Arithmetik auf hyperelliptischen Kurven

Peter Schwabe

Lehrstuhl für Theoretische Informationstechnik, RWTH Aachen

14.12.2005

Überblick

Motivation

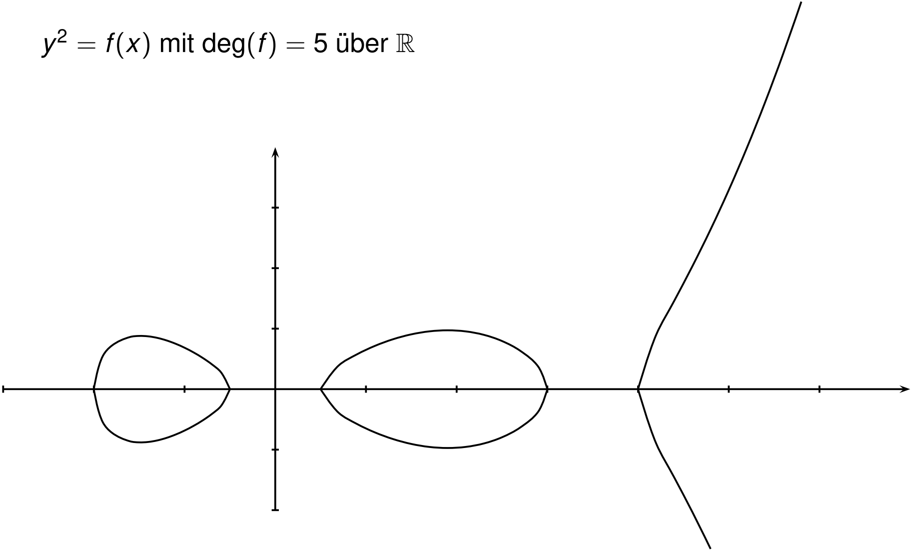
- Arithmetik auf elliptischen Kurven ist bekannt
- Hyperelliptische Kurven stellen eine Verallgemeinerung von elliptischen Kurven dar
- Hyperelliptische Kurven eignen sich für Kryptosysteme

Ziel

Konstruktion einer endlichen Gruppenstruktur mit effizient berechenbarer Gruppenoperation basierend auf hyperelliptischen Kurven.

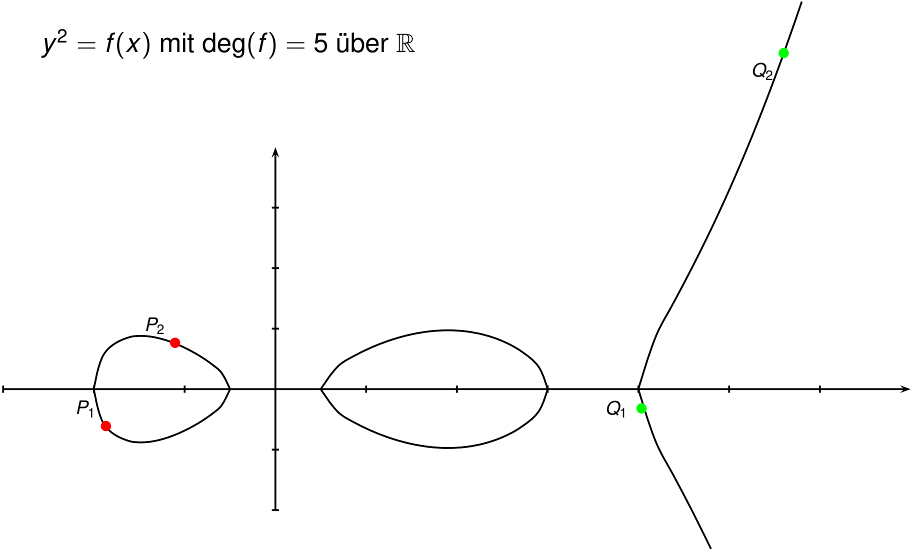
Ein erster Blick auf hyperelliptische Kurven

