Karlsruher Institut für Technologie

KIT-Fakultät für Mathematik
Institut für Algebra und Geometrie
PD Dr. Stefan Kühnlein

Proseminar Sommersemester 2023
Endliche Körper

In diesem Proseminar wollen wir uns Zeit nehmen, Eigenschaften endlicher Körper kennenzulernen und einige Anwendungen dieser Theorie anzusprechen.

Ein endlicher Körper ist ein Körper im Sinne der Algebra, der nur endlich viele Elemente enthält. Aus der Linearen Algebra sind als Beispiele die Restklassenkörper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z},\ p$ eine Primzahl, bekannt. Wir werden diese in Erinnerung bringen und uns überlegen, dass es zu jeder Primzahlpotenz $p^e, e \in \mathbb{N}$, einen Körper mit dieser Elementzahl gibt, aber (bis auf Isomorphie) keine weiteren.
Wir wollen auf die Theorie der linearen Codes eingehen und in einem Vortrag das RSA-Kryptographieverfahren ansprechen, das nach wie vor vielen Verschlüsselungsverfahren zugrunde liegt.
Wir werden weiter sehen, dass ein endlicher Schiefkörper immer kommutativ ist, und werden – eventuell – Matrizengruppen über endlichen Körpern studieren.

Termin des Proseminars:

Donnerstags, 09:45 – 11:15 Uhr in -1.013

Bei Rückfragen wenden Sie sich bitte an mich: `stefan.kuehnlein@kit.edu`