

# **Konstruktive Klassenkörpertheorie in globalen Körpern**

Claus Fieker

University of Sydney  
claus@maths.usyd.edu.au

# Überblick

Klassenkörpertheorie beschäftigt sich mit der Klassifikation von Abelschen Erweiterungen globaler Körper.

Globale Körper sind Zahlkörper oder endliche Erweiterungen von  $\mathbb{F}_q(\boldsymbol{x})$ .

# Anwendung

Klassenkörpertheorie hat Anwendungen in

- Kodierungstheorie
- Kryptographie
- Spezielle Körper (Beispiele und Existenzaussagen)

# Globale Körper

Es gibt zwei verschiedene Typen von globalen Körpern:

- **Zahlkörper**:  $\mathbb{Q}(\alpha)$  mit  $\alpha$  algebraisch über  $\mathbb{Q}$
- **globale Funktionenkörper**: Sei  $k := \mathbb{F}_q(x)$   $f(t) \in k[t]$  irreduzibel, separabel, und  $\alpha$  eine Nullstelle von  $f$  in einem passenden Erweiterungskörper. Dann ist  $K := k(\alpha)$  ein **globaler Funktionenkörper**.

# Zahlkörper

$K := \mathbb{Q}(\alpha)$  mit  $\alpha$  algebraisch (d.h. Nullstelle eines (irreduziblen, normierten) Polynoms  $f \in \mathbb{Q}[t]$ ).

Über  $\mathbb{C}$ :  $f = \prod (t - \alpha_i)$ .

$K$  hat  $n := (K : \mathbb{Q})$  Einbettungen

$$(\cdot)^{(i)} : K \rightarrow \mathbb{C} : \alpha \mapsto \alpha_i$$

Und  $r$  verschiedene Abbildungen  $|\cdot|_i : K \rightarrow \mathbb{R}_{\geq 0} : x \mapsto |x^{(i)}|$ , die **Archimedischen Bewertungen**.

# Maximalordnung

$\beta \in \mathbf{K}$  heisst **ganz algebraisch** falls  $\beta$  Nullstelle eines normierten Polynoms mit ganzen Koeffizienten ist.

$\mathbb{Z}_{\mathbf{K}}$  Ring der ganzen algebraischen Zahlen.

$\mathbb{Z}_{\mathbf{K}}$  ist freier  $\mathbb{Z}$ -Modul vom Rang  $n := (\mathbf{K} : \mathbb{Q})$ .

$\mathbb{Z}_{\mathbf{K}}$  kann berechnet werden (Round2, Round4).

# Dedekind Ringe

$\mathbb{Z}_K$  ist ein **Dedekind Ring**, d.h.

- Noethersch
- ganz abgeschlossen
- all Primideale ( $\neq 0$ ) sind maximal

# Dedekind Ringe

In Dedekind Ringen gilt:

- Ideale bilden eine Gruppe
- Ideale haben eine eindeutige Darstellung als ein Produkt von Primidealen
- Die Idealnorm:  $\mathbf{I}_K \rightarrow \mathbb{N} : \mathfrak{a} \mapsto \#\mathbb{Z}_K/\mathfrak{a}$  ist multiplikativ

# Klassengruppe

Für Zahlkörper  $K$  (genauer für die Maximalordnung  $\mathbb{Z}_K$ ) ist die **Klassengruppe**

$$\text{Cl}_K := \text{Ideale} / \text{Hauptideale}$$

eine endliche Abelsche Gruppe.

Die **Klassenzahl**  $h_K := \# \text{Cl}_K$  misst wie weit  $\mathbb{Z}_K$  von einem Hauptidealring entfernt ist.

Es gibt effektive (heuristische) Methoden zur Berechnung von Klassengruppen.

# Einheiten

Für die Einheitengruppe von  $\mathbb{Z}_K$  gilt

$$U(\mathbb{Z}_K) = \langle \zeta \rangle \times \prod_{i=1}^r \langle \epsilon_i \rangle$$

mit einer Einheitswurzel  $\zeta$  und Fundamenteinheiten  $\epsilon_i$ . Diese Darstellung der Einheitengruppe ist konstruktiv.

# Stellen

Endliche Stellen entsprechen den Bewertungen an Primidealen.

Unendliche Stellen entsprechen den Archimedischen Bewertungen von  $K$ .

Der **Grad** einer Stelle  $P|p$  ist definiert als der Grad der Restklassenkörpererweiterung.

# Divisoren

Divisoren sind formale (endliche) Summen von Stellen

$$D := \sum n_i P_i$$

mit Stellen  $P_i$  und Vielfachheiten  $n_i \in \mathbb{Z}$ .

Der endliche Teil kann durch ein Ideal dargestellt werden

$$D = \mathfrak{a} + \sum n_i | \cdot |_i =: \mathfrak{a} + D_\infty$$

# Divisoren

$D$  heisst **effektiv** ( $D \geq 0$ ) wenn  $n_i \geq 0$  gilt.