$y^2 = f(x)$ mit $\deg(f) = 5$ über $\mathbb{R}$



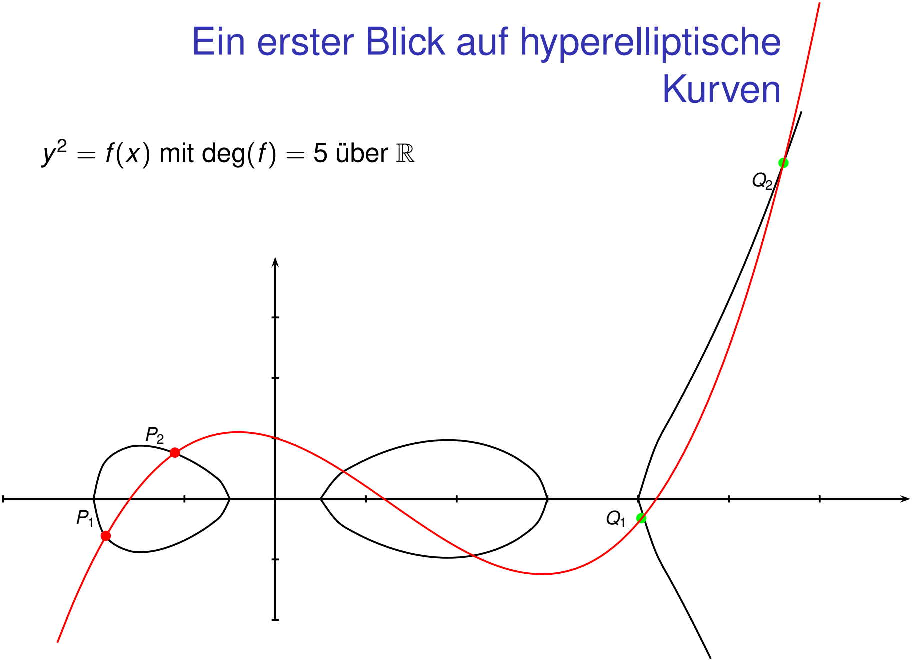
Ein erster Blick auf hyperelliptische Kurven

$y^2 = f(x)$ mit $\deg(f) = 5$ über $\mathbb{R}$



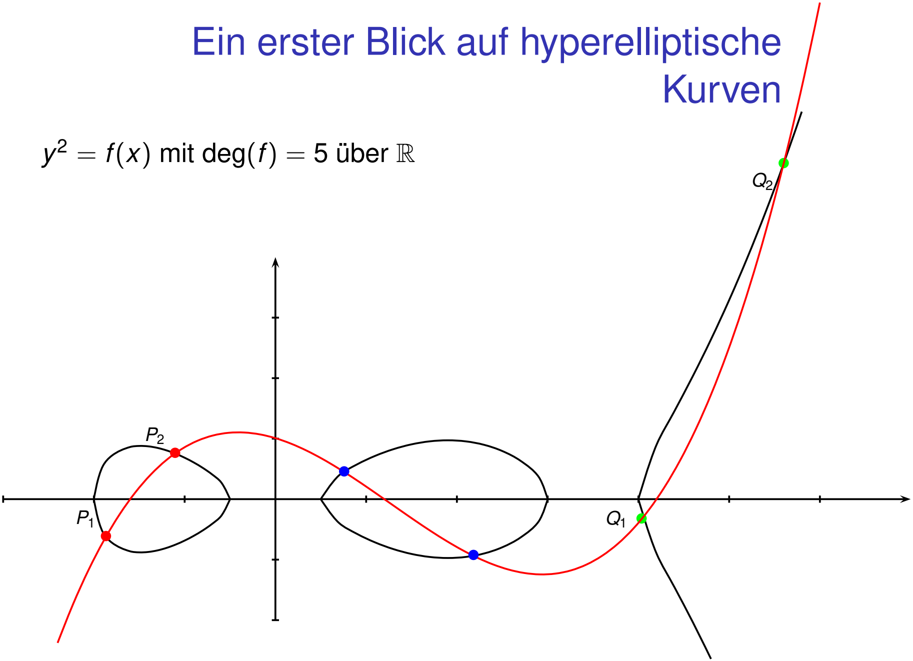
Ein erster Blick auf hyperelliptische Kurven

$y^2 = f(x)$ mit $\deg(f) = 5$ über $\mathbb{R}$



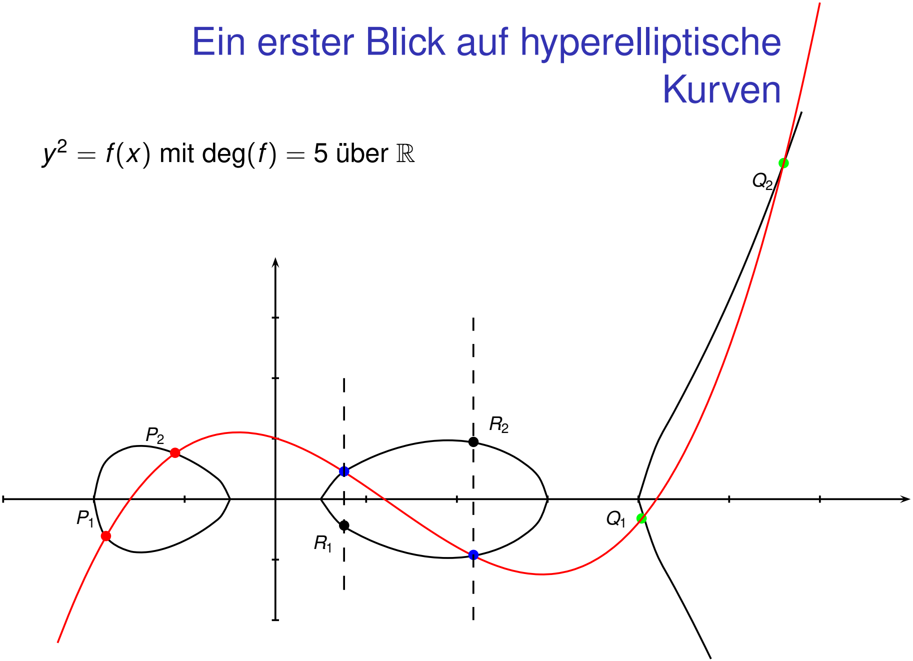
Ein erster Blick auf hyperelliptische Kurven

