Euklid'sche Ringe (Das Rechnen in $\mathbb{Z}$ und in $K[T]$).

Ist K ein Körper und $f \in K[T]$ ein Polynom, so nennt man f *normiert,* falls $f \neq 0$ gilt und der höchste Koeffizient von f gleich 1 ist. (Natürlich gilt: Jedes von Null verschiedene Polynom läßt sich eindeutig als Produkt eines normierten Polynoms und eines Elements $c \in K \setminus \{0\}$ schreiben.)

Vorbemerkung. Wir diskutieren hier gemeinsame Eigenschaften des Rings $\mathbb{Z}$ der ganzen Zahlen und der Polynomringe $K[T]$, wobei K ein Körper ist. In diesen Ringen ist das "Teilen mit Rest" möglich, dies wird im Begriff eines "euklid'schen Rings" axiomatisiert. Wir werden sehen, daß es in derartigen Ringen eine "eindeutige Primfaktorzerlegung" gibt. Ganz wichtig ist die "Bézout'sche Regel".

Teilbarkeit. Sei $(H, \cdot)$ eine kommutative Halbgruppe. Seien $a, b \in H$. Wir schreiben $b|a$ (und sagen b *teilt* a oder auch: b ist ein *Teiler* von a) falls es ein $b' \in H$ gibt mit $bb' = a$. Für jedes Element $a \in R$ schreiben wir $\mathcal{T}(a)$ für die Menge aller Teiler von a. Zwei Elemente a, a' heißen *assoziiert*, falls $\mathcal{T}(a) = \mathcal{T}(a')$ gilt. (Beispiel in $\mathbb{Z}$: es ist $\mathcal{T}(3) = \{\pm 1, \pm 3\} = \mathcal{T}(-3)$. Zwei Elemente $a, a' \in \mathbb{Z}$ sind genau dann assoziiert, wenn sie den gleichen Betrag haben. In $\mathbb{R}[T]$ enthält $\mathcal{T}(T^2-1)$ die Polynome 1, $T+1$, $T-1$ und T^2-1, aber auch die skalaren Vielfachen dieser Polynome mit skalarem Faktor $c \in R \setminus \{0\}$, also etwa auch $3T+3$ und $\frac{1}{2}T - \frac{1}{2}$.)

Sind $a_1, \ldots, a_n$ Elemente von H, so schreiben wir $\mathcal{T}(a_1, \ldots, a_n)$ für die Menge der gemeinsamen Teiler von $a_1, \ldots, a_n$, also $\mathcal{T}(a_1, \ldots, a_n) = \bigcap_i \mathcal{T}(a_i)$. Gibt es ein Element $b \in R$ mit $\mathcal{T}(b) = \mathcal{T}(a_1, \ldots, a_n)$, so nennt man b einen *größten gemeinsamen Teiler* (ggT) der Elemente $a_1, \ldots, a_n$. Die Elemente $a_1, \ldots, a_n$ heißen *teilerfremd*, falls die Menge $\mathcal{T}(a_1, \ldots, a_n)$ nur die invertierbaren Elemente von H enthält.

Wir nennen $p \in H$ ein *irreduzibles* Element, falls einerseits p nicht invertierbar ist und falls andererseits aus $p = p_1 p_2$ folgt, daß p_1 oder p_2 invertierbar ist. Beispiel: In $(\mathbb{Z}, \cdot)$ sind die irreduziblen Elemente gerade die Zahlen $\pm p$, wobei p eine Primzahl ist (das gleiche gilt in der Halbgruppe $(\mathbb{Z} \setminus \{0\}, \cdot)$.)

Wir sagen: $(H, \cdot)$ ist eine Halbgruppe *mit eindeutiger Primfaktorzerlegung*, falls die folgenden beiden Bedingungen erfüllt sind:

(1) (Existenz) Jedes nicht-invertierbare Element a läßt sich als Produkt $a = p_1 p_2 \cdots p_n$ mit irreduziblen Elementen p_i (und $n \geq 1$) schreiben,

(2) (Eindeutigkeit) Ist $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ mit irreduziblen Elementen p_i, q_i, so gilt $n = m$ und es gibt eine Permutation σ von $\{1, \ldots, n\}$ mit: $p_{\sigma(i)}$ ist zu q_i assoziiert, für $1 \leq i \leq n$.

