Arithmetik von Kummer-Varietäten

Jan Steffen Müller

1.2.2011

Definition

Notation.

- Sei k ein Körper.
- Sei A/k eine abelsche Varietät.
- Sei $g = \dim(A)$.

Die Kummer-Varietät von A ist definiert als $K := A/\{\pm 1\}$.

Fakten.

- K ist eine projektive Varietät.
- Man kann K in $\mathbb{P}^{2^g-1}$ einbetten.
- Das Bild von K in $\mathbb{P}^{2^g-1}$ kann durch quartische Gleichungen beschrieben werden (Matev, 2010).

Beispiel.

- Sei $A = E$ eine elliptische Kurve, gegeben durch eine Weierstrass-Gleichung

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in k$$

mit Punkt ∞ im Unendlichen.

$\Rightarrow K = \mathbb{P}^1$

- Eine Surjektion $\kappa : E \to K$ ist explizit gegeben durch

$$\kappa(P) = \begin{cases} (x : 1), & P = (x, y) \in E \setminus \{\infty\} \\ (1 : 0), & P = \infty \end{cases}$$

$g = 2$

- Sei $\mathrm{char}(k) \neq 2$.
- Sei C/k eine glatte projektive Kurve vom Geschlecht 2

$\Rightarrow$ Es gibt eine affine Gleichung $y^2 = f(x)$ von C, mit

$$f(x) = f_0 + f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4 + f_5 x^5 + f_6 x^6 \in k[x]$$

und $\deg(f) \in \{5, 6\}$.

- Sei $A = \mathrm{Jac}(C)$
- $K = A/\{\pm 1\}$ wird Kummer-Fläche genannt.
- Klassisches Objekt im Fall $k = \mathbb{C}$ (Kummer 1864, Cayley 1877, Borchardt 1877, Hudson 1905)

Explizite Kummer–Fläche I

Fragen.

(1) Können wir eine Einbettung $K \hookrightarrow \mathbb{P}^3$ und die induzierte Abbildung $\kappa : A \longrightarrow\!\!\!\!\!\rightarrow K \hookrightarrow \mathbb{P}^3$ explizit beschreiben?

(2) Können wir $\kappa(A) \subset \mathbb{P}^3$ explizit beschreiben?

Strategie.

- Man benutzt $A \cong \mathrm{Pic}^0(C)$.
- Aus Riemann-Roch folgt: Ein Punkt $P = [P_1 - P_2] \in A \setminus \{0\}$ entspricht genau einem ungeordneten Paar $\{P_1, P_2\}$ von Punkten auf C.
- Für $x_1, x_2 \in k$ sei

$$\begin{aligned} F_0(x_1, x_2) &= 2f_0 + f_1(x_1 + x_2) + 2f_2(x_1x_2) + f_3(x_1 + x_2)x_1x_2 \\ &\quad + 2f_4(x_1x_2)^2 + f_5(x_1 + x_2)x_1x_2 + 2f_6(x_1x_2)^3. \end{aligned}$$

Explizite Kummer–Fläche II

Man kann κ z.B. folgendermaßen explizit beschreiben: (Flynn, 1990)

- Seien $P_1 = (x_1, y_1),\ P_2 = (x_2, y_2) \in C$ und $P = [P_1 - P_2] \in A$.
- Dann ist $\kappa = (\kappa_1, \ldots, \kappa_4) : A \longrightarrow\!\!\!\!\!\rightarrow K \hookrightarrow \mathbb{P}^3$ gegeben durch

$$\begin{aligned} \kappa_1(P) &= 1 \\ \kappa_2(P) &= x_1 + x_2 \\ \kappa_3(P) &= x_1 x_2 \\ \kappa_4(P) &= \frac{F_0(x_1, x_2) - 2y_1 y_2}{(x_1 - x_2)^2}. \end{aligned}$$

- Das Bild $K = \kappa(A)$ ist gegeben durch eine explizite quartische Gleichung $K(x) = 0$ in $\mathbb{P}^3$.

