KAPITEL 5

Funktionen, Divisoren und der Satz von Riemann-Roch auf $\mathbb{P}^1$

Der Einfachkeit halber setzen wir in diesem Kapitel voraus, dass K ein algebraisch abgeschlossener Körper ist. Dies hat den Vorteil, dass sich jedes Polynom $f \in K[x] \setminus \{0\}$ in der Form

$$f(x) = c \cdot (x - \alpha_1)^{n_1} \dots (x - \alpha_r)^{n_r}$$

schreiben lässt mit $c \in K^*$, paarweise verschiedenen $\alpha_i \in K$, $n_i \in \mathbb{N}$ und $r \in \mathbb{N}_0$.

1. Funktionen auf $\mathbb{P}^1$

Überlegungen: Wir starten mit

$$\mathbb{P}^1 = \{(p_0 : p_1) : (p_0, p_1) \in K^2 \setminus \{(0,0)\}\}.$$

Sei $A(x_0, x_1) \in K[x_0, x_1]$ ein homogenes Polynom vom Grad d, d.h.

$$A(x_0, x_1) = \sum_{i=0}^{d} a_i x_0^{d-i} x_1^i.$$

Dann gilt

$$A(\lambda x_0, \lambda x_1) = \lambda^d A(x_0, x_1).$$

Das Polynom A können wir (im Fall $d \geq 1$) nicht als Funktion auf $\mathbb{P}^1$ auffassen, da die Repräsentanten (p_0, p_1) und $(\lambda p_0, \lambda p_1)$ eines Punktes im Allgemeinen verschiedene Werte liefern:

$$A(\lambda p_0, \lambda p_1) = \lambda^d A(p_0, p_1).$$

Ist $B(x_0, x_1)$ ein weiteres homogenes Polynom vom Grad d, so gilt natürlich auch

$$B(\lambda p_0, \lambda p_1) = \lambda^d B(p_0, p_1).$$

Ist nun $B(p_0, p_1) \neq 0$, so folgt

$$\frac{A(p_0, p_1)}{B(p_0, p_1)} = \frac{A(\lambda p_0, \lambda p_1)}{B(\lambda p_0, \lambda p_1)},$$

d.h. der Wert von

$$\frac{A(p_0, p_1)}{B(p_0, p_1)}$$

hängt nur von $P = (p_0 : p_1)$ und nicht vom ausgewählten Repräsentanten ab. Daher definiert

$$\frac{A(x_0, x_1)}{B(x_0, x_1)}$$

eine Funktion auf (einer Teilmenge von) $\mathbb{P}^1$, wobei natürlich $B(x_0, x_1)$ nicht das Nullpolynom sein sollte.

DEFINITION. *Wir definieren den* **Funktionenkörper** $K(\mathbb{P}^1)$ *von* $\mathbb{P}^1$ *über* K *als*

$$K(\mathbb{P}^1) \quad = \quad \{\frac{A(x_0, x_1)}{B(x_0, x_1)} : A(x_0, x_1), B(x_0, x_1) \in K[x_0, x_1], B(x_0, x_1) \neq 0,$$
$$A, B \text{ homogene Polynome gleichen Grades}\}.$$

Datei: algku5.tex. Version vom 19.7.2021

Man rechnet in $K(\mathbb{P}^1)$ wie mit Brüchen:

$$\begin{aligned}
\frac{A(x_0,x_1)}{B(x_0,x_1)} = \frac{\widetilde{A}(x_0,x_1)}{\widetilde{B}(x_0,x_1)} \quad &\Longleftrightarrow \quad A(x_0,x_1)\widetilde{B}(x_0,x_1) = \widetilde{A}(x_0,x_1)B(x_0,x_1) \quad \text{in } K[x_0,x_1],\\
\frac{A(x_0,x_1)}{B(x_0,x_1)} + \frac{\widetilde{A}(x_0,x_1)}{\widetilde{B}(x_0,x_1)} \quad &= \quad \frac{A(x_0,x_1)\widetilde{B}(x_0,x_1) + \widetilde{A}(x_0,x_1)B(x_0,x_1)}{B(x_0,x_1)\widetilde{B}(x_0,x_1)}, \quad B(x_0,x_1)\neq 0, \widetilde{B}(x_0,x_1)\neq 0,\\
\frac{A(x_0,x_1)}{B(x_0,x_1)} \cdot \frac{\widetilde{A}(x_0,x_1)}{\widetilde{B}(x_0,x_1)} \quad &= \quad \frac{A(x_0,x_1)\widetilde{A}(x_0,x_1)}{B(x_0,x_1)\widetilde{B}(x_0,x_1)}, \quad B(x_0,x_1)\neq 0, \widetilde{B}(x_0,x_1)\neq 0,\\
\left(\frac{A(x_0,x_1)}{B(x_0,x_1)}\right)^{-1} \quad &= \quad \frac{B(x_0,x_1)}{A(x_0,x_1)}, \quad A(x_0,x_1)\neq 0, B(x_0,x_1)\neq 0.
\end{aligned}$$

Damit gilt:

Satz. *Der Funktionenkörper $K(\mathbb{P}^1)$ ist mit der oben beschriebenen Addition und Multiplikation ein Körper. Nullelement ist das konstante Polynom 0, Einselement ist das konstante Polynom 1.*

Wann ist eine Funktion $f \in K(\mathbb{P}^1)$ in einem Punkt $P = (p_0 : p_1) \in \mathbb{P}^1$ definiert? Wir schreiben $f(x_0,x_1) = \frac{A(x_0,x_1)}{B(x_0,x_1)}$, wo $A(x_0,x_1)$ und $B(x_0,x_1)$ homogene Polynome gleichen Grades sind und $B(x_0,x_1)$ nicht das Nullpolynom ist. Wir unterscheiden drei Fälle:

- **Fall $B(p_0,p_1)\neq 0$:** Dann definiert man
$$f(P) = \frac{A(p_0,p_1)}{B(p_0,p_1)}.$$
Wir sagen, f **ist in P definiert**.
- **Fall $B(p_0,p_1) = 0$ und $A(p_0,p_1)\neq 0$:** Dann ist f **nicht in P definiert**.
- **Fall $B(p_0,p_1) = 0$ und $A(p_0,p_1) = 0$:** Da K algebraisch abgeschlossen ist, zerfallen A und B in Linearfaktoren:
$$A(x_0,x_1) = \prod_{i=1}^{d}(a_ix_0 - b_ix_1) \quad \text{und} \quad B(x_0,x_1) = \prod_{j=1}^{d}(c_jx_0 - d_jx_1).$$
Wegen $A(p_0,p_1) = B(p_0,p_1) = 0$ gibt es Indizes i,j mit
$$a_ip_0 - b_ip_1 = 0 \quad \text{und} \quad c_jp_0 - d_jp_1 = 0.$$
Es folgt (zunächst für $b_i\neq 0$)
$$(p_0:p_1) = (b_ip_0 : b_ip_1) = (b_ip_0 : a_ip_0) = (b_i : a_i) \quad \text{und analog} \quad (p_0:p_1) = (d_j : c_j).$$
Es gibt also $\lambda,\mu \in K^*$ mit $(b_i,a_i) = \lambda(p_0,p_1)$ und $(d_j,c_j) = \mu(p_0,p_1)$, was zu
$$a_ix_0 - b_ix_1 = \lambda(p_1x_0 - p_0x_1) \quad \text{und} \quad c_jx_0 - d_jx_1 = \mu(p_1x_0 - p_0x_1)$$
führt. Die Linearfaktoren $a_ix_0 - b_ix_1$ und $c_jx_0 - d_jx_1$ unterscheiden sich also nur um eine Zahl aus K^* und können daher herausgekürzt werden. Wiederholt man dies bei Bedarf, erreicht man schließlich $(A(p_0,p_1),B(p_0,p_1))\neq(0,0)$ und ist dann bei einem der ersten beiden Fälle.

Beispiele: Wir betrachten
$$f = \frac{2x_0^2 + x_0x_1 - 3x_1^2}{x_0^2 - 3x_0x_1 + 2x_1^2}.$$
Wie verhält sich f im Punkt $P = (1:1)$? Man findet $A(1,1) = B(1,1) = 0$, weswegen sowohl A als auch B durch einen Faktor $x_0 - x_1$ teilber sein sollten. Nun ist
$$f = \frac{(x_0-x_1)(2x_0+3x_1)}{(x_0-x_1)(x_0-2x_1)} = \frac{2x_0+3x_1}{x_0-2x_1} \quad \text{und} \quad f(P) = \frac{5}{-1} = -5,$$
d.h. f ist in $(1:1)$ definiert und nimmt dort den Wert -5 an.

Aus der Definition von Addition und Multiplikation folgt sofort:

Lemma. *Sind $f,g \in K(\mathbb{P}^1)$ in einem Punkt $P\in\mathbb{P}^1$ definiert, so auch $f+g$ und fg.*

Die Funktionen x und u: Wir betrachten zwei spezielle Funktionen:

$$x = \frac{x_1}{x_0} \quad \text{und} \quad u = \frac{x_0}{x_1}.$$

x ist einfach die übliche Koordinatenfunktion im affinen Teil

$$U_0 = \{(1 : x) \in \mathbb{P}^1\} \simeq \mathbb{A}^1.$$

Es gilt dann:

$$x(P) = \begin{cases} p & \text{für } P = (1 : p), \\ \text{nicht definiert} & \text{in } P = (0 : 1). \end{cases}$$

u ist die Koordinatenfunktion im affinen Teil

$$U_1 = \{(u : 1) \in \mathbb{P}^1\} \simeq \mathbb{A}^1.$$

Es gilt:

$$u(P) = \begin{cases} \text{nicht definiert} & \text{in } P = (1 : 0), \\ \frac{1}{p} & \text{für } P = (1 : p) \text{ mit } p \neq 0, \\ 0 & \text{für } P = (0 : 1). \end{cases}$$

Mit Hilfe der Funktionen $x = \frac{x_1}{x_0}$ und $u = \frac{x_0}{x_1}$ können wir alle Funktionen des Funktionenkörpers beschreiben: Seien $A(x_0, x_1), B(x_0, x_1)$ homogen vom Grad d und $B(x_0, x_1) \neq 0$. Wir schreiben

$$A(x_0, x_1) = \sum_{i=0}^{d} a_i x_0^{d-i} x_1^i, \quad B(x_0, x_1) = \sum_{i=0}^{d} b_i x_0^{d-i} x_1^i.$$

Es ist

$$A(x_0, x_1) = \sum_{i=0}^{d} a_i x_0^d (\frac{x_1}{x_0})^i = x_0^d \sum_{i=0}^{d} a_i x^i \quad \text{und analog} \quad B(x_0, x_1) = x_0^d \sum_{i=0}^{d} b_i x^i.$$

Es folgt

$$\frac{A(x_0, x_1)}{B(x_0, x_1)} = \frac{x_0^d \sum_{i=0}^{d} a_i x^i}{x_0^d \sum_{i=0}^{d} b_i x^i} = \frac{\sum_{i=0}^{d} a_i x^i}{\sum_{i=0}^{d} b_i x^i} = \frac{A(1, x)}{B(1, x)}.$$

Ganz analog zeigt man für $u = \frac{x_0}{x_1}$

$$\frac{A(x_0, x_1)}{B(x_0, x_1)} = \frac{A(u, 1)}{B(u, 1)}.$$

Wir fassen dies zusammen:

LEMMA. *Sind $A(x_0, x_1), B(x_0, x_1) \in K[x_0, x_1]$ homogene Polynome gleichen Grad mit $B(x_0, x_1) \neq 0$, so gilt*

$$\frac{A(x_0, x_1)}{B(x_0, x_1)} = \frac{A(1, x)}{B(1, x)} = \frac{A(u, 1)}{B(u, 1)}.$$

Insbesondere gilt dann

$$K(\mathbb{P}^1) = \{\frac{p(x)}{q(x)} : p(x), q(x) \in K[x], q(x) \neq 0\}.$$

Bemerkung: Für den Polynomring in der Variablen x mit Koeffizienten aus K schreibt man

$$K[x].$$

Für den Quotientenkörper schreibt man

$$K(x) = \{\frac{p(x)}{q(x)} : p(x), q(x) \in K[x], q(x) \neq 0\}.$$

Dann gilt also

$$K(\mathbb{P}^1) = K(x).$$

Dies erklärt eventuell die etwas ungewöhnliche Schreibweise für den Funktionenkörper von $\mathbb{P}^1$. Man nennt $K(\mathbb{P}^1) = K(x)$ auch den rationalen Funktionenkörper.

