KAPITEL 13

Hyperelliptische Kurven

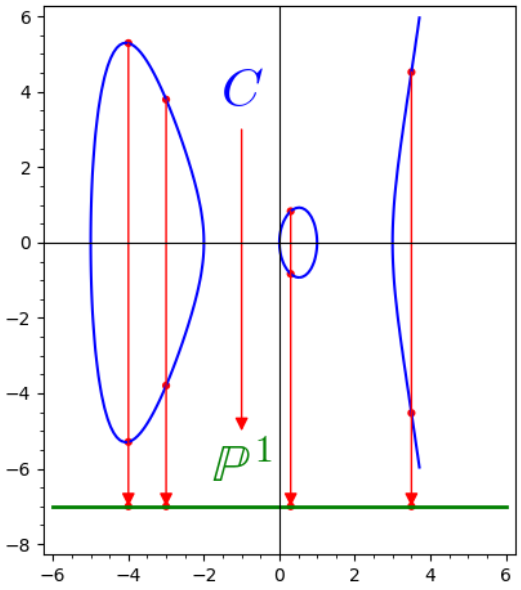
1. Einführung

Wir setzen in diesem Kapitel der Einfachkeit halber voraus, dass die Charakteristik des (vollkommenen) Grundkörpers K von 2 verschieden ist. Wenn nichts anderes gesagt wird, meint Kurve stets eine über K definierte, absolut irreduzible, nichtsinguläre, projektive Kurve.

DEFINITION. *Eine* **hyperelliptische Kurve** C *über* K *ist eine über* K *definierte, absolut irreduzible, nichtsinguläre, projektive Kurve vom Geschlecht* $g \geq 2$*, sodass ein über* K *definierter Morphismus*

$$\phi : C \to \mathbb{P}^1$$

vom Grad 2 *existiert.*



Wie kann man sich hyperelliptische Kurven konkret vorstellen?

LEMMA. *Ist* C *eine über* K *definierte, absolut irreduzible, nichtsinguläre, projektive Kurve und* $\phi : C \to \mathbb{P}^1$ *ein über* K *definierter Morphismus vom Grad* 2*, so gibt es Funktionen* $x, y \in K(C)$ *und ein separables Polynom* $f(X) \in K[X]$ *vom Grad* $n \geq 1$*, sodass gilt*

$$K(C) = K(x, y), \quad y^2 = f(x) \quad \text{und} \quad \phi = (1 : x).$$

Beweis:

Datei: algku13.tex. Version vom 18.7.2021

(1) Bezeichnet $\widetilde{x}$ die Koordinatenfunktion von $\mathbb{P}^1$, so ist $K(\mathbb{P}^1) = K(\widetilde{x})$. Der Funktionenkörper $K(C)$ ist dann eine quadratische Erweiterung von $\phi^*K(\mathbb{P}^1) = \phi^*K(\widetilde{x}) = K(\phi^*(\widetilde{x}))$. Wir schreiben $x = \phi^*(\widetilde{x})$ und haben dann $\phi^*K(\mathbb{P}^1) = K(x)$. Da $K(C)$ eine quadratische Erweiterung von $K(x)$ ist, gibt es eine Funktion $y \in K(C)$, sodass y einer Gleichung
$$a(x)y^2 + b(x)y + c(x) = 0$$
genügt mit rationalen Funktionen $a(X), b(X), c(X) \in K(X)$. Es ist dann
$$K(C) = K(x, y) = K(x)[y].$$
(2) Wir ändern nun y ab, damit die y beschreibende Gleichung etwas einfacher aussieht.
(3) Wegen $y \notin K(x)$ ist $a(x) \neq 0$. Multiplizieren wir obige Gleichung mit $a(x)$, so können wir schreiben
$$(a(x)y)^2 + b(x)(a(x)y) + a(x)c(x) = 0.$$
Betrachten die statt y die Funktion $a(x) \cdot y$, so können wir $a(x) = 1$ annehmen. Die y beschreibende Gleichung wird dann zu
$$y^2 + b(x)y + c(x) = 0.$$
(4) Nun machen wir quadratische Ergänzung, wofür $\mathrm{char}(K) \neq 2$ wichtig ist:
$$\left(y + \frac{1}{2}b(x)\right)^2 = \frac{1}{4}b(x)^2 - c(x).$$
Betrachten wir also statt y die Funktion $y + \frac{1}{2}b(x)$, setzen wir $d(X) = \frac{1}{4}b(X)^2 - c(X)$, so genügt y der Gleichung
$$y^2 = d(x).$$
(5) Nun zerlegen wir in $K(X)$ die rationale Funktion $d(X)$ in das Produkt aus einem Quadrat $e(X)^2$ und einem quadratfreien Polynom $f(X)$:
$$d(X) = e(X)^2 \cdot f(X) \quad \text{mit} \quad e(X) \in K(X) \quad \text{und} \quad f(X) \in K[X] \text{ quadratfrei.}$$
Es ist
$$y^2 = e(x)^2 \cdot f(x).$$
Indem wir statt y die Funktion $\frac{y}{e(x)}$ betrachten, können wir $e(X) = 1$ annehmen, d.h. y genügt der Gleichung
$$y^2 = f(x),$$
wobei nun $f(X) \in K[X]$ ein quadratfreies Polynom ist. (Ist K algebraisch abgeschlossen, so kann man noch erreichen, dass $f(X)$ normiert ist.) Statt quadratfrei kann man natürlich auch separabel sagen, da der Grundkörper als vollkommen vorausgesetzt wurde. Damit ist das Lemma bewiesen. ■

Wir betrachten zunächst die einfachsten Fälle:

LEMMA. *Sei $f(x) \in K[x]$ ein separables Polynom vom Grad n mit $n \in \{1, 2, 3\}$ und C die durch $y^2 = f(x)$ definierte ebene projektive Kurve.*

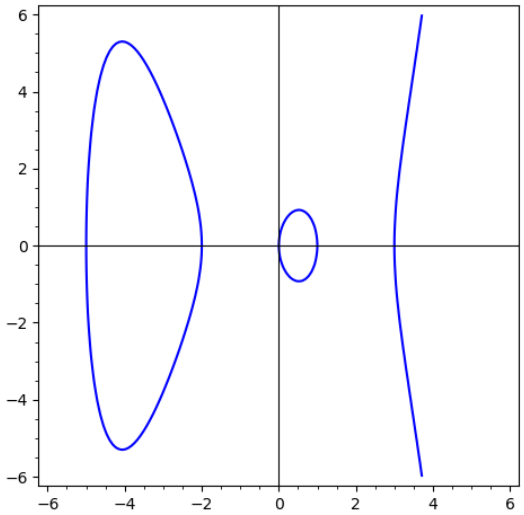
(1) *Im Fall $n = 1$ oder $n = 2$ ist C eine nichtsinguläre projektive ebene Quadrik und hat Geschlecht 0.*
(2) *Im Fall $n = 3$ ist C eine nichtsinguläre projektive ebene Kubik und hat Geschlecht 1.*

Beweis: Übungsaufgabe. ■

LEMMA. *Sei $f(x) \in K[x]$ ein separables Polynom vom Grad $n \geq 4$, d.h. es gibt eine Zahl $c \in K^*$ und paarweise verschiedene Zahlen $\gamma_1, \ldots, \gamma_n \in \overline{K}$ mit*
$$f(x) = c(x - \gamma_1) \ldots (x - \gamma_n).$$
und C_0 die durch
$$y^2 = f(x)$$
definierte projektive ebene Kurve.

(1) *C_0 ist nichtsingulär in Endlichen.*
(2) *C_0 besitzt genau einen Punkt im Unendlichen, nämlich $(0:0:1)$. Der Punkt $(0:0:1)$ ist eine Singularität von C_0.*
(3) *Für einen Punkt $(\alpha,\beta)\in C_0$ mit $\beta\neq 0$ ist $x-\alpha$ uniformisierend, für die Punkte $(\gamma_i,0)\in C$ $(i=1,\dots,n)$ ist y uniformisierend.*

Beispiel: $y^2=\frac{1}{10}x(x-1)(x-3)(x+2)(x+5)$



Beweis:

(1) C_0 wird im Endlichen beschrieben durch
$$g(x,y)=y^2-f(x).$$
Nun ist
$$\frac{\partial g}{\partial x}=-f'(x)\quad\text{und}\quad\frac{\partial g}{\partial y}=2y.$$
Ein Kurvenpunkt ist genau dann singulär, wenn gilt
$$y^2=f(x),\quad f'(x)=0,\quad y=0,\quad\text{also}\quad f(x)=f'(x)=0,\quad y=0.$$
Nun war aber $f(x)$ als separabel vorausgesetzt, weswegen $f(x)$ und $f'(x)$ keine gemeinsame Nullstelle haben. Daher besitzt C_0 keine Singularität im Endlichen. Für $(a,b)\in C_0$ lautet die Tangentengleichung
$$-f'(a)\cdot(x-a)+2b\cdot(y-b)=0.$$
(2) Der projektive Abschluss der affinen Kurve wird durch
$$x_0^{n-2}x_2^2=c(x_1-\gamma_1x_0)\dots(x_1-\gamma_nx_0)$$
beschrieben. Wegen $c\neq 0$ ist $(0:0:1)$ der einzige Punkt im Unendlichen. Verwenden wir die affinen Koordinaten r,s (von U_2) mit $(1:x:y)=(r:s:1)$, so wird die Kurve in U_2 zu
$$r^{n-2}=c(s-\gamma_1r)\dots(s-\gamma_nr).$$
Die Taylorentwicklung in $(r,s)=(0,0)$ ist
$$r^{n-2}-c(s-\gamma_1r)\dots(s-\gamma_nr).$$
Wegen $n\geq 4$ gibt es keinen linearen Term, sodass die Kurve hier singulär ist.
(3) Wir haben bereits unter (1) die Tangentengleichung für einen Punkt $(a,b)\in C_0$ hergeleitet:
$$-f'(a)\cdot(x-a)+2b\cdot(y-b)=0.$$
Ist $b\neq 0$, so ist also $x-a$ uniformisierend, ist $b=0$, so ist y uniformisierend. ■

SATZ. *Sei $f(x) \in K[X]$ ein separables Polynom vom Grad $n \geq 4$, C_0 die durch*

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

definierte projektive ebene Kurve, C ein nichtsinguläres Modell von C_0 (mit birationalem Morphismus $\pi : C \to C_0$) und $\phi : C \to \mathbb{P}^1$ der durch $\phi = (1 : x)$ gegebene Morphismus vom Grad 2. (Wir schreiben $f(x) = c(x - \gamma_1) \dots (x - \gamma_n)$ mit paarweise verschiedenen Zahlen $\gamma_1, \dots, \gamma_n \in \overline{K}$ und $c \in K^*$.)

(1) *Der birationale Morphismus liefert eine Isomorphie*

$$C \setminus \phi^{-1}(\infty) \simeq C_0 \setminus \{(0 : 0 : 1)\}.$$

(2) *Die im Endlichen gelegenen Verzweigungspunkte von ϕ sind genau die Punkte*

$$(\gamma_1, 0), (\gamma_2, 0), \dots, (\gamma_n, 0),$$

jeweils mit Verzweigungsindex 2.