$y^2 = f(x)$ mit $\deg(f) = 5$ über $\mathbb{R}$



Ein erster Blick auf hyperelliptische Kurven

$y^2 = f(x)$ mit $\deg(f) = 5$ über $\mathbb{R}$



Hyperelliptische Kurven

Definition

Sei K ein Körper, $\overline{K}$ der algebraische Abschluss von K. Dann definiert eine Gleichung der Form

$$C: \; y^2 + h(x)y = f(x) \quad \in K[x, y]$$

mit $\deg f(x) = 2g + 1$ und $\deg h(x) \leq g$ eine hyperelliptische Kurve vom Geschlecht g, wenn kein $(u, v) \in \overline{K} \times \overline{K}$ gleichzeitig die Gleichung C und beide partiellen Ableitungen $2y + h(x) = 0$ und $h'(x)v - f'(x) = 0$ erfüllt.

Hyperelliptische Kurven

Definition

Sei K ein Körper, $\overline{K}$ der algebraische Abschluss von K. Dann definiert eine Gleichung der Form

$$C: \; y^2 + h(x)y = f(x) \quad \in K[x, y]$$

mit $\deg f(x) = 2g + 1$ und $\deg h(x) \leq g$ eine hyperelliptische Kurve vom Geschlecht g, wenn kein $(u, v) \in \overline{K} \times \overline{K}$ gleichzeitig die Gleichung C und beide partiellen Ableitungen $2y + h(x) = 0$ und $h'(x)v - f'(x) = 0$ erfüllt.

Definition

Sei L ein Erweiterungskörper von K. Dann heißt die Menge

$$C(L) = \{(u, v) \in L \times L \mid v^2 + h(u)v = f(u)\} \cup \{\mathcal{O}\}$$

die Menge L-rationaler Punkte auf C.
Es gilt: $C(\overline{K}) = C$

Punkte auf C

- Sei $P = (u, v) \in C$, dann heißt $\tilde{P} = (u, -v - h(u))$ der P gegenüberliegende Punkt
- Gilt für einen Punkt $P \in C$, dass $P = \tilde{P}$, so ist P ein spezieller Punkt
  sonst ist P ein gewöhnlicher Punkt.
- Es gilt $\mathcal{O} = \tilde{\mathcal{O}}$

Der Koordinatenring von C über K

Definition

Der Koordinatenring von C über K ist der Quotientenring

$$K[C] = K[x, y]/_{(y^2+h(x)y-f(x))K[x,y]}$$

Analog definiert man den Koordinatenring von C über $\overline{K}$:

$$\overline{K}[C] = \overline{K}[x, y]/_{(y^2+h(x)y-f(x))\overline{K}[x,y]}$$

Die Elemente von $\overline{K}[C]$ heißen Polynomfunktionen.

Der Koordinatenring von C über K

Definition

Der Koordinatenring von C über K ist der Quotientenring

$$K[C] = K[x, y]/_{(y^2+h(x)y-f(x))K[x,y]}$$

Analog definiert man den Koordinatenring von C über $\overline{K}$:

$$\overline{K}[C] = \overline{K}[x, y]/_{(y^2+h(x)y-f(x))\overline{K}[x,y]}$$

Die Elemente von $\overline{K}[C]$ heißen Polynomfunktionen.

Da $(y^2 + h(x)y - f(x))$ über $\overline{K}$ irreduzibel ist, ist $\overline{K}[C]$ ein Integritätsbereich.

Polynomfunktionen

Definition

Sei $G(x, y) = a(x) - b(x)y$ eine Polynomfunktion, dann heißt $\overline{G}(x, y) = a(x) + b(x)(h(x) + y)$ die Konjugierte von G.

Definition

Sei $G(x, y) = a(x) - b(x)y$ eine Polynomfunktion, dann heißt $\overline{G}(x, y) = a(x) + b(x)(h(x) + y)$ die Konjugierte von G.

Definition

Sei $G(x, y) = a(x) - b(x)y$ eine Polynomfunktion. Dann heißt die Polynomfunktion $N(G) = G\overline{G}$ die Norm von G.

Polynomfunktionen

Definition

Sei $G(x, y) = a(x) - b(x)y$ eine Polynomfunktion, dann heißt $\overline{G}(x, y) = a(x) + b(x)(h(x) + y)$ die Konjugierte von G.

Definition

Sei $G(x, y) = a(x) - b(x)y$ eine Polynomfunktion. Dann heißt die Polynomfunktion $N(G) = G\overline{G}$ die Norm von G.

Seien G und H Polynomfunktionen, dann gilt:

- $N(G)$ ist ein Polynom in $\overline{K}[x]$.
- $N(\overline{G}) = N(G)$
- $N(GH) = N(G)N(H)$

Polynomfunktionen

Definition

Sei $G(x,y) = a(x) - b(x)y$ eine Polynomfunktion, dann heißt $\overline{G}(x,y) = a(x) + b(x)(h(x) + y)$ die Konjugierte von G.

