PD Dr. F. Hörmann
Proseminar endliche Körper — Sommer 2020
Vortragsliste

Allgemeines:

- Sollten sich mehr Studierende für das Seminar interessieren, als es Vorträge gibt, so können Sie auch zu zweit einen Vortrag vorbereiten.
- **Kommen Sie bitte 3–4 Wochen vor Ihrem Vortrag zu mir, um die Stoffauswahl im Detail zu besprechen und Fragen zu diskutieren. Während der vorlesungsfreien Zeit bitte mit Anmeldung per eMail.**
- **Suchen Sie auch nach anderer Literatur und schauen Sie nicht nur in die angegebenen Referenzen!** Am Ende jedes Kapitels in [LN] finden Sie z.B. weitere Referenzen.

Literatur:

[LN] Rudolf Lidl, Harald Niederreiter, *Finite fields* , Cambridge University Press, 1997, im Semesterapparat der Bibliothek

[K] Hans Kurzweil, *Endliche Körper*, Springer 2008, verfügbar online über die UB

[Ko] Neil Koblitz, *A Course in Number Theory and Cryptography*, Springer 1987, verfügbar online über die UB

[IR] Kenneth Ireland, Michael Rosen, *A Classical Introduction to Modern Number Theory*, Second Edition, Springer GTM volume 84, Kapitel 7–10, im Semesterapparat der Bibliothek

[H] Xiang-dong Hou, *Lectures on Finite Fields*, AMS Graduate Studies in Mathematics, Volume: 190; 2018 , im Semesterapparat der Bibliothek

Vorträge:

23.4. **1. Grundbegriffe über Gruppen und Ringe**

- Hauptreferenz: [LN], Section I.1–I.2
- Legen Sie den Schwerpunkt auf die Beispiele $\mathbb{Z}/N\mathbb{Z}$, insbesondere für $N = p$, eine Primzahl.
- Lassen Sie die Wiederholung von Begriffen weg, die nur für nicht-kommutative Gruppen wichtig sind (z.B. Normalteiler).

siehe auch [K, Kapitel 1, 6, 8]

30.4. **2. Polynomringe und Grundbegriffe über Körpererweiterungen.**

Die wichtigsten Eigenschaften der Polynomringe $k[X]$ über einem Körper k, insbesondere dass sie Hauptidealringe sind. Für ein Ideal I in $k[X]$: Wann ist $k[X]/I$ wieder ein Körper? Was ist eine Körpererweiterung von k? Wann sind Körpererweiterungen von der Form $k[X]/I$? Was versteht man unter dem Zerfällungskörper eines Polynoms?

- Hauptreferenz: [LN], Section I.3–I.4

siehe auch [K, Kapitel 2–5, 8, 10]

7.5. **3. Konstruktion und Eigenschaften von endlichen Körpern**

Für jede Primzahlpotenz p^n existiert ein (bis auf Isomorphie) eindeutiger Körper $\mathbb{F}_{p^n}$ mit p^n Elementen. Wie beweist man dies? Wie werden diese Körper explizit konstruiert? Führen Sie ein oder zwei Beispiele genau aus (z.B. $\mathbb{F}_4$ oder $\mathbb{F}_9$). Verwenden Sie einige Zeit auf den Beweis von Theorem 2.8 (siehe Referenz unten; die multiplikative Gruppe eines endlichen Körpers ist zyklisch.) Sie können auch alternative Beweise aus den anderen Büchern präsentieren, falls die Ihnen verständlicher erscheinen.

- Hauptreferenz: [LN], Section II.1–II.2

14.5. **4. Lineare Codes**

Eine Nachricht bestehend aus, sagen wir, n Bits kann durch Hinzufügen sehr weniger (im Vergleich mit n) Bits so verändert werden, dass die Wahrscheinlichkeit für Übertragungsfehler beliebig klein wird, und sogar Fehler, die eine feste Anzahl von Bits betreffen, immer mit Sicherheit korrigiert werden können. In diesem und dem nächsten Vortrag sollen solche Codes mit Hilfe der Theorie der endlichen Körper konstruiert werden.