(3) *Es gilt*

$$\#\phi^{-1}(\infty) = \begin{cases} 2, & \text{falls } n \text{ gerade ist,} \\ 1, & \text{falls } n \text{ ungerade ist.} \end{cases}$$

Wir schreiben

$$\phi^{-1}(\infty) = \begin{cases} \{\infty_1, \infty_2\}, & \text{falls } n \text{ gerade ist,} \\ \{\infty\}, & \text{falls } n \text{ ungerade ist.} \end{cases}$$

(4) *Für das Geschlecht von C gilt:*

$$g(C) = \begin{cases} \frac{n-2}{2}, & \text{falls } n \text{ gerade ist,} \\ \frac{n-1}{2}, & \text{falls } n \text{ ungerade ist} \end{cases} \qquad \text{bzw.} \qquad n = \begin{cases} 2g+2, & \text{falls } n \equiv 0 \bmod 2, \\ 2g+1, & \text{falls } n \equiv 1 \bmod 2. \end{cases}$$

(5) *Für ungerades n gilt*

$$\operatorname{ord}_\infty(x) = -2 \quad \text{und} \quad \operatorname{ord}_\infty(y) = -n.$$

Außerdem gilt

$$\operatorname{div}(y) = [(\gamma_1, 0)] + \dots + [(\gamma_n, 0)] - n[\infty]$$

und für $\alpha \in \overline{K}$

$$\operatorname{div}(x - \alpha) = [(\alpha, \sqrt{f(\alpha)})] + [(\alpha, -\sqrt{f(\alpha)})] - 2[\infty].$$

Für $\alpha = \gamma_i$ kann man natürlich auch schreiben

$$\operatorname{div}(x - \gamma_i) = 2[(\gamma_i, 0)] - 2[\infty].$$

(6) *Für gerades n gilt*

$$\operatorname{ord}_{\infty_1}(x) = \operatorname{ord}_{\infty_2}(x) = -1 \quad \text{und} \quad \operatorname{ord}_{\infty_1}(y) = \operatorname{ord}_{\infty_2}(y) = -\frac{n}{2}.$$

Beweis:

(1) Da $C_0 \setminus \{(0 : 0 : 1)\}$ nichtsingulär ist, ist

$$C \setminus \pi^{-1}((0 : 0 : 1)) \xrightarrow{\pi} C_0 \setminus \{(0 : 0 : 1)\}$$

ein Isomorphismus. Wir können also $C \setminus \pi^{-1}((0 : 0 : 1))$ mit $C_0 \setminus \{(0 : 0 : 1)\}$ identifzieren. Der Morphismus

$$C_0 \setminus \{(0 : 0 : 1)\} \to \mathbb{P}^1, \quad (x, y) \mapsto (1 : x)$$

liefert einen Morphismus $\phi : C \to \mathbb{P}^1$ vom Grad 2. Im Unendlichen gilt

$$\phi^{-1}(\infty) = \pi^{-1}((0 : 0 : 1)).$$

(2) Sei $(\alpha, \beta) \in C$.

- **Fall $\beta \neq 0$:** Dann ist $x - \alpha$ uniformisierend in (α, β). Nun ist $\phi((\alpha, \beta)) = \alpha$. Im Bildpunkt ist $\widetilde{x} - \alpha$ uniformisierend, woraus wegen $\phi^*(\widetilde{x} - \alpha) = x - \alpha$ sofort

$$e_\phi((\alpha, \beta)) = 1$$

folgt.

- **Fall** $\beta = 0$**:** Dann ist $(\alpha, \beta) = (\gamma_i, 0)$ für ein i. Im Bild ist $\widetilde{x} - \gamma_i$ uniformisierend, in $(\gamma_i, 0)$ die Funktion y. Es ist $e_\phi((\gamma_i, 0)) = \operatorname{ord}_{(\gamma_i,0)}(\phi^*(\widetilde{x} - \gamma_i)) = \operatorname{ord}_{(\gamma_i,0)}(x - \gamma_i)$. Aus

$$y^2 = (x - \gamma_1) \dots (x - \gamma_i) \dots (x - \gamma_n)$$

sieht man dann

$$e_\phi((\gamma_i, 0)) = \operatorname{ord}_{(\gamma_i,0)}(x - \gamma_i) = 2.$$

(3) Da ϕ Grad 2 hat, gilt

$$\sum_{P \in \phi^{-1}(\infty)} e_\phi(P) = 2.$$

Wegen $e_\phi(P) \in \mathbb{N}$ gibt es also nur zwei Möglichkeiten.

- **Fall** $\#\phi^{-1}(\infty) = 2$**:** Wir schreiben $\phi^{-1}(\infty) = \{\infty_1, \infty_2\}$. Mit obiger Formel folgt

$$e_\phi(\infty_1) = 1 \quad \text{und} \quad e_\phi(\infty_2) = 1.$$

ϕ ist also unverzweigt in den Punkten ∞_1, ∞_2. Die Riemann-Hurwitz-Formel liefert

$$2g - 2 = 2 \cdot (-2) + \sum_{i=1}^{n} e_\phi((\gamma_i, 0)) - 1),$$

also $2g - 2 = -4 + n$, und damit

$$2g = n - 2.$$

Daher ist in diesem Fall n eine gerade Zahl und es gilt

$$g = \frac{n-2}{2} \quad \text{bzw.} \quad n = 2g + 2.$$

- **Fall** $\#\phi^{-1}(\infty) = 1$**:** Wir schreiben $\phi^{-1}(\infty) = \{\infty\}$. (Natürlich hat hier ∞ auf der linken Seite der Gleichung eine andere Bedeutung als auf der rechten Seite.) Dann gilt $e_\phi(\infty) = 2$. Die Riemann-Hurwitz-Formel liefert

$$2g - 2 = 2 \cdot (-2) + (e_\phi(\infty) - 1) + \sum_{i=1}^{n} (e_\phi((\gamma_i, 0)) - 1),$$

also $2g - 2 = -4 + 1 + n$, und damit

$$2g = n - 1.$$

In diesem Fall muss n eine ungerade Zahl sein, und es gilt

$$g = \frac{n-1}{2} \quad \text{bzw.} \quad n = 2g + 1.$$

(4) Wir betrachten den Fall, dass n ungerade ist, d.h. dass $\phi^{-1}(\infty) = \{\infty\}$ gilt. Die Nullstellen von y sind offensichtlich $(\gamma_i, 0)$. Da y in diesen Punkten uniformisierend ist, ist der Nullstellendivisor von y

$$[(\gamma_1, 0)] + \dots + [(\gamma_n, 0)].$$

Da $\operatorname{div}(y)$ Grad 0 hat und es nur einen Punkt im Unendlichen gibt, folgt

$$\operatorname{div}(y) = [(\gamma_1, 0)] + \dots + [(\gamma_n, 0)] - n[\infty].$$

Sei $\alpha \in \overline{K}$. Setzt man $x = \alpha$ in $y^2 = f(x)$ ein, so folgt $y^2 = f(\alpha)$. Nach eventueller Fallunterscheidung und Betrachtung der Uniformisierenden erhält man

$$\operatorname{div}(x - \alpha) = [(\alpha, \sqrt{f(\alpha)})] + [(a, -\sqrt{f(\alpha)}] - 2[\infty].$$

Auf die weiteren Details verzichten wir hier.

(5) Auf den Fall, dass n gerade ist, gehen wir an dieser Stelle nicht näher ein. ■

Im Folgenden werden wir uns auf den Fall beschränken, dass n ungerade ist. Dann gibt es im Unendlichen nur einen Punkt. Es gilt dann $n = 2g + 1$. Außerdem ist dann ∞ ein Verzweigungspunkt.

FOLGERUNG. *Sei C eine hyperelliptische Kurve vom Geschlecht 2, gegeben durch eine Gleichung $y^2 = f(x)$ mit einem Polynom $f(x)$ vom Grad 5. Dann gilt:*

$$\begin{aligned}
\mathcal{L}(0\cdot[\infty]) &= \overline{K},\\
\mathcal{L}(1\cdot[\infty]) &= \overline{K},\\
\mathcal{L}(2\cdot[\infty]) &= \overline{K}+\overline{K}\cdot x,\\
\mathcal{L}(3\cdot[\infty]) &= \overline{K}+\overline{K}\cdot x,\\
\mathcal{L}(4\cdot[\infty]) &= \overline{K}+\overline{K}\cdot x+\overline{K}\cdot x^2,\\
\mathcal{L}(5\cdot[\infty]) &= \overline{K}+\overline{K}\cdot x+\overline{K}\cdot x^2+\overline{K}\cdot y,\\
\mathcal{L}(6\cdot[\infty]) &= \overline{K}+\overline{K}\cdot x+\overline{K}\cdot x^2+\overline{K}\cdot y+\overline{K}\cdot x^3.
\end{aligned}$$

Beweis: Die Inklusionen $\supseteq$ folgen sofort aus

$$\operatorname{ord}_\infty(x) = -2, \quad \operatorname{ord}_\infty(x^2) = -4, \quad \operatorname{ord}_\infty(y) = -5, \quad \operatorname{ord}_\infty(x^3) = -6.$$

Nun gilt nach Riemann-Roch mit $K_C = 2[\infty]$ für $n \geq 3$

$$\ell(n\cdot[\infty] = n+1-2+\ell(2[\infty]-n[\infty]) = n-1+\ell((2-n)[\infty]) = n-1,$$

woraus dann für $n \geq 3$ die Gleichheiten folgen. ■

Ist C eine hyperelliptische Kurve, gegeben durch eine Gleichung $y^2 = f(x)$, so ist

$$\iota : C \to C, \quad (x,y) \mapsto (x,-y)$$

ein Automorphismus mit $\iota^2 = \mathrm{id}_C$. Der Automorphismus ι wird auch **hyperelliptische Involution** genannt. Für $P \in C$ gilt dann

$$\phi^{-1}(\phi(P)) = \{P, \iota(P)\} \quad \text{und} \quad \phi^*([\phi(P)]) = [P] + [\iota(P)].$$

Wir geben noch eine andere Charakterisierung hyperelliptischer Kurven.

