Checkliste zur Klausurvorbereitung für die

Algebra und Zahlentheorie 2

(a) Liste der behandelten Begriffe

- normale Erweiterung, separable Erweiterung, Galois-Erweiterung
- Galoisgruppe $\mathrm{Gal}(L|K)$ einer Galois-Erweiterung $L|K$
- Kreisteilungspolynom, Kreisteilungskörper
- kubische Resolvente eines Polynoms vierten Grades
  (Die Formel braucht nicht auswendig gelernt werden. Es genügt zu wissen, wie man aus den Nullstellen der kubischen Resolvente die Nullstellen des Polynoms vierten Grades erhält.)
- quadratische Resolvente eines Polynoms dritten Grades
  (Hier gilt dasselbe wie in Grad 4.)
- symmetrisches und elementarsymmetrisches Polynom
- algebraische Unabhängigkeit einer Menge von Polynomen
- allgemeines Polynom, allgemeine Gleichung
- Fixkörper L^G einer Untergruppe $G \leq \mathrm{Aut}(L)$
- Frobenius-Endomorphismus eines Rings der Primzahlcharakteristik p, Frobenius-Automorphismus eines endlichen Körpers, Frobenius-Automorphismus der Erweiterung $\mathbb{F}_{q^n}|\mathbb{F}_q$
- reine Gleichung
- n-te Wurzel eines Polynoms
- Lagrange'sche Resolvente eines Elements $\alpha \in L$ bezüglich eines Elements σ einer zyklischen Galoisgruppe $\mathrm{Gal}(L|K)$
- Kompositum von Körpern
- Radikalerweiterung, Radikal (oder Radikalelement) über einem Körper K, durch Radikale auflösbares Polynom
- reelle Radikalerweiterung, reelles Radikal
- elementar konstruierbarer Punkt, Menge der aus einer Teilmenge $\mathcal{P} \subseteq \mathbb{R}^2$ konstruierbaren Punkte, Definition der Mengen $\mathcal{P}_{\mathbb{R}}$ und $(\mathcal{P}_{\mathrm{con}})_{\mathbb{R}}$

(b) Wichtige Sätze und Zusammenhänge, Verständnisfragen

- Zwischen welchen beiden Mengen werden im Hauptsatz der Galoistheorie zueinander inverse Bijektionen definiert? Welche Gesetzmäßigkeiten gelten für diese Bijektionen bezüglich der Inklusionsrelation auf diesen beiden Mengen?
- Welche Regel gilt bezüglich Untergruppenordnung und dem Grad der Körpererweiterungen? Wenn U_1 und U_2 Untergruppen von $\mathrm{Gal}(L|K)$ mit $U_1 \subseteq U_2$ und $(U_2 : U_1) = 3$ sind, was lässt sich dann über die Fixkörper L^{U_1} und L^{U_2} aussagen?
- Auf welche Weise lassen sich den Elementen der Galoisgruppe eines Polynoms Elemente der symmetrischen Gruppe S_n zuordnen, sobald eine Nummerierung der Nullstellen gewählt wurde?
- Wenn K ein Körper der Charakteristik 0 und $f \in K[x]$ ein irreduzibles Polynom vom Grad n ist, warum ist die Ordnung von $\mathrm{Gal}(f|K)$ dann stets durch n teilbar? Existiert in der zugehörigen Untergruppe von S_n dann immer ein n-Zykel?
- Für jede Primzahlpotenz $q > 1$ und jedes $n \in \mathbb{N}$ gilt $\mathbb{Z}/n\mathbb{Z} \cong \mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$. Wie lässt sich ein solcher Gruppenisomorphismus mit Hilfe des Frobenius-Automorphismus definieren? Wenn d ein Teiler von n ist, welcher Zwischenkörper von $\mathbb{F}_{q^n}|\mathbb{F}_q$ entspricht der Untergruppe $\langle d + n\mathbb{Z}\rangle$?
- Wie lassen sich die Elemente der Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ einer Kreisteilungserweiterung explizit beschreiben, d.h. wie lässt sich jedem Element der primen Restklassengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ ein Element der Galoisgruppe zuordnen?
- Laut Vorlesung ist die Galoisgruppe eines Zerfällungskörpers des allgemeinen Polynoms isomorph zu S_n. Wie lässt sich dieser Isomorphismus explizit beschreiben? Welchem Element der Galoisgruppe entspricht beispielsweise das Element $(1\ 2\ 3)(4\ 5) \in S_5$?
- Welche genaue Beziehung besteht zwischen Galois-Erweiterungen mit zyklischer Galoisgruppe und reinen Gleichungen? Welche Rolle spielen dabei die Lagrange'schen Resolventen?
- Wenn K einen Körper der Charakteristik 0 mit einer primitiven n-ten Einheitswurzel $\zeta \in K$ bezeichnet und $x^n - a = 0$ eine irreduzible reine Gleichung, wie sehen die Elemente der Galoisgruppe dieses Polnyoms aus?
- Was besagt der Verschiebungssatz der Galoistheorie?
- Welche genaue Beziehung besteht zwischen Gleichungen, die durch Radikale auflösbar sind, und auflösbaren Gruppen? (Mit anderen Worten, wie lautet das Hauptergebnis von § 24?) Wie ergibt sich aus dem Hauptergebnis, dass jedes Polynom vom Grad ≤ 4 über einem Körper der Charakteristik 0 durch Radikale auflösbar ist?
- Wie wurde gezeigt, dass das Polyom $x^5 - 4x + 2$ über $\mathbb{Q}$ nicht durch Radikale auflösbar ist?
- Gibt es in $\mathbb{Q}[x]$ ein irreduzibles Polyom dritten Grades mit einer Nullstelle gegeben durch ein reelles Radikal? Was lässt sich allgemein sagen, wenn alle drei Nullstellen des Polynoms reell sind?
- Wie lassen sich die Elemente aus $(\mathcal{P}_{\mathrm{con}})_{\mathbb{R}}$ algebraisch charakterisieren? Was gilt insbesondere für die Erweiterung $L(a)|L$, wenn $L = \mathbb{Q}(\mathcal{P}_{\mathbb{R}})$, wenn a aus $\mathcal{P}$ konstruierbar ist?
- Für welche n lässt sich das regelmäßige n-Eck im Einheitskreis aus der Punktmenge $\{(0,0),(1,0)\}$ konstruieren?

(c) Themen der Übungsaufgaben

- Nachweis von normalen Erweiterungen und Galois-Erweiterungen (B1A1,B6A1)
- inseparable Erweiterungen (B1A2)
- Diskriminanten von Polynomen und symmetrische Polynome (B2A1,B2A2,B4A1)
- Anwendung des Hauptsatzes der Galoistheorie und seiner Ergänzungen (B3A1,B3A2,B6A2,B8A2)
- Bestimmung aller Zwischenkörper einer Galois-Erweiterung (B4A2)
- Galoistheorie endlicher Körper (B5A1)
- Galoisgruppen und Zwischenkörper von Kreisteilungskörpern (B5A2,B9A2)
- Bestimmung des Isomorphietyps einer Galoisgruppe (B6A1,B9A1)
- Galoisgruppen biquadratischer Polynome (B7A1,B7A2)
- Auflösbarkeit eines Polynoms durch Radikale (B8A1,B10A1)
- Bestimmung des Zerfällungskörpers eines Polynoms (B8A2)
- Auflösbarkeit durch reelle Radikale (B10A2)
- Konstruierbarkeit von Punkten (B10A2,B11A1,B11A2)
- Gleichungen vierten Grades und ihre kubische Resolvente (B11A2)