Beispiele: Wir rechnen zunächst ausführlich:

$$\begin{aligned} f &= \frac{2x_0^2 + x_0x_1 - 3x_1^2}{x_0^2 - 3x_0x_1 + 2x_1^2} = \frac{x_0^2 \cdot (2 + \frac{x_1}{x_0} - 3(\frac{x_1}{x_0})^2)}{x_0^2 \cdot (1 - 3\frac{x_1}{x_0} + 2(\frac{x_1}{x_0})^2)} = \\ &= \frac{2 + x - 3x^2}{1 - 3x + 2x^2} = \frac{(x-1)(-3x-2)}{(x-1)(2x-1)} = \frac{-3x-2}{2x-1}. \end{aligned}$$

Nun kürzer, in dem wir für (x_0, x_1) einfach $(1, x)$ bzw. $(u, 1)$ einsetzen:

$$g = \frac{x_0^2 + 2x_0x_1 + 3x_1^2}{3x_0^2 + 2x_0x_1 + x_1^2} = \frac{1 + 2x + 3x^2}{3 + 2x + x^2} = \frac{u^2 + 2u + 3}{3u^2 + 2u + 1}.$$

Wir wollen noch sehen, wie man aus einer rationalen Funktion in x eine Darstellung als Quotient homogener Polynome gleichen Grades erhält. Sei

$$f = \frac{p(x)}{q(x)}.$$

Dabei sei

$$p(x) = p_m x^m + p_{m-1}x^{m-1} + \cdots + p_0, \quad q(x) = q_n x^n + q_{n-1}x^{n-1} + \cdots + q_0.$$

Wir nehmen an, dass $p_m \neq 0$ und $q_n \neq 0$ gilt, d.h. $p(x)$ hat Grad m und $q(x)$ hat Grad n. Dann folgt

$$\begin{aligned} f &= \frac{p_m x^m + p_{m-1}x^{m-1} + \cdots + p_0}{q_n x^n + q_{n-1}x^{n-1} + \cdots + q_n} = \frac{p_m(\frac{x_1}{x_0})^m + p_{m-1}(\frac{x_1}{x_0})^{m-1} + \cdots + p_0}{q_n(\frac{x_1}{x_0})^n + q_{n-1}(\frac{x_1}{x_0})^{n-1} + \cdots + q_0} = \\ &= \frac{x_0^n}{x_0^m} \cdot \frac{p_m x_1^m + p_{m-1}x_0x_1^{m-1} + \cdots + p_0x_0^m}{q_n x_1^n + q_{n-1}x_0x_1^{n-1} + \cdots + q_0x_0^n} = \\ &= \frac{x_0^n \cdot (p_m x_1^m + p_{m-1}x_0x_1^{m-1} + \cdots + p_0x_0^m)}{x_0^m \cdot (q_n x_1^n + q_{n-1}x_0x_1^{n-1} + \cdots + q_0x_0^n)}. \end{aligned}$$

In der letzten Darstellung hat man f als Quotienten homogener Polynome vom Grad $m+n$ geschrieben. Natürlich sollte man noch Potenzen von x_0 kürzen, soweit möglich.
Es ist

$$\mathbb{P}^1 = \{(p_0 : p_1) : (p_0, p_1) \in K^2 \setminus \{(0,0)\}\} = \{(1 : p) : p \in K\} \cup \{(0 : 1)\}.$$

Identifizieren wir $(1 : p)$ mit p, schreiben wir $\infty = (0 : 1)$, so ist

$$\mathbb{P}^1 \simeq K \cup \{\infty\}.$$

Mit diesen Abkürzungen gilt für $x = \frac{x_1}{x_0}$ und $u = \frac{x_0}{x_1}$:

$$x \text{ ist nicht definiert in } \infty, \quad x(\alpha) = \alpha \text{ für } \alpha \in K$$

und

$$u \text{ ist nicht definiert in } 0 \in K, \quad u(\alpha) = \frac{1}{\alpha} \text{ für } \alpha \in K \setminus \{0\}, \quad u(\infty) = 0.$$

2. Ordnung (Bewertung) einer Funktion in einem Punkt

Sei $f(x) \in K(x)$ und $P \in \mathbb{P}^1$. Wir schreiben $f(x) = \frac{p(x)}{q(x)}$ mit Polynomen $p(x), q(x) \in K[x] \setminus \{0\}$. (Beide Polynome seien von 0 verschieden.) Wir betrachten das Verhalten von f in den Punkten von $\mathbb{P}^1$.

- **Fall** $P = (1 : \alpha) \simeq \alpha$**:** Dabei ist $\alpha \in K$. Wir klammern $x - \alpha$ so oft wie möglich aus:

$$p(x) = (x-\alpha)^{e_p}\widetilde{p}(x) \text{ mit } \widetilde{p}(\alpha) \neq 0$$

und

$$q(x) = (x-\alpha)^{e_q}\widetilde{q}(x) \text{ mit } \widetilde{q}(\alpha) \neq 0.$$

Setzen wir

$$e = e_p - e_q \text{ und } g(x) = \frac{\widetilde{p}(x)}{\widetilde{q}(x)},$$

so gilt

$$f(x) = (x-\alpha)^e \cdot g(x), \text{ wobei } g \text{ in } \alpha \text{ definiert ist und } g(\alpha) \neq 0 \text{ gilt.}$$

Wir nennen e **die Ordnung von f in α** und schreiben

$$\operatorname{ord}_\alpha(f) = e.$$

(Statt Ordnung findet man auch die Bezeichnung **Bewertung** und $v_\alpha(f)$.) Ist $e \geq 0$, so ist f in α definiert. Wir nennen die Funktion $x - \alpha$ auch eine **Uniformisierende im Punkt** α. Es gibt drei Fälle:

- **Fall $e > 0$:** Dann ist $f(\alpha) = 0$. Die Funktion f hat in α eine **Nullstelle der Ordnung** $e = \operatorname{ord}_\alpha(f)$.
- **Fall $e = 0$:** Dann gilt $f(\alpha) = g(\alpha) \neq 0$.
- **Fall $e < 0$:** Die Funktion f ist in α nicht definiert. Man sagt, f hat in α einen **Pol der Ordnung** $|\operatorname{ord}_\alpha(f)| = -\operatorname{ord}_\alpha(f)$.

- **Fall $P = (0:1) \simeq \infty$:** Wir schreiben

$$p(x) = p_0 + p_1 x + \cdots + p_m x^m, \quad q(x) = q_0 + q_1 x + \cdots + q_n x^n \text{ mit } p_m \neq 0, q_n \neq 0.$$

Wegen $xu = 1$ folgt

$$f(x) = \frac{u^n}{u^m} \cdot \frac{u^m(p_0 + p_1 x + \cdots + p_m x^m)}{u^n(q_0 + q_1 x + \cdots + q_n x^n)} = u^{n-m} \cdot \frac{p_0 u^m + p_1 u^{m-1} + \cdots + p_m}{q_0 u^n + q_1 u^{n-1} + \cdots + q_n}.$$

Wegen $u(\infty) = 0$ ist die Funktion

$$g(x) = \frac{p_0 u^m + p_1 u^{m-1} + \cdots + p_m}{q_0 u^n + q_1 u^{n-1} + \cdots + q_n}$$

in ∞ definiert und hat den Wert $g(\infty) = \frac{p_m}{q_n} \neq 0$.

Wir haben die Zerlegung

$$f = u^{n-m} \cdot g.$$

Wir nennen $n - m$ die Ordnung von f in ∞ und schreiben

$$\operatorname{ord}_\infty(f) = n - m.$$

Die Funktion $u = \frac{1}{x}$ wird eine **Uniformisierende im Punkt** ∞ genannt. Wir unterscheiden drei Fälle:

- **Fall $m < n$, also $\operatorname{ord}_\infty(f) > 0$:** Dann ist $f(\infty) = 0$. Die Funktion f hat in ∞ eine **Nullstelle der Ordnung** $\operatorname{ord}_\infty(f) = n - m$.
- **Fall $m = n$, also $\operatorname{ord}_\infty(f) = 0$:** Dann gilt $f(\infty) = \frac{p_m}{q_n} \neq 0$.
- **Fall $m > n$, also $\operatorname{ord}_\infty(f) < 0$:** Die Funktion f ist in ∞ nicht definiert. Man sagt, f hat in ∞ einen **Pol der Ordnung** $|\operatorname{ord}_\infty(f)| = -\operatorname{ord}_\alpha(f) = m - n$.

Wir fassen dies nochmals zusammen:

LEMMA. *Definiert man für $P \in \mathbb{P}^1$*

$$u_P = \begin{cases} x - \alpha & \text{für } P = (1:\alpha) \simeq \alpha, \quad \alpha \in K, \\ u = \frac{1}{x} & \text{für } P = (0:1) \simeq \infty, \end{cases}$$

so lässt sich jede Funktion $f \in K(\mathbb{P}^1) \setminus \{0\}$ schreiben als

$$f = u_P^e \cdot g,$$

wobei g in P definiert ist mit $g(P) \neq 0$ und $e \in \mathbb{Z}$ gilt. e heißt die Ordnung von f in P, $\operatorname{ord}_P(f) = e$. Es ist $u_P(P) = 0$. (u_P ist eine Uniformisierende im Punkt P.)

- **Fall $e > 0$:** *f ist in P definiert mit $f(P) = 0$. f hat in P eine Nullstelle der Ordnung e.*
- **Fall $e = 0$:** *f ist in P definiert mit $f(P) \neq 0$.*
- **Fall $e < 0$:** *f ist in P nicht definiert. f hat in P einen Pol der Ordnung $|e| = -e$.*

Es gilt:

$$\begin{aligned} \operatorname{ord}_P(f) = 0 \quad &\iff \quad f \text{ hat in } P \text{ weder eine Nullstelle noch eine Polstelle} \quad \iff \\ &\iff \quad f \text{ ist in } P \text{ definiert mit } f(P) \neq 0. \end{aligned}$$

SATZ (Eigenschaften der Ordnungsfunktion). *Für $P \in \mathbb{P}^1$ und $f, g \in K(\mathbb{P}^1) \setminus \{0\}$ gilt:*

- $\operatorname{ord}_P(fg) = \operatorname{ord}_P(f) + \operatorname{ord}_P(g)$,
- $\operatorname{ord}_P(f+g) \geq \min(\operatorname{ord}_P(f), \operatorname{ord}_P(g))$ *im Fall* $f+g \neq 0$.
- *Im Fall* $\operatorname{ord}_P(f) \neq \operatorname{ord}_P(g)$ *gilt* $\operatorname{ord}_P(f+g) = \min(\operatorname{ord}_P(f), \operatorname{ord}_P(g))$.