SATZ. *Eine Kurve C vom Geschlecht $g \geq 2$ ist genau dann hyperelliptisch, wenn es einen Divisor D vom Grad 2 mit $\ell(D) = 2$ gibt.*

Beweis:

- Ist C hyperelliptisch und $\phi : C \to \mathbb{P}^1$ ein Morphismus vom Grad 2, so ist $D = \phi^*([\infty])$ ein Divisor vom Grad 2 und $1, x \in \mathcal{L}(D)$, also $\ell(D) \geq 2$. Schreibt man $D = [P_1] + [P_2]$, so gilt

  $$\overline{K} \subseteq \mathcal{L}([P_1] \subseteq \mathcal{L}([P_1]+[P_2]) = \mathcal{L}(D).$$

  Da C Geschlecht > 0 hat, gilt $\mathcal{L}([P_1]) = \overline{K}$. Da $\ell([P_1]+[P_2]) \leq \ell([P_1])+1$ gilt, folgt $\ell(D) = 2$.
- Ist D ein Divisor vom Grad 2 mit $\ell(D) = 2$, ist $\mathcal{L}(D) = \overline{K}\cdot f_0 + \overline{K}\cdot f_1$, so definiert

  $$\phi = (f_0 : f_1)$$

  einen Morphismus vom Grad 2. ■

FOLGERUNG. *Jede Kurve vom Geschlecht 2 ist hyperelliptisch.*

Beweis: Für jeden kanonischen Divisor K_C gilt $\operatorname{grad}(K_C) = 2\cdot 2 - 2 = 2$ und $\ell(K_C) = 2$. Der vorangegangene Satz liefert dann die Behauptung. ■

Beispiele: Hier sind Beispiele von hyperelliptischen Kurven, die über $\mathbb{F}_3$ durch eine Gleichung $y^2 = f(x)$ mit $\operatorname{grad}(f) = 5$ definiert sind.

$\#C(\mathbb{F}_3)$	$f(x)$	$C(\mathbb{F}_p)$
1	$x^5 + 2x + 2$	$\{\infty\}$
2	$x^5 + 2x^2 + 2$	$\{\infty, (2,0)\}$
3	$x^5 + x^2 + 2$	$\{\infty, (1,1), (1,2)\}$
4	$x^5 + 1$	$\{\infty, (0,1), (0,2), (2,0)\}$
5	$x^5 + 2x^2 + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2)\}$
6	$x^5 + x^2 + 1$	$\{\infty, (0,1), (0,2), (1,0), (2,1), (2,2)\}$
7	$x^5 + 2x + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2), (2,1), (2,2)\}$

2. Effektive kanonische Divisoren

SATZ. *Sei C eine hyperelliptische Kurve vom Geschlecht $g \geq 2$, gegeben durch eine Gleichung $y^2 = f(x)$ mit einem separablen Polynom $f(x) \in K[x]$ vom Grad $2g+1$.*

(1) *Die effektiven kanonischen Divisoren sind genau die Divisoren der Gestalt*

$$D = \sum_{i=1}^{r} ([(\alpha_i, \beta_i)] + [(\alpha_i, -\beta_i)]) + 2(g-1-r)[\infty]$$

mit Kurvenpunkten (α_i, β_i) und $r \leq g-1$.

(2) *Die effektiven kanonischen Divisoren sind genau die Divisoren der Gestalt*

$$\phi^*([P_1]) + \phi^*([P_2]) + \cdots + \phi^*([P_{g-1}]),$$

wo $P_1, \ldots, P_{g-1}$ beliebige Punkte in $\mathbb{P}^1$ sind.

(3) *Die effektiven kanonischen Divisoren sind genau die Divisoren der Gestalt*

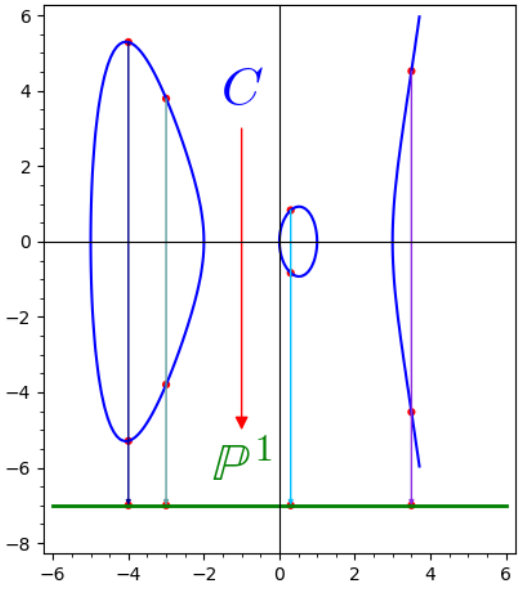
$$[P_1] + [\iota(P_1)] + [P_2] + [\iota(P_2)] + \cdots + [P_{g-1}] + [\iota(P_{g-1})],$$

wo $P_1, \ldots, P_{g-1}$ beliebige Punkte von C sind.

Beispiel: Bei einer hyperelliptischen Kurve vom Geschlecht 2 haben die effektiven kanonischen Divisoren also die Gestalt

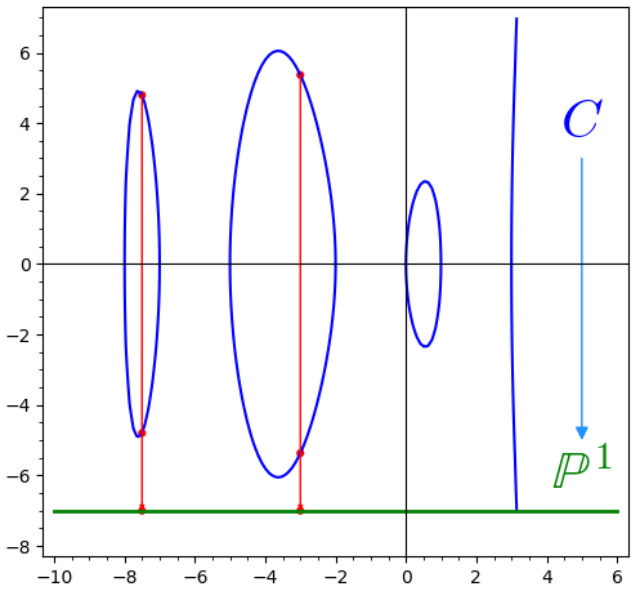
$$\phi^*([\widetilde{P}]) \text{ mit } \widetilde{P} \in \mathbb{P}^1 \quad \text{bzw.} \quad [P] + [\iota(P)] \text{ mit } P \in C.$$

Das Bild zeigt die Kurve $y^2 = \frac{1}{10}x(x-1)(x-3)(x+2)(x+5)$. Im Bild bilden je zwei „übereinanderliegende Punkte“ einen effektiven kanonischen Divisor.



Beispiel: $y^2 = \frac{1}{100}x(x-1)(x-3)(x+2)(x+5)(x+7)(x+8)$ definiert eine hyperelliptische Kurve vom Geschlecht 3. Die effektiven kanonischen Divisoren bestehen jeweils aus 4 Punkten der Form

$$[P_1] + [\iota(P_1)] + [P_2] + [\iota(P_3)] \text{ mit } P_1, P_2 \in C.$$



Beweis des Satzes:

(1) Ist $f(x) = c(x-\gamma_1)\dots(x-\gamma_{2g+1})$, so ist der Verzweigungsdivisor von ϕ

$$R = \sum_{i=1}^{2g+1} [(\gamma_i, 0)] + [\infty].$$

Wir wollen die Riemann-Hurwitz-Formel anwenden. Sei $\widetilde{x}$ die Koordinatenfunktion auf $\mathbb{P}^1$. Dann ist $x = \phi^*(\widetilde{x})$. Es ist

$$\operatorname{div}(d\widetilde{x}) = -2[\infty] \quad \text{und} \quad \phi^*(\operatorname{div}(d\widetilde{x})) = -4[\infty].$$

Es folgt

$$\begin{aligned} \operatorname{div}(dx) &= \operatorname{div}(\phi^*(d\widetilde{x})) = \phi^*(\operatorname{div}(d\widetilde{x})) + R = -4[\infty] + \sum_{i=1}^{2g+1} [(\gamma_i, 0)] + [\infty] = \\ &= \sum_{i=1}^{2g+1} [(\gamma_i, 0)] - 3[\infty]. \end{aligned}$$

(2) Der Divisor von y ist

$$\operatorname{div}(y) = \sum_{i=1}^{2g+1} [(\gamma_i, 0)] - (2g+1)[\infty].$$

Mit dem Divisor von dx ergibt sich

$$\operatorname{div}(\frac{dx}{y}) = 2(g-1)[\infty].$$

(3) Die Funktionen x^i mit $0 \le i \le g-1$ haben nur in ∞ eine Polstelle, und zwar gilt

$$\operatorname{ord}_\infty(x^i) = -2i \in \{0, -2, -4, \dots, -2(g-1)\}.$$

Es folgt

$$\operatorname{div}(x^i \cdot \frac{dx}{y}) \ge 0 \text{ für } i = 0, 1, \dots, g-1,$$

also

$$1, x, x^2, \ldots, x^{g-1} \in \mathcal{L}(\mathrm{div}(\frac{dx}{y})).$$

Wegen $\ell(K_C) = g$ folgt

$$\mathcal{L}(\mathrm{div}(\frac{dx}{y})) = \overline{K} \cdot 1 + \overline{K} \cdot x + \cdots + \overline{K} \cdot x^{g-1} = \{g(x) \in \overline{K}[x] : \mathrm{grad}(g(x)) \leq g-1\}.$$

Die Divisoren

$$\mathrm{div}(g(x)\frac{dx}{y}) \text{ mit } g(x) \in \{g(x) \in \overline{K}[x] : \mathrm{grad}(g(x)) \leq g-1\} \setminus \{0\}$$

sind dann genau die effektiven kanonischen Divisoren. Zerlegt man

$$g(x) = c(x-\alpha_1)\ldots(x-\alpha_r) \text{ mit } r \leq g-1,$$

so gilt wegen $\mathrm{div}(x-\alpha_i) = \phi^*([\alpha_i]) - 2[\infty]$

$$\begin{aligned} \mathrm{div}(g(x)\frac{dx}{y}) &= \sum_{i=1}^{r} \mathrm{div}(x-\alpha_i) + 2(g-1)[\infty] = \\ &= \sum_{i=1}^{r} (\phi^*([\alpha_i] - 2[\infty]) + 2(g-1)[\infty] = \\ &= \sum_{i=1}^{r} \phi^*([\alpha_i]) + 2(g-1-r)[\infty]. \end{aligned}$$

Mit $\phi^*([\alpha_i]) = [(\alpha_i, \beta_i)] + [(\alpha_i, -\beta_i)]$ ergibt sich die erste Darstellung. Die zweite folgt so:

$$\mathrm{div}(g(x)\frac{dx}{y}) = \sum_{i=1}^{r} \phi^*([\alpha_i]) + (g-1-r)\phi^*([\infty]).$$

Analog folgt die dritte Darstellung. Dies beweist die Behauptungen. ■

Mit diesem Hilfsmittel können wir folgenden Satz zeigen:

SATZ. *Eine nichtsinguläre projektive ebene Kurve C vom Geschlecht $g \geq 2$ ist nicht hyperelliptisch.*

Beweis: Sei $C \subseteq \mathbb{P}^2$ eine ebene Kurve vom Grad d. Wegen $g = \frac{1}{2}(d-1)(d-2)$ folgt $d \geq 4$. Sei K_C ein kanonischer Divisor von C und H der Divisor eines Geradenschnitts. Dann ist

$$K_C \sim (d-3)H$$

nach der Adjunktionsformel. Angenommen, C wäre hyperelliptisch mit hyperelliptischer Involution ι. Sei $P \in C$ mit $P \neq \iota(P)$. Sei $\ell = 0$ eine Gerade, die durch P, aber nicht durch $\iota(P)$ geht. Dann ist $\widetilde{K} = (d-3)\mathrm{div}(\ell)$ ein effektiver kanonischer Divisor, also

$$\widetilde{K} = (d-3)([P] + [P_2] + \cdots + [P_d]) = (d-3)[P] + (d-3)[P_2] + \cdots + (d-3)[P_d].$$

