Leitfaden: Lineare Algebra II

Einschub: 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 in diesem Abschnitt 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" $H = (\{1, 4, 8, 12, 16, \ldots\}, \cdot) = (\{1\} \cup 4\mathbb{N}_1, \cdot)$. Irreduzible Elemente sind:

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

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 $r' = r$.

Hier ein Beispiel für das Teilen mit Rest: Sei $a = T^4 - T^3 + T - 1$, $b = T^3 - 1$. Dann ist

$$T^4 - T^3 + T - 1 = (T - 1)(T^3 - 1) + (2T - 2)$$

(hier ist also $q = T - 1$ und $r = 2T - 2$). Beim Rechnen geht man wie bei der

schriftlichen Division vor:

$$\begin{array}{rl} (T^4 - T^3 \quad\quad + T \;\; - 1 \;) : (T^3 - 1) \;=\; \underbrace{T - 1}_{q} \\ \underline{T^4 \quad\quad\quad\quad - T} \\ \quad -T^3 \quad + 2\,T \\ \quad \underline{-T^3 \quad\quad\quad + 1} \\ \quad\quad\quad \underbrace{2\,T \;\; - 2}_{r} \end{array}$$

Folgerung. *Sei $f \in K[T]$ und $\gamma \in K$. Genau dann gilt $f(\gamma) = 0$, wenn $T - \gamma$ ein Teiler von f ist.*

Beweis. Einerseits: Sei $(T - \gamma)g = f$. Ersetze T durch γ. Links erhalten wir 0, also $f(\gamma) = 0$. Umgekehrt: Sei $f(\gamma) = 0$. Teile f duch $T - \gamma$ mit Rest, also $f = q \cdot (T - \gamma) + r$ mit Polynomen q, r, wobei entweder $r = 0$ gilt oder aber $r \neq 0$ und $\deg r < \deg(T - \gamma) = 1$. In jedem Fall ist r ein konstantes Polynom. Ersetze in $f = q \cdot (T - \gamma) + r$ die Variable T durch γ. Wir erhalten $r(\gamma) = 0$, d.h. einsetzen von γ in das konstante Polynom r liefert 0, das heißt aber: $r = 0$.

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.)

Beispiel 1. Betrachte die Zahlen 255 und 221. Es ist

$$\begin{aligned}
&(1) && 255 = 1 \cdot 221 + 34 \\
&(2) && 221 = 6 \cdot 34 \ + 17 \\
&(3) && 34 = 2 \cdot 17 \ + 0
\end{aligned}$$

demnach ist 17 der ggT von 255 und 221. Zurückrechnen liefert

$$\begin{aligned}
17 &\overset{(2)}{=} 221 - 6 \cdot 34 \\
&\overset{(1)}{=} 221 - 6 \cdot (255 - 221) \\
&= 7 \cdot 221 - 6 \cdot 255
\end{aligned}$$

Beispiel 2. Betrachte die beiden Polynome $f = T^3 + 2$ und $g = T^3 + T^2 + 1$. Wir teilen mit Rest:

$$\begin{aligned}
&(1) && T^3 + 2 = && 1 \cdot (T^3 + T^2 + 1) && + (-T^2 + 1) \\
&(2) && (T^3 + T^2 + 1) = && (-T - 1) \cdot (-T^2 + 1) && + (T + 2) \\
&(3) && (-T^2 + 1) = && (-T + 2) \cdot (T + 2) && + (-3) \\
&(4) && (T + 2) = && (-\tfrac{1}{3}T - \tfrac{2}{3}) \cdot (-3) &&
\end{aligned}$$

Wir sehen also: die Polynome f und g sind teilerfremd. Rechnen wir rückwärts, so erhalten wir:

$$\begin{aligned}
-3 &\overset{(3)}{=} (-T^2+1)-(-T+2)(T+2)\\
&\overset{(2)}{=} (-T^2+1)-(-T+2)\big((T^3+T^2+1)-(-T-1)(-T^2+1)\big)\\
&= \big(1-(-T+2)(T+1)\big)(-T^2+1)-(-T+2)(T^3+T^2+1)\\
&= (T^2-T-1)(-T^2+1)-(-T+2)(T^3+T^2+1)\\
&\overset{(1)}{=} (T^2-T-1)\big((T^3+2)-(T^3+T^2+1)\big)-(-T+2)(T^3+T^2+1)\\
&= (T^2-T-1)(T^3+2)+\big(-(T^2-T-1)-(-T+2)\big)(T^3+T^2+1)\\
&= (T^2-T-1)f+(-T^2+2T-1)g,
\end{aligned}$$