Definition

Sei $G(x,y) = a(x) - b(x)y$ eine Polynomfunktion. Dann heißt die Polynomfunktion $N(G) = G\overline{G}$ die Norm von G.

Seien G und H Polynomfunktionen, dann gilt:

- $N(G)$ ist ein Polynom in $\overline{K}[x]$.
- $N(\overline{G}) = N(G)$
- $N(GH) = N(G)N(H)$

Definition

Sei $G = a(x) - b(x)y$ eine Polynomfunktion, dann ist der Grad von G:

- $\deg(G) = \deg_x(N(G))$
- $\deg(G) = \max(2\deg_x(a), 2g + 1 + 2\deg_x(b))$

Der Funktionenkörper von C über K

Definition

Der Quotientenkörper von $K[C]$ heißt Funktionenkörper von C über K (Bezeichnung: $K(C)$), der Quotientenkörper von $\overline{K}[C]$ analog Funktionenkörper von C über $\overline{K}$ (Bezeichnung: $\overline{K}(C)$).

Der Funktionenkörper von C über K

Definition

Der Quotientenkörper von $K[C]$ heißt Funktionenkörper von C über K (Bezeichnung: $K(C)$), der Quotientenkörper von $\overline{K}[C]$ analog Funktionenkörper von C über $\overline{K}$ (Bezeichnung: $\overline{K}(C)$).
Die Elemente von $\overline{K}(C)$ heißen rationale Funktionen auf C.

Die Ordnung von Polynomfunktionen in einem Punkt

Sei G eine Polynomfunktion und sei $P \in C$. Die Ordnung von G in P ($ord_P(G)$) ist:

- 0 ,wenn $P \neq \mathcal{O}$ und $G(P) \neq 0$.

Die Ordnung von Polynomfunktionen in einem Punkt

Sei G eine Polynomfunktion und sei $P \in C$. Die Ordnung von G in P ($ord_P(G)$) ist:

- 0 ,wenn $P \neq \mathcal{O}$ und $G(P) \neq 0$.
- “Die Vielfachheit der Nullstelle”, wenn $P \neq \mathcal{O}$ und $G(P) = 0$.

Die Ordnung von Polynomfunktionen in einem Punkt

Sei G eine Polynomfunktion und sei $P \in C$. Die Ordnung von G in P ($ord_P(G)$) ist:

- 0 ,wenn $P \neq \mathcal{O}$ und $G(P) \neq 0$.
- “Die Vielfachheit der Nullstelle”, wenn $P \neq \mathcal{O}$ und $G(P) = 0$.
- - $-\deg(G)$, wenn $P = \mathcal{O}$.

Die Ordnung von Polynomfunktionen in einem Punkt

Sei G eine Polynomfunktion und sei $P \in C$. Die Ordnung von G in P ($ord_P(G)$) ist:

- 0 ,wenn $P \neq \mathcal{O}$ und $G(P) \neq 0$.
- "Die Vielfachheit der Nullstelle", wenn $P \neq \mathcal{O}$ und $G(P) = 0$.
- - $-\deg(G)$, wenn $P = \mathcal{O}$.

Die Ordnung einer rationalen Funktion $R = G/H$ in einem Punkt $P \in C$ ist:

Die Ordnung von Polynomfunktionen in einem Punkt

Sei G eine Polynomfunktion und sei $P \in C$. Die Ordnung von G in P ($ord_P(G)$) ist:

- 0 ,wenn $P \neq \mathcal{O}$ und $G(P) \neq 0$.
- “Die Vielfachheit der Nullstelle”, wenn $P \neq \mathcal{O}$ und $G(P) = 0$.
- - $-\deg(G)$, wenn $P = \mathcal{O}$.

Die Ordnung einer rationalen Funktion $R = G/H$ in einem Punkt $P \in C$ ist:

- $ord_P(R) = ord_P(G) - ord_P(H))$

Definition

Ein Divisor ist eine formale Summe von Punkten auf C:

$$D = \sum_{P \in C} m_P P \qquad , m_P \in \mathbb{Z}$$

wenn nur eine endliche Anzahl der Werte m_P ungleich 0 ist.

Divisoren

Definition

Ein Divisor ist eine formale Summe von Punkten auf C:

$$D = \sum_{P \in C} m_P P \qquad , m_P \in \mathbb{Z}$$

wenn nur eine endliche Anzahl der Werte m_P ungleich 0 ist.

- Die Menge aller Divisoren $\mathbb{D}$ bildet eine additive Gruppe mit der Addition:

$$\sum_{P \in C} m_P P + \sum_{P \in C} n_P P = \sum_{P \in C} (m_P + n_P) P$$

Divisoren

Definition

Ein Divisor ist eine formale Summe von Punkten auf C:

$$D = \sum_{P \in C} m_P P \qquad , m_P \in \mathbb{Z}$$

wenn nur eine endliche Anzahl der Werte m_P ungleich 0 ist.

