Seminar: Lösen Spezieller Gleichungen

Wintersemester 2009/2010

Prof. Dr. Annette Huber-Klawitter
Betreuer: Stephen Enright-Ward

Ort und Zeit: Dienstag, 14-16 Uhr, SR 127

Inhalt: Wir wollen uns in diesem Seminar mit einer losen Folge von Themen beschäftigen, bei denen es um das Lösen von Gleichungen (meist zahlentheoretischer Natur) geht. Dies sind z.B.

- Lösungsformeln für die Gleichungen vom Grad 3 und 4.
- Die Pellsche Gleichung $x^2 - dy^2 = 1$ und Kettenbrüche.
- Die Fermatsche Gleichung $x^n + y^n = z^n$ für $n = 2, 3, 4$.

Der Schwerpunkt liegt also auf den Vorstellem von Beispielen, nicht der Entwicklung allgemeiner Theorie.

Organisatorisches: Als Prüfungsleistung zählt der eigene Vortrag, darüber hinaus wird erwartet, dass jeder Teilnehmer zu den Vortragsterminen anwesend ist. Bei inhaltlichen und organisatorischen Fragen in der Vorbereitungsphase vereinbaren Sie bitte einen Termin mit dem Betreuer. Sie sollten sich mindestens einmal nach der Einarbeitungsphase und spätestens zwei Wochen vor Ihrem Vortrag mit dem Betreuer über den Inhalt Ihres Vortrags absprechen.

1. Kettenbrüche (rationale Zahlen).

• Definition eines Kettenbruchs, Ausrechnungsmethode durch den Algorithmus von Euklid.

• Endliche Kettenbrüche = rationale Zahlen. Die Darstellung einer rationalen Zahl durch einen Kettenbruch ist (fast!) eindeutig ([7], Theorem 7.2; [2], Theorem 162).

Referenzen:

1. ([2], Kapitel X).
2. ([7], Kapitel 7).

2. Kettenbrüche (irrationale Zahlen).

• Die Darstellung einer irrationalen Zahl durch einen Kettenbruch ist eindeutig ([7], Theorem 7.9; [2], Theorem 170).

• Periodische Kettenbrüche = (irrationale) quadratische Ganzzahlen.([7], Theorem 7.2; [2], Theorems 176 und 177).

• Mögliche Anwendungen: (i) Gute Approximationen von reellen Zahlen durch Kettenbrüche ([2], Theorem 171), (ii) Für jede Primzahl p gibt es eine Fibonaccizahl f, die ein Vielfaches von p ist ([2], Theorem 180).

Referenzen:

1. ([2], Kapitel X).
2. ([7], Kapitel 7).

3. Pellsche Gleichungen.

• Definition (a) einer Pellschen Gleichung, (b) ihrer Fundamentallösung. Reduktion auf den Fall $d \neq$ Quadrat.

• Beobachtung, dass alle Lösungen (x_n, y_n) der Gleichung $x^2 - ny^2 = 1$ aus der Fundamentalösung (x_1, y_1) enstehen, durch die Formel

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n.$$

([7], Theorem 7.26).

• Ist (a, b) eine Lösung der Gleichung $x^2 - ny^2 = 1$, so ist a/b ein Teilbruch des Kettenbruchs von $\sqrt{n}$ ([7], Theorem 7.25).

• Numerische Beispiele.

Referenzen:

1. ([7], Kapitel 7).
2. [5].

4. Einfache Fermatsche Gleichungen.

• Aussage der Fermatschen Vermutung $S(n)$ für alle $n > 2$; Bemerkung, dass es reicht, $S(4)$ und $S(p)$ für alle p prim zu beweisen.

• Allgemeine Lösung der Gleichung $x^2 + y^2 = z^2$ nach Reduktion auf den Fall $\mathrm{ggt}(x, y) = 1$, $x, y = 0, 1 \pmod 2$. ([2], Theorem 225.)