Warnung: Die Eindeutigkeit der Primfaktorzerlegung ist nichts Selbstverständliches! Hier ein Beispiel einer Halbgruppe H ohne eindeutige Primfaktorzerlegung: die der "Viererzahlen" $H = (\{1, 4, 8, 12, 16, \dots\}, \cdot) = (\{1\} \cup 4\mathbb{N}_1, \cdot)$. Irreduzible Elemente sind:

$$4, 8, 12, 20, 24, 28, \dots$$

dagegen sind nicht irreduzibel: $16 = 4 \cdot 4$, $32 = 4 \cdot 8$ usw. Verschiedene Faktorisierungen haben:

$$64 = 8^2 = 4^3, \qquad 96 = 8 \cdot 12 = 4 \cdot 24.$$

Eines der Ziele dieses Abschnitts ist zu zeigen, daß sowohl $(\mathbb{Z} \setminus \{0\}, \cdot)$ als auch $(K[T] \setminus \{0\}, \cdot)$ (dabei sei K ein Körper) Halbgruppen mit eindeutiger Primfaktorzerlegung sind. Wir zeigen dies in zwei Schritten (Satz A und Satz B), dazu führen wir den Begriff eines "euklid'schen Rings" ein.

Unter einem *euklid'schen Ring* vestehen wir einen kommutativen Ring R mit einer Funktion $\rho\colon R \setminus \{0\} \to \mathbb{N}_0$ mit folgenden Eigenschaften:

(1) ("Nullteilerfreiheit") Sind $a, b \in R$ beide von Null verschieden, so ist auch ab von Null verschieden.

(2) Sind $a, b \in R$ beide von Null verschieden und ist b nicht invertierbar, so ist $\rho(a) < \rho(ab)$.

(3) ("Teilen mit Rest") Sind $a, b \in R$ gegeben mit $b \neq 0$, so gibt es $q, r \in R$ mit $a = qb + r$ und $r = 0$ oder $\rho(r) < \rho(b)$.

(Teilen mit Rest: r ist der Rest, wenn wir versuchen, a durch b zu teilen. Dabei soll eben entweder $r = 0$ gelten (dann ist b Teiler von a) oder r soll zumindest "klein" sein, und zwar "kleiner" als b, dies wird durch $\rho(r) < \rho(b)$ formuliert.)

Satz A. *Der Ring $R = \mathbb{Z}$ (mit $\rho(z) = |z|$) ist ein euklid'scher Ring. Ist K ein Körper, so ist der Polynomring $R = K[T]$ (mit $\rho(a) = \deg a$) ein euklid'scher Ring.*

(Beachte den kleinen Unterschied: Im Fall $R = \mathbb{Z}$ ist ρ auf ganz R definiert, im Fall $R = K[T]$ ist ρ nur für von Null verschiedene Elemente definiert, aber das ist alles, was wir brauchen).

Beweis von (3) im Fall $R = K[T]$. Ist $a = 0$, so ist nichts zu zeigen (nimm $q = 0$, $r = 0$). Also können wir $a \neq 0$ voraussetzen. Sei $a = \sum_{i=0}^{m} a_i T^i$ und $b = \sum_{j=1}^{n} b_i T^i$ mit $a_m \neq 0$ und $b_n \neq 0$. Ist $m < n$, so ist nichts zu zeigen: Nimm $q = 0$ und $r = a$, es ist $a = 0 \cdot b + r$ und $\deg r = \deg a < \deg b$. Sei nun $m \geq n$. Bilde nun $\frac{a_m}{b_n} T^{m-n}$ und bilde die Differenz $c = a - \frac{a_m}{b_n} T^{m-n} b$. Wir bilden also die Differenz zweier Polynome vom Grad m, diese Differenz hat demnach Grad höchstens m. Der

höchste Koeffizient ist $a_m - \frac{a_m}{b_n} b_n = 0$, also ist $\deg c < m$. Nach Induktion über den Grad können wir voraussetzen, daß sich c durch b mit Rest teilen läßt, etwa $c = q'b + r'$, mit $\deg r' < \deg b$. Demnach ist

$$a = c + \frac{a_m}{b_n} T^{m-n} b = q'b + r' + \frac{a_m}{b_n} T^{m-n} b = \big(q' + \frac{a_m}{b_n} T^{m-n}\big) b + r'.$$

Wir setzen also $q = q' + \frac{a_m}{b_n} T^{m-n}$ und $r' = r$.

Satz (Bézout). *Sei R ein euklid'scher Ring. Seien $g_1, \ldots, g_n \in R$: Dann gibt es h mit $\mathcal{T}(g_1, \ldots, g_n) = \mathcal{T}(h)$. Und für jedes h mit $\mathcal{T}(g_1, \ldots, g_n) = \mathcal{T}(h)$ gibt es Elemente $a_i \in R$ mit $h = \sum a_i g_i$.* (Der Satz besagt also: je n Elemente haben einen größten gemeinsamen Teiler und dieser läßt sich als Linearkombination darstellen.)

Beweis: Es genügt, den Fall $n = 2$ zu beweisen, der allgemeine Fall folgt dann mit Induktion.