also auch

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

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 $a=p_1p_2\cdots p_n$ 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 $a=p_1p_2\cdots p_n=q_1q_2\cdots q_m$ 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 $p_1p_1'=q_1$. 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 $p_1p_2\cdots p_n=p_1p_1'q_2\cdots q_m$, daß gilt $p_2p_n=p_1'q_2\cdots q_m$. 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*

$$a = \epsilon p_1 \dots p_n$$

schreiben mit $\epsilon = \pm 1$ und Primzahlen $p_1 \leq p_2 \leq \dots \leq p_n$ 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*

$$f = \gamma p_1 \dots p_n$$

schreiben mit $\gamma \in K \setminus \{0\}$ und normierten irreduziblen Polynomen $p_1, p_2, \dots, p_n$ mit $n \geq 0$. Ist $\gamma p_1 \dots p_n = \delta q_1 \dots q_m$ 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 $\{1, 2, \dots, n\}$ 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*.

Irreduzible Polynome. Für jeden Körper K sind die Polynome der Form $T - a$ mit $a \in K$ irreduzibel. Ob dies die einzigen normierten irreduziblen Polynome sind, hängt vom Körper K ab. Hier einige Spezialfälle:

$\mathbb{C}$. Der "Fundamentalsatz der Algebra" besagt gerade, daß jedes irreduzible Polynom über $\mathbb{C}$ linear ist; die einzigen normierten irreduziblen Polynome in $\mathbb{C}[T]$ sind also die Polynome der Form $T - a$ mit $a \in \mathbb{C}$.

$\mathbb{R}$. Der "Fundamentalsatz der Algebra" läßt sich auch so formulieren: jedes irreduzible Polynom über $\mathbb{R}$ hat Grad 1 oder 2. Die normierten irreduziblen Polynome in $\mathbb{R}[T]$ vom Grad 2 sind gerade die Polynome der Form $T^2 + a_1 T + a_0$ mit $a_1^2 < 4a_0$ (und dies sind gerade die Polynome der Form $(T - a)^2 + c$ mit $a, c \in \mathbb{R}$ und $c > 0$).

$\mathbb{Q}$. Zu jeder natürlichen Zahl $n \geq 1$ gibt es irreduzible Polynome in $\mathbb{Q}[T]$ vom Grad n, zum Beispiel $T^n - 2$. Das Studium der irreduziblen Polynome in $\mathbb{Q}[T]$ ist eine wichtige Aufgabe von Algebra und Zahlentheorie.

$\mathbb{Z}/p\mathbb{Z}$, mit p Primzahl. Auch hier gibt es zu jeder natürlichen Zahl $n \geq 1$ irreduzible Polynome in $\mathbb{Z}/p\mathbb{Z}[T]$ vom Grad n.

Bemerkung. Wir haben gesehen: In euklid'schen Ringen kann jedes von Null verschiedene Element als Produkt von irreduziblen Elementen geschrieben werden. Eine derartige Faktorisierung zu finden kann aber mit viel Aufwand verbunden sein! Man verwendet dies heute zum Verschlüsseln von Nachrichten. Leicht dagegen ist die Bestimmung größter gemeinsamer Teiler, denn hier gibt es ein effektives Verfahren, den euklid'schen Algorithmus.

Das Minimal-Polynom einer quadratischen Matrix. Sei K ein Körper und $A \in M(n \times n, K)$. Sei $\mu_A \in K[T]$ ein normiertes Polynom kleinstmöglichen Grads mit $\mu_A(A) = 0$. *Ist $f \in K[T]$ ein Polynom mit $f(A) = 0$, so ist μ_A ein Teiler von f.* (Beweis: Teile f durch μ_A mit Rest, etwa $f = q\mu_A + r$ und setze die Matrix A ein, wir erhalten $r(A) = 0$. Da nach Voraussetzung μ_A den kleinstmöglichen Grad hat, muß $r = 0$ gelten.) Daraus folgt:

(a) *Das Polynom μ_A ist eindeutig bestimmt* (man nennt μ_A das *Minimalpolynom* von A).