• $x^4 + y^4 = z^4$. Zentral zu diesem Beweis ist *Fermats Abstiegsmethode*, wobei man zeigt, wie eine hypothetische Lösung (x, y, z) mit $x, y, z > 0$, eine neue Lösung (x', y', z') mit $x', y', z' > 0$ liefert, die in gewissem Sinn streng kleiner als die erste Lösung ist. Durch Induktion liefert dieser Prozess eine unendliche, absteigende Familie von immer noch positiven Lösungen, was natürlich unmöglich ist, also darf es keine Lösungen geben.

Referenzen:

1. [2], Kapitel XIII.

5. Die Fermatsche Gleichung $x^3 + y^3 = z^3$.

• Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}[\rho]$ wobei $\rho = e^{2\pi/3}$.

• Unlösbarkeit von der Gleichung $x^3 + y^3 = z^3$ ([2], Theorem 227).

Referenzen:

1. [2], Kapitel XIII.

6. Konstruktionen mit Zirkel und Lineal.

• Die Definition einer *konstruierbaren Untermenge* von $\mathbb{C}$ relativ zu einer gegebenen Teilmenge $M \subseteq \mathbb{C}$ (meistens $M = \{0, 1\}$), die Notation $\mathfrak{K}(M)$, $\mathbb{Q}(M \cup \overline{M})$.

• Jeder konstruierbare Punkt liegt in einer Galois-Erweiterung L von $\mathbb{Q}(M \cup \overline{M})$, deren Grad $[L : \mathbb{Q}(M \cup \overline{M})]$ eine Potenz von 2 ist ([1], Kapitel 6.4, Satz 1 und Korollar 2; c.f. [6] Theorem 1.36).

• Die Unlösbarkeit der folgenden drei klassischen Problemen:

(i) *Quadratur des Kreises.* Gegeben ein Kreis mit konstruierbaren Mittelpunkt und Radius, kann man ein flächengleiches Quadrat konstruieren?

(ii) *Würfelverdoppelungs.* Gegeben ein Würfel, deren Kanten von Einheitslängen sind, kann man einen neuen Würfel konstruieren, dessen Volumen genau doppel so groß ist?

(iii) *Das Problem der Winkeldreiteilung.* Man lernt in der Grundschule, wie ein beliebiger Winkel mit Zirkel und Lineal halbieren werden kann. Gibt es eine Methode, einen beliebegen Winkel mit Zirkel und Lineal zu dritteln? ([1], Seite 287; [6], Corollaries 1.38–1.40).

Referenzen:

1. [1], Kapitel 6.4.
2. [6], Kapitel 1.
3. [9], Kapitel 19.

7. Galoistheorie und die Konstruktion des n-Ecks.

• Formulierung des Hauptsatzes der Galoistheorie.

• Die Eulersche φ-Funktion und Fermatsche Primzahlen.

• Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn n von der Gestalt $2^m p_1 \cdots p_n$ ist, wobei die p_i alle *fermatsche Primzahlen* sind. ([1], Seite 287–289; [6], Corollaries 1.38–1.40).

• Explizit Konstruktion des zugehörigen Kettenkörpers eines 5-Ecks.

Referenzen:

1. [1], Kapitel 6.4.
2. [6], Kapitel 1.
3. [10].

8. Lösungsformeln für Kubische Gleichungen (elementar).

• Reduktion auf den Fall der "deprimierten" kubischen Gleichung X^3+pX+q.

• Herleitung der kubischen Formel entweder via

(i) Die Methode von Cardano (geschickte Einsetzungen), oder

(ii) Lagranges Methode von Resolventen.

N.B. In der Betrachtung der kubischen Gleichungen ([1], Kapitel 6.2) wird ein bisschen Galoistheorie angewendet in Zusammenhang mit Resolventen. Man kann diese Methode jedoch gut anwenden ohne Galoistheorie verstehen zu müssen (der Zusammenhang zur Galoistheorie wird in Vortrag 11 erläutert werden).

• Explizite Beschreibung, wie man die kubischen Wurzeln

$$\sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{3}{27}}}$$

wählt, damit die Formel stimmt.