Arithmetik auf K I

Die Gruppenstruktur auf A wird teilweise auf K reflektiert, z.B.:

- $\kappa(2P) = \kappa(-2P) \Rightarrow$ Verdopplung auf K wohldefiniert.
- $Q \in A[2] \Rightarrow \kappa(P+Q) = \kappa(-P+Q) \Rightarrow$ Addition von $\kappa(Q)$ auf K wohldefiniert.

Genauer. (Flynn 1990): Es gibt ein Quadrupel $\delta = (\delta_1, \delta_2, \delta_3, \delta_4)$ von homogenenen quartischen Polynomen $\delta_i(x_1, \ldots, x_4)$ mit Koeffizienten in $\mathbb{Z}[f_0, \ldots, f_6]$ und eine lineare Abbildung $W_Q : \mathbb{P}^3 \longrightarrow \mathbb{P}^3$, sodass

$$\begin{array}{ccc} A & \xrightarrow{[2]} & A \\ \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa} \\ K & \xrightarrow{\delta} & K \end{array} \qquad \text{und} \qquad \begin{array}{ccc} A & \xrightarrow{\tau_Q} & A \\ \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa} \\ K & \xrightarrow{W_Q} & K \end{array}$$

kommutieren, wobei $\tau_Q(P) = P + Q$ ist.

Arithmetik auf K II

- Seien $P, Q \in A$.
- I.A. können wir $\kappa(P+Q)$ nicht aus $\{\kappa(P), \kappa(Q)\}$ berechnen.
- Aber: Wir können $\{\kappa(P+Q), \kappa(P-Q)\}$ aus $\{\kappa(P), \kappa(Q)\}$ berechnen!

Genauer. (Flynn 1990):
Es gibt biquadratische Formen B_{ij} in den $\kappa_i(P), \kappa_i(Q)$ mit Koeffizienten in $\mathbb{Z}[f_0, \ldots, f_6]$, sodass projektiv

$$\begin{aligned} B_{ij}(\kappa(P), \kappa(Q)) &= \kappa_i(P+Q)\kappa_j(P-Q) + \kappa_j(P+Q)\kappa_i(P-Q),\ i \neq j \\ B_{ii}(\kappa(P), \kappa(Q)) &= \kappa_i(P+Q)\kappa_i(P-Q) \end{aligned}$$

gilt.

Geschlecht 2 in Charakteristik 2

Frage. Können wir Flynns Resultate auf beliebige Charakteristik verallgemeinern?

- Sei k ein beliebiger Körper.
- Sei C/k eine glatte projektive Kurve vom Geschlecht 2.

$\Rightarrow$ Es gibt eine affine Gleichung

$$y^2 + h(x)y = f(x)$$

von C, mit

$$\begin{aligned} f(x) &= f_0 + f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4 + f_5 x^5 + f_6 x^6 \in k[x] \\ h(x) &= h_0 + h_1 x + h_2 x^2 + h_3 x^3 \in k[x]. \end{aligned}$$

- Seien $A = \mathrm{Jac}(C)$ und $K = A/\{\pm 1\}$.

Kummer-Fläche in Charakteristik 2

Sei $P = [P_1 - P_2] \in A$ mit $P_1 = (x_1, y_1),\ P_2 = (x_2, y_2) \in C$.
Dann kann $\kappa : A \longrightarrow\!\!\!\!\!\rightarrow K \hookrightarrow \mathbb{P}^3$ durch

$$\begin{aligned}
\kappa_1 &= 1 \\
\kappa_2 &= x_1 + x_2 \\
\kappa_3 &= x_1 x_2 \\
\kappa_4 &= \frac{F_0(x_1, x_2) - 2y_1y_2 - h(x_1)y_2 - h(x_2)y_1}{(x_1 - x_2)^2},
\end{aligned}$$

beschrieben werden.

Das Bild $K = \kappa(A)$ ist gegeben durch eine explizite quartische Gleichung $K(x) = 0$ in $\mathbb{P}^3$.

Frage. Wie können wir die Abbildungen δ, B_{ij} und W_Q finden?

