Das Geschlecht algebraischer Kurven

Moritz Meisel, Prof. Dr. Marc Nieper-Wißkirchen
Institut für Mathematik, Universität Augsburg
Lehrstuhl für Algebra und Zahlentheorie

Zusammenfassung

In der Arbeit werden zwei verschiedene Herangehensweisen zur Definition des Geschlechts g einer algebraischen Kurve dargestellt sowie die eine aus Sicht der anderen interpretiert. Es wird auch ein konstruktives Verfahren zur Bestimmung des Geschlechts nach H. Edwards beschrieben. Anschließend werden ein paar interessante Ergebnisse für Kurven von Geschlecht 1, sogenannte elliptische Kurven, präsentiert. Diese lassen sich bis auf Isomorphie durch die sogenannte j-Invariante klassifizieren, welche Werte im Grundkörper k annimmt. Außerdem existiert eine natürliche Gruppenstruktur auf der Menge der Punkte einer elliptischen Kurve.

Satz von Riemann

Ein *Funktionenkörper* (bzw. eine *abstrakte Kurve*) K ist eine endlich erzeugte Körpererweiterung eines Grundkörpers k vom Transzendenzgrad 1, wobei k in K algebraisch abgeschlossen ist.

Ein *Divisor* D ist ein Element der von den *Primdivisoren*, also den maximalen Idealen der diskreten k-Bewertungsringe von K, erzeugten freien abelschen Gruppe Div(X).

Für einen Divisor D ist $L_K(D) := \{x \in K^\times \mid [x] \geq -D\} \cup \{0\}$ ein endlich-dimensionaler k-linearer Unterraum von K. Er enthält diejenigen rationalen Funkionen, welche den durch den Divisor D festgelegten Null- und Polstellenbedingungen genügen.

Satz 1. *(Satz von Riemann) Für einen Funktionenkörper K gibt es nur von K abhängige natürliche Zahlen g und N, so dass für beliebige Divisoren D auf K die Ungleichung*

$$g \geq \deg D + 1 - \dim L(D)$$

erfüllt ist und für alle Divisoren vom Grad mindestens N Gleichheit gilt.

Die natürliche Zahl g wird als das *Geschlecht* des Funktionenkörpers K bezeichnet.

Normalbasen

Im Essay *The Genus of an Algebraic Curve* von H. Edwards lautet die Definition des Geschlechts wie folgt:

$$g := n_0\nu + 1 - \dim_{\Theta(x^0)} \Theta(x^\nu), \text{ für } \nu \gg 0.$$

Dabei sei $\Theta(x^\nu)$ der Raum der über x ganzen Funktionen ($\theta \in K$ heißt *ganz* über x, falls es Nullstelle eines normierten Polynoms mit Koeffizienten in $\mathbb{Q}[x]$ ist) von Ordnung höchstens ν in $x = \infty$ (d. h. ν ist die kleinste Zahl, so dass θ/x^ν ganz über $1/x$ ist). Weiterhin bezeichne n_0 den Grad der Körpererweiterung von $K = \mathbb{Q}(x)[y]/(f(x,y))$ über $\Theta(x^0)[x]$ und n den von K über $\mathbb{Q}[x]$.

Der im Verlauf des Essays beschriebene Algorithmus zur Bestimmung des Geschlechts für ein gegebenes in y normiertes, irreduzibles Polynom $f(x,y)$ beruht im Wesentlichen auf der Konstruktion einer Normalbasis.

Für ein K wie oben ist eine *Ganzheitsbasis* eine Basis $y_1, \ldots, y_n$ von K über $\mathbb{Q}(x)$, so dass für jedes Element $w = \sum_{i=1}^n \phi_i(x) y_i \in K$ die Koeffizienten $\phi_i(x)$ der Basisdarstellung genau dann in $\mathbb{Q}[x]$ liegen, wenn w über x ganz ist. Eine solche Ganzheitsbasis heißt *Normalbasis*, falls zusätzlich folgende Eigenschaft erfüllt ist:

$$w \in \Theta(x^\nu) \Leftrightarrow \mathrm{deg}\phi_i + \lambda_i \leq \nu,$$

wobei λ_i die Ordnung von y_i in $x = \infty$ bezeichnet.
Mithilfe einer solchen Normalbasis lässt sich nun das Geschlecht relativ einfach bestimmen. Die Gradeinschränkung an die Koeffizienten in der Basisdarstellung von $w \in \Theta(x^\nu)$ liefert nämlich

$$\dim_{\mathbb{Q}} \Theta(x^\nu) = \sum_{\lambda_i \leq \nu} \nu - \lambda_i + 1.$$