(b) *Das Minimalpolynom μ_A ist ein Teiler des charakteristischen Polynoms χ_A.*

(c) *Ähnliche Matrizen haben das gleiche Minimalpolynom.* (Seien A, B ähnliche Matrizen, also $B = S^{-1}AS$ mit einer invertierbaren $(n \times n)$-Matrix S. Es ist $0 = \mu_B(B) = \mu_B(S^{-1}AS) = S^{-1}\mu_B(A)S$, also $\mu_B(A) = 0$ und demnach ist μ_A ein Teiler von μ_B. Entsprechend ist aber μ_B auch ein Teiler von μ_A).

Lemma. *Sei K ein Körper, sei $A \in M(n \times n, K)$. Hat das Minimalpolynom μ_A den Grad m, so gilt: Alle Potenzen A^i mit $i \in \mathbb{N}_0$ liegen im Unterraum* $\operatorname{span}(I, A, A^2, \ldots, A^{m-1})$ *des Vektorraums $M(n \times n, K)$.*

Beweis: Sei $\mu_A(T) = \sum_{j=0}^{m} a_j T^j$ mit $a_j \in K$ und $a_m = 1$. Wegen $\mu_A(A) = 0$ gilt $\sum_{j=0}^{m} a_j A^j = 0$, also

$$A^m = -\sum_{j=0}^{m-1} a_j A^j.$$

Multiplizieren wir diese Gleichung mit A^s mit $s \geq 0$, so erhalten wir

$$A^{m+s} = -\sum_{j=0}^{m-1} a_j A^{j+s}.$$

Dies zeigt: Die Matrizen der Form A^{m+s} mit $s \geq 0$ lassen sich als Linearkombinationen von Matrizen der Form A^r mit $r < m + s$ schreiben. Induktiv sieht man, daß sich die Matrizen der Form A^{m+s} mit $s \geq 0$ als Linearkombination der Matrizen der Form A^r mit $r < m$ schreiben lassen.

Folgerung. *Sei K ein Körper, sei $A \in M(n \times n, K)$. Das Minimalpolynom μ_A habe den Grad m. Ist $v \in K^n$, so sind die Vektoren $v, Av, \ldots, A^m v$ linear abhängig.*

Beweis: Es ist $A^m \in \operatorname{span}(I, A, A^2, \ldots, A^{m-1})$, also $A^m = \sum_{i=0}^{m-1} c_i A^i$ mit $c_i \in K$. Dann ist $A^m v = \sum_{i=0}^{m-1} c_i A^i v$.

Lemma. *Seien $c_0, \ldots, c_{n-1} \in K$. Die Matrix*

$$A = \begin{bmatrix} 0 & \cdots & \cdots & 0 & c_0 \\ 1 & \ddots & & \vdots & c_1 \\ 0 & 1 & \ddots & \vdots & c_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & c_{n-1} \end{bmatrix}$$

hat das Minimalpolynom $T^n - \sum_{i=0}^{n-1} c_i T^i$. (Man nennt diese Matrix A die *Begleitmatrix* zum Polynom $T^n - \sum_{i=0}^{n-1} c_i T^i$).

Beweis: Man rechnet leicht nach $\chi_A = T^n - \sum_{i=0}^{n-1} c_i T^i$. Zu zeigen ist, daß das Minimalpolynom den Grad n hat. Es ist $Ae_i = e_{i+1}$, für $0 \leq i \leq n-1$, demnach ist $A^i e_1 = e_{i+1}$, ebenfalls für $0 \leq i \leq n-1$. Insbesondere sehen wir, daß die Vektoren $A^i e_1$ mit $0 \leq i \leq n-1$ linear unabhängig sind. Also hat das Minimalpolynom μ_A den Grad n. Da μ_A Teiler von χ_A ist, muß $\mu_A = \chi_A$ gelten.