- Die Menge aller Divisoren $\mathbb{D}$ bildet eine additive Gruppe mit der Addition:
$$\sum_{P \in C} m_P P + \sum_{P \in C} n_P P = \sum_{P \in C} (m_P + n_P) P$$
- Der größte gemeinsame Divisor zweier Divisoren $D_1 = \sum_{P \in C} m_P P$ und $D_2 = \sum_{P \in C} n_P P$ ist:
$$\gcd(D_1, D_2) = \sum_{P \in C} \min(m_P, n_P) P$$

Divisoren

- Der Grad eines Divisors D ($\deg D$) ist $\sum_{P \in C} m_P$

Divisoren

- Der Grad eines Divisors D ($\deg D$) ist $\sum_{P \in C} m_P$
- Die Ordnung eines Divisors D im Punkt P ist m_P, Schreibweise: $ord_P(D) = m_P$

Divisoren

- Der Grad eines Divisors D (deg D) ist $\sum_{P \in C} m_P$
- Die Ordnung eines Divisors D im Punkt P ist m_P, Schreibweise: $ord_P(D) = m_P$
- Die Menge der Divisoren von Grad 0 bildet eine Untergruppe der Gruppe $(\mathbb{D}, +)$, Bezeichnung: $\mathbb{D}^0$

Hauptdivisoren

Definition

Sei $R \in \overline{K}(C)$ eine rationale Funktion, $R \neq 0$. Der Divisor von R ist

$$\mathrm{div}(R) = \sum_{P \in C} (ord_P(R))P$$

Hauptdivisoren

Definition

Sei $R \in \overline{K}(C)$ eine rationale Funktion, $R \neq 0$. Der Divisor von R ist

$$\operatorname{div}(R) = \sum_{P \in C} (ord_P(R))P$$

Definition

Ein Divisor D heißt Hauptdivisor, falls $D = \operatorname{div}(R)$ für eine rationale Funktion $R \in \overline{K}(C),\ R \neq 0$.

Hauptdivisoren

Definition

Sei $R \in \overline{K}(C)$ eine rationale Funktion, $R \neq 0$. Der Divisor von R ist

$$\operatorname{div}(R) = \sum_{P \in C} (ord_P(R))P$$

Definition

Ein Divisor D heißt Hauptdivisor, falls $D = \operatorname{div}(R)$ für eine rationale Funktion $R \in \overline{K}(C),\ R \neq 0$.

- Es gilt: $\deg(\operatorname{div}(R)) = 0 \quad \forall R \in \overline{K}(C),\ R \neq 0$.

Hauptdivisoren

Definition

Sei $R \in \overline{K}(C)$ eine rationale Funktion, $R \neq 0$. Der Divisor von R ist

$$\mathrm{div}(R) = \sum_{P \in C} (ord_P(R))P$$

Definition

Ein Divisor D heißt Hauptdivisor, falls $D = \mathrm{div}(R)$ für eine rationale Funktion $R \in \overline{K}(C),\ R \neq 0$.

- Es gilt: $\deg(\mathrm{div}(R)) = 0 \quad \forall R \in \overline{K}(C),\ R \neq 0$.
- Beispiel:
  - Sei $P = (u, v)$ gewöhnlich, dann ist $\mathrm{div}(x - u) = P + \tilde{P} - 2\mathcal{O}$
  - Sei $P = (u, v)$ speziell, dann ist $\mathrm{div}(x - u) = 2P - 2\mathcal{O}$

Hauptdivisoren

Definition

Sei $R \in \overline{K}(C)$ eine rationale Funktion, $R \neq 0$. Der Divisor von R ist

$$\mathrm{div}(R) = \sum_{P \in C} (ord_P(R))P$$

Definition

Ein Divisor D heißt Hauptdivisor, falls $D = \mathrm{div}(R)$ für eine rationale Funktion $R \in \overline{K}(C),\ R \neq 0$.

- Es gilt: $\deg(\mathrm{div}(R)) = 0 \quad \forall R \in \overline{K}(C),\ R \neq 0$.
- Beispiel:
  - Sei $P = (u, v)$ gewöhnlich, dann ist $\mathrm{div}(x - u) = P + \tilde{P} - 2\mathcal{O}$
  - Sei $P = (u, v)$ speziell, dann ist $\mathrm{div}(x - u) = 2P - 2\mathcal{O}$
- Die Menge aller Hauptdivisoren heißt $\mathbb{P}$, es gilt: $\mathbb{P}$ ist eine Untergruppe von $\mathbb{D}^0$.

Der Jacobian von C

Definition

Die Quotientengruppe $\mathbb{J} = \mathbb{D}^0/\mathbb{P}$ heißt Jacobian der hyperelliptischen Kurve C.
Für $D_1, D_2 \in \mathbb{D}^0$ gilt: D_1 und D_2 sind äquivalente Divisoren ($D_1 \sim D_2$), wenn $D_1 - D_2 \in \mathbb{P}$.