Da C nach Annahme hyperelliptisch ist, gibt es Punkte $P_2', \ldots, P_{g-1}'$ mit

$$\widetilde{K} = [P] + [\iota(P)] + [P_2'] + [\iota(P_2')] + \cdots + [P_{g-1}'] + [\iota(P_{g-1}')].$$

Da aber $\iota(P)$ kein Punkt der Geraden $\ell = 0$ ist, ist dies ein Widerspruch. ■

3. Reduzierte Divisoren - Beschreibung von $\mathrm{Pic}^0(C)$

Wir wollen die Divisorenklassengruppe $\mathrm{Pic}^0(C)$ für eine hyperelliptische Kurve C vom Geschlecht $g \geq 2$ mit genau einem Punkt ∞ im Unendlichen beschreiben. Früher haben wir für allgemeine Kurven C gezeigt, dass jeder Divisor vom Grad 0 zu einem Divisor der Gestalt

$$[P_1] + \cdots + [P_g] - g[\infty]$$

linear äquivalent ist. Eine wichtige Frage ist dann, wann zwei solcher Divisoren untereinander äquivalent sind.
Wird C gegeben durch

$$y^2 = c(x - \gamma_1) \dots (x - \gamma_{2g+1}),$$

so gilt für einen Punkt $P = (\alpha, \beta)$ mit der hyperelliptischen Involution ι

$$\mathrm{div}(x - \alpha) = [(\alpha, \beta)] + [(\alpha, -\beta)] - 2[\infty] = [P] + [\iota(P)] - 2[\infty].$$

Insbesondere gilt

$$[P] + [\iota(P)] \sim 2[\infty].$$

Es gilt auch $\mathcal{L}(2[\infty]) = \overline{K} \cdot 1 + \overline{K} \cdot x$, also $\ell(2[\infty]) = 2$.

LEMMA. *Ist C eine hyperelliptische Kurve vom Geschlecht $g \geq 2$ mit ∞ als einzigem Punkt im Unendlichen, sind $P_1, \dots, P_n \in C$ (nicht notwendig verschiedene) Punkte mit $n \leq g$, dann gilt:*

$$\ell([P_1] + \cdots + [P_n]) \geq 2 \quad \Longleftrightarrow \quad \text{es gibt Indizes } i \neq j \text{ mit } P_j = \iota(P_i).$$

Beweis:

$\Longleftarrow$ Gibt es Indizes $i \neq j$ mit $P_j = \iota(P_i)$, so ist

$$[P_i] + [\iota(P_i)] = [P_i] + [P_j] \leq [P_1] + \cdots + [P_n],$$

und mit $[P_i] + [\iota(P_i)] \sim 2[\infty]$ und $\ell(2[\infty]) = 2$ folgt

$$2 = \ell(2[\infty]) = \ell([P_i] + [\iota(P_i)]) = \ell([P_i] + [P_j]) \leq \ell([P_1] + \cdots + [P_n]),$$

was die eine Richtung der Behauptung beweist.

$\Longrightarrow$ **Fall $n = g$:** Wir betrachten zunächst den Fall $n = g$ und setzen voraus, dass $\ell([P_1]+\cdots+[P_g]) \geq 2$ gilt. Riemann-Roch liefert, wenn K_C einen kanonischen Divisor bezeichnet,

$$2 \leq \ell([P_1] + \cdots + [P_g]) = g + 1 - g + \ell(K_C - ([P_1] + \cdots + [P_g])),$$

also

$$\ell(K - ([P_1] + \cdots + [P_g])) \geq 1.$$

Für $f \in \mathcal{L}(K_C - ([P_1]+\cdots+[P_g])) \setminus \{0\}$ folgt $K_C - ([P_1]+\cdots+[P_g]) + \mathrm{div}(f) \geq 0$. Da K_C Grad $2g-2$ hat gibt es Punkte $Q_1, \dots, Q_{g-2}$ mit $K_C - ([P_1]+\cdots+[P_g]) + \mathrm{div}(f) = [Q_1]+\cdots+[Q_{g-2}]$, also

$$K_C + \mathrm{div}(f) = [P_1] + \cdots + [P_g] + [Q_1] + \cdots + [Q_{g-2}].$$

Da $K_C + \mathrm{div}(f)$ ein effektiver kanonischer Divisor ist, gibt es Punkte $R_1, \dots, R_{g-1}$ mit

$$[P_1] + \cdots + [P_g] + [Q_1] + \cdots + [Q_{g-2}] = [R_1] + [\iota(R_1)] + \cdots + [R_{g-1}] + [\iota(R_{g-1})].$$

Also muss es Indizes $i \neq j$ geben mit $P_j = \iota(P_i)$, was wir zeigen wollten.
Fall $n < g$: Sei nun $n < g$ und $\ell(P_1 + \cdots + P_n) \geq 2$. Wir wählen einen Punkt Q mit $Q \neq \iota(Q)$ und

$$Q \notin \{P_1, \dots, P_n, \iota(P_1), \dots, \iota(P_n)\}.$$

Dann gilt

$$\ell([P_1] + \cdots + [P_n] + (g - n)[Q]) \geq \ell([P_1] + \cdots + [P_n]) \geq 2.$$

Nach dem eben Gezeigten gibt es Indizes $i \neq j$ mit $P_j = \iota(P_i)$, was wir zeigen wollten. ∎

DEFINITION. *Sei C eine hyperelliptische Kurve vom Geschlecht $g \geq 2$ mit genau einem Punkt ∞ im Unendlichen. Ein Divisor D vom Grad 0 heißt* **reduziert**, *wenn er die Gestalt*

$$D = [P_1] + \cdots + [P_n] - n[\infty]$$

hat, wobei folgende Eigenschaften erfüllt sind:

- $0 \leq n \leq g$, $P_i \neq \infty$. *(Die Punkte P_i müssen nicht verschieden sein.)*
- *Für Indizes $i \neq j$ ist $P_j \neq \iota(P_i)$.*

Die entscheidene Bedeutung reduzierter Divisoren kommt in folgendem Satz zum Ausdruck:

SATZ. *Sei C eine hyperelliptische Kurve vom Geschlecht $g \geq 2$ mit genau einem Punkt ∞ im Unendlichen. Jeder Divisor D vom Grad 0 ist dann zu genau einem reduzierten Divisor linear äquivalent. (Die Menge der reduzierten Divisoren ist also ein Repräsentantensystem der Divisorenklassengruppe $\mathrm{Pic}^0(C)$.)*

Beweis:

(1) Sei D ein Divisor vom Grad 0. Nach Riemann-Roch gilt:

$$\ell(D + g[\infty]) = g + 1 - g + \ell(K_C - (D + g[\infty]) \geq 1.$$

Wählt man $f \in \mathcal{L}(D + g[\infty]) \setminus \{0\}$, so ist $D + g[\infty] + \mathrm{div}(f) \geq 0$, d.h. es gibt Punkte $P_1, \ldots, P_g$ mit $D + g[\infty] + \mathrm{div}(f) = [P_1] + \cdots + [P_g]$. Es folgt

$$D \sim ([P_1] + \cdots + [P_g]) - g[\infty].$$

Sind einige der P_i identisch mit ∞, so können wir die Darstellung zu

$$D \sim ([P_1] + \cdots + [P_n]) - n[\infty] \quad \text{mit} \quad 0 \leq n \leq g$$

verkürzen. Gibt es jetzt Indizes $i \neq j$ mit $\iota(P_i) = P_j$, so ist

$$[P_i] + [P_j] - 2[\infty] = [P_i] + [\iota(P_i)] - 2[\infty] \sim 0,$$

also können wir die Darstellung weiter verkürzen. Dies geht, bis wir eine Darstellung

$$D \sim [P_1] + \cdots + [P_n] - n[\infty] \quad \text{mit} \quad 0 \leq n \leq g \text{ und } P_j \neq \iota(P_i) \text{ für } i \neq j$$

erreicht haben. Hier ist $[P_1] + \cdots + [P_n] - n[\infty]$ ein reduzierter Divisor.

(2) Seien $[P_1] + \cdots + [P_n] - n[\infty]$ und $[Q_1] + \cdots + [Q_m] - m[\infty]$ zwei reduzierte Divisoren, die linear äquivalent sind, d.h.

$$[P_1] + \cdots + [P_n] - n[\infty] \sim [Q_1] + \cdots + [Q_m] - m[\infty].$$

Wir können o.E. $n \geq m$ voraussetzen und erhalten dann

$$[P_1] + \cdots + [P_n] \sim [Q_1] + \cdots + [Q_m] + (n - m)[\infty].$$

Also gibt es $f \in \overline{K}(C)^*$ mit

$$[P_1] + \cdots + [P_n] + \mathrm{div}(f) = [Q_1] + \cdots + [Q_m] + (n - m)[\infty].$$

Daher sind $1, f \in \mathcal{L}([P_1] + \cdots + [P_n])$. Mit dem vorangegangenen Lemma folgt aber aus der Reduziertheit die Eigenschaft $\ell(P_1 + \cdots + P_n) = 1$, d.h. f ist konstant, was sofort $m = n$ und $[P_1] + \cdots + [P_n] = [Q_1] + \cdots + [Q_m]$ impliziert. ■

Wir wollen reduzierte Divisoren noch konkreter beschreiben. Dazu denken wir uns C gegeben durch $y^2 = f(x)$, wo $f(x)$ ein separables Polynom vom Grad $2g + 1$ ist.

- Ist D ein reduzierter Divisor, so können wir schreiben

$$D = \sum_{i=1}^{n} [(\alpha_i, \beta_i)] - n[\infty]$$

mit $n \leq g$ und $(\alpha_j, \beta_j) \neq \iota((\alpha_i, \beta_i))$ für $i \neq j$.

- Fassen wir gleiche Punkte zusammen, so können wir schreiben

$$D = \sum_{i=1}^{r} n_i \cdot [(\alpha_i, \beta_i)] - (\sum_{i=1}^{r} n_i)[\infty]$$

mit $(\alpha_i, \beta_i) \neq (\alpha_j, \beta_j)$ für $i \neq j$. Ist $\beta_i \neq 0$, so darf $(\alpha_i, -\beta_i)$ nicht vorkommen, was einfach durch $\alpha_i \neq \alpha_j$ für $i \neq j$ ausgedrückt werden kann. Ist $\beta_i = 0$, so muss $n_i = 1$ gelten. Natürlich muss auch $n_i \geq 1$ und $\sum_{i=1}^{r} n_i \leq g$ gelten.