• Ausgearbeitetes Beispiel.

Referenzen:

1. ([1], Kapitel 6.2).
2. [11].

9. Lösungsformeln für Quartische Gleichungen (elementar).

• Reduktion auf dem Fall der "deprimierten" quartischen Gleichung.

• Herleitung der quartischen Formel entweder via

(i) Die Methode von Ferrari (geschickte Einsetzungen), oder

(ii) Rechnungen mit symmetrischen Funktionen, Reduktion auf dem kubischen Fall (siehe [1], Seite 275).

• Ausgearbeitetes Beispiel.

Referenzen:

1. ([1], Kapitel 6.2).
2. [12].

10. Kummertheorie.

• Wiederholung der Definitionen von abelschen und zyklischen Galois-Erweiterungen.

• *Die Galoistheorie der zyklischen Erweiterungen:* K ein Körper, der die n-ten Einheitswurzeln enthält, $(n, \mathrm{char}(K)) = 1$. Zyklische Galois-Erweiterungen L/K von Grad n sind genau die Körper L, die durch Adjunktion einer n-ten Wurzel eines Elements K erzeugt sind. ([1], Kapitel 4.8, Satz 3)

• Anwendung: Konkrete Beschreibung vom Fall $\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}$.

Referenzen:

1. [1], Kapitel 4.8, 4.9.
2. [4], Kapitel VI.8, VI.9.
3. [6], Kapitel 5.

11. Kubische und quartische Gleichungen durch Galoistheorie.

• Wiederherleitung der Formeln für die Wurzeln eines kubischen/quartischen Polynoms f von den vorangehenden Vorträgen, mit Hilfe der Galoistheorie bzw. Kummertheorie.

Kurze Beschreibung der Strategie: In beiden Fällen (Grad $= n = 3, 4$) schreibt man zuerst eine Normalreihe von $\mathrm{Sym}(n)$ hin, zusammen mit ihrer zugehörigen Körperkette, die sich durch die Kummertheorie konkret beschreiben lässt. Nun wird es eine Kombination zwischen der Methode der Lagrange-Resolventen und elementaren Rechnungen mit der klassichen Polynomwurzelidentitäten angewendet, um die Formel für die Wurzeln des Polynoms f in Termen seiner Koeffizienten zu bekommen. Siehe ([1], Kapitel 6.2).

Referenzen:

1. [1], Kapitel 6.2.
2. [4], Kapitel VI.2.
3. [6], Kapitel 4.

12. Struktur der endlichen Körper.

• Definition eines endlichen Körpers, Beweis, dass sie nur von Primpotenzkardinalität sind.

• Man kann $\mathbb{F}_p$ als $\mathbb{Z}/p\mathbb{Z}$ hinschreiben, allerdings $\mathbb{F}_q \neq \mathbb{Z}/q\mathbb{Z}$ für $q = p^r$, $r > 1$, sondern ist $\mathbb{F}_q$ der Zerfällungskörper von $X^q - X$ (explizit ausschreiben).

• $\mathbb{F}_q^\times$ ist eine zyklische Gruppe. *Referenzen:*

1. [3], Kapitel 3.
2. [8], Kapitel 1.
3. [9], Kapitel 20.

13. RSA Algorithmus.

• Kleiner Fermatscher Satz:

$$a^{p-1} \equiv 1 \pmod{p}, \quad \text{für alle} \quad a \not\equiv 0 \pmod{p}.$$

und ihre Verallgemeinerung auf den Fall der Restklassen modulo ein *Produkt* pq von Primzahlen ([3], Kapitel 3, Theorem 3.1).

• Methode, mit dem man Wurzeln modulo einem Produkt von zwei Primzahlen N ausrechnen kann, vorausgesetzt, dass die Faktorisierung $N = pq$ gewissen ist ([3], Kapitel 3, Theorem 3.4).

• Beschreibung des RSA Algorithmus, Babybeispiel.

Referenzen:

1. [3], Kapitel 3.