Seien $f, g \in R$. Wir zeigen zuerst: es gibt $a, b \in R$ mit $\mathcal{T}(f, g) = \mathcal{T}(af + bg)$ (also: es gibt einen ggT und dieser ist als Linearkombination darstellbar.)

Ist $g = 0$, so ist $\mathcal{T}(f, g) = \mathcal{T}(f)$. Also können wir voraussetzen, daß f, g beide von Null verschieden sind. Sei $\rho(f) \geq \rho(g)$. Sei $f_0 = f, f_1 = g$. Teile f_0 durch f_1 mit Rest, also etwa $f_0 = q_1 f_1 + f_2$. Es ist entweder $f_2 = 0$ oder $\rho(f_1) > \rho(f_2)$. Ist $f_2 \neq 0$, so teilen wir f_1 durch f_2 mit Rest, usw. Algemein erhalten wir eine Folge von Gleichungen

$$\begin{aligned} f_0 &= q_1 f_1 + f_2 \\ f_1 &= q_2 f_2 + f_3 \\ &\cdots \\ f_{i-1} &= q_i f_i + f_{i+1} \end{aligned}$$

mit $\rho(f_1) > \rho(f_2) > \cdots > \rho(f_i) > \rho(f_{i+1})$. Da jede absteigende Folge natürlicher Zahlen abbricht, muß dieses Verfahren abbrechen, etwa nach n Schritten:

$$(*) \qquad \begin{aligned} f_{n-2} &= q_{n-1} f_{n-1} + f_n \\ f_{n-1} &= q_n f_n \end{aligned}$$

Haben wir eine Gleichung der Form $f = qg + r$, so gilt offensichtlich $\mathcal{T}(f, g) = \mathcal{T}(g, r)$. Wir sehen also hier:

$$\mathcal{T}(f, g) = \mathcal{T}(f_0, f_1) = \mathcal{T}(f_1, f_2) = \cdots \mathcal{T}(f_{n-1}, f_n) = \mathcal{T}(f_n),$$

das Element f_n ist also ein größter gemeinsamer Teiler.

Die i-te Gleichung zeigt jeweils, daß sich f_{i+1} als Linearkombination von f_{i-1} und f_i ausdrücken läßt:

$$f_{i+1} = f_{i-1} - q_i f_i.$$

Wir verwenden nun zuerst die Gleichung $(*)$, um f_n als Linearkombination von f_{n-2} und f_{n-1} auszudrücken

$$f_n = f_{n-2} - q_{n-1} f_{n-1}$$

und ersetzen jeweils f_{i+1} durch $f_{i-1} - q_i f_i$, für $i = n-1, n-2, \ldots, 3, 2$. Dies zeigt: f_n läßt sich in der Form $af_0 + bf_1 = af + bg$ mit $a, b \in R$ schreiben.

Sei nun h beliebig mit $\mathcal{T}(h) = \mathcal{T}(f, g)$. Wegen $\mathcal{T}(h) = \mathcal{T}(f, g) = \mathcal{T}(af + bg)$ ist $af + bg$ ein Teiler von h, etwa $h = c(af + bg)$ für ein $c \in R$. Dann ist aber $h = a'f + b'g$ mit $a' = ca$ und $b' = cb$. Damit ist der Satz bewiesen.

Man nennt dieses Verfahren den **Euklid'schen Algorithmus zur Bestimmung des ggT.** (Genauer: **eines** ggT, denn in einem beliebigen euklid'schen Ring braucht es kein Verfahren zu geben, um in der Menge der Elemente h mit $\mathcal{T}(h) = \mathcal{T}(f, g)$ ein wohlbestimmten Element auszuwählen. Im Ring $\mathbb{Z}$ nimmt man im Fall daß mindestens eines der Elemente f, g von Null verschieden ist, die (einzige) positive Zahl h mit $\mathcal{T}(h) = \mathcal{T}(f, g)$, im Polynomring $K[T]$ das (einzige) normierte Polynom h mit dieser Eigenschaft, und nennt dies **den** ggT von f und g.)

Folgerung. *Sei R ein euklid'scher Ring. Ist $p \in R$ irreduzibel und ist p ein Teiler von uv $(u, v \in R)$, so ist p ein Teiler von u oder von v.*

Beweis: Sei etwa $pc = uv$. Wir nehmen an, daß p kein Teiler von u ist. Dann sind p, u teilerfremd, also gibt es $a, b \in R$ mit $1 = ap + bu$. Also ist $v = (ap + bu)v = apv + buv = apv + bpc = p(av + bc)$.