Folgerung. *Ist p ein normiertes Polynom in $K[T]$ vom Grad n, so gibt es $A \in M(n \times n, K)$ mit $\mu_A = p$.*

Wir wissen, daß das Minimalpolynom μ_A ein Teiler des charakteristischen Polynoms χ_A ist. Schreiben wir also $\chi_A = p_1^{e_1} \cdots p_s^{e_s}$ mit paarweise verschiedenen normierten irreduziblen Polynomen $p_1, \ldots, p_s$ und natürlichen Zahlen $e_i \in \mathbb{N}_1$, so sieht man

$$\mu_A = p_1^{d_1} \cdots p_s^{d_s} \quad \text{mit Vielfachheiten} \quad 0 \leq d_i \leq e_i.$$

Bemerkung: Man kann zeigen, daß immer $1 \leq d_i$ gilt: Jeder irreduzible Faktor von χ_A ist auch Faktor von μ_A; die beiden Polynome χ_A und μ_A unterscheiden sich höchstens durch die Vielfachheiten, mit denen ein solcher Faktor auftritt. (Für den allgemeinen Fall muß auf die Vorlesung ALGEBRA verwiesen werden. Ist $p_i = T - \gamma$ ein **linearer** Faktor von χ_A, so sieht man sehr einfach, daß p_i auch ein Faktor von μ_A sein muß: Ist $T - \gamma$ Teiler von χ_A, so ist γ ein Eigenwert von A, es gibt also einen Vektor $0 \neq v \in K^n$ mit $Av = \gamma v$. Wäre $T - \gamma$ kein Faktor des Minimalpolynoms μ_A, so wären die Polynome μ_A und $T - \gamma$ teilerfremd. Es gäbe dann Polynome a, b mit $a \cdot \mu_A + b \cdot (T - \gamma) = 1$. Setze hier die Matrix A ein und wende beide Seiten, also $a(A) \cdot \mu_A(A) + b(A) \cdot (A - \gamma I_n)$ und I_n, auf v an: links erhalten wir den Nullvektor, rechts den Vektor v. Dies ist unmöglich, denn Eigenvektoren sind von Null verschieden.)

(4.5) A-invariante Unterräume.

Sei $A \in M(n \times n, K)$. Ein Unterraum $U \subseteq K^n$ heißt *A-invariant,* falls gilt: Ist $u \in U$, so ist $Au \in U$. Entsprechend wird definiert: Ist $f\colon V \to V$ ein Endomorphismus eines Vektorraums V, so heißt ein Unterraum $U \subseteq V$ *f-invariant*, falls $f(u) \in U$ für alle $u \in U$ gilt.

Ist v ein Eigenvektor von $f\colon V \to V$, so ist $\operatorname{span}(v)$ ein f-invarianter Unterraum von V, der eindimensional ist. Auch umgekehrt gilt: Ist U ein eindimensionaler f-invarianter Unterraum von V, so ist jeder von Null verschiedene Vektor $v \in U$ ein Eigenvektor.

Wofür braucht man A-invariante Unterräume?

Offensichtlich gilt: Sei U ein A-invarianter Unterraum von K^n der Dimension m. Sei $u_1, \ldots, u_m$ eine Basis von U, setze sie durch $u_{m+1}, \ldots u_n$ zu einer Basis von K^n fort. Bezüglich dieser Basis $(u_1, \ldots, u_n)$ hat f_A eine Matrizen-Darstellung der Form

$$\begin{bmatrix} B & D \\ 0 & C \end{bmatrix},$$

dabei ist B eine $(m \times m)$-Matrix.

Sind A-invariante Unterräume U, V mit $U \cap V = 0$ und $U + V = K^n$ gegeben, so nennt man das Paar (U, V) eine *A-invariante Zerlegung* des K^n. Wählt man eine Basis $u_1, \ldots, u_m$ von U und eine Basis $u_{m+1}, \ldots, u_n$ von V, so hat f_A bezüglich dieser Basis $(u_1, \ldots, u_n)$ eine Matrizen-Darstellung der Form

$$\begin{bmatrix} B & 0 \\ 0 & C \end{bmatrix},$$

dabei ist B wieder eine $(m \times m)$-Matrix.

Seien U, W Unterräume eines Vektorraums V. Gilt $U \cap W = 0$ und $U + W = V$, so schreibt man $U \oplus W = V$ und sagt, daß V die *direkte Summe* der Unterräume U und W ist. Beachte: genau dann gilt $V = U \oplus W$, wenn sich jedes Element $v \in V$ eindeutig in der Form $v = u + w$ mit $u \in U, w \in W$ schreiben läßt.