Der Jacobian von C

Definition

Die Quotientengruppe $\mathbb{J} = \mathbb{D}^0/\mathbb{P}$ heißt Jacobian der hyperelliptischen Kurve C.
Für $D_1, D_2 \in \mathbb{D}^0$ gilt: D_1 und D_2 sind äquivalente Divisoren ($D_1 \sim D_2$), wenn $D_1 - D_2 \in \mathbb{P}$.

Definition

Sei $D = \sum_{P \in C} m_P P$ ein Divisor. Der Träger (*support*) von D ist die Menge

$$supp(D) = \{P \in C \mid m_P \neq 0\}$$

Semi-reduzierte Divisoren

Definition

Ein semi-reduzierter Divisor ist ein Divisor der Form

$$D = \sum_{P \in C, P \neq \mathcal{O}} m_P P - \Big(\sum_{P \in C, P \neq \mathcal{O}} m_P\Big)\mathcal{O},$$

wenn alle $m_P \geq 0$ und wenn für jeden endlichen Punkt P gilt, dass

$$P \in supp(D) \Rightarrow \tilde{P} \notin supp(D),$$

es sei denn, dass $P = \tilde{P}$, in diesem Falle ist $m_P = 1$.

Semi-reduzierte Divisoren

Definition

Ein semi-reduzierter Divisor ist ein Divisor der Form

$$D = \sum_{P \in C, P \neq \mathcal{O}} m_P P - \Big(\sum_{P \in C, P \neq \mathcal{O}} m_P \Big) \mathcal{O},$$

wenn alle $m_P \geq 0$ und wenn für jeden endlichen Punkt P gilt, dass

$$P \in supp(D) \Rightarrow \tilde{P} \notin supp(D),$$

es sei denn, dass $P = \tilde{P}$, in diesem Falle ist $m_P = 1$.

Lemma

Zu jedem Divisor $D \in \mathbb{D}^0$ existiert ein semi-reduzierter Divisor D', so dass $D \sim D'$.

Darstellung semi-reduzierter Divisoren

Satz

Sei $D = \sum m_i P_i - (\sum m_i)\mathcal{O}$ ein semi-reduzierter Divisor, $P_i = (u_i, v_i)$.
Sei $a(x) = \Pi(x - u_i)^{m_i}$

Darstellung semi-reduzierter Divisoren

Satz

Sei $D = \sum m_i P_i - (\sum m_i)\mathcal{O}$ ein semi-reduzierter Divisor, $P_i = (u_i, v_i)$.
Sei $a(x) = \Pi(x - u_i)^{m_i}$
Dann existiert genau ein Polynom $b(x)$ für das das folgende gilt:

- $\deg_x(b) < \deg_x(a)$
- $b(u_i) = v_i \quad \forall i : m_i \neq 0$
- $a(x) \mid (N(b(x) - y))$

Darstellung semi-reduzierter Divisoren

Satz

Sei $D = \sum m_i P_i - (\sum m_i)\mathcal{O}$ ein semi-reduzierter Divisor, $P_i = (u_i, v_i)$.
Sei $a(x) = \Pi(x - u_i)^{m_i}$
Dann existiert genau ein Polynom $b(x)$ für das das folgende gilt:

- $\deg_x(b) < \deg_x(a)$
- $b(u_i) = v_i \quad \forall i : m_i \neq 0$
- $a(x) \mid (N(b(x) - y))$

Dann ist $D = \gcd(div(a(x)), div(b(x) - y))$.

Darstellung semi-reduzierter Divisoren

Satz

Sei $D = \sum m_i P_i - (\sum m_i)\mathcal{O}$ ein semi-reduzierter Divisor, $P_i = (u_i, v_i)$.
Sei $a(x) = \Pi(x - u_i)^{m_i}$
Dann existiert genau ein Polynom $b(x)$ für das das folgende gilt:

- $\deg_x(b) < \deg_x(a)$
- $b(u_i) = v_i \quad \forall i : m_i \neq 0$
- $a(x) \mid (N(b(x) - y))$

Dann ist $D = \gcd(div(a(x)), div(b(x) - y))$.

Schreibweise: $D = \text{div}(a(x), b(x))$ oder $D = \text{div}(a, b)$ Diese Darstellung heißt Mumford-Darstellung.

Reduzierte Divisoren

Definition

Sei D ein Divisor. Dann ist

$$|D| = \sum_{P \in C \setminus \{\mathcal{O}\}} |m_P|$$

die Norm von D.

Reduzierte Divisoren

Definition

Sei D ein Divisor. Dann ist

$$|D| = \sum_{P \in C \setminus \{\mathcal{O}\}} |m_P|$$

die Norm von D.

Definition

Sei D ein semi-reduzierter Divisor. Wenn $|D| \leq g$, dann ist D ein reduzierter Divisor.

Reduzierte Divisoren

Definition

Sei D ein Divisor. Dann ist

$$|D| = \sum_{P \in C \setminus \{\mathcal{O}\}} |m_P|$$

die Norm von D.

Definition

Sei D ein semi-reduzierter Divisor. Wenn $|D| \leq g$, dann ist D ein reduzierter Divisor.