Der **Grad** von  $D$  ist definiert als

$$\deg(D) := \sum n_i \deg(P_i)$$

Für Hauptdivisoren  $(x)$  gilt die **Produktformel**:

$$\deg((x)) = 0$$

# mod\*

Für einen effektiven Divisor  $D$  und  $x \in K$  schreiben wir:

$$x \equiv 1 \pmod{*D}$$

falls für jede endliche Stelle  $P$  mit  $P|D$  gilt:

$$v_P(x - 1) \geq v_P(D)$$

und für die Archimedischen Stellen  $|\cdot|_i$  mit  $n_i > 0$  gilt

$$x^{(i)} > 0$$

# Strahlklassengruppe

Für einen effektiven Divisor  $D = \mathfrak{a} + D_\infty$  schreiben wir:

$$I^D := \{\text{Ideal } \mathfrak{b} \text{ koprim zu } \mathfrak{a}\}$$

und

$$P_D := \{x \in K \mid x \equiv 1 \pmod{*D}\}$$

Die **Strahlklassengruppe** modulo  $D$  ist nun definiert als

$$\text{Cl}_D := I^D / P_D$$

# Strahlklassengruppe

Die exakte Sequenz

$$1 \rightarrow U(\mathbb{Z}_K) \cap P_D \rightarrow (\mathbb{Z}_K/D)^* \rightarrow \text{Cl}_D \rightarrow \text{Cl}_K \rightarrow 1$$

kann sowohl benutzt werden um  $\text{Cl}_D$  zu berechnen als auch um die Endlichkeit zu zeigen.

# Restklassenringe

Für ein ganzes Ideal  $\mathfrak{a} = \prod \mathfrak{p}_i^{v_i}$  gilt

$$\left(\mathbb{Z}_K / \mathfrak{a}\right)^* = \prod \left(\mathbb{Z}_K / \mathfrak{p}_i^{v_i}\right)^*$$

und

$$\left(\mathbb{Z}_K / \mathfrak{p}^v\right) = \left(\mathbb{Z}_K / \mathfrak{p}\right)^* \times \left(1 + \mathfrak{p} / 1 + \mathfrak{p}^v\right)^+$$

Diese Darstellung erlaubt die Berechnung der Restklassenringe.

# Globale Körper

Ersetze  $\mathbb{Z}$  durch  $\mathbb{F}_q[x]$  und  $\mathbb{Q}$  durch  $\mathbb{F}_q(x)$ . Unterschiede:

- Alle Bewertungen sind diskret,
- Es gibt keine Archimedischen Stellen,
- Alle Stellen können durch Primideale (in verschiedenen Ringen) repräsentiert werden.

# Divisorklassengruppe

Statt der Klassengruppe betrachte die **Divisorklassengruppe**:

$$\text{Cl}_K := \text{Divisoren} / \text{Hauptdivisoren}$$

Im Unterschied zu der (Ideal-)Klassengruppe ist diese nicht endlich.

$$\text{Cl}_K = \text{Cl}_K^0 \times \mathbb{Z}$$

wo

$$\text{Cl}_K^0 := \text{Divisoren vom Grad } 0 / \text{Hauptdivisoren}$$

eine endliche Abelsche Gruppe ist.

# Strahlklassengruppe

In Funktionenkörpern betrachte eine modifizierte exakte Sequenz um die Strahlklassengruppe zu definieren:

$$1 \rightarrow \mathbb{F}_q \rightarrow \left( K \cap I^D / P_D \right)^* \rightarrow \text{Cl}_D \rightarrow \text{Cl}_K \rightarrow 1$$

Für  $D > D'$  ist

$$\phi_{D,D'} : \text{Cl}_D \rightarrow \text{Cl}_{D'}$$

surjektiv.

# Führer

Für jede Untergruppe  $U < \text{Cl}_D$  gibt es einen minimalen Divisor  $F < D$ , so dass

$$\text{Cl}_D/U \rightarrow \text{Cl}_F/\phi_{D,F}(U)$$

injektiv ist.

$F$  heisst der **Führer** von  $U$ .

# Artin-Abbildung

Sei  $K/k$  eine Abelsche Erweiterung globaler Körper und  $d_{K/k}$  der Diskriminantendivisor.

Die Abbildung

$$\text{Art} : I^d \rightarrow \text{Aut}(K/k)$$

die Stellen auf die Frobenius-Automorphismen abbildet ist wohldefiniert und trivial auf  $P_d$  und daher definiert für

$$\text{Cl}_d \rightarrow \text{Aut}(K/k).$$

Sie heisst **Artin-Abbildung**.

# Klassenkörper

Hauptsatz:

Die Zuordnung von Abelschen Erweiterungen und (Untergruppen von) Strahlklassengruppen ist eine 1-1 Abbildung.

Die unverzweigten Stellen vom Grad 1 in  $K/k$  sind genau die Stellen, die in  $U$  liegen.

