

Mathematisch-Naturwissenschaftliche Fakultät

Institut für Mathematik

Fachgebiet: Mathematik

Betreuerin: Prof. Dr. Gohar Kyureghyan

Doktorand: Max Schulz

(e-mail: maxschulz97@web.de)

Irreducible Polynomials over Finite Fields and Rational Transformations

Englische Zusammenfassung

Finite fields play an important role in modern coding theory and cryptography. Probably the most common way of representing a finite field is as a residue class ring modulo an ideal generated by an irreducible polynomial. The multiplicative arithmetic of the constructed finite field depends significantly on the properties of the chosen irreducible polynomial. There are many ways of how to construct irreducible polynomials. One such construction is the so-called *rational transformation* of polynomials. In the context of constructing irreducible polynomials over finite fields, rational transformations have been studied extensively for almost 60 years now. In this thesis, we look at rational transformations with rational functions arising from invariant subfields of the rational function field. The polynomials we obtain by this construction factorize into an orbit of a group action on the irreducible polynomials that has attracted quite some interest in the finite field context since the papers by Garefalakis (2011) and Stichtenoth and Topuzoğlu (2012). By establishing this connection, we are able to obtain new results about irreducible polynomials over finite fields, invariant polynomials, and rational transformations.

Deutsche Zusammenfassung

Endliche Körper spielen eine wichtige Rolle in der heutigen Codierungstheorie und Kryptographie. Meist werden endliche Körper als Quotientenring repräsentiert. Um diesen Quotientenring zu konstruieren benötigt man ein irreduzibles Polynom, welches die multiplikative Arithmetik des derart konstruierten endlichen Körpers maßgeblich beeinflusst. Es gibt viele Konstruktionsverfahren für irreduzible Polynome. Eines dieser Verfahren ist die sogenannte *rationale Transformation* von Polynomen. Rationale Transformationen werden nun schon seit ungefähr 60 Jahren als Verfahren zur Konstruktion von irreduziblen Polynomen über endlichen Körpern studiert. In dieser Arbeit betrachten wir rationale Transformationen mit rationalen Funktionen aus invarianten Unterkörpern des rationalen Funktionenkörpers. Die Polynome die wir auf diese Weise konstruieren, faktorisieren als Orbit einer Gruppenwirkung auf den irreduziblen Polynomen, welche seit den Veröffentlichungen von Garefalakis (2011) und Stichtenoth und Topuzoğlu (2012) vermehrt im Kontext von endlichen Körpern Beachtung fanden. Wir benutzen diese von uns gefundene Verbindung, um neue Ergebnisse über irreduzible Polynome über endlichen Körpern, invarianten Polynomen, und rationalen Transformationen zu gewinnen.