Formeln in Charakteristik 2

Strategie für δ, B_{ij} und W_Q.

(1) Wir nehmen $\mathrm{char}(k) \neq 2$ an.

(2) Sei $C' : y^2 = 4f(x) + h(x)^2$. Dann ist C birational äquivalent zu C'.

(3) Sei K' die Kummer-Fläche zur Jacobischen von C'. Dann gilt $K \cong K'$.

(4) Wir finden einen expliziten Isomorphismus $\tau : K \longrightarrow K'$ und transportieren die Formeln von K' nach K.

(5) Wir modifizieren die erhaltenen Formeln, sodass sie wohldefiniert und nichttrivial modulo 2 sind.

(6) Wir nehmen $\mathrm{char}(k) = 2$ an und liften K und die Formeln zu Objekten über dem Ring $W(k)$ der Witt-Vektoren von k. Verträglichkeit mit Reduktion modulo $2W(k)$ zeigt die Korrektheit der Formeln.

Verdopplung in Charakteristik 2

Sei $\mathrm{char}(k) \neq 2$. Ein expliziter Isomorphismus ist z.B. gegeben durch

$$\begin{array}{rcl} \tau : K & \longrightarrow & K' \\ (x_1, x_2, x_3, x_4) & \mapsto & (x_1, x_2, x_3, 4x_4 - 2(h_0h_2x_1 + h_0h_3x_2 + h_1h_2x_3)) \,. \end{array}$$

Sei $\delta : K \to K$, sodass

$$\begin{array}{ccc} K & \xrightarrow{\delta} & K \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau} \\ K' & \xrightarrow{\delta'} & K' \end{array}$$

kommutiert, wobei δ' die Verdopplungsabbildung auf K' ist.
Durch einfache Manipulationen erhalten wir

$$\delta = (\delta_1, \ldots, \delta_4) : K \to K$$

mit $\delta_i(x) \in \mathbb{Z}[f_0, \ldots, f_6, h_0, \ldots, h_3][x]$ nichttrivial modulo 2.

Verdopplung in Charakteristik 2 – Beweis

- Sei $\mathrm{char}(k) = 2$.
- Sei $W(k)$ der Ring der Witt-Vektoren über k mit Quotientenkörper l.
- Sei A_W eine Jacobische Fläche über l mit Kummer-Fläche K_W, sodass $A_W \equiv A \pmod{2W(k)}$ gilt.
- Sei $P \in A_W$ und $\tilde{P} = P \pmod{2W(k)}$. Wegen $\delta_W(\kappa(P)) = \kappa(2P)$ gilt

$$\delta(\kappa(\tilde{P})) = \kappa(2\tilde{P})$$

oder

$$\delta_i(\kappa(\tilde{P})) = 0 \text{ für alle } i.$$

- Wir zeigen explizit, dass für $x \in \mathbb{A}^4$ aus $K(x) = 0$ und $(\delta_1(x), \ldots, \delta_4(x)) = (0,0,0,0)$ immer $x = (0,0,0,0)$ folgt.

$\Rightarrow$ δ ist die korrekte Verdopplungsabbildung auf K.

Seien $x, y \in K$ und für $i, j \in \{1, \ldots, 4\}$ sei b'_{ij} gegeben durch

$$b'_{ij} := B'_{ij}(\tau(x), \tau(y)).$$

wobei B'_{ij} die beschriebenen biquadratischen Formen auf K' sind.

- Wegen $\tau(\kappa_i) = \kappa_i$ für $i = 1, 2, 3$ gilt $B_{ij}(x, y) = b'_{ij}$ für $i = 1, 2, 3$.
- Die Formen B_{i4} können als Linearkombinationen der b'_{ij} berechnet werden.
- Es gilt: $B_{ij}(x, y) := 1/16 B_{ij}(x, y) \in \mathbb{Z}[f_0, \ldots, f_6, h_0, \ldots, h_3][x, y]$ ist nichttrivial mod 2 für alle i, j.
- Liften über $W(k)$ und Nichtverschwinden aller $B_{ij}(x, y)$ für $x, y \in \mathbb{A}^4 \setminus \{0\}$ zeigt die Korrektheit der B_{ij}.