Satz B. *Ist R ein euklid'scher Ring, so ist $(R \setminus \{0\}, \cdot)$ eine Halbgruppe mit eindeutiger Primfaktorzerlegung.*

Beweis: Als erstes zeigen wir die Existenzaussage: jedes nicht-invertierbare Element a läßt sich als Produkt $a = p_1 p_2 \cdots p_n$ mit irreduziblen Elementen p_i (und $n \geq 1$) schreiben. Sei also $a \in R \setminus \{0\}$ nicht-invertierbar. Wir verwenden Induktion nach $\rho(a)$. Ist a selbst irreduzibel, so ist nichts zu zeigen. Andernfalls können wir a in der Form $a = bc$ schreiben, wobei keiner der beiden Faktoren b, c invertierbar ist. Dann ist aber $\rho(b) < \rho(a)$ und auch $\rho(c) < \rho(a)$, wegen der Bedingung (2) in der Definition eines euklid'schen Rings. Nach Induktion lassen sich b, c beide als Produkte von irreduziblen Elementen schreiben, also auch a.

Nun die Eindeutigkeit: Sei $a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ mit irreduziblen Elementen p_i, q_i. Hier verwenden wir Induktion nach n. Wir sehen, daß p_1 ein Teiler von $q_1 \cdots q_m$ ist, also ist p_1 ein Teiler von q_j für ein j; nach Umnumerieren der q_i können wir voraussetzen $j = 1$, also ist p_1 ein Teiler von q_1, etwa $p_1 p_1' = q_1$. Da q_1 irreduzibel ist, muß p_1' invertierbar sein, also sind die Elemente p_1 und q_1 assoziiert. Falls $n = 1$ folgt aus $p_1 = p_1(p_1' q_2 \cdots q_m)$, daß $p_1' q_2 \cdots q_m = 1$ gilt, denn R ist nullteilerfrei und $p_1 \neq 0$. Daraus folgt aber $m = 1$.

Sei nun $n > 1$. Wieder verwenden wir die Nullteilerfreiheit und schließen aus $p_1 p_2 \cdots p_n = p_1 p_1' q_2 \cdots q_m$, daß gilt $p_2 p_n = p_1' q_2 \cdots q_m$. Da p_1' invertierbar ist, ist mit q_2 auch $p_1' q_2$ irreduzibel, also steht rechts ein Produkt von $m-1$ irreduziblen Faktoren. Nach Induktion sehen wir $n - 1 = m - 1$, und es gibt eine Permutation σ der Indizes $2, \ldots, n$, so daß $p_{\sigma(2)}$ und $p_1' q_2$ assoziert sind und entsprechend für $i > 2$ jeweils $p_{\sigma(i)}$ und q_i assoziiert sind. Natürlich ist dann auch $p_{\sigma(1)}$ zu q_2 assoziiert. Da wir schon wissen, daß p_1 und q_1 assoziert sind, folgt die Behauptung.

Eindeutige Primfaktorzerlegung im Ring $\mathbb{Z}$. *Jede von Null verschiedene ganze Zahl a läßt sich eindeutig als Produkt*

$$a = \epsilon p_1 \ldots p_n$$

schreiben mit $\epsilon = \pm 1$ und Primzahlen $p_1 \leq p_2 \leq \cdots \leq p_n$ mit $n \geq 0$.

Eindeutige Primfaktorzerlegung in Polynomringen. *Sei K ein Körper. Jedes von Null verschiedene Polynom $f \in K[T]$ läßt sich in der Form*

$$f = \gamma p_1 \ldots p_n$$

schreiben mit $\gamma \in K \setminus \{0\}$ und normierten irreduziblen Polynomen $p_1, p_2, \ldots, p_n$ mit $n \geq 0$. Ist $\gamma p_1 \ldots p_n = \delta q_1 \ldots q_m$ mit $\gamma, \delta \in K \setminus \{0\}$ und normierten irreduziblen Polynomen p_i, q_j, so ist $n = m$, $\gamma = \delta$, und es gibt eine Permutation σ von $\{1, 2, \ldots, n\}$ mit $p_{\sigma(i)} = q_i$ für alle i.

Wir verwenden, daß in $\mathbb{Z}$ jedes irreduzible Element zu einer positiven Primzahl assoziiert ist, und daß entsprechend in $K[T]$ jedes irreduzible Polynom zu einem normierten irreduziblen Polynom assoziiert ist. In $\mathbb{Z}$ haben wir zusätzlich die Möglichkeit, die auftretenden Primzahlen der Größe nach zu notieren, auf diese Weise erhalten wir eine eindeutige Faktorisierung. In $K[T]$ erhalten wir Eindeutigkeit bis auf Permutation.

Ist $f = \gamma p_1 \cdots p_n$ mit $\gamma \in K \setminus \{0\}$ und normierten irreduziblen Polynomen p_i, so nennt man die Anzahl der Indizes i mit $p = p_i$ die *Vielfachheit von p in f*. Ist $p = T - \delta$ mit $\delta \in K$, so nennt man die Vielfachheit von $T - \delta$ in f die *Vielfachheit der Nullstelle δ*.