Beweis: Wir schreiben

$$f = u_P^a F, \quad g = u_P^b G \text{ mit } a, b \in \mathbb{Z}, F, G \in K(\mathbb{P}^1), F(P) \neq 0, G(P) \neq 0.$$

Dann ist

$$fg = u_P^{a+b} FG.$$

Da F und G in P definiert sind, ist es auch FG; wegen $(FG)(P) = F(P)G(P) \neq 0$, kann man die Ordnung von fg aus obiger Gleichung ablesen:

$$\operatorname{ord}_P(fg) = a + b = \operatorname{ord}_P(f) + \operatorname{ord}_P(g).$$

(Fortsetzung des Beweises mit $f = u_P^a F$ und $g = u_P^b G$) Für die Summe $f+g$ unterscheiden wir zwei Fälle:

- **Fall** $a \neq b$**:** O.E. können wir $a < b$ annehmen. Dann ist

  $$f + g = u_P^a F + u_P^b G = u_P^a \cdot \left(F + u_P^{b-a} G\right).$$

  Die Funktion $F + u_P^{b-a} G$ ist in P definiert und erfüllt

  $$(F + u_P^{b-a} G)(P) = F(P) + u_P(P)^{b-a} G(P) = F(P) \neq 0,$$

  weswegen wir

  $$\operatorname{ord}_P(f+g) = a = \operatorname{ord}_P(f) = \min(\operatorname{ord}_P(f), \operatorname{ord}_P(g))$$

  erhalten.
- **Fall** $a = b$**:** Es ist

  $$f + g = u_P^a (F + G).$$

  Da F und G in P definiert sind, ist es auch $F+G$ und wir können zerlegen

  $$F + G = u_P^c H,$$

  wo H in P definiert ist mit $H(P) \neq 0$ und $c \geq 0$ gilt. Dann ist

  $$f + g = u_P^{a+c} H$$

  und

  $$\operatorname{ord}_P(f+g) = a + c = \operatorname{ord}_P(f) + c \geq \operatorname{ord}_P(f) = \min(\operatorname{ord}_P(f), \operatorname{ord}_P(g)).$$

Damit ist der Satz bewiesen. ■

Im folgenden Lemma geht wesentlich ein, dass der Grundkörper K als algebraisch abgeschlossen vorausgesetzt wurde.

LEMMA. *Sei* $f \in K(\mathbb{P}^1) \setminus \{0\}$ *geschrieben als*

$$f = c \cdot \frac{(x-\alpha_1)^{m_1} \dots (x-\alpha_r)^{m_r}}{(x-\beta_1)^{n_1} \dots (x-\beta_s)^{n_s}}.$$

Dabei seien die Zahlen $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s$ *paarweise verschieden und* $m_i, n_j \in \mathbb{N}$, $c \in K^*$, $r, s \in \mathbb{N}_0$. *Dann gilt:*

$$\operatorname{ord}_P(f) = \begin{cases} m_i & \text{für } P = \alpha_i, \\ -n_j & \text{für } P = \beta_j, \\ (n_1 + \dots + n_s) - (m_1 + \dots + m_r) & \text{für } P = \infty, \\ 0 & \text{sonst.} \end{cases}$$

Beweis: Mit $u = \frac{1}{x}$ gilt

$$\begin{aligned} f &= c \cdot \frac{(x-\alpha_1)^{m_1} \dots (x-\alpha_r)^{m_r}}{(x-\beta_1)^{n_1} \dots (x-\beta_s)^{n_s}} = \\ &= c \cdot \frac{u^{n_1+\dots+n_s} \cdot (1-\alpha_1 u)^{m_1} \dots (1-\alpha_r u)^{m_r}}{u^{m_1+\dots+m_r} \cdot (1-\beta_1 u)^{n_1} \dots (1-\beta_s u)^{n_s}}. \end{aligned}$$

Daraus kann man sofort ablesen:

$$\operatorname{ord}_{\alpha_i}(f) = m_i, \quad \operatorname{ord}_{\beta_j}(f) = -n_j, \quad \operatorname{ord}_{\infty}(f) = (n_1 + \dots + n_s) - (m_1 + \dots + m_r).$$

In allen anderen Punkten ist f definiert und nimmt einen von 0 verschiedenen Wert an, sodass die Ordnung 0 ist. ■

Das letzte Lemma hat eine erstaunliche Konsequenz:

SATZ. *Jede Funktion $f \in K(\mathbb{P}^1) \setminus \{0\}$ hat nur endliche viele Null- und Polstellen. Es gilt*

$$\sum_{P \in \mathbb{P}^1} \operatorname{ord}_P(f) = 0.$$

Mit Vielfachheiten gezählt, hat f also genau so viele Null- wie Polstellen.

Beweis: Das folgt sofort aus dem letzten Lemma, wenn man alle Ordnungen aufaddiert. ■

Beispiele:

$$\operatorname{ord}_0(x) = 1, \quad \operatorname{ord}_{\infty}(x) = -1.$$

Für $c \in K \setminus \{0\}$ gilt

$$\operatorname{ord}_c(x-c) = 1, \quad \operatorname{ord}_{\infty}(x-c) = \operatorname{ord}_{\infty}(\frac{1}{u} - c) = \operatorname{ord}_{\infty}(\frac{1}{u} \cdot (1-uc)) = -1.$$

Beispiel: Ist $p(x) \in K[x] \setminus \{0\}$ ein Polynom vom Grad m, so weiß man, dass p mit Vielfachheiten gezählt genau m Nullstellen hat. Betrachtet man p als Funktion auf $\mathbb{P}^1$, so folgt, dass p in ∞ einen Pol der Ordnung m hat.

FOLGERUNG. *Die einzigen Funktionen in $K(\mathbb{P}^1)$ ohne Polstellen sind die konstanten Funktionen. Anders ausgedrückt: Für $f \in K(\mathbb{P}^1) \setminus \{0\}$ gilt:*

$$\operatorname{ord}_P(f) \geq 0 \text{ für alle } P \in \mathbb{P}^1 \quad \Longleftrightarrow \quad f \in K^*.$$

Beweis: Ist f konstant, so ist nichts zu zeigen. Wir können annehmen, dass f nicht konstant ist. Sei $f = \frac{p(x)}{q(x)}$, wobei die Darstellung gekürzt sein soll. Ist $q(x)$ ein nichtkonstantes Polynom, so hat es eine Nullstelle β, d.h. $q(\beta) = 0$. Dann hat aber f eine Polstelle in β und es gilt $\operatorname{ord}_P(f) < 0$. Ist $f = p(x)$, so ist p nicht konstant. Es gibt also eine Nullstelle α. Dann ist $f(\alpha) = 0$. Dann hat aber f in ∞ eine Polstelle. ■

DEFINITION. *Sei $f \in K(\mathbb{P}^1)$ und $\lambda \in K$. Wir sagen, f nimmt den Wert λ in $P \in \mathbb{P}^1$ an, wenn gilt $f(P) = \lambda$.*
In diesem Fall sagen wir genauer: f nimmt den Wert λ in P mit Vielfachheit $\operatorname{ord}_P(f - \lambda)$ an, wenn $f \notin K$ gilt. (Im Fall $\lambda = 0$ ist diese Vielfachheit einfach die Nullstellenordnung.)

Beispiel: Wir betrachten

$$f = \frac{3x^2 - 2x + 5}{x^2 + 2}.$$

In $P = 1$ nimmt f den Wert 2 an: $f(1) = 2$. Mit welcher Vielfachheit? Es ist

$$\begin{aligned} f - 2 &= \frac{3x^2 - 2x + 5}{x^2 + 2} - 2 = \frac{(3x^2 - 2x + 5) - 2(x^2 + 2)}{x^2 + 2} = \\ &= \frac{x^2 - 2x + 1}{x^2 + 2} = (x-1)^2 \cdot \frac{1}{x^2 - 2}, \end{aligned}$$

also $\operatorname{ord}_1(f-2) = 2$, d.h. f nimmt den Wert 2 in 1 mit Vielfachheit 2 an.

SATZ. *Sei $f \in K(\mathbb{P}^1) \setminus K$ geschrieben als*

$$f = \frac{p(x)}{q(x)} \text{ mit teilerfremden Polynomen } p(x), q(x).$$

(Die Darstellung $f = \frac{p(x)}{q(x)}$ soll also gekürzt sein.) Für $\lambda \in K$ nimmt die Funktion f den Wert λ in genau

$$\max(\operatorname{grad}(p(x)), \operatorname{grad}(q(x)))$$

Punkten an, wenn man mit Vielfachheiten zählt, d.h.

$$\sum_{\substack{P \in \mathbb{P}^1 \\ f(P)=\lambda}} \operatorname{ord}_P(f-\lambda) = \max(\operatorname{grad}(p(x)), \operatorname{grad}(q(x))).$$

Dies ist auch gleich der (mit Vielfachkeit gezählten) Anzahl der Polstellen von f, d.h.

$$\sum_{\substack{P \in \mathbb{P}^1 \\ \operatorname{ord}_P(f)<0}} |\operatorname{ord}_P(f)| = \max(\operatorname{grad}(p), \operatorname{grad}(q)).$$

Beweis:

- Wir zählen zunächst die Polstellen von f. Wir schreiben wieder

$$\begin{aligned} f &= c \cdot \frac{(x-\alpha_1)^{m_1} \dots (x-\alpha_r)^{m_r}}{(x-\beta_1)^{n_1} \dots (x-\beta_s)^{n_s}} = \\ &= c \cdot \frac{u^{n_1+\dots+n_s} \cdot (1-\alpha_1 u)^{m_1} \dots (1-\alpha_r u)^{m_r}}{u^{m_1+\dots+m_r} \cdot (1-\beta_1 u)^{n_1} \dots (1-\beta_s u)^{n_s}} = \\ &= c \cdot u^{\operatorname{grad}(q)-\operatorname{grad}(p)} \cdot \frac{(1-\alpha_1 u)^{m_1} \dots (1-\alpha_r u)^{m_r}}{(1-\beta_1 u)^{n_1} \dots (1-\beta_s u)^{n_s}}. \end{aligned}$$

  Im Endlichen sind die Polstellen von f die Punkte $\beta_1, \dots, \beta_s$, mit Vielfachheit gezählt also

$$n_1 + \dots + n_s = \operatorname{grad}(q(x)).$$

  Wir unterscheiden zwei Fälle:
  - **Fall** $\operatorname{grad}(p) > \operatorname{grad}(q)$**:** Dann ist $\operatorname{ord}_\infty(f) = \operatorname{grad}(q) - \operatorname{grad}(p) = -(\operatorname{grad}(p) - \operatorname{grad}(q))$, f hat in ∞ einen Pol der Ordnung $\operatorname{grad}(p) - \operatorname{grad}(q)$. Mit Vielfachheiten gezählt gibt es also

$$\operatorname{grad}(q) + (\operatorname{grad}(p) - \operatorname{grad}(q)) = \operatorname{grad}(p) = \max(\operatorname{grad}(p), \operatorname{grad}(q))$$

    Polstellen von f.
  - **Fall** $\operatorname{grad}(p) \leq \operatorname{grad}(q)$**:** Dann ist f in ∞ definiert. Die einzigen Polstellen liegen im Endlichen, ihre Anzahl ist

$$\operatorname{grad}(q) = \max(\operatorname{grad}(p), \operatorname{grad}(q)).$$

  Zusammengefasst:

$$\sum_{\substack{P \in \mathbb{P}^1 \\ \operatorname{ord}_P(f)<0}} |\operatorname{ord}_P(f)| = \max(\operatorname{grad}(p), \operatorname{grad}(q)).$$

- Die Funktion $f - \lambda$ hat die gleichen Polstellen wie f, weil dies gerade die Punkte sind, in denen f nicht definiert ist. Mit der Formel des letztes Satzes

$$\sum_{P \in \mathbb{P}^1} \operatorname{ord}_P(f) = 0$$

angewandt auf $f-\lambda$ erhält man daher

$$\begin{aligned} 0 &= \sum_{P\in\mathbb{P}^1} \operatorname{ord}_P(f-\lambda) = \sum_{\substack{P\in\mathbb{P}^1\\ \operatorname{ord}_P(f-\lambda)>0}} \operatorname{ord}_P(f-\lambda) + \sum_{\substack{P\in\mathbb{P}^1\\ \operatorname{ord}_P(f-\lambda)<0}} \operatorname{ord}_P(f-\lambda) = \\ &= \sum_{\substack{P\in\mathbb{P}^1\\ f(P)=0}} \operatorname{ord}_P(f-\lambda) - \sum_{\substack{P\in\mathbb{P}^1\\ \operatorname{ord}_P(f-\lambda)<0}} |\operatorname{ord}_P(f-\lambda)| = \\ &= \sum_{\substack{P\in\mathbb{P}^1\\ f(P)=0}} \operatorname{ord}_P(f-\lambda) - \max(\operatorname{grad}(p),\operatorname{grad}(q)). \end{aligned}$$