Wir fassen dies zusammen:

LEMMA. *Sei C eine hyperelliptische Kurve vom Geschlecht $g \geq 2$, gegeben durch $y^2 = f(x)$ mit einem Polynom $f(x)$ vom Grad $2g+1$. Ein Divisor D ist genau dann reduziert, wenn er sich in der Form*

$$D = \sum_{i=1}^{r} n_i \cdot [(\alpha_i, \beta_i)] - (\sum_{i=1}^{r} n_i)[\infty]$$

schreiben lässt mit

- $r \geq 0$,
- $(\alpha_i, \beta_i) \in C$,
- $\alpha_i \neq \alpha_j$ *für* $i \neq j$,
- $n_i \geq 1$ *und* $\sum_{i=1}^{r} n_i \leq g$,
- $n_i = 1$, *falls* $\beta_i = 0$.

Beispiel: Wie sehen die reduzierten Divisoren für eine hyperelliptische Kurve vom Geschlecht 2 (mit genau einem Punkt ∞ im Unendlichen) aus?

- 0 ist ein reduzierter Divisor.
- Jeder Kurvenpunkt (α, β) liefert einen reduzierten Divisor $D = [(\alpha, \beta)] - [\infty]$.
- Ist (α, β) ein Kurvenpunkt mit $\beta \neq 0$, so ist auch $D = 2[(\alpha, \beta)] - 2[\infty]$ ein reduzierter Divisor.
- Sind $(\alpha_1, \beta_1), (\alpha_2, \beta_2)$ zwei Kurvenpunkte mit $\alpha_1 \neq \alpha_2$, so ist $D = [(\alpha_1, \beta_1)] + [(\alpha_2, \beta_2)] - 2[\infty]$ ein reduzierter Divisor.

DEFINITION. *Ist $f(x) \in K[x]$ ein separables Polynom vom Grad $2g+1$ mit $g \geq 2$, ist C die durch $y^2 = f(x)$ definierte hyperelliptische Kurve, so sei*

$$\mathcal{R}(f, K)$$

die Menge der über K definierten reduzierten Divisoren und

$$\mathcal{R}(f, \overline{K})$$

die Menge aller reduzierten Divisoren von C.

Da jede Divisorenklasse genau einen reduzierten Divisor enthält, ist klar, dass sowohl

$$\mathcal{R}(f, \overline{K}) \to \mathrm{Pic}^0(C)$$

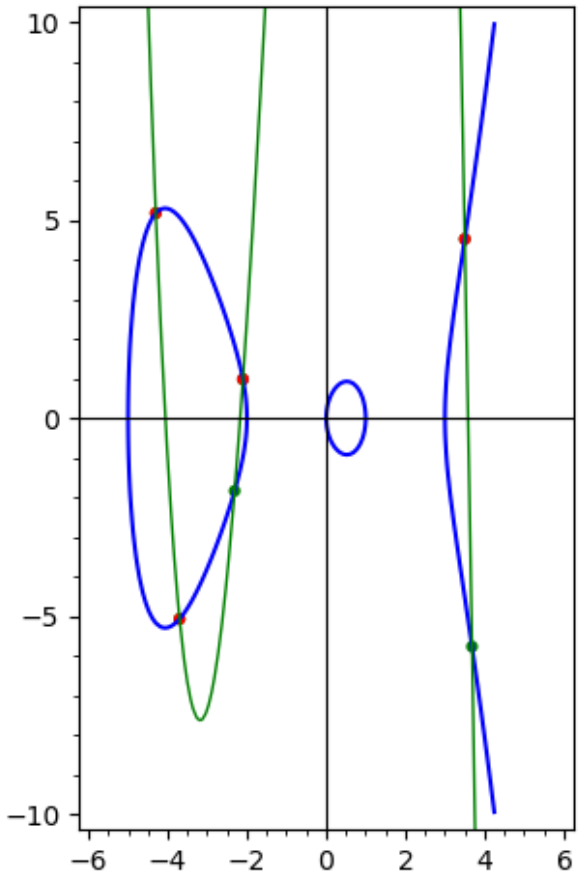
also auch

$$\mathcal{R}(f, K) \to \mathrm{Pic}^0_K(C)$$

ein Bijektionen sind.

Frage: Kann man die Addition in der Divisorenklassengruppe $\mathrm{Pic}^0(C)$ einer hyperelliptischen Kurve geometrisch deuten, ähnlich wie es bei ebenen Kubiken der Fall ist?

Überlegung: Sei C eine hyperelliptische Kurve vom Geschlecht 2, gegeben durch eine Gleichung $y^2 = f(x)$, wo $f(x)$ ein Polynom vom Grad 5 ist. Man sieht in diesem Zusammenhang manchmal Bilder folgender Art:



Seien $[P_1]+[P_2]-2[\infty]$ und $[Q_1]+[Q_2]-2[\infty]$ zwei Repräsentanten von Divisorenklassen. Wir schreiben

$$P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2), \quad Q_1 = (x_3, y_3), \quad Q_2 = (x_4, y_4).$$

Wir nehmen an, dass alle x_i verschieden sind. Dann gibt es ein kubisches Polynom $g(x)$ mit

$$g(x_1) = y_1, \quad g(x_2) = y_2, \quad g(x_3) = y_3, \quad g(x_4) = y_4.$$

Die Punkte P_1, P_2, Q_1, Q_2 sind also Nullstellen der Funktion

$$y - g(x) \in \mathcal{L}(6 \cdot [\infty]).$$

Hat $g(x)$ Grad 3, so gilt $\mathrm{ord}_\infty(y - g(x)) = -6$, also gibt es zwei Punkte R_1, R_2 mit

$$\mathrm{div}(y - g(x)) = [P_1] + [P_2] + [Q_1] + [Q_2] + [R_1] + [R_2] - 6[\infty].$$

In der obigen Skizze sind die Punkte P_1, P_2, Q_1, Q_2 rot gezeichnet, die neuen Punkte R_1, R_2 grün. Grün ist auch die kubische Funktion $x \mapsto g(x)$ gezeichnet.
In $\mathrm{Pic}^0(C)$ gilt dann

$$\overline{[P_1] + [P_2] - 2[\infty]} + \overline{[Q_1] + [Q_2] - 2[\infty]} + \overline{[R_1] + [R_2] - 2[\infty]} = 0.$$

Aus $[R_i] + [\iota(R_i)] \sim 2[\infty]$ folgt $-\overline{[R_i] - [\infty]} = \overline{[\iota(R_i)] - [\infty]}$, sodass wir erhalten

$$\overline{[P_1] + [P_2] - 2[\infty]} + \overline{[Q_1] + [Q_2] - 2[\infty]} = \overline{[\iota(R_1)] + [\iota(R_2)] - 2[\infty]}.$$

Ähnlich wie bei ebenen Kubiken im Fall von Geschlecht 1 haben wir also die Addition in $\mathrm{Pic}^0(C)$ geometrisch gedeutet.

Wir werden diese eben vorgestellten Überlegungen nicht weiterverfolgen, sondern einen Weg einschlagen, der von der Zahlentheorie inspiriert ist.

Ist der Grundkörper K nicht algebraisch abgeschlossen, so ist obige Beschreibung reduzierter Divisoren für das Rechnen nicht besonders geeignet. Es gibt aber einen Weg, der zunächst nicht sehr motiviert erscheint.

Die folgenden Abschnitte müssen noch überarbeitet werden.

4. Beschreibung von reduzierten Divisoren durch Polynome

Vorbemerkung: Die hyperelliptische Kurve C vom Geschlecht $g \geq 2$ sei gegeben durch eine Gleichung $y^2 = f(x)$ mit einem separablen Polynom $f(x)$ vom Grad $2g+1$. Dann hat die Kurve genau einen Punkt im Unendlichen. Die affine Kurve $y^2 = f(x)$ hat den Koordinatenring

$$R = K[x,y]/(y^2 - f(x)) \simeq K[x][\sqrt{f(x)}] = \{a + b\sqrt{f} : a, b \in K[x]\}.$$

Ein (endlicher) Kurvenpunkt $P = (\alpha, \beta)$ liefert ein maximales Ideal in R:

$$\mathfrak{m}_P = (x - \alpha, y - \beta) = (x - \alpha, \beta - \sqrt{f}).$$

(Die folgenden Aussagen werden hier nicht bewiesen.) Die von 0 verschiedenen Ideale von R lassen sich darstellen in der Form

$$\mathfrak{a} = A\left(K[x] \cdot a + K[x] \cdot (b - \sqrt{f})\right)$$

mit Polynomen $A, a, b \in K[x]$, wobei A und a normiert sind, $\operatorname{grad}(b) < \operatorname{grad}(a)$ und

$$a \mid f - b^2, \quad \text{d.h.} \quad f \equiv b^2 \bmod a$$

gilt. Unter diesen Bedingungen sind die Polynome A, a, b eindeutig bestimmt. Die Bedingung $a \mid f - b^2$ kommt daher, dass $\mathfrak{a}$ unter Multiplikation mit $\sqrt{f}$ abgeschlossen sein muss; es ist nämlich

$$\sqrt{f} \cdot \begin{pmatrix} a \\ b - \sqrt{f} \end{pmatrix} = \begin{pmatrix} b & a \\ \frac{b^2 - f}{a} & -b \end{pmatrix} \begin{pmatrix} a \\ b - \sqrt{f} \end{pmatrix}.$$

Man kann zeigen, dass die Divisorenklassengruppe von C isomorph zur Klassengruppe des Ringes R ist. Der Ring R ist ähnlich aufgebaut wie die Ringe $\mathbb{Z}[\sqrt{-d}]$ für quadratfreie $d \in \mathbb{N}$ mit $d \not\equiv 3 \bmod 4$. Wie man dort Klassengruppen berechnet, überträgt sich auf die Kurvensituation.

Wir definieren

$$\mathcal{P}(f, K) = \{(a, b) : a, b \in K[x], \operatorname{grad}(b) < \operatorname{grad}(a) \leq g, a \text{ normiert }, f \equiv b^2 \bmod a\}.$$

Überlegungen:

(1) Sei $(a, b) \in \mathcal{P}(f, \overline{K})$. Wir faktorisieren zunächst a:

$$a(x) = \prod_{i=1}^{r} (x - \alpha_i)^{n_i}$$

mit paarweise verschiedenen Zahlen $\alpha_1, \ldots, \alpha_r \in \overline{K}$ und $n_i \in \mathbb{N}$ mit $\sum_{i=1}^{r} n_i \leq g$.

(2) Aus $a \mid f - b^2$ folgt dann $(x - \alpha_i)^{n_i} \mid f - b^2$, also existiert ein Polynom c_i mit

$$(x - \alpha_i)^{n_i} c_i(x) = f(x) - b(x)^2.$$

Setzen wir $x = \alpha_i$ ein, so ergibt sich

$$f(\alpha_i) = b(\alpha_i)^2, \quad \text{d.h.} \quad (\alpha_i, b(\alpha_i)) \in C.$$

Ist $b(\alpha_i) = 0$, so gilt $x - \alpha_i \mid b(x)$, also $(x - \alpha_i)^2 \mid b(x)^2$. Da $f(x)$ separabel ist, muss $n_i = 1$ gelten.

(3) Daher ist

$$D = \sum_{i=1}^{r} n_i \cdot [(\alpha_i, b(\alpha_i))] - (\sum_{i=1}^{r} n_i)[\infty]$$

ein reduzierter Divisor.