# Berechnung

Reduktion:

$$\text{Cl}_{D/U} = \prod \text{Cl}_{D/U_i}$$

wobei die Faktoren

$$\text{Cl}_{D/U_i} \approx C_{p^l}$$

zyklisch sind.

$$K/k = \prod K_i/k$$

und

$$\text{Aut}(K_i/k) \approx \text{Cl}_{D/U_i}$$

# Kummer-Fall

Im Fall  $p \neq \text{char } k$  funktioniert Kummer Theorie wenn genügend viele Einheitswurzeln hinzugefügt werden:

$$E := k(\zeta_{p^l})$$

Dann folgt

$$KE = K(\zeta_{p^l}) = E(\sqrt[p^l]{\epsilon})$$

mit  $\epsilon \in U_S$  eine  $S$ -Einheit für eine explizite Menge  $S$  von Stellen.

# Kummer-Fall

Wir finden  $K(\zeta_{p^l})$  als Teilkörper von  $E(\sqrt[p^l]{U_S})$ . Es gilt

$$\text{Aut}(E(\sqrt[p^l]{U_S})/E) \approx (\mathbb{Z}/p^l\mathbb{Z})^s$$

Die Abbildung

$$\text{Art} : \mathbf{I}_d^E \rightarrow (\mathbb{Z}/p^l\mathbb{Z})^s$$

ist explizit. Sie erlaubt das finden des Erzeugers  $\epsilon$  durch lineare Algebra.

# Kummer-Fall

In einem letzten Schritt muss nun die Einheitswurzel wieder entfernt werden. Auf Grund der Konstruktion wissen wir, dass  $K(\zeta_{p^l})/k$  eine Abelsche Erweiterung ist. Die Artin-Abbildung kann auch hier explizit berechnet werden. Zusammen mit den Automorphismen kann Galoistheorie benutzt werden um  $K$  als Teilkörper zu finden.

# Artin-Schreier Fall

Sei  $p = \text{char}(k)$  und  $\wp(x) := x^p + x$ .

Satz (Artin-Schreier):  $K/k$  zyklisch vom Grad  $p$ . Dann gilt  $K = k(\alpha)$  mit  $\wp(\alpha) \in k$ .

Satz: Es gibt ein  $\alpha \in \mathcal{L}(D + pD_0)$  wobei  $D_0$  nur von  $k$  abhängt.

Satz: Für  $\alpha, \beta$  in  $k$  gilt  $k(\wp^{-1}(\alpha)) = k(\wp^{-1}(\beta))$  genau dann, wenn  $\alpha - \beta \in \wp(k)$  ist.

# Artin-Schreier Fall

Analog zum Kummer Fall gilt nun auch hier:

$$K = k(\wp^{-1}(\alpha))$$

ist ein Teilkörper von

$$F := k(\wp^{-1}(\mathcal{L}))$$

Es gilt

$$\text{Aut}(F/k) \approx (\mathbb{Z}/\mathfrak{p}\mathbb{Z})^s$$

mit einer expliziten Abbildung

$$\text{Art} : I_d^k \rightarrow (\mathbb{Z}/\mathfrak{p}\mathbb{Z})^s$$

.

# Anwendung - Zahlkörper

(mit Jürgen Klüners (Kassel), in KASH).

Berechnung von minimalen Grad 8 Körpern die einen Quadratischen Teilkörper haben. (Die mögliche Galois Gruppen sind auflösbar. Klassenkörpertheorie kann benutzt werden um auflösbare Erweiterungen zu bestimmen)

Cohen, Olivier, Diaz y Diaz (Bordeaux, in Pari): Berechnung von minimalen Grad 8 Körpern die einen Teilkörper vom Grad 4 haben. (Quadratische Erweiterungen sind stets Klassenkörper)

# Anwendung - Funktionenkörper

Funktionenkörper können als Kurven interpretiert werden. Stellen vom Grad 1 entsprechen dann den rationalen Punkten auf diesen.

Gute Geometrische Codes basieren auf Kurven mit kleinem Geschlecht und vielen Punkten.

Klassenkörpertheorie erlaubt das (gezielte) Konstruieren von geeigneten Kurven.

Viele der besten bekannten Codes basieren auf Existenzbeweisen für gute Kurven. (Diese Codes sind i.allg. **nicht** explizit und können daher **nicht** benutzt werden)

# Anwendung - Funktionenkörper

Aufbauend auf Florian Heß (Bristol) Magma und Kash Programmen zur Berechnung von Divisorklassengruppen und Riemann-Roch Räumen in Funktionenkörpern unter Benutzung von Roland Auers Darstellung der Restklassenringe gibt es nun Magma (seit Version 2.10) Funktionen für alle Schritte die benötigt werden um explizite Gleichungen zu finden.

Markus Grassl (Karlsruhe) hat dies benutzt um neue gute Codes zu finden und um explizite Darstellungen für einige der bereits bekannten Codes zu bestimmen.

# Generische Algorithmen

In Magma werden generische Algorithmen für endliche Erweiterungen eingesetzt. Speziell wird eine generische Round2 Implementierung und gemeinsame Ideal-Arithmetik benutzt. Vorteile:

- weniger Code
- die mathematische Struktur wird stark betont
- investierte Arbeit in einem Fall kommt allen anderen zu Gute

# Generische Algorithmen

Es gibt jedoch auch Nachteile:

- die Programmierung ist komplizierter
- gemeinsame Methoden sind oft langsamer
- gemeinsame Optimierung ist oft unmöglich.