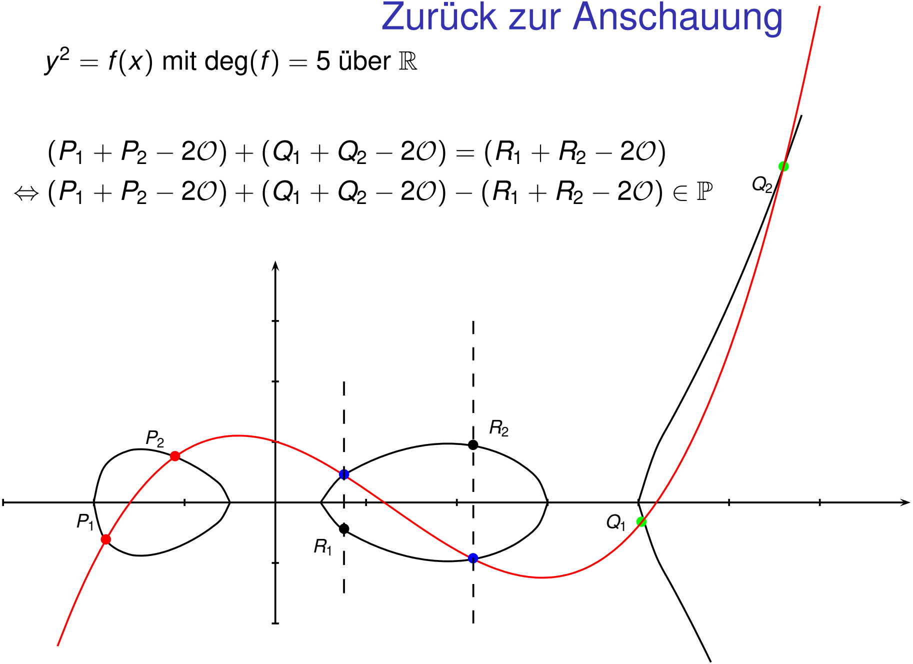
Satz

Für jeden Divisor $D \in \mathbb{D}^0$ existiert genau ein reduzierter Divisor D', so dass $D \sim D'$.

Zurück zur Anschauung

$y^2 = f(x)$ mit $\deg(f) = 5$ über $\mathbb{R}$

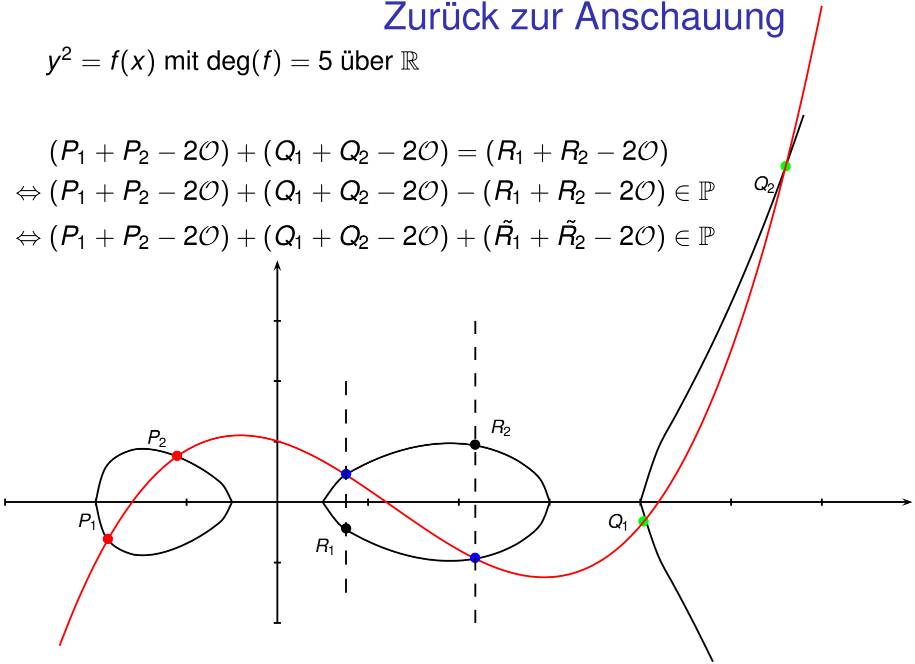
$$(P_1 + P_2 - 2\mathcal{O}) + (Q_1 + Q_2 - 2\mathcal{O}) = (R_1 + R_2 - 2\mathcal{O})$$
$$\Leftrightarrow (P_1 + P_2 - 2\mathcal{O}) + (Q_1 + Q_2 - 2\mathcal{O}) - (R_1 + R_2 - 2\mathcal{O}) \in \mathbb{P}$$



Zurück zur Anschauung

$y^2 = f(x)$ mit $\deg(f) = 5$ über $\mathbb{R}$

$$(P_1 + P_2 - 2\mathcal{O}) + (Q_1 + Q_2 - 2\mathcal{O}) = (R_1 + R_2 - 2\mathcal{O})$$
$$\Leftrightarrow (P_1 + P_2 - 2\mathcal{O}) + (Q_1 + Q_2 - 2\mathcal{O}) - (R_1 + R_2 - 2\mathcal{O}) \in \mathbb{P}$$
$$\Leftrightarrow (P_1 + P_2 - 2\mathcal{O}) + (Q_1 + Q_2 - 2\mathcal{O}) + (\tilde{R}_1 + \tilde{R}_2 - 2\mathcal{O}) \in \mathbb{P}$$



Konstruktion einer endlichen Gruppe

Sei C eine hyperelliptische Kurve über einem endlichen Körper K.
Sei $P = (u, v) \in C$ und sei σ ein Automorphismus von $\overline{K}$ über K.
Dann ist $P^\sigma := (\sigma(u), \sigma(v)) \in C$.