(4) Damit haben wir eine Abbildung
$$\mathcal{P}(f, \overline{K}) \to \mathcal{R}(f, \overline{K})$$
definiert.

Wir werden jetzt herleiten, wie man umgekehrt einem reduzierten Divisor ein Element $(a, b) \in \mathcal{P}(f, \overline{K})$ zuordnen kann.

LEMMA. *Gegeben seien ein Körper K der Charakteristik $\neq 2$, ein Polynom $g(t) \in K[t]$ und eine Zahl $h_0 \in K \setminus \{0\}$ mit $g(0) = h_0^2$.*
Beginnend mit h_0 werden rekursiv werden Zahlen $h_1, h_2, h_3, \ldots$ wie folgt definiert: Kennt man für $n \geq 1$ bereits $h_0, h_1, \ldots, h_{n-1}$, ist c_n der Koeffizient des Polynoms $(\sum_{i=0}^{n-1} h_i t^i)^2 - g(t)$ bei t^n, d.h.
$$\left(\sum_{i=0}^{n-1} h_i t^i\right)^2 - g(t) = \cdots + c_n t^n + \ldots,$$
so definiert man
$$h_n = -\frac{c_n}{2h_0}.$$
Dann gilt:
$$\left(\sum_{i=0}^{n-1} h_i t^i\right)^2 \equiv g(t) \bmod t^n \text{ für alle } n \in \mathbb{N}.$$

Beweis: Wir beweisen die Aussage durch Induktion nach n. Für $n = 1$ folgt die Aussage einfach aus $h_0^2 = g(0)$. Sei nun $n \in \mathbb{N}$ und die Aussage bereits für n gezeigt, d.h.
$$\left(\sum_{i=0}^{n-1} h_i t^i\right)^2 \equiv g(t) \bmod t^n.$$
Dann gilt mit der im Lemma definieren Zahl c_n
$$\left(\sum_{i=0}^{n-1} h_i t^i\right)^2 - g(t) = c_n t^n + \text{ höhere Terme in } t.$$
Modulo t^{n+1} ergibt sich
$$\begin{aligned}
\left(\sum_{i=0}^{n} h_i t^i\right)^2 - g(t) &= \left(\sum_{i=0}^{n-1} h_i t^i + h_n t^n\right)^2 - g(t) = \\
&= \left(\sum_{i=0}^{n-1} h_i t^i\right)^2 + 2\left(\sum_{i=0}^{n-1} h_i t^i\right) \cdot h_n t^n + h_n^2 t^{2n} - g(t) = \\
&= \left(\sum_{i=0}^{n-1} h_i t^i\right)^2 - g(t) + \sum_{i=0}^{n-i} 2h_i h_n t^{i+n} + h_n^2 t^{2n} = \\
&= (c_n t^n + \ldots) + (2h_0 h_n t^n + \ldots) + \cdots = \\
&= (c_n + 2h_0 h_n) t^n + \cdots = 0 \cdot t^n + \cdots \equiv 0 \bmod t^{n+1}.
\end{aligned}$$
Dies beweist die Behauptung. ■

Eine zugehörige SAGE-Funktion könnte so aussehen:
```
def L(g,h0,n,K):
  R.<t>=K[]
  h=R(h0)
  for k in range(1,n):
    c=(h^2-g).coefficients(sparse=False)[k]
    h=h-c/(2*h0)*t^k
```

```
  return h
```

LEMMA. *Sei K ein Körper der Charakteristik $\neq 2$, $f(x) \in K[x]$, $x_0, y_0 \in K$ mit $y_0^2 = f(x_0)$, $y_0 \neq 0$ und $n \in \mathbb{N}$. Dann existiert ein Polynom $b(x) \in K[x]$ vom Grad $\leq n-1$ mit*

$$f(x) \equiv b(x)^2 \bmod (x-x_0)^n \quad \text{und} \quad b(x_0) = y_0.$$

Konkret: Wählt man im letzten Lemma $g(t) = f(x_0+t)$, $h_0 = y_0$, so erhält man ein Polynom $h(t) \in K[t]$ vom Grad $\leq n-1$ mit $h(t)^2 \equiv g(t) \bmod t^n$ und $h(0) = y_0$. Dann löst $b(x) = h(x-x_0)$ das Problem.

Beweis: Es gibt ein Polynom $\ell(t)$ mit

$$h(t)^2 = g(t) + t^n \cdot \ell(t).$$

Setzen wir nun $t = x - x_0$ ein, so ergibt sich

$$h(x-x_0)^2 = g(x-x_0) + (x-x_0)^n \ell(x-x_0).$$

Nun ist aber $g(x-x_0) = f(x)$, sodass sich

$$h(x-x_0)^2 = f(x) + (x-x_0)^n \cdot \ell(x-x_0)$$

ergibt. Mit $h(x_0-x_0) = h(0) = y_0$ folgt, dass $b(x) = h(x-x_0)$ das Problem löst. ■

```
def L0(g,h0,n,K):
  R.<t>=K[]
  h=R(h0)
  for k in range(1,n):
    c=(h^2-g).coefficients(sparse=False)[k]
    h=h-c/(2*h0)*t^k
  return h

def L(f,x0,y0,n,K):
  R.<x>=K[]
  S.<t>=K[]
  f=R(f)
  if y0^2!=f(x=x0):
    return 'Fehler: y0^2!=f(x0)!'
  g=f(x=x0+t)
  h=L0(g,y0,n,K)
  b=h(t=x-x0)
  return b
```

SATZ. *Sei K ein Körper der Charakteristik $\neq 2$, $f(x) \in K[x]$, Punkte (x_i, y_i) für $i = 1, \ldots, r$ mit paarweise verschiedenen Zahlen x_i und $y_i^2 = f(x_i)$, Zahlen $n_1, \ldots, n_r \in \mathbb{N}$, sodass $n_i = 1$ im Fall $y_i = 0$ gilt. Man definiere*

$$a(x) = (x-x_1)^{n_1} \ldots (x-x_r)^{n_r}.$$

Dann gibt es genau ein Polynom $b(x) \in K[x]$ mit $\operatorname{grad}(b) < \operatorname{grad}(a)$, sodass gilt

$$f(x) \equiv b(x)^2 \bmod a(x) \quad \text{und} \quad b(x_i) = y_i \text{ für } i = 1, \ldots, r.$$

Beweis: Mit dem vorangegangenen Lemma finden wir im Fall $y_i \neq 0$ Polynome $b_i(x)$ mit

$$f(x) \equiv b_i(x)^2 \bmod (x-x_i)^{n_i}, \quad \operatorname{grad}(b_i(x)) < n_i \quad \text{und} \quad b_i(x_i) = y_i.$$

Im Fall $y_i = 0$ wählen wir einfach $b_i(x) = 0$, sodass auch in diesem Fall die letzte Aussage gilt. Mit dem chinesischen Restsatz finden wir ein Polynom $b(x)$ mit

$$b(x) \equiv \begin{cases} b_1(x) \bmod (x - x_1)^{n_1}, \\ b_2(x) \bmod (x - x_2)^{n_2}, \\ \vdots \\ b_r(x) \bmod (x - x_r)^{n_r}. \end{cases}$$

Dabei können wir $\operatorname{grad}(b(x)) < n_1 + \cdots + n_r = \operatorname{grad}(a(x))$ annehmen. Auch $b(x_i) = y_i$ ist klar.
Warum ist $b(x)$ durch diese Bedingungen eindeutig bestimmt?

- Sei $\widetilde{b}(x)$ ein weiteres Polynom mit diesen Eigenschaften. Dann folgt
$$\widetilde{b}(x)^2 \equiv f(x) \equiv b(x)^2 \bmod (x - x_i)^{n_i},$$
also
$$(x - x_i)^{n_i} \mid (\widetilde{b}(x) - b(x)) \cdot (\widetilde{b}(x) + b(x)).$$
Im Fall $y_i \neq 0$ ist $\widetilde{b}(x_i) + b(x_i) = 2y_i \neq 0$, also gilt $x - x_i \nmid \widetilde{b}(x) + b(x)$. Daher folgt
$$(x - x_i)^{n_i} \mid \widetilde{b}(x) - b(x),$$
also
$$\widetilde{b}(x) \equiv b(x) \bmod (x - x_i)^{n_i}.$$
Im Fall $y_i = 0$ ist $\widetilde{b}(x_i) = b(x_i) = 0$, sodass natürlich auch hier
$$\widetilde{b}(x) \equiv b(x) \bmod (x - x_i),$$
und wegen $n_i = 1$ dann auch
$$\widetilde{b}(x) \equiv b(x) \bmod (x - x_i)^{n_i}$$
gilt.
- Es folgt $a(x) \mid \widetilde{b}(x) - b(x)$. Aus der Gradbedingung folgt dann $\widetilde{b}(x) = b(x)$. ■

FOLGERUNG. *Sei $f(x) \in K[x]$ ein separables Polynom vom Grad $2g + 1$ und C die durch $y^2 = f(x)$ definierte hyperelliptische Kurve vom Geschlecht g. Dann ist*

$$\mathcal{P}(f, \overline{K}) \to \mathcal{R}(f, \overline{K})$$

mit

$$(a(x), b(x)) \mapsto \sum_{i=1}^{r} n_i \cdot [(\alpha_i, b(\alpha_i)] - (\sum_{i=1}^{r} n_i)[\infty] \text{ mit } a(x) = \prod_{i=1}^{r} (x - \alpha_i)^{n_i}$$

bijektiv. Schränkt man sich auf Divisoren, die über K definiert sind, ein, so erhält man eine Bijektion

$$\mathcal{P}(f, K) \simeq \mathcal{R}(f, K).$$

Wir erhalten damit eine Bijektion

$$\operatorname{Pic}_K^0(C) \simeq \mathcal{P}(f, K).$$

Im Folgenden werden wir die Elemente aus $\operatorname{Pic}_K^0(C)$ durch Polynompaare $(a(x), b(x)) \in \mathcal{P}(f, K)$ angeben. Diese Darstellung wird auch als **Mumford representation** bezeichnet.