14. Quadratische Formen im allgemeinen.

• Definition einer quadratischen Form Q, eines quadratischen Moduls (Q, V), das zugehörige Skalarprodukt und die Matrix einer Form, ([8], Kapitel IV.1.1).

• Morphismen zwischen quadratischen Formen, Begriff von Äquivalenz zweier quadratischen Formen, die Diskriminante einer quadratischen Form, nichtdegenerierte Formen.

• Orthogonalität zweier Vektoren, der Begriff einer orthogonalen Zerlegung $\oplus_i U_i$ von V, jede quadratische Form besitzt eine orthogonale Basis, also lässt sich so

$$f = a_1 X_1^2 + \cdots + a_n X_n^2$$

schreiben. Der Rang einer Form (diese ist die Anzahl der a_i, die nicht Null sind).

• Die Notation $\dot{+}$ und $\dot{-}$; die Definition einer hyperbolischen Form ([8], IV, Definition 4).

• [8], IV, Proposition 3' und ihr Korollar.

Referenzen:

1. [8], Kapitel IV.

15. Quadratische Formen über $\mathbb{F}_q$.

• Der Satz von Chevalley-Warning ([8] Kapitel I.2, Theorem 3) und die beiden Korollare (jede quadratische Form über einen endlichen Körper besitzt eine Nullstelle.)

• Beweis, dass eine quadratische Form f über $\mathbb{F}_q$ von Rang ≥ 2 (bzw. ≥ 3) alle Elemente von $\mathbb{F}_q^\times$ (bzw. $\mathbb{F}_q$) repräsentiert ([8] Kapitel IV.1.7, Proposition 4).

• Jede nicht-degenerierte quadratische Form f über $\mathbb{F}_q$ lässt sich als einer

der folgenden zwei Gestalten

$$X_1^2+\cdots+X_{n-1}^2+X_n^2 \qquad \text{oder} \qquad X_1^2+\cdots+X_{n-1}^2+aX_n^2, \qquad [\text{wo } a \in \mathbb{F}_q^\times \backslash (\mathbb{F}_q^\times)^2]$$

schreiben, je nachdem ob die Diskriminante ein Quadrat in $\mathbb{F}_q$ ist ([8] Kapitel IV.1.7, Proposition 5).

• Zwei quadratische Formen über $\mathbb{F}_q$ sind äquivalent genau dann, wenn sie den gleichen Rang und die gleiche Diskriminante haben ([8] Kapitel IV.1, Korollar zu Proposition 5).

Referenzen:

1. [8], Kapitel IV.1.7.
2. [8], Kapitel I.2.1 (für den Satz von Chevalley-Warning).

Literatur

[1] Bosch, S. *Algebra*. Springer, 2009.

[2] Hardy, G., and Wright, E. *An introduction to the theory of numbers*. Oxford University Press, 1979.

[3] Hoffstein, J., Pipher, J., and Silverman, J. *An Introduction to Mathematical Cryptography*. Springer Publishing Company, Incorporated, 2008.

[4] Lang, S. *Algebra*, revised third ed., vol. 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[5] Lenstr Jr., H. Solving the pell equation. *Notices Amer. Math. Soc. 49*, 2 (2002), 182–192.

[6] Milne, J. *Field and Galois Theory*. Taiaroa Publishing, 2005.

[7] Niven, I., and Zuckerman, H. *An introduction to the theory of numbers*. Oxford University Press, 1980.

[8] Serre, J. *A course in arithmetic*, second ed., vol. 7 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1973.

[9] Stewart, I. *Galois Theory*, third ed. CRC Mathematics. Chapman and Hall, Florida, 2004.

[10] Wikipedia. Compass and straightedge constructions. http://en.wikipedia.org/wiki/Compass_and_straightedge_constructions.

[11] Wikipedia. Cubic Function. http://en.wikipedia.org/wiki/Cubic_function.

[12] Wikipedia. Quartic Function. http://en.wikipedia.org/wiki/Quartic_function.