Alternative Ansätze I

Duquesne (2008).

- K, δ, B_{ij}, W_Q für $\mathrm{char}(k) = 2$ und $h_3 = 0$
- Für diesen Spezialfall gleiche Resultate
- Methode: Imitation des Originalansatzes von Flynn
- Problem: Nicht auf beliebige Charakteristik zu verallgemeinern
- Ziel: Anwendungen in der Kryptographie

Alternative Ansätze II

Gaudry (2008).

- Sei $\mathrm{char}(k) \neq 2$.
- Ansatz: Beschreibe K sowie Arithmetik auf K mittels Parametrisierung durch Theta-Funktionen.
- Geht zurück auf Hudson (1905).
- Vorteil: Einfachere Formeln als bei Flynn;
- Nachteil: Formeln nur über $k(A[2])$ definiert.

Gaudry-Lubicz (2009).

- Sei $\mathrm{char}(k) = 2$.
- Ähnliche Methoden liefern Parametrisierungen mit den gleichen Vor- und Nachteilen.

Schnelle Multiplikation I

- Sei k ein (großer) endlicher Körper.
- Sei $P \in A(k)$, $n \in \mathbb{Z}$.

Frage.

Wie kann man nP möglichst schnell berechnen?

- Wichtige Frage für die Effizienz von kryptographischen Verfahren, die auf dem DLP in Geschlecht 2 aufbauen.
- Antwort hängt von k und C ab.

Schnelle Multiplikation II

Erinnerung.

- $\kappa(P),\ \kappa(Q)$ für $P, Q \in A(k)$ bekannt $\not\Rightarrow$ $\kappa(P+Q)$ kann auf K berechnet werden.

$\Rightarrow$ K nicht interessant für Double-and-add oder Sliding-Window Methoden.

Aber.

- $\kappa(P),\ \kappa(Q),\ \kappa(P-Q)$ für $P, Q \in A(k)$ bekannt $\not\Rightarrow$ $\kappa(P+Q)$ kann auf K berechnet werden.

$\Rightarrow$ K interessant für Montgomery-Leiter Methode!

Montgomery–Leiter: Algorithmus

- Sei $P \in A(k)$ und sei $n = \sum_{i=0}^{m} n_i 2^i$ mit $n_i \in \{0, 1\}$ für alle i.
- Setze $(x, y) := (\kappa(0), \kappa(P))$.
- Für alle i von m bis 0
  - setze $(x, y) := (2x, x + y)$ falls $n_i = 0$;
  - setze $(x, y) := (x + y, 2y)$ falls $n_i = 1$.
- Dann gilt $x = \kappa(nP)$.

Fakten.

- In jedem Schritt gilt $x = \kappa(sP)$ und $y = \kappa((s + 1)P)$ für ein $s \in \mathbb{N}$.

$\Rightarrow$ Alle Additionen sind wohldefiniert auf K.

Montgomery–Leiter: Eigenschaften

Effizienz.

- Besonders effizient für $\mathrm{char}(k) = 2$;
- für Kurven mit $\mathrm{char}(k) = 2$ und $h_3 = h_2 = 0 \neq h_1$ schnellste verfügbare Methode zur Multiplikation (Gaudry-Lubicz hier nicht möglich);
- Für Kurven mit $\mathrm{char}(k) = 2$ und $h_3 = 0$, $h_2 = h_1 = 1$ ist Gaudry-Lubicz ca. 20% schneller;
- Bei vergleichbarer Sicherheit schneller als Montgomery-Leiter Methoden für elliptische Kurven.

Sicherheit.

- Nicht anfällig für Seitenkanalattacken

$\Rightarrow$ Besonders interessant für Hardware-Implementierungen.

Punktsuche

Sei k ein Zahlkörper oder Funktionenkörper.

Frage.
Wie können wir Punkte $P = [P_1 - P_2] \in A(k)$ konstruieren?

