

Dozent: Prof. Dr. Uwe Jannsen

<http://www.mathematik.uni-regensburg.de/Jannsen/index.html>

Vorlesung (51 005): Lineare Algebra I

Zeit und Ort: 4 st., Mo, Do 10-12 Uhr, H 31

Zentralübung (51 007): Mi 12-14 Uhr im H 31

Übungen (51 006): 2st. in kleinen Gruppen nach Vereinbarung

Vorkenntnisse: Schulwissen

Inhalt: Pflichtteil der Grundausbildung für Mathematikstudenten (Bachelor und Lehramt vertieft). Einmalige Veranstaltung wegen des doppelten Abiturjahrgangs 2011.

Stichworte: Lineare Gleichungssysteme, Matrizen, Vektorräume, Basen, Lineare Abbildungen, Eigenwerte, Gaußverfahren, Hauptachsentransformation

Literatur: Bosch, Lineare Algebra, Springer.
Fischer, Lineare Algebra, Vieweg.

Anschlussveranstaltung: Lineare Algebra II im Wintersemester 2011/12

Benoteter Leistungsnachweis: ja

Erfolgreiche Teilnahme an den Übungen und Bestehen einer benoteten Klausur

Unbenoteter Leistungsnachweis: ja

Erfüllen der zur Klausurzulassung notwendigen Kriterien

Regelungen im modularisiertem Studium (Bachelor/Lehramt):

Die Veranstaltung kann in folgenden Modulen angerechnet werden: BGLA, LGyLA

Art der Modulprüfungen: schriftliche Klausur am Mo. 01.08.2011 um 9.00 Uhr. Wiederholungsprüfung Mitte Oktober 2011. Weitere Details werden rechtzeitig bekannt gegeben.

Anmeldeverfahren zur Modulprüfung: Flexnow. Anmeldefrist wird rechtzeitig in der Vorlesung bekannt gegeben.

Anrechenbare Leistungspunktzahl (ECTS): Die obigen Klausuren sind Teilprüfungen der Module BGLA und LGyLA (20 LP bei Bestehen des gesamten Moduls)

Seminar/Hauptseminar (51 225 und 51 231) über Zahlentheorie (mit Patrick Forré und Bernd Schober):

Titel: Zahlentheorie und Kryptographie

Zeit und Ort: 2 st., Fr 10 – 12, M 101 und Di, 12–14, M 006.

Inhalt: Kryptographie befasst sich mit Methoden Nachrichten so zu verschlüsseln, dass diese nur dem Adressaten zugänglich werden. In diesem Seminar werden wir die grundsätzlichen Konzepte der Verschlüsselungsverfahren kennenlernen wie die

symmetrischen Verfahren und Public-Key-Systeme. Wir werden die arithmetischen Grundlagen aus der elementaren Zahlentheorie und der algebraischen Geometrie entwickeln/wiederholen, um verschiedene Kryptosysteme begreifen zu können. Dazu zählen insbesondere das RSA-Verfahren und das DL-Verfahren auf elliptischen Kurven.

Literatur:

- Buchmann, J., *Einführung in die Kryptographie*, 5. Aufl., Springer 2010.
- Koblitz, N., *A Course in Number Theory and Cryptography*, 2nd ed., GTM 114, Springer 1994.
- Werner, A., *Elliptische Kurven in der Kryptographie*, Springer 2002.

Vorkenntnisse: Algebra (Gruppen, Körper, endliche Körper, Chinesischer Restsatz, Polynome, Hauptsatz über endlich erzeugte abelsche Gruppen u.ä.).

Vorbesprechung: Dienstag 8. Februar 2011 im Raum M006 um 14-16 Uhr.

Kontakt: Patrick Forré, Raum M223, Tel. 2772, patrick.forre@mathematik.uni-r.de.

Seminar (51 263): Diplomanden- und Bachelorseminar

Zeit und Ort: Mi 12-14 Uhr im M 104, Beginn 04.05.2011.

Vorkenntnisse: Arbeit an einer Diplom- oder Bachelorarbeit bei mir.

Inhalt: Diplomanden (bzw. Bachelor-Studenten) tragen zweimal (bzw. einmal) über ihre Diplomarbeit (bzw. Bachelorarbeit) vor. Es soll der Inhalt erläutert werden und die Präsentation von mathematischen Inhalten geübt werden.

Anschlussveranstaltung: Das Seminar wird in jedem Semester angeboten.

Benoteter Leistungsnachweis: ja (für Bachelor-Studenten) Erfolgreiche Präsentation.

Unbenoteter Leistungsnachweis: nein

Regelung im modularisierten Studium (Bachelor): Die Veranstaltung kann in folgenden Modulen angerechnet werden: BSem

Art der Modulprüfung: Bewertung der Präsentation

Anmeldeverfahren zur Modulprüfung: Flexnow. Anmeldung bis 04.05.2011.

Anrechenbare Leistungspunkte (ECTS): 3LP für das Bachelor-Seminar.

Seminar (51 277): Oberseminar Arithmetische Geometrie (gemeinsam mit G. Kings, K. Künnemann und N. Naumann) Es werden wechselnde Themen aus der Arithmetischen Geometrie gemeinsam erarbeitet. Das Thema wird in einer Vorbesprechung am 10.02.2011 beschlossen.

Zeit und Ort: 2 st., 14-16 Uhr M 104

Seminar (51 278): Seminar der Forschergruppe (gemeinsam mit G. Kings, K. Künnemann und N. Naumann) Gäste und Mitglieder der Forschergruppe berichten über ihre wissenschaftliche Arbeit

Zeit und Ort: 2 st., 13-15 Uhr M 104