Daraus folgt dann

$$\sum_{\substack{P\in\mathbb{P}^1\\ f(P)=\lambda}} \operatorname{ord}_P(f-\lambda) = \max(\operatorname{grad}(p),\operatorname{grad}(q)),$$

wie behauptet. ■

Beispiel: Wir betrachten

$$f = \frac{3x^2-2x+5}{x^2+2}.$$

Es ist

$$f = 3\cdot\frac{(x-\frac{1+\sqrt{-14}}{3})(x-\frac{1-\sqrt{-14}}{3})}{(x-\sqrt{-2})(x+\sqrt{-2})},$$

insbesondere ist die Darstellung gekürzt. f hat zwei Polstellen erster Ordnung, nämlich in $\pm\sqrt{-2}$, zwei Nullstellen erster Ordnung, nämlich in $\frac{1\pm\sqrt{-14}}{3}$. Wegen

$$f = \frac{3x^2-2x+5}{x^2+2} = \frac{3-2u+5u^2}{1+2u^2}$$

gilt $f(\infty)=3$. Mit welcher Vielfachheit wird der Wert 3 in ∞ angenommen? Es ist

$$f-3 = \frac{3-2u+5u^2}{1+2u^2} - 3 = \frac{(3-2u+5u^2)-3(1+2u^2)}{1+2u^2} = \frac{-2u-u^2}{1+2u^2} = u\cdot\frac{-2-u}{1+2u^2}.$$

Also $\operatorname{ord}_\infty(f-3)=1$, sodass der Wert 3 in ∞ mit Vielfachheit 1 angenommen wird. An welchem Punkt wird der Wert 3 sonst noch angenommen?

$$\begin{aligned} f-3 &= \frac{3x^2-2x+5}{x^2+2} - 3 = \frac{(3x^2-2x+5)-3(x^2+2)}{x^2+2} = \\ &= \frac{-2x-1}{x^2+2} = -\frac{1}{2}\cdot\frac{x+\frac{1}{2}}{x^2+2}. \end{aligned}$$

Also wird der Wert 3 noch im Punkt $-\frac{1}{2}$ angenommen.

3. Divisoren

Ein **Divisor** D der Kurve $\mathbb{P}^1$ ist eine formale ganzzahlige Linearkombination von endlich vielen Punkten auf $\mathbb{P}^1$:

$$D = \sum_{P\in\mathbb{P}^1} n_P[P] \quad \text{mit} \quad n_P\in\mathbb{Z} \quad \text{und} \quad \#\{P\in\mathbb{P}^1 : n_P\neq 0\} < \infty.$$

Beispiele: (für $K=\mathbb{C}$)

$D_1 = 2[1]-3[5]+3[\infty] = 2[(1:1)]-3[(1:5)]+3[(0:1)]$, $D_2=0$, $D_3 = 2[1+i]-3[\pi]+5[\infty]$.

(Die eckigen Klammern bei $[P]$ dienen dazu, die Punkte nicht mit Zahlen zu vermischen.)

Dabei soll gelten

$$\sum_{P\in\mathbb{P}^1} m_P[P] = \sum_{P\in\mathbb{P}^1} n_P[P] \quad\Longleftrightarrow\quad m_P = n_P \text{ für alle } P\in\mathbb{P}^1.$$

(Man kann also „Koeffizientenvergleich“ machen.)
Divisoren kann man addieren und subtrahieren:

$$\left(\sum_{P\in\mathbb{P}^1} m_P[P]\right) + \left(\sum_{P\in\mathbb{P}^1} n_P[P]\right) = \sum_{P\in\mathbb{P}^1} (m_P + n_P)[P]$$

und

$$\left(\sum_{P\in\mathbb{P}^1} m_P[P]\right) - \left(\sum_{P\in\mathbb{P}^1} n_P[P]\right) = \sum_{P\in\mathbb{P}^1} (m_P - n_P)[P].$$

Damit bilden die Divisoren eine abelsche Gruppe, die **Divisorengruppe** von $\mathbb{P}^1$:

$$\mathrm{Div}(\mathbb{P}^1) = \{\sum_{P\in\mathbb{P}^1} n_P[P] : n_P \in \mathbb{Z} \text{ und } \#\{P \in \mathbb{P}^1 : n_P \neq 0\} < \infty\}.$$

(In der Sprache der Algebra: $\mathrm{Div}(\mathbb{P}^1)$ ist die freie abelsche Gruppe, die von den Punkten von $\mathbb{P}^1$ erzeugt wird.)
Wir definieren den **Grad eines Divisors** durch

$$\mathrm{grad}(\sum_{P\in\mathbb{P}^1} n_P[P]) = \sum_{P\in\mathbb{P}^1} n_P.$$

Beispiele: Für die obigen Divisoren

$$D_1 = 2[1] - 3[5] + 3[\infty], \quad D_2 = 0, \quad D_3 = 2[1+i] - 3[\pi] + 5[\infty]$$

gilt

$$\mathrm{grad}(D_1) = 2, \quad \mathrm{grad}(D_2) = 0, \quad \mathrm{grad}(D_3) = 4.$$

Wir erhalten also eine Abbildung

$$\mathrm{grad} : \mathrm{Div}(\mathbb{P}^1) \to \mathbb{Z}.$$

Die Formel für die Addition von Divisoren zeigt sofort, dass die Grad-Abbildung additiv ist, d.h. ein Gruppenhomomorphismus ist.

Die **Divisoren vom Grad** 0 bilden eine Untergruppe in der Divisorengruppe:

$$\mathrm{Div}_0(\mathbb{P}^1) = \{D \in \mathrm{Div}(\mathbb{P}^1) : \mathrm{grad}(D) = 0\}.$$

Beispiel: $D = 3[\pi] - 7[i] + 4[\infty]$ ist ein Divisor vom Grad 0.
Die eigentliche Bedeutung der Divisoren kommt von den Hauptdivisoren: Sei $f \in K(\mathbb{P}^1) \setminus \{0\}$. Wir definieren den zu f gehörigen **Hauptdivisor** durch

$$\mathrm{div}(f) = \sum_{P\in\mathbb{P}^1} \mathrm{ord}_P(f)[P].$$

Da wir gesehen haben, dass eine von 0 verschiedene Funktion nur endlich viele Null- und Polstellen hat, ist $\mathrm{div}(f)$ wohldefiniert. (Ein Divisor D heißt **Hauptdivisor**, wenn es eine Funktion $f \in K(\mathbb{P}^1)\setminus\{0\}$ gibt mit $D = \mathrm{div}(f)$.) Der Divisor $\mathrm{div}(f)$ stellt also Informationen über die Null- und Polstellen der Funktion f zusammen.

Beispiele:

- Ist $\lambda \in K^*$, so hat λ als Element von $K(\mathbb{P}^1)$ weder Null- noch Polstellen, es gilt also
$$\mathrm{div}(\lambda) = 0.$$
- Die Funktion x hat einen Pol 1. Ordnung in ∞ und eine Nullstelle 1. Ordnung in 0. Daher ist
$$\mathrm{div}(x) = [0] - [\infty].$$
- Die Funktion $u = \frac{1}{x}$ hat einen Pol 1. Ordnung in 0 und eine Nullstelle 1. Ordnung in ∞:
$$\mathrm{div}(u) = [\infty] - [0].$$

- Wir hatten die Funktion
$$f = \frac{3x^2 - 2x + 5}{x^2 + 2} = 3 \cdot \frac{(x - \frac{1+\sqrt{-14}}{3})(x - \frac{1-\sqrt{-14}}{3})}{(x - \sqrt{-2})(x + \sqrt{-2})}$$
betrachtet. In ∞ ist wegen $f(\infty) = 3$ weder eine Null- noch eine Polstelle, sodass wir erhalten
$$\operatorname{div}(f) = [\frac{1+\sqrt{-14}}{3}] + [\frac{1-\sqrt{-14}}{3}] - [\sqrt{-2}] - [-\sqrt{-2}].$$

Wenn wir Zähler und Nenner einer rationalen Funktion f in Linearfaktoren zerlegen können, können wir sofort den zugehörigen Hauptdivisor aufschreiben:

SATZ. *Sei $f \in K(\mathbb{P}^1)$ mit*
$$f = c \cdot \frac{(x - \alpha_1)^{m_1} \dots (x - \alpha_r)^{m_r}}{(x - \beta_1)^{n_1} \dots (x - \beta_s)^{n_s}},$$
wo $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s$ paarweise verschiedene Zahlen aus K sind und $m_1, \dots, m_r, n_1, \dots, n_s \in \mathbb{N}$, $r, s \in \mathbb{N}_0$, $c \in K^*$ gilt. Dann ist
$$\operatorname{div}(f) = ((n_1 + \dots + n_s) - (m_1 + \dots + m_r))[\infty] + m_1[\alpha_1] + \dots + m_r[\alpha_r] - n_1[\beta_1] - \dots - n_s[\beta_s].$$

Beweis: Wir hatten gezeigt:
$$\operatorname{ord}_P(f) = \begin{cases} m_i & \text{für } P = \alpha_i, \\ -n_j & \text{für } P = \beta_j, \\ (n_1 + \dots + n_s) - (m_1 + \dots + m_r) & \text{für } P = \infty, \\ 0 & \text{sonst.} \end{cases}$$
Daraus folgt die Behauptung. ■

SATZ. *Jeder Hauptdivisor hat Grad 0, d.h. für $f \in K(\mathbb{P}^1) \setminus \{0\}$ gilt*
$$\operatorname{grad}(\operatorname{div}(f)) = 0.$$

Achtung: Der Ausdruck $\operatorname{grad}(\operatorname{div}(f))$ hat nichts mit dem Gradienten und der Divergenz bei Vektorfeldern zu tun.

Beweis: Wegen
$$\sum_{P \in \mathbb{P}^1} \operatorname{ord}_P(f) = 0$$
gilt
$$\operatorname{grad}(\operatorname{div}(f)) = \operatorname{grad}(\sum_{P \in \mathbb{P}^1} \operatorname{ord}_P(f)[P]) = \sum_{P \in \mathbb{P}^1} \operatorname{ord}_P(f) = 0,$$
wie behauptet. ■

LEMMA. *Für $f, g \in K(\mathbb{P}^1)^*$ gilt*
$$\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g) \quad \textit{und} \quad \operatorname{div}(\frac{1}{f}) = -\operatorname{div}(f).$$
Die Abbildung
$$K(\mathbb{P}^1)^* \to \operatorname{Div}_0(\mathbb{P}^1), \quad f \mapsto \operatorname{div}(f)$$
ist also ein Gruppenhomomorphismus.