- $P_1, P_2 \in C(k) \Rightarrow$ einfache Punktsuche auf $C(k)$.
- I.A. $P_1, P_2 \in C(l)$ mit $[l : k] = 2$
- A lässt sich in $\mathbb{P}^{15}$ als Schnitt von 72 Quadriken einbetten $\Rightarrow$ Suche nicht praktikabel
- Ansatz (Flynn, Smart, Stoll): Es gilt $P \in A(k) \Rightarrow \kappa(P) \in K(k)$.
- Suche $x \in \mathbb{P}^3(k)$ sodass $K(x) = 0$ gilt (z.B. mittels Siebmethoden) und versuche nach $A(k)$ zu liften.

Höhenfunktion

- Sei k ein globaler Körper und M_k die Menge der Primstellen von k.
- Für $N \geq 1$ ist die Höhe auf $\mathbb{P}^N(k)$ definiert durch

$$h(x_0, \ldots, x_N) = \sum_{v \in M_k} \log \max\{|x_0|_v, \ldots, |x_N|_v\}.$$

- Sei A/k eine abelsche Varietät mit Kummer-Varietät K und explizitem $\kappa : A \twoheadrightarrow K \hookrightarrow \mathbb{P}^{2^g-1}$.
- Die (naive) Höhe von $P \in A(k)$ ist definiert durch

$$h(P) := h(\kappa(P)).$$

Kanonische Höhe

Definition.
Die kanonische Höhe von $P \in A(k)$ ist definiert durch

$$\hat{h}(P) := \lim_{n\to\infty} \frac{1}{4^n} h(2^n P)).$$

Eigenschaften.

- $\hat{h}$ ist eine quadratische Form auf $A(k)$.
- $\hat{h} - h$ ist beschränkt.
- $\hat{h}(P) \geq 0$ für alle $P \in A(k)$ und $\hat{h}(P) = 0 \Leftrightarrow P$ hat endliche Ordnung.

Anwendungen

Sei Λ eine Untergruppe des freien Anteils von $A(k)$ von endlichem Index. Angenommen wir können

(1) $\hat{h}(P)$ für $P \in A(k)$ berechnen,

(2) $\max\{|\hat{h}(P) - h(P)| : P \in A(k)\}$ beschränken,

(3) $\{P \in A(k) : h(P) < B\}$ für geeignete B in $\mathbb{R}$ finden.

Anwendungen.

- Berechnung von Erzeugern von $A(k)$,
- Numerische Verifikation der Vermutung von Birch und Swinnerton-Dyer in Beispielen.

Lokale Zerlegung

Sei $\delta : \mathbb{P}^{2^g-1} \longrightarrow \mathbb{P}^{2^g-1}$ sodass $\delta(\kappa(P)) = \kappa(2P)$ für alle $P \in A$ gilt.

Satz. (Néron, Lang) Es gibt für alle $v \in M_k$ beschränkte Funktionen $\mu_v : A(k_v) \longrightarrow \mathbb{R}$, sodass

$$\hat{h}(P) - h(P) = \sum_v \mu_v(\kappa(P))$$

für alle $P \in A(k)$ gilt. Hierbei durchläuft v die

- Stellen schlechter Reduktion von A
- archimedischen Stellen von k.

Fakt.
Man kann die Funktionen μ_v durch $\delta^{\circ n}(\kappa(P))$ ausdrücken.

Resultate für kleine Dimension

Es gibt effiziente Algorithmen zur

(1) Berechnung von $\hat{h}(P)$ für $P \in A(k)$,

(2) Beschränkung von $\max\{|\hat{h}(P) - h(P)| : P \in A(k)\}$,

(3) Bestimmung von $\{P \in A(k) : h(P) < B\}$ für geeignete B in $\mathbb{R}$.

in den Fällen

- $g = 1$ (Néron, 1965, Tate, 1976; Silverman, 1988; Siksek, 1994)
- $g = 2$ (Flynn-Smart, 1997; Stoll, 1999, 2001; M., 2009)

Schnitttheorie

Alternative für die Berechnung von $\hat{h}(P)$ ohne explizite Kummer-Varietät: Arakelov-Schnitttheorie über $\mathrm{Spec}(\mathcal{O}_k)$ (Hriljac, 1980).

