Stichworte zur Vorlesung Algebra II, Frühjahrssemester 2009

Teil C: Körper

Körpertheorie ist das Studium von Körpererweiterungen, insbesondere ihre Konstruktion, Klassifikation, und das Lösen von Gleichungen darin. Einige Themen, die auch gut in die Vorlesung passen würden — insbesondere transzendente Körpererweiterungen, inseparable Körpererweiterungen in positiver Charakteristik, und unendliche Galoistheorie — werden im begleitenden Seminar behandelt.

1. Körpererweiterungen

- Körpererweiterung L/K
- Oberkörper
- Unterkörper
- Zwischenkörper
- Körperturm
- Jeder Körperhomomorphismus ist injektiv und kann daher als Körpererweiterung betrachtet werden.
- Jeder Körper hat einen eindeutigen kleinsten Unterkörper
- Primkörper
- Charakteristik
- Erzeugter Zwischenkörper $K(S)$
- endlich erzeugte Körpererweiterung $K(x_1,...,x_n)$
- einfache Körpererweiterung $K(x)$
- Körpergrad $[L/K]$
- Multiplikativität des Körpergrads: $[M/K] = [M/L] \cdot [L/K]$
- endliche Erweiterung
- M/K ist endlich <==> M/L und L/K sind endlich
-

2. Einzelne Elemente einer Körpererweiterung

- algebraisch über K
- transzendent über K
- Auswertungshomomorphismus
- Für a transzendent über K ist $K(a) \cong K(X)$ = rationaler Funktionenkörper
- Für a algebraisch über K ist $K(a) = K[a] \cong K[X]/(f_a)$
- Minimalpolynom f_a
- äquivalente Charakterisierungen des Minimalpolynoms
- $[K(a)/K] = \deg(f_a)$
- $K(a)/K$ ist endlich <==> a ist algebraisch über K
- Stammkörper eines irreduziblen Polynoms
- Existenz und Eindeutigkeit
- Explizites Invertieren in $K[X]/(f)$ mit Hilfe des euklidischen Algorithmus

3. Algebraische Körpererweiterungen

- algebraische Erweiterung
- L/K endlich ==> L/K algebraisch
- $L=K(a_1,...,a_n)$ mit a_i algebraisch über K ==> L/K endlich
- endlich <==> algebraisch und endlich erzeugt
- L/K von algebraischen Elementen erzeugt ==> algebraisch
- M/K algebraisch <==> M/L und L/K algebraisch

4. Konstruktion mit Zirkel und Lineal

- aus einer Punktmenge S konstruierbare Punkte K(S) \subset \C
- K(S) ist der kleinste Unterkörper von \C, der unter komplexer Konjugation und Quadratwurzeln abgeschlossen ist und der S enthält
- konstruierbare Längen
- konstruierbare Winkel
- Jedes L/K vom Grad 2 mit \char(K)\not=2 ist von einer Quadratwurzel erzeugt
- K(S) ist die Vereinigung aller quadratischen Körpertürme in \C beginnend mit \Q(S\cup\bar S)
- Jeder aus S konstruierbaren Punkt ist algebraisch über \Q(S\cup\bar S) und sein Grad ist eine Zweierpotenz
- Quadratur des Kreises
- Verdoppelung des Würfels
- Dreiteilung des Winkels

5. Algebraischer Abschluss

- K algebraisch abgeschlossen <==> Jede algebraische Erweiterung ist trivial
- algebraischer Abschluss
- Jeder Körper besitzt einen algebraischen Abschluss
- Konstruktion

6. Homomorphismen zwischen Körpererweiterungen

- Homomorphismus über K
- Algebraizität und Minimalpolynom bleiben erhalten
- Hom(K(a),L') \cong {Nullstellen in L' des MinPols von a}
- jeder Homomorphismus in einen algebraisch abgeschlossenen Körper ist auf jede algebraische Erweiterung fortsetzbar
- algebraischer Abschluss ist eindeutig bis auf Isomorphie
- ... aber der Isomorphismus ist i.a. nicht eindeutig!
- Automorphismus über K
- L/K algebraisch ==> Hom_K(L,L) = Aut_K(L)
- L/K endlich ==> #Hom_K(L,M) \le [L/K]