Beweis: Es gilt
$$\begin{aligned} \operatorname{div}(fg) &= \sum_{P \in \mathbb{P}^1} \operatorname{ord}_P(fg)[P] = \sum_{P \in \mathbb{P}^1} (\operatorname{ord}_P(f) + \operatorname{ord}_P(g))[P] = \\ &= \sum_{P \in \mathbb{P}^1} \operatorname{ord}_P(f)[P] + \sum_{P \in \mathbb{P}^1} \operatorname{ord}_P(g)[P] = \operatorname{div}(f) + \operatorname{div}(g), \end{aligned}$$
was zu zeigen war. ■

LEMMA. *Für $f, g \in K(\mathbb{P}^1)^*$ gilt*

$$\operatorname{div}(f) = 0 \quad \Longleftrightarrow \quad f \in K^*$$

und

$$\operatorname{div}(f) = \operatorname{div}(g) \quad \Longleftrightarrow \quad \text{es gibt ein } \lambda \in K^* \text{ mit } g = \lambda f.$$

Beweis:

- Ist $\operatorname{div}(f) = 0$, so hat f weder Null- noch Polstellen, ist also konstant, wie wir zuvor früher gesehen haben. Die Umkehrung ist klar.
- $\Longrightarrow$ Ist $\operatorname{div}(f) = \operatorname{div}(g)$, so folgt $\operatorname{div}(\frac{g}{f}) = 0$, nach dem ersten Teil ist $\frac{g}{f}$ konstant, also $\frac{g}{f} = \lambda$ für eine Zahl $\lambda \in K^*$. Dann ist $g = \lambda f$, wie behauptet.
  $\Longleftarrow$ Wegen $\operatorname{div}(\lambda) = 0$ folgt
  $$\operatorname{div}(g) = \operatorname{div}(\lambda f) = \operatorname{div}(\lambda) + \operatorname{div}(f) = \operatorname{div}(f).$$
  Damit ist alles gezeigt. ■

Bemerkung: Die Begriffe *Ordnung einer Funktion in einem Punkt*, *Uniformisierende*, *Divisor*, *Divisorengruppe*, *Hauptdivisor* lassen sich auch auf beliebigen nichtsingulären projektiven Kurven C einführen. Folgender Satz ist aber typisch für $\mathbb{P}^1$ und gilt für allgemeine Kurven nicht:

SATZ. *Jeder Divisor vom Grad 0 auf $\mathbb{P}^1$ ist ein Hauptdivisor. Genauer: Ist*

$$D = n_\infty[\infty] + m_1[\alpha_1] + \cdots + m_r[\alpha_r] - n_1[\beta_1] - \cdots - n_s[\beta_s],$$

wobei $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s$ paarweise verschiedene Zahlen aus K sind und $m_1, \ldots, m_r, n_1, \ldots, n_s \in \mathbb{N}$, $r, s \in \mathbb{N}_0$ ein Divisor vom Grad 0, so hat die Funktion

$$f = \frac{(x-\alpha_1)^{m_1} \ldots (x-\alpha_r)^{m_r}}{(x-\beta_1)^{n_1} \ldots (x-\beta_s)^{n_s}}$$

den Divisor D, d.h. $\operatorname{div}(f) = D$.

Beweis: Natürlich können wir D wir im Satz schreiben. Da D Grad 0 haben soll, folgt

$$n_\infty = (n_1 + \cdots + n_s) - (m_1 + \cdots + m_r).$$

Nun betrachten wir die Funktion

$$f = \frac{(x-\alpha_1)^{m_1} \ldots (x-\alpha_r)^{m_r}}{(x-\beta_1)^{n_1} \ldots (x-\beta_s)^{n_s}}.$$

Wir haben zuvor gezeigt, dass gilt

$$\operatorname{div}(f) \quad = \quad ((n_1 + \cdots + n_s) - (m_1 + \cdots + m_r))[\infty] + m_1[\alpha_1] + \cdots + m_r[\alpha_r] - n_1[\beta_1] - \cdots - n_s[\beta_s].$$

Dann gilt aber offensichtlich $D = \operatorname{div}(f)$, was die Behauptung beweist. ■

Nochmals anders ausgedrückt: Auf $\mathbb{P}^1$ sind die Divisoren vom Grad 0 genau die Hauptdivisoren.

Beispiel: Der Divisor

$$D = 2[1] - 3[\pi] + 4[e] - 3[\sqrt{2}]$$

ist ein Divisor vom Grad 0. Ein zugehöriger Hauptdivisor $\operatorname{div}(f)$ wird gegeben durch

$$f = \frac{(x-1)^2(x-e)^4}{(x-\pi)^3(x-\sqrt{2})^3}.$$

DEFINITION. *Zwei Divisoren $D_1, D_2 \in \operatorname{Div}(\mathbb{P}^1)$ heißen* **linear äquivalent**, *in Zeichen $D_1 \sim D_2$, wenn sie sich nur um einen Hauptdivisor unterscheiden:*

$$D_1 \sim D_2 \quad \Longleftrightarrow \quad \text{es gibt eine Funktion } f \in K(\mathbb{P}^1)^* \text{ mit } D_1 = D_2 + \operatorname{div}(f).$$

Beispiel: Es ist $\operatorname{div}(x) = [0] - [\infty]$, also $[\infty] + \operatorname{div}(x) = [0]$, woraus

$$[0] \sim [\infty]$$

folgt.

LEMMA. *Die lineare Äquivalenz von Divisoren auf $\mathbb{P}^1$ ist eine Äquivalenzrelation.*

Beweis:

- $D \sim D$: Dies folgt aus $D = D + \operatorname{div}(1)$.
- $D_1 \sim D_2 \Longrightarrow D_2 \sim D_1$: Ist $D_1 \sim D_2$, so gibt es eine Funktion f mit $D_1 = D_2 + \operatorname{div}(f)$. Dann ist aber $D_2 = D_1 - \operatorname{div}(f) = D_1 + \operatorname{div}(\frac{1}{f})$, also $D_2 \sim D_1$.
- $D_1 \sim D_2, D_2 \sim D_3 \Longrightarrow D_1 \sim D_3$: Es gibt Funktionen f, g mit $D_1 = D_2 + \operatorname{div}(f)$ und $D_2 = D_3 + \operatorname{div}(g)$. Es folgt $D_1 = D_2 + \operatorname{div}(f) + \operatorname{div}(g) = D_2 + \operatorname{div}(fg)$, also $D_1 \sim D_3$. ■

Bemerkung: Man definiert die **Divisorenklassengruppe** von $\mathbb{P}^1$ als Faktorgruppe $\operatorname{Div}(\mathbb{P}^1)/\{\text{Hauptdivisoren}\}$. Sie mit mit $\operatorname{Pic}(\mathbb{P}^1)$ (Picard-Gruppe) bezeichnet. Für zwei Divisoren gilt

$$D_1 \sim D_2 \quad \Longleftrightarrow \quad \overline{D_1} = \overline{D_2} \text{ in } \operatorname{Pic}(\mathbb{P}^1).$$

Bemerkung: Die Definitionen der linearen Äquivalenz und der Picard-Gruppe verallgemeinern sich auf nichtsinguläre projektive Kurven. Auf $\mathbb{P}^1$ ist die lineare Äquivalenz aber einfach zu entscheiden:

SATZ. *Für $D_1, D_2 \in \operatorname{Div}(\mathbb{P}^1)$ gilt:*

$$D_1 \sim D_2 \quad \Longleftrightarrow \quad \operatorname{grad}(D_1) = \operatorname{grad}(D_2),$$

zwei Divisoren sind also genau dann linear äquivalent, wenn sie den gleichen Grad haben.

Beweis:

- $\Longrightarrow$ Sei $D_1 \sim D_2$. Dann existiert eine Funktion $f \in K(\mathbb{P}^1) \setminus \{0\}$ mit $D_2 = D_1 + \operatorname{div}(f)$. Es folgt

  $$\operatorname{grad}(D_2) = \operatorname{grad}(D_1 + \operatorname{div}(f)) = \operatorname{grad}(D_1) + \operatorname{grad}(\operatorname{div}(f)) = \operatorname{grad}(D_1),$$

  da Hauptdivisoren Grad 0 haben. Dies beweist die Behauptung.
- $\Longleftarrow$ Sei umgekehrt $\operatorname{grad}(D_1) = \operatorname{grad}(D_2)$. Für den Divisor $D = D_2 - D_1$ gilt dann $\operatorname{grad}(D) = \operatorname{grad}(D_2) - \operatorname{grad}(D_1) = 0$. Da aber auf $\mathbb{P}^1$ jeder Divisor vom Grad 0 ein Hauptdivisor ist, gibt es eine Funktion $f \in K(\mathbb{P}^1) \setminus \{0\}$ mit $D = \operatorname{div}(f)$, und damit

  $$D_2 = D_1 + D = D_1 + \operatorname{div}(f), \quad \text{also} \quad D_2 \sim D_1,$$

  wie behauptet. ■

Beispiel: Sind $\alpha_1, \alpha_2 \in K$, so gilt

$$[\alpha_1] + [\alpha_2] \sim 2[\infty],$$

da beide Divisoren gleichen Grad haben. Wir erhält man einen zugehörigen Hauptdivisor, d.h. eine Funktion f mit

$$[\alpha_1] + [\alpha_2] = 2[\infty] + \operatorname{div}(f)?$$

Wir setzen

$$f = (x - \alpha_1)(x - \alpha_2).$$

Dann ist

$$\operatorname{div}(f) = [\alpha_1] + [\alpha_2] - 2[\infty],$$

wie gewünscht.

4. Die Vektorräume $\mathcal{L}(D)$ und der Satz von Riemann-Roch für $\mathbb{P}^1$

Wir führen nun eine Ordnungsrelation für Divisoren ein:

DEFINITION. *Sind $D_1 = \sum m_P[P]$ und $D_2 = \sum n_P[P]$ zwei Divisoren auf $\mathbb{P}^1$, so definiert man*

$$D_1 \geq D_2 \iff m_P \geq n_P \text{ für alle } P \in \mathbb{P}^1.$$

(Dafür kann man natürlich auch $D_2 \leq D_1$ schreiben.) Man nennt einen Divisor D **effektiv**, *wenn $D \geq 0$ gilt.*

Beispiele: Es gilt

$$2[i] + 3[\pi] - [13] \geq [\pi] - [13] \geq -[13] \geq -5[13].$$

Der Divisor

$$3[\infty] + 4[\pi] + 7[13]$$

ist effektiv.

LEMMA. *Für Divisoren auf $\mathbb{P}^1$ gilt:*

- *$\geq$ ist eine Ordnungsrelation auf $\mathrm{Div}(\mathbb{P}^1)$.*
- *Jeder Divisor ist Differenz effektiver Divisoren.*
- *Jeder effektive Divisor hat Grad ≥ 0.*
- *Aus $D_1 \geq D_2$ folgt $\mathrm{grad}(D_1) \geq \mathrm{grad}(D_2)$.*
- *Aus $D_1 \geq D_2$ und $\mathrm{grad}(D_1) = \mathrm{grad}(D_2)$ folgt $D_1 = D_2$.*

Beweis:

- Die erste Eigenschaft folgt aus der entsprechenden für die ganzen Zahlen.
- Ist $D = \sum n_P[P]$, so kann man D so als Differenz effektiver Divisoren schreiben:

$$D = \sum_{\substack{P\in\mathbb{P}^1\\ n_P>0}} n_P[P] + \sum_{\substack{P\in\mathbb{P}^1\\ n_P<0}} n_P[P] = \left(\sum_{\substack{P\in\mathbb{P}^1\\ n_P>0}} n_P[P]\right) - \left(\sum_{\substack{P\in\mathbb{P}^1\\ n_P<0}} |n_P|[P]\right).$$

- Die dritte Eigenschaft folgt aus der vierten Eigenschaft.
- Ist $D_1 = \sum m_P[P]$ und $D_2 = \sum n_P[P]$, so ist $D_1 \geq D_2$ gleichwertig mit $m_P \geq n_P$ für alle P. Daraus folgt $\mathrm{grad}(D_1) = \sum m_P \geq \sum n_P = \mathrm{grad}(D_2)$, also die vierte Eigenschaft. Gilt zusätzlich $\mathrm{grad}(D_1) = \mathrm{grad}(D_2)$, also $\sum m_P = \sum n_P$, so folgt aus $m_P \geq n_P$ natürlich $m_P = n_P$ für alle Punkte P, also die fünfte Eigenschaft. ■