Beispiele:

- Die Klasse $0 \in \operatorname{Pic}^0(C)$ wird durch $(1, 0)$ repräsentiert.
- Ist $(\alpha, \beta) \in C$, so wird die zugehörige Klasse $\overline{[(\alpha, \beta)] - [\infty]}$ durch das Paar $(x - \alpha, \beta)$ repräsentiert:
$$(\alpha, \beta) \longrightarrow \overline{[(\alpha, \beta)] - [\infty]} \simeq (x - \alpha, \beta).$$

Beispiele: Wir betrachten hyperelliptische Kurven über $\mathbb{F}_3$ vom Geschlecht 2 mit genau einem Punkt im Unendlichen:

$\#C(\mathbb{F}_3)$	$\#\mathrm{Pic}^0_{\mathbb{F}_3}(C)$	f, $C(\mathbb{F}_3)$, $\mathrm{Pic}^0_{\mathbb{F}_3}(C)$
1	5	$f = x^5 + 2\,x + 2$ $C(\mathbb{F}_3) = \{\infty\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0)\,,\,(x^2+1,x)\,,\,(x^2+1,2x)\,,\,(x^2+x+2,x+1)\,,\,(x^2+x+2,2x+2)\}$
2	8	$f = x^5 + 2\,x^2 + 2$ $C(\mathbb{F}_3) = \{\infty,(2,0)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0)\,,\,(x+1,0)\,,\,(x^2+2x+2,x)\,,\,(x^2+2x+2,2x)\,,\,(x^2+x+2,1),$ $(x^2+1,2x+1)\,,\,(x^2+x+2,2)\,,\,(x^2+1,x+2)\}$
3	6	$f = x^5 + x^2 + 2$ $C(\mathbb{F}_3) = \{\infty,(1,1)\,,(1,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0)\,,(x+2,1)\,,(x+2,2)\,,(x^2+2x+2,0)\,,(x^2+x+1,x+1)\,,$ $(x^2+x+1,2x+2)\}$
4	10	$f = x^5 + 1$ $C(\mathbb{F}_3) = \{\infty,(0,1)\,,(0,2)\,,(2,0)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0)\,,(x,1)\,,(x,2)\,,(x+1,0)\,,(x^2+x+2,x)\,,(x^2+x+2,2x)\,,(x^2,1)\,,$ $(x^2+x,x+1)\,,(x^2,2)\,,(x^2+x,2x+2)\}$
5	14	$f = x^5 + 2\,x^2 + 1$ $C(\mathbb{F}_3) = \{\infty,(0,1)\,,(0,2)\,,(1,1)\,,(1,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0)\,,(x,1)\,,(x,2)\,,(x+2,1)\,,(x+2,2)\,,(x^2+x+2,0)\,,(x^2,1)\,,(x^2+2x,1),$ $(x^2+x+1,1)\,,(x^2+2x,x+1)\,,(x^2,2)\,,(x^2+2x,2)\,,(x^2+x+1,2),$ $(x^2+2x,2x+2)\}$
6	24	$f = x^5 + x^2 + 1$ $C(\mathbb{F}_3) = \{\infty,(0,1)\,,(0,2)\,,(1,0)\,,(2,1)\,,(2,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0)\,,(x,1)\,,(x,2)\,,(x+2,0)\,,(x+1,1)\,,(x+1,2)\,,(x^2,1)\,,(x^2+x,1),$ $(x^2+2x+1,1)\,,(x^2+x+2,x+1)\,,(x^2+2x+2,x+1)\,,(x^2+x,2x+1),$ $(x^2+2x,2x+1)\,,(x^2+1,2x+1)\,,(x^2+2,2x+1)\,,(x^2,2)\,,(x^2+x,2),$ $(x^2+2x+1,2)\,,(x^2+x,x+2)\,,(x^2+2x,x+2)\,,(x^2+1,x+2),$ $(x^2+2,x+2)\,,(x^2+x+2,2x+2)\,,(x^2+2x+2,2x+2)\}$
7	29	$f = x^5 + 2\,x + 1$ $C(\mathbb{F}_3) = \{\infty,(0,1)\,,(0,2)\,,(1,1)\,,(1,2)\,,(2,1)\,,(2,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0)\,,(x,1)\,,(x,2)\,,(x+2,1)\,,(x+2,2)\,,(x+1,1)\,,(x+1,2)\,,(x^2+2x+1,x),$ $(x^2+2,x)\,,(x^2+2x+2,x)\,,(x^2+2x+1,2x)\,,(x^2+2,2x)\,,(x^2+2x+2,2x),$ $(x^2+x,1)\,,(x^2+2x,1)\,,(x^2+1,1)\,,(x^2+2,1)\,,(x^2,x+1)\,,(x^2+2x,x+1),$ $(x^2+x+1,x+1)\,,(x^2+x,2x+1)\,,(x^2+x,2)\,,(x^2+2x,2)\,,(x^2+1,2),$ $(x^2+2,2)\,,(x^2+x,x+2)\,,(x^2,2x+2)\,,(x^2+2x,2x+2)\,,(x^2+x+1,2x+2)\}$

Beispiele: Nun betrachten wir hyperelliptische Kurven über $\mathbb{F}_3$ vom Geschlecht 2 mit $C(\mathbb{F}_3) = 3$. Die Beispiele zeigen verschiedene Möglichkeiten für $\mathrm{Pic}^0_{\mathbb{F}_3}(C)$.

$\#C(\mathbb{F}_3)$	$\#\mathrm{Pic}^0_{\mathbb{F}_3}(C)$	f, $C(\mathbb{F}_3)$, $\mathrm{Pic}^0_{\mathbb{F}_3}(C)$
3	4	$f = x^5 + x^3 + x^2 + 2x$ $C(\mathbb{F}_3) = \{\infty, (0,0), (2,0)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0), (x,0), (x+1,0), (x^2+x, 0)\}$
3	5	$f = x^5 + x^2 + x + 2$ $C(\mathbb{F}_3) = \{\infty, (2,1), (2,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0), (x+1,1), (x+1,2), (x^2+2x+1, x), (x^2+2x+1, 2x)\}$
3	6	$f = x^5 + x^2 + 2$ $C(\mathbb{F}_3) = \{\infty, (1,1), (1,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0), (x+2,1), (x+2,2), (x^2+2x+2, 0), (x^2+x+1, x+1), (x^2+x+1, 2x+2)\}$
3	7	$f = x^5 + x^3 + x^2 + 2x + 2$ $C(\mathbb{F}_3) = \{\infty, (1,1), (1,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0), (x+2,1), (x+2,2), (x^2+2x+2, x), (x^2+2x+2, 2x), (x^2+x+1, 1),$ $(x^2+x+1, 2)\}$
3	8	$f = x^5 + x^2 + x$ $C(\mathbb{F}_3) = \{\infty, (0,0), (1,0)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0), (x,0), (x+2,0), (x^2+2x, 0), (x^2+x+2, x), (x^2+2x+2, x),$ $(x^2+x+2, 2x), (x^2+2x+2, 2x)\}$
3	9	$f = x^5 + x^3 + x^2 + 2$ $C(\mathbb{F}_3) = \{\infty, (2,1), (2,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0), (x+1,1), (x+1,2), (x^2+1, 1), (x^2+2x+1, 1), (x^2+x+2, 2x+1),$ $(x^2+1, 2), (x^2+2x+1, 2), (x^2+x+2, x+2)\}$
3	10	$f = x^5 + x^2 + 2x + 1$ $C(\mathbb{F}_3) = \{\infty, (0,1), (0,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0), (x,1), (x,2), (x^2+1, 0), (x^2, x+1), (x^2+x+2, 2x+1),$ $(x^2+2x+2, 2x+1), (x^2+x+2, x+2), (x^2+2x+2, x+2), (x^2, 2x+2)\}$
3	11	$f = x^5 + 2x^3 + x^2 + x + 2$ $C(\mathbb{F}_3) = \{\infty, (1,1), (1,2)\}$ $\mathrm{Pic}^0_{\mathbb{F}_3}(C) = \{(1,0), (x+2,1), (x+2,2), (x^2+x+1, x), (x^2+x+1, 2x), (x^2+1, 1),$ $(x^2+x+2, 1), (x^2+2x+2, 2x+1), (x^2+1, 2), (x^2+x+2, 2), (x^2+2x+2, x+2)\}$

5. Addition in $\mathrm{Pic}^0_K(C)$

Wir identifizieren

$$\mathrm{Pic}^0_K(C) \simeq \{(a,b) \in K[x] \times K[x] : \mathrm{grad}(b) < \mathrm{grad}(a) \leq g, a \text{ normiert}, a \mid f - b^2\}.$$

Der folgende Algorithmus ist findet sich in [**Cohen-Frey**, S.308, Algorithm 14.7]. Er wird dort auch als **Algorithmus von Cantor** bezeichnet. (Wir werden die Richtigkeit des Algorithmus hier nicht beweisen.)

Eingabe: K, $f(x) \in K[x]$ separabel vom Grad $2g+1$
Eingabe: $(a_1, b_1), (a_2, b_2) \in \mathcal{P}(f, K)$
Ausgabe: $(a, b) \in \mathcal{P}(f, K)$ mit $(a, b) = (a_1, b_1) + (a_2, b_2)$ in $\mathrm{Pic}^0_K(C)$

1: $d_1 \leftarrow \mathrm{ggT}(a_1, a_2)$ und e_1, e_2 mit $d_1 = e_1 a_1 + e_2 a_2$
2: $d \leftarrow \mathrm{ggT}(d_1, b_1 + b_2)$ und c_1, c_2 mit $d = c_1 d_1 + c_2 (b_1 + b_2)$
3: $s_1 \leftarrow c_1 e_1$, $s_2 \leftarrow c_1 e_2$, $s_3 \leftarrow c_2$
4: $a \leftarrow \frac{a_1 a_2}{d^2}$, $b \leftarrow \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3 (b_1 b_2 + f)}{d} \bmod a$
5: **while** $\mathrm{grad}(b) > g$ **do**
6: $\quad a \leftarrow \frac{f - b^2}{a}$
7: $\quad b \leftarrow (-b) \bmod a$
8: **end while**
9: Dividiere a durch den höchsten Koeffizienten, sodass a dann normiert ist
10: **return** (a, b)

Eine zugehörige SAGE-Funktion könnte so aussehen:

```
def hek_add(ab1,ab2,f,K):
  R.<x>=K[]
  f=R(f)
  g=(f.degree()-1)/2
  a1,b1=ab1
  a2,b2=ab2
  a1,b1,a2,b2=R(a1),R(b1),R(a2),R(b2)
  d1,e1,e2=a1.xgcd(a2)
  d,c1,c2=d1.xgcd(b1+b2)
  s1,s2,s3=c1*e1,c1*e2,c2
  a,_=(a1*a2).quo_rem(d^2)
  b,_=(s1*a1*b2+s2*a2*b1+s3*(b1*b2+f)).quo_rem(d)
  b=b%a
  while a.degree()>g:
    a,_=(f-b^2).quo_rem(a)
    b=(-b)%a
  if a.leading_coefficient()!=1:
    a=a/a.leading_coefficient()
  return (a,b)
```

Um in $\mathrm{Pic}_K^0(C)$ das n-fache von $\mathfrak{a}$ zu berechnen, benutzen wir eine „square-and-multiply“-Methode:
Eingabe: K, $f(x) \in K[x]$ separabel vom Grad $2g+1$
Eingabe: $\mathfrak{a} \in \mathrm{Pic}_K^0(C)$, $n \in \mathbb{N}_0$
Ausgabe: $n \cdot \mathfrak{a} \in \mathrm{Pic}_K^0(C)$

1: $\mathfrak{b} = (1,0)$, $\mathfrak{c} = \mathfrak{a}$
2: **while** $n > 0$ **do**
3: **if** $n \bmod 2 = 0$ **then**
4: $\mathfrak{c} \leftarrow \mathfrak{c} + \mathfrak{c}$, $n \leftarrow \left\lfloor \frac{n}{2} \right\rfloor$
5: **else**
6: $\mathfrak{b} \leftarrow \mathfrak{b} + \mathfrak{c}$, $n \leftarrow n - 1$
7: **end if**
8: **end while**
9: **return** $\mathfrak{b}$

Beispiel: Über $\mathbb{Q}$ betrachten wir die durch

$$f = -4\,x^5 + 8\,x^3 + 8\,x^2 + 4\,x + 1$$

definierte hyperelliptische Kurve C vom Geschlecht 2. In $C(\mathbb{Q})$ gibt es den Punkt $(0,1)$, der in $\mathrm{Pic}^0(C)$ durch $\mathfrak{a} = (x,1)$ dargestellt wird. Wir berechnen die Vielfachen:

n	$n \cdot \mathfrak{a}$
1	$(x, 1)$
2	$\left(x^2, 2x+1\right)$
3	$\left(x^2+x, -1\right)$
4	$(x+1, -1)$
5	$\left(x^2+x, 2x+1\right)$
6	$\left(x^2-x-1, -2x-1\right)$
7	$\left(x^2+2x+1, -4x-3\right)$
8	$\left(x^2+2x+1, 4x+3\right)$
9	$\left(x^2-x-1, 2x+1\right)$
10	$\left(x^2+x, -2x-1\right)$
11	$(x+1, 1)$
12	$\left(x^2+x, 1\right)$
13	$\left(x^2, -2x-1\right)$
14	$(x, -1)$
15	$(1, 0)$

Also hat $\mathfrak{a}$ Ordnung 15 in der Divisorenklassengruppe.

