهای دوری و منفی-دوری

پایان‌نامه کارشناسی ارشد ریاضی محض

عارف ارفع‌نژاد

استاد راهنما

دکتر بیژن طائری

۱۳۸۵

فهرست مطالب

۱	فصل اول پیش‌نیازها
۱	۱-۱ تاریخچه و مقدمه
۴	۲-۱ تعاریف و مفاهیم پایه
۵	۳-۱ حلقه‌های جابه‌جایی موضعی
۱۱	۴-۱ حلقه‌های گالوا
۱۷	فصل دوم تجزیه چندجمله‌ای‌ها روی حلقه‌های گالوا
۱۹	۱-۲ محک تحویل‌ناپذیری برای چندجمله‌ای‌های ابتدایی روی حلقه‌های گالوا
۲۳	۲-۲ تجزیه‌ی چندجمله‌ای‌های ابتدایی روی $GR(p^2, r)$
۳۱	۳-۲ تجزیه‌ی $x^n - 1$ و $x^n + 1$
۴۳	فصل سوم ایدال‌های حلقه‌های متناهی خاص
۴۵	۱-۳ ایدال‌های حلقه‌های متناهی که به صورت $R[x]/\langle f \rangle$ هستند
۵۱	فصل چهارم کدهای دوری از طول 2^e روی Z_4
۵۲	۱-۴ کدهای دوری روی Z_4
۵۷	فصل پنجم کدهای منفی دوری از طول 2^s روی حلقه‌های گالوا
۵۹	۱-۵ ساختار کدهای منفی دوری
۶۳	۲-۵ فاصله همینگ
۷۹	ضمیمه: برنامه‌های کامپیوتری

واژه‌نامه انگلیسی به فارسی

۸۹

مراجع

۹۳

چکیده:

فرض کنید R یک حلقه موضعی متناهی با ایدال ماکسیمال M باشد. تمام عناصر M پوچ توان هستند و عناصر $R \setminus M$ یکه هستند. میدان $K := R/M$ را میدان مانده‌ای R گوئیم. تصویر $c \in R$ تحت همریختی کانونی μ از R به K را با \bar{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 گوئیم اگر $\bar{f}(x)$ در $K[x]$ تحویل‌ناپذیر باشد. اگر $f(x) \in \mathbb{Z}_{p^n}[x]$ و $f(x)$ یک چندجمله‌ای تکین تحویل‌ناپذیر اساسی از درجه 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 ارائه 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 دوری از طول n می‌نامیم. در آخر کدهای دوری از طول 2^s روی \mathbb{Z}_4 و کدهای منفی دوری از طول 2^s را روی حلقه‌های گالوا به دست می‌آوریم.