Welche effektiven Hauptdivisoren gibt es? D.h. für welche Funktionen $f \neq 0$ gilt $\mathrm{div}(f) \geq 0$, d.h. $\mathrm{ord}_P(f) \geq 0$ für alle $P \in \mathbb{P}^1$. Wir hatten zuvor gesehen, dass die einzigen Funktionen ohne Polstellen die Konstanten sind. Wir formulieren dies als Satz:

SATZ. *Für $f \in K(\mathbb{P}^1)$ haben wir die Äquivalenz:*

$$\mathrm{div}(f) \geq 0 \iff f \in K^* \iff \mathrm{div}(f) = 0.$$

Bemerkung: Was bedeutet $\mathrm{div}(f) \geq -n[P]$, wenn f eine Funktion, P ein Punkt und n eine natürliche Zahl ist? Es bedeutet, dass gilt

$$\mathrm{ord}_P(f) \geq -n \quad \text{und} \quad \mathrm{ord}_Q(f) \geq 0 \text{ für alle } Q \in \mathbb{P}^1 \setminus \{P\},$$

dass also f in P höchstens einen Pol n-ter Ordnung besitzt, sonst aber überall definiert ist. Wir schauen uns einen Spezialfall in folgendem Lemma an:

LEMMA. *Für eine Funktion $f \in K(\mathbb{P}^1) \setminus \{0\}$ und $n \in \mathbb{N}_0$ gilt*

$$\mathrm{div}(f) \geq -n[\infty] \iff f \text{ ist ein Polynom vom Grad } \leq n.$$

Beweis:

- Es gelte $\operatorname{div}(f) \geq -n[\infty]$. Dann ist
$$\operatorname{ord}_\beta(f) \geq 0 \text{ für alle } \beta \in K \quad \text{und} \quad \operatorname{ord}_\infty(f) \geq -n.$$
Wir schreiben $f = \frac{p(x)}{q(x)}$ als Quotient gekürzter Polynome. Wäre $q(x)$ nichtkonstant, so gäbe es ein $\beta \in K$ mit $q(\beta) = 0$, β wäre eine Polstelle von f und $\operatorname{ord}_\beta(f) \leq -1$, im Widerspruch zu $\operatorname{ord}_\beta(f) \geq 0$. Also ist $q(x)$ konstant und o.E. $q(x) = 1$. Wir haben also $f = p(x)$. Sei m der Grad von $p(x)$:
$$p(x) = p_0 + p_1 x + p_2 x^2 + \cdots + p_m x^m \text{ mit } p_m \neq 0.$$
Dann ist
$$f = p(x) = \frac{1}{u^m} \cdot (p_m + p_{m-1} u + \cdots + p_0 u^m) \quad \text{und} \quad \operatorname{ord}_\infty(f) = -m.$$
Aus $\operatorname{ord}_\infty(f) \geq -n$ folgt dann $m \leq n$, also die Behauptung.
- Die Umkehrung sieht man, wenn man den ersten Teil des Beweises rückwärts liest. ■

DEFINITION. *Für einen Divisor $D \subseteq \operatorname{Div}(\mathbb{P}^1)$ definiert man*
$$\mathcal{L}(D) = \{f \in K(\mathbb{P}^1)^* : D + \operatorname{div}(f) \geq 0\} \cup \{0\}.$$
($\mathcal{L}(D)$ ist eine Teilmenge des Funktionenkörpers $K(\mathbb{P}^1)$.) Ist $D = \sum_{P \in \mathbb{P}^1} n_P[P]$, so gilt
$$\mathcal{L}(D) = \{f \in K(\mathbb{P}^1)^* : \operatorname{ord}_P(f) \geq -n_P \text{ für alle } P \in \mathbb{P}^1\} \cup \{0\}.$$

Wir schreiben die letzte Darstellung in der Definition noch etwas ausführlicher: Ist $D = m_1[P_1] + \cdots + m_r[P_r] - n_1[Q_1] - \cdots - n_s[Q_s]$ mit $m_i, n_j \in \mathbb{N}$, so gilt für $f \in K(\mathbb{P}^1)^*$
$$\begin{aligned} f \in \mathcal{L}(D) \quad \Longleftrightarrow \quad & \operatorname{ord}_{P_1}(f) \geq -m_1, \ldots, \operatorname{ord}_{P_r}(f) \geq -m_r, \\ & \operatorname{ord}_{Q_1}(f) \geq n_1, \ldots, \operatorname{ord}_{Q_s}(f) \geq n_s, \\ & \operatorname{ord}_R(f) \geq 0 \text{ für alle } R \in \mathbb{P}^1 \setminus \{P_1, \ldots, P_r, Q_1, \ldots, Q_s\}, \end{aligned}$$
d.h. $\mathcal{L}(D)$ besteht genau aus den Funktionen, die in $P_1, \ldots, P_r$ höchstens einen Pol der Ordnung $m_1, \ldots, m_r$, in $Q_1, \ldots, Q_s$ mindestens eine Nullstelle der Ordnung $n_1, \ldots, n_s$ haben und sonst überall definiert sind.
Bemerkung: Die Definition
$$\mathcal{L}(D) = \{f \in K(\mathbb{P}^1)^* : D + \operatorname{div}(f) \geq 0\} \cup \{0\}$$
ist genau so gemacht, dass die folgende Menge von Divisoren
$$\{D + \operatorname{div}(f) : f \in \mathcal{L}(D) \setminus \{0\}\} \subseteq \operatorname{Div}(\mathbb{P}^1)$$
genau aus den effektiven Divisoren besteht, die linear äquivalent zu D sind.

Beispiel: Wir betrachten den Nulldivisor. Für eine Funktion $f \neq 0$ gilt:
$$f \in \mathcal{L}(0) \quad \Longleftrightarrow \quad \operatorname{div}(f) \geq 0 \quad \Longleftrightarrow \quad f \in K^*,$$
wobei wir die letzte Äquivalenz kurz zuvor gezeigt haben. Mit der 0 zusammen ergibt sich
$$\mathcal{L}(0) = K.$$

Beispiel: Mit dem vorangegangenen Lemma erhalten wir für $n \in \mathbb{N}$:
$$\begin{aligned} \mathcal{L}(n[\infty]) &= \{f \in K(\mathbb{P}^1)^* : \operatorname{div}(f) \geq -n[\infty]\} \cup \{0\} = \\ &= \{p_0 + p_1 x + \cdots + p_n x^n : p_0, p_1, \ldots, p_n \in K\} = \\ &= K + Kx + Kx^2 + \cdots + Kx^n. \end{aligned}$$

Da wir das Ergebnis noch benutzen werden, formulieren wir es als Satz:

SATZ. *Für $n \in \mathbb{N}_0$ gilt*
$$\begin{aligned} \mathcal{L}(n[\infty]) &= \{p_0 + p_1 x + \cdots + p_n x^n : p_0, p_1, \ldots, p_n \in K\} = \\ &= K + Kx + \cdots + Kx^n. \end{aligned}$$
$\mathcal{L}(n[\infty])$ ist der K-Vektorraum der Polynome vom Grad $\leq n$, eine K-Basis bilden die Monome $1, x, \ldots, x^n$. Insbesondere gilt $\dim \mathcal{L}(D) = n + 1$.

LEMMA. *Für einen Divisor $D \in \mathrm{Div}(\mathbb{P}^1)$ ist $\mathcal{L}(D)$ ein K-Vektorraum.*

Beweis:

- $0 \in \mathcal{L}(D)$: Dies gilt nach Definition von $\mathcal{L}(D)$.
- $\lambda \in K, f \in \mathcal{L}(D) \Longrightarrow \lambda f \in L(D)$: Ist $f \in \mathcal{L}(D) \setminus \{0\}$ und $\lambda \in K^*$, so folgt $D + \mathrm{div}(f) \geq 0$ und wegen $\mathrm{div}(\lambda f) = \mathrm{div}(f)$ auch $D + \mathrm{div}(\lambda f) \geq 0$, also $\lambda f \in \mathcal{L}(D)$.
- $f, g \in \mathcal{L}(D) \Longrightarrow f + g \in \mathcal{L}(D)$: Seien $f, g \in \mathcal{L}(D) \setminus \{0\}$. Ist $f + g = 0$, so gilt trivialerweise $f + g \in \mathcal{L}(D)$. Sei also $f + g \neq 0$. Schreiben wir $D = \sum n_P[P]$, so gilt
$$\mathrm{ord}_P(f) \geq -n_P \text{ und } \mathrm{ord}_P(g) \geq -n_P \text{ für alle } P \in \mathbb{P}^1.$$
Dies impliziert
$$\mathrm{ord}_P(f+g) \geq \min(\mathrm{ord}_P(f), \mathrm{ord}_P(g)) \geq -n_P,$$
und damit $f + g \in \mathcal{L}(D)$.

Dies beweist, dass $\mathcal{L}(D)$ ein K-Vektorraum ist. ■

LEMMA. *Für $D \in \mathrm{Div}(\mathbb{P}^1)$ und $f \in K(\mathbb{P}^1)^*$ gilt:*

- $\mathcal{L}(0) = K$.
- $\mathcal{L}(\mathrm{div}(f)) = K\frac{1}{f}$.
- $\mathcal{L}(D + \mathrm{div}(f)) = \frac{1}{f}\mathcal{L}(D)$.

Beweis:

- Dies haben wir bereits gezeigt.
- Für $g \in K(\mathbb{P}^1)^*$ gilt: $g \in \mathcal{L}(\mathrm{div}(f)) \iff \mathrm{div}(g) + \mathrm{div}(f) \geq 0 \iff \mathrm{div}(gf) \geq 0$, was äquivalent damit ist, dass gf konstant ist, d.h. $gf \in K$, also $g \in K\frac{1}{f}$. (Natürlich folgt die Eigenschaft auch aus (1) und (3).)
- Für $g \in K(\mathbb{P}^1)^*$ gilt:
$$\begin{aligned} g \in \mathcal{L}(D + \mathrm{div}(f)) &\iff D + \mathrm{div}(f) + \mathrm{div}(g) \geq 0 \iff \\ &\iff D + \mathrm{div}(fg) \geq 0 \iff \\ &\iff fg \in \mathcal{L}(D) \iff g \in \frac{1}{f}\mathcal{L}(D), \end{aligned}$$
was die Behauptung beweist. ■

Beispiel: Wir wollen für einen Punkt $P \in \mathbb{P}^1$ den K-Vektorraum $\mathcal{L}(-[P])$ bestimmen. Für $f \in K(\mathbb{P}^1)^*$ gilt:
$$f \in \mathcal{L}(-[P]) \iff \mathrm{div}(f) - [P] \geq 0 \iff \mathrm{div}(f) \geq [P].$$
f dürfte also keine Polstelle haben, müsste also konstant sein, andererseits müsste f aber in P eine Nullstelle haben. Das geht nicht, und daher folgt $\mathcal{L}(-[P]) = 0$.