7. Separable Körpererweiterungen

- separables irreduzibles Polynom
- f separabel <==> f'\not=0
- in Charakteristik 0 ist jedes irreduzible Polynom separabel
- in Charakteristik p>0 ist jedes irreduzible Polynom gleich g(X^{P^r}) für ein separables irreduzibles Polynom g(Y)
- Frobenius-Homomorphismus
- perfekter Körper
- K perfekt <==> char(K)=0 oder Frob_p:K—>K bijektiv
- jeder endliche Körper ist perfekt
- separables Element
- separable Körpererweiterung
- ... <==> Erzeugende sind separabel
- Charakterisierung durch Homomorphismen in algebraischen Abschluss
- M/K separabel <==> M/L und L/K separabel
- Satz vom primitiven Element
- radizielle / rein inseparable Körpererweiterung

8. Normale Körpererweiterungen

- Zerfällungskörper
- Existenz und Eindeutigkeit
- normale Körpererweiterung
- ... verschiedene äquivalente Charakterisierungen
- M/K normal ==> M/L normal für M/L/K
- M/L und L/K normal =/=> M/K normal
- normale Hülle
- Existenz und Eindeutigkeit

9. Endliche Körper

- hat Charakteristik p>0 und Ordnung p^n für [L/IF_p]=n
- hat zyklische multiplikative Gruppe
- Frobenius-Automorphismus
- jedes Element a erfüllt a^{p^n}=a
- Für jede Primpotenz p^n existiert ein Körper der Ordnung p^n
- ... und dieser ist eindeutig bis auf (uneindeutige) Isomorphie
- ... und ist Zerfällungskörper von X^{p^n}-X

10. Galois-Erweiterungen

- galoissch <==> algebraisch, separabel, und normal
- Galoisgruppe Gal(L/K)
- L/K endlich galoissch ==> #Gal(L/K) = [L/K]
- Fixkörper L^G unter einer endlichen Automorphismengruppe G
- L über L^G ist endlich galoissch mit Galoisgruppe G
- Beispiel: Symmetrische Funktionen
- Beispiel: Endliche Körper

11. Galoiskorrespondenz

- Hauptsatz der Galoistheorie:
- inklusionsumkehrende Korrespondenz:
- Zwischenkörper <---> Untergruppen
- konjugierte Erweiterungen
- normale Zwischenkörper <---> Normalteiler
- Faktorgruppe
- Folge: L/K endlich separabel ==> nur endlich viele Zwischenkörper
- Galoisgruppe eines separablen Polynoms vom Grad n
- ... ist natürlich eingebettet in die symmetrische Gruppe S_n
- ... ist transitiv <==> Polynom irreduzibel

12. Explizite Konstruktion von Zwischenkörpern

- Erzeugung durch Koeffizienten eines Hilfspolynoms
- Quadratwurzel der Diskriminante

13. Abelsche Körpererweiterungen

- Einheitswurzeln
- Kreisteilungskörper
- ... ist abelsche Erweiterung
- $Q(\mu_n)/Q$ hat Galoisgruppe $(Z/nZ)^*$
- Konstruktion des regelmässigen Polygons mit Zirkel und Lineal
- einfache Radikalerweiterung
- Kummer-Theorie: Radikalerweiterungen versus zyklische Erweiterungen

14. Auflösbare Körpererweiterungen

- Radikalturm
- L/K auflösbar durch Radikale <==> $Gal(L/K)$ auflösbar
- Allgemeine Gleichung n-ten Grades:
- Nichtauflösbarkeit für $n\ge5$
- Explizite Formeln für $n=3$ und 4

15. Explizite Bestimmung der Galoisgruppe eines separablen Polynoms

- Bestimmung der Galoisgruppe durch Zerlegung eines Hilfspolynoms in irreduzible Faktoren
- Reduktionskriterium für normiertes ganzzahliges Polynom F: Die Zerlegung von F modulo p in irreduzible Faktoren liefert Konjugationsklassen in der Galoisgruppe von F.