Für $\nu \gg 0$ ist also $\dim_{\mathbb{Q}} \Theta(x^\nu) = n(\nu+1) - \sum \lambda_i$. Wählt man $\nu = 0$, zeigt sich, dass $[\Theta(x^0) : \mathbb{Q}] =: c$ gerade gleich der Anzahl der verschwindenden λ_i ist.
Mit obiger Definition des Geschlechts ergibt sich

$$g = n_0\nu - \frac{1}{c}\left((\nu+1)n - \sum \lambda_i\right) + 1 = \frac{\sum \lambda_i}{c} - (n_0 - 1).$$

Elliptische Kurven

Es sei k algebraisch abgeschlossen. Für eine abstrakte Kurve K von Geschlecht 1 existieren dann $x, y \in K$, so dass $K = k(x,y)$, wobei $y^2 = x(x-1)(x-\lambda)$ für ein $\lambda \in k\ \{0,1\}$.

Die j-*Invariante* von K ist definiert als

$$j(K) := \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda-1)^2}.$$

Satz 2. *Die Abbildung $K \mapsto j(K)$ induziert eine wohldefinierte Bijektion zwischen den Isomorphieklassen elliptischer Kurven K über k und den Elementen von k.*

Nach dem folgenden Satz ist auf der Menge der Punkte einer elliptischen Kurve eine natürliche Gruppenstruktur definiert.

Satz 3. *Sei P_0 ein beliebiger Punkt (Primdivisor von Grad 1) von K. Dann definiert die Zuordnung $P \mapsto P - P_0$ eine Bijektion zwischen der Menge der Punkte von K und der Gruppe $\mathrm{Cl}^0(K)$.*

Dabei ist $\mathrm{Cl}^0(K)$ der Kern der Gradabbildung auf der *Divisorenklassengruppe*

$$\mathrm{Cl}(K) := \mathrm{Div}(K)/\sim, \text{ wobei } D \sim D' :\Leftrightarrow D - D' = [x] \text{ für ein } x \in K^\times.$$

Die Gradabbildung ist wohldefiniert auf Cl(K), da Hauptdivisoren auf Kurven von Grad 0 sind.

Interpretation

Zur Interpretation der Definition von Edwards aus Sicht des Satzes von Riemann sei $\mathbb{Q} = \Theta(x^0)$ und $n = |K : \mathbb{Q}(x)|$.

Zur Definition des Geschlechts genügt prinzipiell ein einziger Divisor von hinreichend großem Grad. Betrachte dazu

$$D = \nu[x]_\infty = [x^\nu]_\infty.$$

Der Raum $L(D)$ der Funktionen, die nur maximal die Pole von x^ν besitzen, lässt sich dann auch als $\Theta(x^\nu)$, den Raum der über x ganzen Funktionen der maximalen Ordnung ν in $x = \infty$, verstehen.
Andererseits ist

$$\deg[x]_\infty = [K : \mathbb{Q}(x)],$$

womit die Verbindung zur Definition $g = n\nu + 1 - \dim \Theta(x^\nu)$ hergestellt ist.

Die Wahl eines anderen Divisors D von genügend großem Grad zur Ermittlung eines alternativen Bestimmungsverfahrens scheint aufgrund der Natürlichkeit der obigen Wahl nicht vielversprechend.

References

1. D. Goldschmidt, *Algebraic Functions and Projective Curves*, Graduate Texts in Mathematics, Springer: New York 2003.
2. H. M. Edwards, *Essays in Constructive Mathematics*, Springer, New York 2005.
3. R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, Springer, New York 1977.