Beispiel: Hamming Codes

- Hauptreferenz: [LN], Section IX.1

28.5. **5. zyklische Codes**

Beispiel: Reed-Solomon Codes

- Hauptreferenz: [LN], Section IX.2

siehe auch [K, Kapitel 12]

18.6. **6. Einführung in Kryptographie**

Wir kann man Nachrichten so verschlüsseln, dass die Verschlüsselungsmethode nicht, oder nur mit unpraktikabel grossem Rechenaufwand aus dem verschlüssten Text rekonstruiert werden kann? Dieser Vortrag gibt eine Einführung in die Grundbegriffe der Kryptographie und stellt einige weniger sichere, "naive" Verschlüsselungsmethoden vor und diskutiert ihre Angreifbarkeit.

- Hauptreferenz: [Ko, III, 1.]

25.6. **7. Public-Key- und RSA-Kryptographie**

Dieser Vortrag diskutiert die Idee der Public-Key-Kryptographie. Hier ist die **Ver**schlüsselungsmethode vollständig bekannt, jeder kann also Nachrichten verschlüsseln. Dennoch kann die umgekehrte Operation, das Entschlüsseln, daraus nicht rekonstruiert werden. Zusätzliche Information (ein privater Schlüssel) sind nötig. Das bekannteste solche Verfahren ist die RSA-Verschlüsselung, der das Rechnen mit Kongruenzen (zu dem auch die endlichen Körper gehören) zugrunde liegt.

- Hauptreferenz: [Ko, IV, 1.–2.]

2.7. **8. Die Sätze von Waring und Chevalley**

Jede polynomiale Gleichung, wie z.B.

$$X^{17} + X \cdot Y^{20} + Z^5 = 0$$

hat über einem endlichen Körper offensichtlich nur endlich viele Lösungen. Heuristisch würde man vermuten, dass es um so mehr Lösungen gibt, je mehr Variablen vorhanden sind. Dennoch ist überraschend, dass bereits gilt: Eine polynomiale Gleichung p mit $p(0, \ldots, 0) = 0$ hat auf jeden Fall eine weitere Lösung, falls es mehr Variablen gibt als der Grad von p angibt. Dies ist der Satz von Chevalley, der in diesem Vortrag bewiesen werden soll.

- Hauptreferenz: [LN], Section VI.1

9.7. **9. Charaktere und Gausssummen.**

Wenn man nach der genauen *Anzahl* von Lösungen einer polynomialen Gleichung, hier

$$x^n + y^n = 1$$

in $\mathbb{F}_p$ fragt, dann stellt man erstaunliche kombinatorische Gesetzmässigkeiten fest. Z.B. gibt es einen Zusammenhang dieser Anzahl für $n = 3$ und den Darstellungen von p in der Form $p = \omega \cdot \overline{\omega}$, wobei ω eine *komplexe* Zahl der Form

$$a + b\zeta_3, \quad a, b \in \mathbb{Z}$$

ist, worin $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ eine dritte Einheitswurzel ist.

Dieser und der folgende Vortrag untersuchen diese Art von Gesetzmässigkeiten.

- Hauptreferenz: [IR, Chapter 8, §1–§2]
- Multiplikative Charaktere (§1, Ch. 8)
- Prop. 8.1.1–8.1.2
- Prop. 8.1.5
- Definition der Gausssumme (§2)
- Prop. 8.2.1–8.2.2

siehe auch [LN, Chapter VI]

16.7. **10. Jacobisummen und die Gleichung $x^n + y^n = 1$ in $\mathbb{F}_p$.**

- Hauptreferenz: [IR, Chapter 8, §3–§4)]
- Beispiel auf Seite 92–93
- Definition der Jacobisumme
- Theorem 1 und Corollary
- Beweis von Prop. 8.3.1–8.3.2
- Beweis von Theorem 2
- Verallgemeinerung §4

siehe auch [LN, Chapter VI]

23.7. **11. Der Satz von Wedderburn**

Im Seminar ging es um endliche Körper. Warum sollte man nicht auch endliche Schiefkörper, also bei denen die Multiplikation nicht notwendigerweise kommutativ ist, untersuchen? Es zeigt sich jedoch, dass es solche nicht-kommutativen endlichen Schiefkörper gar nicht gibt. Dies ist der Gegenstand des Satzes von Wedderburn, der in diesem Vortrag bewiesen werden soll.

- Hauptreferenz: [LN], Section II.6