WS 07/08

Seminar der WE AℓZAGK

Do 8:30 - 10:00 in MZH 7200

Im WS 07/08 wollen wir Einblicke in 3 ThemenBereiche geben, die für unsere WE von Bedeutung sind: Endliche Körper, CodierungsTheorie, Gröbner Basics. Gedacht ist an jeweils 4-5 Vorträge, in denen relativ leicht zugängliche Tatsachen vorgestellt werden.

Endliche Körper *(M. Hortmann; michaelh@informatik.uni-bremen.de)*
Endliche Körper sind Grundbausteine der Kryptographie und CodierungsTheorie. Sie entstehen ganz einfach als Restklassenringe von $\mathbb{Z}$ bez. einer Primzahl bzw. von $\mathbb{F}[X]$ bez. eines irreduziblen Polynoms (wobei $\mathbb{F}$ schon ein endlicher Körper ist) und bieten eine schöne und reichhaltige Theorie.
Behandelt werden können: Struktur der multiplikativen Gruppe, Anzahl und Konstruktion irreduzibler Polynome, Nullstellen und Faktorisierung von Polynomen, Konstruktion und Eigenschaften von Normalbasen.

CodierungsTheorie *(E. Oeljeklaus; oel@math.uni-bremen.de)*
Die CodierungsTheorie beschäftigt sich mit der Entwicklung und Analyse von Codes, die einen effizienten und verlässlichen Datentransfer über nicht störungsfreie elektronische Kanäle ermöglichen. Eine wesentliche Aufgabe der Theorie besteht darin, Verfahren zu entwickeln, mit denen fehlerhaft übertragene Daten korrigiert werden können. Die theoretischen und technischen Möglichkeiten der CodierungsTheorie sind heute so weit entwickelt, dass z.B. ein guter CD-Player etwa 4000 in Folge zerstörte Audiobits rekonstruieren kann, ohne dass der Fehler auf der CD vom menschlichen Ohr wahrnehmbar ist.
Im Seminar wollen wir uns mit einigen interessanten theoretischen Fragestellungen der CodierungsTheorie beschäftigen, deren Lösung im Rahmen eines Seminarvortrages dargestellt werden kann.

Gröbner Basics *(J. Gamst: gamst@math.uni-bremen.de)*
GröbnerBasen sind besonders nützliche Erzeugendensysteme von Polynomidealen $\mathfrak{a}$ in $K[X_1, \ldots, X_n]$. Der Umgang mit ihnen erfordert den Einsatz von Computern. Sie sind deswegen populär geworden, weil man mit Hilfe von GröbnerBasen viele Aufgaben der Idealtheorie algorithmisch lösen kann: Bestimmen von Basen für Restklassenringe $K[X_1, \ldots, X_n]/\mathfrak{a}$, Erzeugung des Durchschnittes zweier Ideale, Eliminationstheorie.
Im Seminar sollen zunächst die Definition, Charakterisierung und Herstellung von GröbnerBasen behandelt werden, dann vor allem die Anwendung in der Eliminationstheorie.

Näheres bei

J. Gamst, MZH 7110, Di 10-12; gamst@math.uni-bremen.de