6. Anwendungen in der Kryptographie

Heutzutage werden elliptische Kurven über endlichen Körpern kryptographisch eingesetzt. Offizielle staatliche Informationen dazu gibt es beispielsweise in Deutschland beim BSI (Bundesamt für Sicherheit in der Informationstechnik) BSI TR-03111: Elliptic Curve Cryptography und in den USA beim NIST (National Institute of Standards and Technology) NIST: Elliptic Curve Cryptography.

Wir stellen hier ein **Schlüsseleinigungsverfahren** vor, das Diffie und Hellman in ihrer Arbeit „New Directions in Cryptography“ 1976 vorgeschlagen haben [**Diffie-Hellman**]. Aktuelle Informationen zum Thema „Schlüsseleinigungsverfahren“ findet man wieder beim Bundesamt für Sicherheit in der Informationstechnik BSI TR-02102-1.

Situation: Zwei Personen A und B (oder zwei durch das Internet verbundene Rechner oder ...) wollen sich auf einen gemeinsamen Schlüssel einigen um dann damit ein Verschlüsselungsverfahren mit dem gleichen Schlüssel benutzen zu können.

Diffie-Hellman-Schlüsselaustausch (multiplikative Version)

- Sei G eine multiplikativ geschriebene Gruppe (oder Halbgruppe), in der sich zwei Elemente schnell multiplizieren lassen. (Dann lassen sich auch Potenzen a^n für $a \in G$ und $n \in \mathbb{N}$ mit einer „square-and-multiply“-Methode schnell berechnen.)
- Sei weiter $g \in G$.
- A wählt sich eine Zahl $e_A \in \mathbb{N}$ und berechnet
$$f_A = g^{e_A} \in G.$$
A gibt f_A als seinen öffentlichen Schlüssel (public key) bekannt. e_A ist der geheime Schlüssel (private key oder secret key) von A.
- B wählt sich eine Zahl $e_B \in \mathbb{N}$ und berechnet
$$f_B = g^{e_A} \in G.$$
B gibt f_B als seinen öffentlichen Schlüssel bekannt. e_B ist der geheime Schlüssel von B.
- Der gemeinsame Schlüssel von A und B ist
$$k_{AB} = g^{e_A e_B}.$$
A kann sich diesen gemeinsamen Schlüssel wegen $k_{AB} = g^{e_A e_B} = (g^{e_B})^{e_A} = f_B^{e_A}$ als
$$k_{AB} = f_B^{e_A}$$

berechnen, da A den öffentlichen Schlüssel f_B und seinen eigenen geheimen Schlüssel e_A kennt. Analog kann sich B den gemeinsamen Schlüssels mittels der Gleichung

$$k_{AB} = f_A^{e_B}$$

berechnen.

- Wann ist dieses Schlüsselaustauschverfahren sicher? Ein Außenstehender C kennt g, f_A, f_B bzw. g, g^{e_A}, g^{e_B}. Wie kann man aus diesen drei Größen $g^{e_A e_B}$ berechnen?

$$g, g^{e_A}, g^{e_B} \xrightarrow{\text{Wie erhält aus den Größen links, die Größe rechts?}} g^{e_A e_B}$$

  Dies nennt man das Diffie-Hellman-Problem.
- Wenn C einen **diskreten Logarithmus** von f_A zur Basis g in G berechnen kann, d.h. eine Zahl $\ell \in \mathbb{N}$ mit

$$g^\ell = f_A,$$

  so erhält C leicht den gemeinsamen Schlüssel:

$$k_{AB} = f_A^{e_B} = g^{\ell e_B} = f_B^\ell.$$

- Für die Sicherheit ist es daher ganz wichtig, dass sich diskrete Logarithmen in der Gruppe G (im Allgemeinen) praktisch nicht berechnen lassen.

Der (klassische) Diffie-Hellman-Schlüsselaustausch arbeitet mit der multiplikativen Gruppe $\mathbb{F}_p^*$ eines endlichen Körpers $\mathbb{F}_p$.

Beispiel: Als Gruppe wird $\mathbb{F}_p^*$ mit nachfolgender 256-Bit-Primzahl p. Öffentlich bekannt seien folgende Zahlen:

$$\begin{aligned}
p &= 115792089237316195423570985008687907853269984665640564039457584007913129603823,\\
g &= 5,\\
f_A &= 64962785370846188965139123186170717661240903020815441595800807346182307706906,\\
f_B &= 45104316737573767517415679239486371089462170346686659863014273814977828980340.
\end{aligned}$$

Man versuche, daraus den gemeinsamen Schlüssel $k_{AB} = g^{e_A e_B} \in \mathbb{F}_p^*$ zu berechnen.

Da die Verknüpfung auf elliptischen Kurven und in der Divisorenklassengruppe von hyperelliptischen Kurven additiv geschrieben wird, schreiben wir den Diffie-Hellman-Schlüsselaustausch auch noch additiv auf:

Diffie-Hellman-Schlüsselaustausch (additive Version)

- Sei G eine additiv geschriebene Gruppe (oder Halbgruppe), in der sich zwei Elemente schnell addieren lassen. (Dann lässt sich auch für $a \in G$ und $n \in \mathbb{N}$ das Produkt $n \cdot a$ mit einer „square-and-multiply“-Methode schnell berechnen.)
- Sei weiter $g \in G$.
- A wählt sich eine Zahl $e_A \in \mathbb{N}$ und berechnet

$$f_A = e_A \cdot g \in G.$$

  A gibt f_A als seinen öffentlichen Schlüssel bekannt. e_A ist der geheime Schlüssel von A.
- B wählt sich eine Zahl $e_B \in \mathbb{N}$ und berechnet

$$f_B = e_B \cdot g \in G.$$

  B gibt f_B als seinen öffentlichen Schlüssel bekannt. e_B ist der geheime Schlüssel von B.
- Der gemeinsame Schlüssel von A und B ist

$$k_{AB} = e_A e_B \cdot g,$$

  den sich A mittels der Gleichung

$$k_{AB} = e_A \cdot f_B$$

und B mittels der Gleichung

$$k_{AB} = e_B \cdot f_A$$

berechnen können.

- Das Diffie-Hellman-Problem schreibt sich additiv so:

$$g, \quad e_A \cdot g, \quad e_B \cdot g \xrightarrow{\text{Wie erhält man aus den Größen links die rechte Seite?}} e_A e_B \cdot g.$$

Der Diffie-Hellman-Schlüsselaustausch ist sicher, solange sich das Diffie-Hellman-Problem praktisch nicht lösen lässt.

- Kann ein Außenstehender C in G einen **diskreten Logarithmus** von f_A zur Basis g berechnen, d.h. ein $\ell \in \mathbb{N}$ mit

$$f_A = \ell \cdot g,$$

so kann sich C auch den gemeinsamen Schlüssel so berechnen:

$$k_{AB} = e_A e_B \cdot g = e_B \cdot (e_A \cdot g) = e_B \cdot f_A = e_B \cdot (\ell \cdot g) = \ell \cdot (e_B \cdot g) = \ell \cdot f_B.$$

(In Analogie zur multiplikativen Version spricht man auch hier von diskreten Logarithmen.)

- Die Gruppe G muss also so beschaffen sein, dass sich diskrete Logarithmen praktisch nicht berechnen lassen.

Beispiel: Wir starten mit der 128-Bit-Primzahl

$$p = 2^{128} - 2487 = 340282366920938463463374607431768208969$$

und der durch

$$y^2 = x^5 + 13x$$

über $\mathbb{F}_p$ definierten hyperelliptischen Kurve vom Geschlecht 2. Die Kurve enthält den Punkt

$$(-13, 285852928819727726285868778105170894 33),$$

der in Pic^0 durch das Polynompaar

$$g = (x + 13, 285852928819727726285868778105170894 33)$$

repräsentiert wird. Da die Anzahl der $\mathbb{F}_p$-rationalen Punkte in der Größenordnung von $p^2 \approx 2^{256}$ (mit 78 Dezimalstellen) ist, wählen sich A und B unabhängig voneinander geheim zufällige 78-stellige Zahlen:

$$\begin{aligned} e_A &= 580319470382655966752835662324659168309974697178860516645533695751153002193277, \\ e_B &= 239109625614480018658086848783454775487453455922591154544399323497106959176065 \end{aligned}$$

berechnen damit ihre öffentlichen Schlüssel $f_A = e_A \cdot g$ bzw. $f_B = e_B \cdot g$ (in Pic^0)

$$\begin{aligned} f_A &= (x^2 + 187463483300877865555744358426021948548x + 173980684735284072477484642855119428093, \\ &\quad 312665874328081155780823073521258635811x + 109239510534601665073609894657722958853, \\ f_B &= (x^2 + 315410667712437507494356901716774216242x + 174070099365157486861119806563952150122, \\ &\quad 273079014832786731550022518067456128940x + 293097856848975605637487900771010101861) \end{aligned}$$

und geben diese öffentlich bekannt. Der gemeinsame Schlüssel von A und B ist dann

$$\begin{aligned} k_{AB} &= (x^2 + 164581974200092893758430516115421764363x + 156551275646432782596354239240206183 53, \\ &\quad 242847628149725977241194695079710562435x + 228888472326255063036427011105138660978), \end{aligned}$$

wobei sich A und B den gemeinsamen Schlüssel über eine der Gleichungen

$$k_{AB} = e_A \cdot f_B = e_B \cdot f_B$$

berechnet haben. Will man eine einzige Zahl als Schlüssel haben, könnte man beispielsweise die Koeffizienten bei x und 1 der ersten Komponente von k_{AB} aneinanderhängen:

$$164581974200092893758430516115421764363156551275646432782596354239240206183 53.$$