Das Phänomen des letztes Satzes lässt sich leicht verallgemeinern:

SATZ. *Für $D \in \mathrm{Div}(\mathbb{P}^1)$ gilt die Implikation:*
$$\mathrm{grad}(D) < 0 \quad \Longrightarrow \quad \mathcal{L}(D) = 0.$$

Beweis: Angenommen, es gäbe eine Funktion $f \in \mathcal{L}(D) \setminus \{0\}$. Dann wäre $D + \mathrm{div}(f) \geq 0$, und damit $\mathrm{grad}(D + \mathrm{div}(f)) \geq 0$. Es würde
$$\mathrm{grad}(D) = \mathrm{grad}(D) + \mathrm{grad}(\mathrm{div}(f)) = \mathrm{grad}(D + \mathrm{div}(f)) \geq 0$$
folgen, im Widerspruch zur Voraussetzung $\mathrm{grad}(D) < 0$. Also muss $\mathcal{L}(D) = 0$ gelten. ■

Beschreibung von $\mathcal{L}(D)$ im Fall $\mathrm{grad}(D) \geq 0$: Wir schreiben
$$D = n_1[\alpha_1] + \cdots + n_r[\alpha_r] + n_\infty[\infty]$$

mit (beliebigen) ganzen Zahlen $n_1, \ldots, n_r, n_\infty$ und paarweise verschiedenen Zahlen $\alpha_1, \ldots, \alpha_r$ aus K. Wir definieren

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

Dann ist

$$\operatorname{div}(f) = n_1[\alpha_1] + \cdots + n_r[\alpha_r] - (n_1 + \cdots + n_r)[\infty]$$

und daher

$$D - \operatorname{div}(f) = (n_\infty + (n_1 + \cdots + n_r))[\infty] = \operatorname{grad}(D) \cdot [\infty].$$

Mit einem früheren Satz folgt

$$\begin{aligned} \mathcal{L}(D) &= \mathcal{L}(\operatorname{grad}(D)[\infty] + \operatorname{div}(f)) = \frac{1}{f}\mathcal{L}(\operatorname{grad}(D)[\infty]) = \\ &= \frac{1}{f}(K + Kx + \cdots + Kx^{\operatorname{grad}(D)}). \end{aligned}$$

Wir fassen das Ergebnis in einem Satz zusammen:

Satz. *Ist*

$$D = n_1[\alpha_1] + \cdots + n_r[\alpha_r] + n_\infty[\infty]$$

ein Divisor vom Grad ≥ 0 *mit paarweise verschiedenen Zahlen* $\alpha_1, \ldots, \alpha_r$ *und ganzen Zahlen* $n_1, \ldots, n_r, n_\infty$, *definiert man*

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

so gilt

$$\mathcal{L}(D) = K \cdot \frac{1}{f} + K \cdot \frac{x}{f} + K \cdot \frac{x^2}{f} + \cdots + K \cdot \frac{x^{\operatorname{grad}(D)}}{f},$$

die Funktionen $\frac{x^i}{f}$ *mit* $i = 0, \ldots, \operatorname{grad}(D)$ *bilden also eine* K*-Basis von* $\mathcal{L}(D)$. *Insbesondere gilt*

$$\dim \mathcal{L}(D) = \operatorname{grad}(D) + 1.$$

Beispiel: Wir betrachten $D = [1] + [2] + [3]$. Der Vektorraum $\mathcal{L}(D)$ besteht aus den Funktionen, die in 1,2,3 höchstens jeweils einen Pol 1. Ordnung haben und sonst überall definiert sind. Wir bilden

$$f = (x-1)(x-2)(x-3).$$

Wegen $\operatorname{grad}(D) = 3$ bilden die Funktionen

$$\frac{1}{(x-1)(x-2)(x-3)}, \quad \frac{x}{(x-1)(x-2)(x-3)}, \quad \frac{x^2}{(x-1)(x-2)(x-3)}, \quad \frac{x^3}{(x-1)(x-2)(x-3)}$$

eine Basis von $\mathcal{L}(D)$.

Die Dimensionsaussagen für $\mathcal{L}(D)$ fassen wir nochmals zusammen:

Satz (Riemann-Roch für $\mathbb{P}^1$). *Für einen Divisor* $D \in \operatorname{Div}(\mathbb{P}^1)$ *gilt*

$$\dim \mathcal{L}(D) = \begin{cases} 0 & \text{für } \operatorname{grad}(D) < 0, \\ \operatorname{grad}(D) + 1 & \text{für } \operatorname{grad}(D) \geq 0. \end{cases}$$

Beispiel: Für $n \in \mathbb{N}$ ist $\mathcal{L}(n[\infty])$ der Vektorraum der Polynome vom Grad $\leq n$. Eine Basis ist $1, x, x^2, \ldots, x^n$, die Dimension also $n + 1$, was mit $\operatorname{grad}(n[\infty]) + 1$ übereinstimmt.

Es gibt einen Satz von Riemann-Roch für nichtsinguläre projektive Kurven, der allerdings deutlich anspruchsvoller ist als der hier gezeigte Satz für $\mathbb{P}^1$.
Wir geben noch eine Darstellung für $\mathcal{L}(D)$ im Fall effektiver Divisoren an, die auf der Partialbruchzerlegung rationaler Funktionen beruht:

SATZ (Partialbruchzerlegung über einem algebraisch abgeschlossenen Grundkörper K). *Jede rationale Funktion $f \in K(x)^*$ hat eine (bis auf Summationsreihenfolge) eindeutige „Partialbruchzerlegung“*

$$\begin{aligned} f &= \left(\frac{b_{1,1}}{x-\alpha_1} + \frac{b_{1,2}}{(x-\alpha_1)^2} + \cdots + \frac{b_{1,n_1}}{(x-\alpha_1)^{n_1}}\right) + \cdots + \left(\frac{b_{r,1}}{x-\alpha_r} + \frac{b_{r,2}}{(x-\alpha_r)^2} + \cdots + \frac{b_{r,n_r}}{(x-\alpha_r)^{n_r}}\right) + \\ &\quad + c_0 + c_1 x + c_2 x^2 + \cdots + c_m x^m. \end{aligned}$$

Kürzer geschrieben:

$$f = \sum_{i=1}^{r} \sum_{j=1}^{n_i} \frac{b_{i,j}}{(x-\alpha_i)^j} + \sum_{k=0}^{m} c_k x^k.$$

Dabei sind $\alpha_i, b_{i,j}, c_k \in K$, $n_i \in \mathbb{N}$, $\alpha_1, \ldots, \alpha_r$ paarweise verschieden und $r, m \in \mathbb{N}_0$.

Beispiele:

$$\begin{aligned} \frac{1}{x^2-1} &= \frac{1}{(x-1)(x+1)} = \frac{\frac{1}{2}((x+1)-(x-1))}{(x-1)(x+1)} = \frac{\frac{1}{2}}{x-1} - \frac{\frac{1}{2}}{x+1}, \\ \frac{1}{x^2+1} &= \frac{1}{(x-i)(x+i)} = \frac{\frac{1}{2i}((x+i)-(x-i))}{(x-i)(x+i)} = \frac{\frac{1}{2i}}{x-i} - \frac{\frac{1}{2i}}{x+i}, \\ \frac{x^3}{x^2-1} &= \frac{\frac{1}{2}}{x-1} + \frac{\frac{1}{2}}{x-1} + x. \end{aligned}$$

Bemerkung: Wir betrachten $f \in K(\mathbb{P}^1)$ mit der Partialbruchzerlegung

$$f = \sum_{i=1}^{r} \sum_{j=1}^{n_i} \frac{b_{i,j}}{(x-\alpha_i)^j} + \sum_{k=0}^{m} c_k x^k,$$

wobei $\alpha_i, b_{i,j}, c_k \in K$, $n_i \in \mathbb{N}$, $\alpha_1, \ldots, \alpha_r$ paarweise verschieden und $r, m \in \mathbb{N}_0$ sind.
Wir betrachten die Polstellen der Summanden:

- $\frac{1}{(x-\alpha_i)^j}$ hat Ordnung $-j$ in α_i und ist sonst definiert.
- Daher: $\operatorname{ord}_{\alpha_i}(f) \geq -n_i$ mit Gleichheit, falls $b_{i,n_i} \neq 0$.
- x^k hat Ordnung $-k$ in ∞ und ist sonst definiert.
- Daher: $\operatorname{ord}_{\infty}(f) \geq -m$ mit Gleichheit, falls $c_m \neq 0$.
- In allen anderen Punkten gilt $\operatorname{ord}_P(f) \geq 0$.

Daraus ersieht man

$$f \in \mathcal{L}(n_1[\alpha_1] + \cdots + n_r[\alpha_r] + m[\infty]).$$

Durch Betrachtung der Partialbruchzerlegung ist auch umgekehrt leicht zu sehen, dass jedes Element aus $\mathcal{L}(n_1[\alpha_1] + \cdots + n_r[\alpha_r] + m[\infty])$ obige Gestalt hat. Wir fassen zusammen:

SATZ. *Seien $r, m \in \mathbb{N}_0$, $\alpha_1, \ldots, \alpha_r \in K$ paarweise verschieden, $n_1, \ldots, n_r \in \mathbb{N}$, $n_\infty \in \mathbb{N}_0$. Dann gilt für den effektiven Divisor*

$$D = n_1[\alpha_1] + \cdots + n_r[\alpha_r] + n_\infty[\infty]$$

$$\mathcal{L}(D) = \left\{ \sum_{i=1}^{r} \sum_{j=1}^{n_i} \frac{b_{i,j}}{(x-\alpha_i)^j} + \sum_{k=0}^{n_\infty} c_k x^k : b_{i,j}, c_k \in K \right\}.$$

Die Funktionen

$$\frac{1}{(x-\alpha_i)^j}, i = 1, \ldots, r, j = 1, \ldots, n_i, \quad x^k, k = 0, \ldots, n_\infty$$

bzw. ausgeschrieben

$$\frac{1}{x-\alpha_1}, \ldots, \frac{1}{(x-\alpha_1)^{n_1}}, \ldots, \frac{1}{x-\alpha_r}, \ldots, \frac{1}{(x-\alpha_r)^{n_r}}, 1, x, \ldots, x^{n_\infty}$$

bilden eine K-Basis von $\mathcal{L}(D)$. Insbesondere gilt $\dim \mathcal{L}(D) = \operatorname{grad}(D) + 1$.

Beispiel: Für $D = 2[3] + 3[2] + 5[\infty]$ ist

$$\frac{1}{x-3}, \frac{1}{(x-3)^2}, \frac{1}{x-2}, \frac{1}{(x-2)^2}, \frac{1}{(x-2)^3}, 1, x, x^2, x^3, x^4, x^5$$

eine K-Basis von $\mathcal{L}(D)$. Beim zuvor dargestellten Vorgehen bildet man

$$f = (x-3)^2(x-2)^3$$

und erhält dann wegen $\operatorname{grad}(D) = 10$ als K-Basis von $\mathcal{L}(D)$

$$\frac{1}{(x-3)^2(x-2)^3}, \quad \frac{x}{(x-3)^2(x-2)^3}, \quad \dots \quad \frac{x^{10}}{(x-3)^2(x-2)^3}.$$

5. Eine Anwendung in der Codierungstheorie

Beim Übertragen von Nachrichten auf elektronischem Weg können Fehler passieren. Was macht man, wenn z.B. die 0-1-Folge

`01001101011000010111010001101000011001010110110101100001011101000110100101101011`

gesendet wird, dafür aber

`00001001111000011011010001101000011001010011110100100001010101000110101101101011`

ankommt?
Die Idee der Codierungstheorie ist es, Redundanz einzufügen, sodass man trotz vorhandener Fehler auf die ursprüngliche Nachricht schließen kann.

Beispiel: Ersetzen wir 0 durch 000 und 1 durch 111, so wird beispielsweise die Folge 0110 zunächst in

$$000 \quad 111 \quad 111 \quad 000$$

übersetzt und dann gesendet. Erhält der Empfänger die Folge

$$010 \quad 111 \quad 011 \quad 000,$$

so liegt es nahe, dass

$$000 \quad 111 \quad 111 \quad 000$$

gemeint war; durch „Fehlerkorrektur“ erhält man also die ursprüngliche Nachricht. (Der „Code“ ist auch unter dem Namen Hamming-Code $[3,1]$ bekannt.)
Ein $[n,k]$**-Code** C (über $\mathbb{F}_2$) ist ein k-dimensionaler Untervektorraum von $\mathbb{F}_2^n$, er wird gegeben durch eine $k \times n$-Matrix $M = (m_{ij}) \in \mathrm{M}(k \times n, \mathbb{F}_2)$. (Die Zeilen von M bilden eine Basis von C.)
Die zu übertragende Nachricht, die als 0-1-Folge gegeben ist, unterteilt man in eine Folge von Blöcken $(a_1 \dots a_k)$ der Länge k. Der Block $(a_1 \dots a_k)$ wird dann transformiert in

$$(a_1 \dots a_k) \begin{pmatrix} m_{11} & m_{12} & \dots & m_{1n} \\ \vdots & \vdots & & \vdots \\ m_{k1} & m_{k2} & \dots & m_{kn} \end{pmatrix} = (b_1\, b_2 \dots b_n)$$

und der neue Block $(b_1 \dots b_n)$ wird gesendet.
Beispiel: Der Hamming-Code $[7,4]$ wird (beispielsweise) gegeben durch folgende Matrix

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

(SAGE: `codes.HammingCode(GF(2),3).generator_matrix()`). Je 4 Bits werden in 7 Bits umgewandelt:

```
0000 -> 0000000
0001 -> 0001111
0010 -> 0010110
0011 -> 0011001
0100 -> 0100101
0101 -> 0101010
0110 -> 0110011
0111 -> 0111100
1000 -> 1000011
1001 -> 1001100
1010 -> 1010101
```

```
1011 -> 1011010
1100 -> 1100110
1101 -> 1101001
1110 -> 1110000
1111 -> 1111111
```

Welche Eigenschaften soll ein guter Code haben?