Benötigt:

- Desingularisierung von arithmetischen Flächen,
- explizite Schnittzahlberechnung auf arithmetischen Flächen,
- Berechnung von Thetafunktionen über $\mathbb{C}$.

Bis jetzt implementiert für hyperelliptische Kurven (Holmes, 2010; M., 2010).

Rekord: $g = 10$.

Problem.
Nicht bekannt, wie $h(P)$ berechnet werden kann.

Verallgemeinerung auf $g = 3$

Frage.
Können wir die Resultate für $g = 2$ auf höhere Dimension verallgemeinern?

- Sei $\mathrm{char}(k) \neq 2$.
- Sei $C : y^2 = f_0 + f_1 x + \ldots + f_7 x^7$ eine glatte hyperelliptische Kurve vom Geschlecht 3, $A = \mathrm{Jac}(C)$ und $K = A/\{\pm 1\}$.

Dann kennen wir

- eine explizite Beschreibung von $\kappa : A \longrightarrow\!\!\!\!\!\rightarrow K \hookrightarrow \mathbb{P}^7$ (Stubbs, 1999);
- eine explizite Beschreibung von $\kappa(A) \subset \mathbb{P}^7$ als Schnitt von einer Quadrik und 34 Quartiken (Stubbs, M., 2010),
- für alle $Q \in A[2]$ die lineare Abbildung $W_Q : \mathbb{P}^7 \longrightarrow \mathbb{P}^7$ mit $W_Q(\kappa(P)) = \kappa(P + Q)$ für alle $P \in A$ (Duquesne, 2001).

Biquadratische Formen für $g = 3$

Proposition. (M., 2010) Es gibt keine biquadratischen Formen $B_{ij}(x, y)$, $1 \leq i, j \leq 8$, sodass

$$\begin{aligned} B_{ij}(\kappa(P), \kappa(Q)) &= \kappa_i(P+Q)\kappa_j(P-Q) + \kappa_j(P+Q)\kappa_i(P-Q),\ i \neq j \\ B_{ii}(\kappa(P), \kappa(Q)) &= \kappa_i(P+Q)\kappa_i(P-Q) \end{aligned}$$

für alle $P, Q \in A$ gilt.

Frage.
Können wir solche biquadratischen Formen lokal finden?

Ein Beispiel

Beispiel. (Duquesne, 2010)
Sei

$$C : y^2 = 4 + x^2 + x^3 + 4x^4 + 2x^5 - 4x^6 + x^7$$

und seien

$$Q = [(0, 2) + (1, 3) + (1, 1) - 3(\infty)] \in A$$

und

$$P = [(x_1, y_1) + (4, y_2) + (2, 4) - 3(\infty)] \in A$$

mit x_1 beliebig. Dann ist

$$\kappa_4(P)\kappa_5(Q) + \kappa_5(P)\kappa_4(Q)$$

weder quadratisch noch quartisch in den $\kappa_1(P), \ldots, \kappa_8(P)$.

Verdopplung für $g = 3$

Aber: Durch Modifikation der biquadratischen Formen für $Q \in A[2]$ erhalten wir quartische Formen $\delta_1(x_1, \ldots, x_8), \ldots, \delta_8(x_1, \ldots, x_8)$ mit Koeffizienten in $\mathbb{Z}[f_0, \ldots, f_7]$.

Vermutung. (M., 2010) Es gilt $\delta(\kappa(P)) = \kappa(2P)$ für alle $P \in A$.

- Funktioniert in numerischen Beispielen.
- Durch allgemeinere Vermutungen gestützt;
- Würde für Höhenanwendungen ausreichen.

Weitere Verallgemeinerungen.

- Ebene Quartiken: Ansatz von Stoll (2010)
- verwendet $\mathrm{Pic}^4(C) \cong \mathrm{Pic}^0(C)$