Konstruktion einer endlichen Gruppe

Sei C eine hyperelliptische Kurve über einem endlichen Körper K.
Sei $P = (u, v) \in C$ und sei σ ein Automorphismus von $\overline{K}$ über K.
Dann ist $P^\sigma := (\sigma(u), \sigma(v)) \in C$.

Definition

Ein Divisor $D = \sum m_P P$ ist definiert über K, wenn
$D^\sigma := \sum m_P P^\sigma = D$ für alle Automorphismen σ von $\overline{K}$ über K.

Konstruktion einer endlichen Gruppe

Sei C eine hyperelliptische Kurve über einem endlichen Körper K.
Sei $P = (u, v) \in C$ und sei σ ein Automorphismus von $\overline{K}$ über K.
Dann ist $P^\sigma := (\sigma(u), \sigma(v)) \in C$.

Definition

Ein Divisor $D = \sum m_P P$ ist definiert über K, wenn
$D^\sigma := \sum m_P P^\sigma = D$ für alle Automorphismen σ von $\overline{K}$ über K.

- Die Menge $\mathbb{J}(K)$ der Divisorklassen, die einen Divisor enthalten, der über K definiert ist, ist eine endliche abelsche Untergruppe von $\mathbb{J}$.

Konstruktion einer endlichen Gruppe

Sei C eine hyperelliptische Kurve über einem endlichen Körper K.
Sei $P = (u, v) \in C$ und sei σ ein Automorphismus von $\overline{K}$ über K.
Dann ist $P^\sigma := (\sigma(u), \sigma(v)) \in C$.

Definition

Ein Divisor $D = \sum m_P P$ ist definiert über K, wenn
$D^\sigma := \sum m_P P^\sigma = D$ für alle Automorphismen σ von $\overline{K}$ über K.

- Die Menge $\mathbb{J}(K)$ der Divisorklassen, die einen Divisor enthalten, der über K definiert ist, ist eine endliche abelsche Untergruppe von $\mathbb{J}$.
- Jedes der Elemente aus $\mathbb{J}(K)$ enthält einen reduzierten Divisor D, mit einer Darstellung $D = \mathrm{div}(a, b)$ wobei $a, b \in K[X]$.

Addition von Divisoren in der Mumford-Darstellung

Addieren von Divisoren: Cantors Algorithmus

1. Schritt:

- Input: 2 semi-reduzierte Divisoren $D_1 = \mathrm{div}(a_1, b_1)$ und $D_2 = \mathrm{div}(a_2, b_2)$.
- Output: 1 semi-reduzierter Divisor $D \sim D_1 + D_2$.
- Der Algorithmus verwendet nur a_1, a_2, b_1, b_2.

Addition von Divisoren in der Mumford-Darstellung

Addieren von Divisoren: Cantors Algorithmus

1. Schritt:
   - Input: 2 semi-reduzierte Divisoren $D_1 = \mathrm{div}(a_1, b_1)$ und $D_2 = \mathrm{div}(a_2, b_2)$.
   - Output: 1 semi-reduzierter Divisor $D \sim D_1 + D_2$.
   - Der Algorithmus verwendet nur a_1, a_2, b_1, b_2.
2. Schritt:
   - Input: 1 semi-reduzierter Divisor $D = \mathrm{div}(a, b)$.
   - Output: 1 reduzierter Divisor D' mit $D \sim D'$.
   - Auch dieser Algorithmus verwendet nur a, b.

Zusammenfassung und Ausblick

Zusammenfassung

Gruppenstruktur basierend auf hyperelliptischen Kurven

- Elemente der Menge sind Divisoren (formale Summen von Punkten)
- Darstellung nach Mumford benötigt nur zwei Polynome über einem endlichen Körper
- Gruppenoperation effizient berechenbar mit Cantors Algorithmus

Zusammenfassung und Ausblick

Zusammenfassung

Gruppenstruktur basierend auf hyperelliptischen Kurven

- Elemente der Menge sind Divisoren (formale Summen von Punkten)
- Darstellung nach Mumford benötigt nur zwei Polynome über einem endlichen Körper
- Gruppenoperation effizient berechenbar mit Cantors Algorithmus

Ausblick

- Effizientere Algorithmen für besonders relevante Spezialfälle von hyperelliptischen Kurven
- Schnelle Arithmetik auf *elliptischen* Kurven