- Gute Fehlerkorrektur.
- Hohe Informationsrate.
- Einfaches Codieren, einfaches Decodieren.

Wir werden die Situation etwas allgemeiner betrachten. Statt des Grundkörpers $\mathbb{F}_2$ werden wir einen allgemeinen Körper K zugrundelegen.
Codes: Ein $[n,k]$**-Code** C über einem Körper K ist ein k-dimensionaler Untervektorraum von K^n. Schreibt man eine Basis von C zeilenweise in eine Matrix, so erhält man eine $k \times n$-Matrix $M \in \mathrm{M}(k \times n, K)$, die auch Erzeugermatrix genannt wird. Eine Folge von k Zahlen aus K, also $(a_1 \dots a_k)$ wird dann zu $(b_1 \dots b_n)$ codiert mit

$$(b_1 \dots b_n) = (a_1 \dots a_k) \begin{pmatrix} m_{11} & \dots & m_{1n} \\ \vdots & & \vdots \\ m_{k1} & \dots & m_{kn} \end{pmatrix} : \quad (a_1 \dots a_k) \longrightarrow (b_1 \dots b_n).$$

Hamming-Abstand: Auf K^n definiert man den **Hamming-Abstand** zweier Vektoren $v, w \in K^n$ (mit $v = (v_1, \dots, v_n)$, $w = (w_1, \dots, w_n)$) durch

$$d_{\text{Hamming}}(v,w) = \#\{i : v_i \neq w_i\}.$$

Der Hamming-Abstand gibt also an, an wievielen Stellen sich die Vektoren unterscheiden.

Ist $C \subseteq K^n$ ein $[n,k]$-Code, so definiert man den **Minimalabstand** $d(C)$ des Codes durch

$$d(C) = \min\{d_{\text{Hamming}}(v,w) : v, w \in C, v \neq w\}.$$

Zwei verschiedene Wörter des Codes unterscheiden sich also an mindestens $d(C)$ Stellen. Da C ein Untervektorraum von K^n ist, gilt auch

$$d(C) = \min\{d_{\text{Hamming}}(v,0) : v \in C \setminus \{0\}\}.$$

Man nennt den Code dann auch einen $[n,k,d(C)]$-Code.
Beispiel: Der oben erwähnte Hamming-Code $[7,4]$ über $\mathbb{F}_2$ ist ein $[7,4,3]$-Code.

Beispiel: Wir betrachten in $\mathbb{F}_2^4$ den $\mathbb{F}_2$-Untervektorraum

$$C = \{(x_1,x_2,x_3,x_4) \in \mathbb{F}_2^4 : x_1 + x_2 + x_3 + x_4 = 0\}.$$

Die Elemente von C kann man leicht auflisten:

$$(0,0,0,0), (1,1,0,0), (1,0,1,0), (1,0,0,1), (0,1,1,0), (0,1,0,1), (0,0,1,1), (1,1,1,1).$$

Es ist $\dim(C) = 3$ und $d(C) = 2$. Also handelt es sich um einen $[4,3,2]$-Code über $\mathbb{F}_2$.

Goppa-Codes oder algebraisch-geometrische Codes: Goppa hat um 1975 bemerkt, dass man mit algebraischen Kurven interessante Codes konstruieren kann. Wir skizzieren zunächst die Idee:
Gegeben ist eine Kurve C, bei uns $\mathbb{P}^1$, ein Divisor D und Kurvenpunkte $P_1, \dots, P_n$. Dabei soll jede Funktion $f \in \mathcal{L}(D)$ in $P_1, \dots, P_n$ definiert sein. Dann ist

$$\alpha : \mathcal{L}(D) \to K^n, \quad f \mapsto (f(P_1), \dots, f(P_n))$$

eine K-lineare Abbildung. Also ist

$$C = \mathrm{Bild}(\alpha)$$

ein Code. Durch geeignete Parameterwahl kommt man zu interessanten Codes, worauf wir hier aber nicht eingehen wollen.

LEMMA. *Sei* $D = m_1[Q_1] + \dots + m_r[Q_r] \in \mathrm{Div}(\mathbb{P}^1)$ *ein Divisor.*

- *Ist $P \in \mathbb{P}^1 \setminus \{Q_1, \dots, Q_r\}$, so ist jede Funktion $f \in \mathcal{L}(D)$ in P definiert.*
- *Für paarweise verschiedene Punkte $P_1, \dots, P_n \in \mathbb{P}^1 \setminus \{Q_1, \dots, Q_r\}$ gilt*

$$f(P_1) = \cdots = f(P_n) = 0 \quad \Longleftrightarrow \quad f \in \mathcal{L}(D - [P_1] - \cdots - [P_n]).$$

Beweis:

- Ist $f \in \mathcal{L}(D) \setminus \{0\}$, so gilt $\operatorname{div}(f) + D \geq 0$, also $\operatorname{ord}_{Q_j}(f) \geq -m_j$ für $j = 1, \dots, r$ und $\operatorname{ord}_P(f) \geq 0$ für $P \in \mathbb{P}^1 \setminus \{Q_1, \dots, Q_r\}$. Dies beweist die Behauptung.
- Es gilt für $f \in \mathcal{L}(D) \setminus \{0\}$:

$$\begin{aligned} f(P_1) = \cdots = f(P_n) = 0 \quad &\Longleftrightarrow \quad \operatorname{ord}_{P_1}(f) \geq 1, \dots, \operatorname{ord}_{P_n}(f) \geq 1 \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad \operatorname{div}(f) \geq -m_1[Q_1] - \cdots - m_r[Q_r] + [P_1] + \cdots + [P_n] \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad \operatorname{div}(f) \geq -D + [P_1] + \cdots + [P_n] \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad \operatorname{div}(f) + D - [P_1] - \cdots - [P_n] \geq 0 \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad f \in \mathcal{L}(D - [P_1] - \cdots - [P_n]). \end{aligned}$$

  Es folgt die Behauptung. ■

Satz. *Sei $D = m_1[Q_1] + \cdots + m_r[Q_r] \in \mathbb{P}^1$ ein Divisor vom Grad ≥ 0 und $P_1, \dots, P_n \in \mathbb{P}^1 \setminus \{Q_1, \dots, Q_r\}$ paarweise verschiedene Punkte mit $n > \operatorname{grad}(D)$. Dann ist*

$$\alpha : \mathcal{L}(D) \to K^n, \quad f \mapsto (f(P_1), \dots, f(P_n))$$

eine injektive K-lineare Abbildung. $C = \operatorname{Bild}(\alpha)$ ist ein $[n, k, d]$-Code über K mit

$$k = \operatorname{grad}(D) + 1, \quad d = n - \operatorname{grad}(D).$$

(Es ist $k = \dim(C)$ die Dimension von C und $d = d(C)$ der Minimalabstand von C.)

Beweis:

- Das vorangegangene Lemma zeigt, dass die Abbildung α definiert ist. Die Linearität ist dann klar.
- Das Lemma zeigt:

$$\operatorname{Kern}(\alpha) = \mathcal{L}(D - [P_1] - \cdots - [P_n]).$$

  Nun gilt aber $\operatorname{grad}(D - [P_1] - \cdots - [P_n]) = \operatorname{grad}(D) - n < 0$, was $\mathcal{L}(D - [P_1] - \cdots - [P_n]) = 0$ und damit die Injektivität von α liefert.
- Es ist

$$k = \dim(C) = \dim(\operatorname{Bild}(\alpha)) = \dim(\mathcal{L}(D)) \overset{\text{RR}}{=} \operatorname{grad}(D) + 1.$$

- Sei $d = d(C)$. Dann gibt es eine Funktion $f \in \mathcal{L}(D) \setminus \{0\}$, sodass nach eventueller Umnummeriung der Punkte $P_1, \dots, P_n$ gilt

$$f(P_1) \neq 0, \dots, f(P_d) \neq 0, \quad f(P_{d+1}) = 0, \dots, f(P_n) = 0.$$

  Es folgt

$$f \in \mathcal{L}(D - [P_{d+1}] - \cdots - [P_n]) \setminus \{0\},$$

  und damit

$$0 \leq \operatorname{grad}(D - [P_{d+1}] - \cdots - [P_n]) = \operatorname{grad}(D) - (n - d) = \operatorname{grad}(D) - n + d,$$

  also

$$d \geq n - \operatorname{grad}(D).$$

- Wir konstruieren nun eine Funktion, die zeigt, dass die letzte Ungleichung sogar eine Gleichheit ist. Der Divisor

$$D - [P_1] - \cdots - [P_{\operatorname{grad}(D)}]$$

  hat Grad 0, also gibt es eine Funktion

$$f \in \mathcal{L}(D - [P_1] - \cdots - [P_{\operatorname{grad}(D)}]) \setminus \{0\}.$$

  Nach dem Lemma gilt

$$f(P_1) = \cdots = f(P_{\operatorname{grad}(D)}) = 0,$$

und damit

$$d_{\text{Hamming}}(\alpha(f)) \leq n - \text{grad}(D).$$

Dies impliziert

$$d \leq n - \text{grad}(D).$$

Zusammen mit der Abschätzung aus dem letzten Punkt folgt

$$d = n - \text{grad}(D),$$

wie behauptet. ■

Beispiel: Als Grundkörper betrachten wir $\mathbb{F}_5$ (oder $\overline{\mathbb{F}}_5$). Wir wählen

$$P_1 = 1, \quad P_2 = 2, \quad P_3 = 3, \quad P_4 = 4, \quad D = [\infty].$$

Dann ist $n = 4$ und $\text{grad}(D) = 1$, also $n > \text{grad}(D)$. Wir brauchen eine Basis von $\mathcal{L}(D) = \mathcal{L}([\infty])$ und wählen $f_1 = 1$, $f_2 = x$. In der zum Code gehörigen Erzeugermatrix stehen dann die Zahlen $f_i(\alpha)$ mit $i = 1, 2$ und $\alpha \in \{1, 2, 3, 4\}$:

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

Nach unserem Satz hat der Code Dimension $k = \text{grad}(D) + 1 = 2$ und Minimalabstand $d(C) = n - \text{grad}(D) = 3$. Es handelt sich also um einen $[4, 2, 3]$-Code über $\mathbb{F}_5$.

```
00 -> 0000
10 -> 1111
20 -> 2222
30 -> 3333
40 -> 4444
01 -> 1234
11 -> 2340
21 -> 3401
31 -> 4012
41 -> 0123
02 -> 2413
12 -> 3024
22 -> 4130
32 -> 0241
42 -> 1302
03 -> 3142
13 -> 4203
23 -> 0314
33 -> 1420
43 -> 2031
04 -> 4321
14 -> 0432
24 -> 1043
34 -> 2104
44 -> 3210
```

(SAGE kennt den Code als `codes.ReedSolomonCode(GF(5),4,2)`.

Literatur: [**Geer-Lint**], [**Luetkebohmert**]