Allgemeiner: Sind $U_1, \ldots, U_s$ Unterräume eines Vektorraums V und läßt sich jedes Element $v \in V$ eindeutig in der Form $v = \sum_{i=1}^{s} u_i$ mit $u_i \in U_i$ schreiben, so nennt man V die *direkte Summe* der Unterräume U_i und schreibt $V = \bigoplus_{i=1}^{s} U_i = U_1 \oplus U_2 \oplus \cdots \oplus U_s$. Genau dann gilt $V = \bigoplus_{i=1}^{s} U_i$, wenn einerseits $V = \sum_{i=1}^{s} U_i$ gilt und andererseits $U_j \cap \sum_{i \neq j} U_i = 0$ für alle $1 \leq j \leq s$ gilt.

Ist $f \colon V \to V$ ein Endomorphismus und läßt sich V als direkte Summe $V = \bigoplus_{i=1}^{s} U_i$ schreiben mit f-invarianten Unterräumen U_i, und wählen wir Basen der Unterräume U_{γ_i}, so erhalten wir als Vereinigung eine Basis von K^n und bezüglich dieser Basis hat f eine Matrizendarstellung der Form

$$A = \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & A_s \end{bmatrix},$$

dabei ist A_i eine Matrizendarstellung der Einschränkung der Abbildung f auf U_i. Zur Abkürzung schreibt man $A = \bigoplus_{i=1}^{s} A_i$ oder auch nur $A = \bigoplus_i A_i$.

Wie findet man A-invariante Unterräume?

Lemma. *Sind $A, B \in M(n \times n, K)$ mit $AB = BA$, so ist* $\operatorname{Ker} f_B = \{v \in K^n \mid Bv = 0\}$ *ein A-invarianter Unterraum.*

Beweis: Sei $Bu = 0$. Dann ist auch $B(Au) = 0$, denn $BAu = ABu = A0 = 0$.

Wie findet man zu einer Matrix A Matrizen B mit $AB = BA$? Am einfachsten: man nimmt für B eine Matrix der Form $B = p(A)$ mit $p \in K[T]$.

Sei $A \in M(n \times n, K)$ mit charakteristischem Polynom χ_A. Schreibe

$$\chi_A = g_1 \cdots g_s$$

mit paarweise teilerfremden Polynomen $g_1, \ldots, g_s$. Für jedes Polynom g_i setze

$$U(g_i) = \{v \in K^n \mid g_i(A)v = 0\}.$$

Lemma. *Alle Unterräume $U(g_i)$ sind A-invariant und es ist $K^n = \bigoplus_{i=1}^s U(g_i)$.*

Beweis: Für jedes i schreiben wir

$$\chi_A = g_i h_i, \quad \text{dabei ist} \quad h_i = g_1 \cdots g_{i-1} g_{i+1} \cdots g_s.$$

Beachte: Die Polynome $h_1, \ldots, h_s$ sind teilerfremd, also gibt es Polynome a_i mit $\sum_{i=1}^s a_i h_i = 1$. Da g_i und h_i teilerfremd sind, gibt es Polynome b_i, c_i mit $b_i g_i + c_i h_i = 1$.

(1) Wegen $A \cdot g_i(A) = g_i(A) \cdot A$ wissen wir, daß $U(g_i)$ ein A-invarianter Unterraum ist.

(2) Es ist $V = \sum U(g_i)$. Denn sei $v \in K^n$. Setze $v_i = a_i(A)h_i(A)v$. Dieser Vektor v_i gehört zu $U(g_i)$, denn

$$g_i(A)v_i = g_i(A)a_i(A)h_i(A)v = a_i(A)\chi_A(A)v = 0.$$

Wegen $\sum_{i=1}^s a_i h_i = 1$ ist $\sum v_i = v$.

(3) Für jedes i gilt $U(g_i) \cap \sum_{j \neq i} U(g_j) = 0$. Zum Beweis bemerken wir, daß $h_i(A)U(g_j) = 0$ für jedes $i \neq j$ gilt, da g_j ein Teiler von h_i ist. Daraus folgt $h_i \sum_{j \neq i} U(g_j) = 0$. Ist nun u im Durchschnitt $U(g_i) \cap \sum_{j \neq i} U(g_j) = 0$, so ist sowohl $g_i(A)u = 0$ als auch $h_i(A)u = 0$. Also ist $u = \big(b_i(A)g_i(A) + c_i(A)h_i(A)\big)u = 0$.

(4.4) Die Jordan'sche Normalform.

Sei K ein Körper. Sei $A \in M(n \times n, K)$ eine Matrix, deren charakteristisches Polynom in Linearfaktoren zerfällt. Sei also

$$\chi_A = (T - \gamma_1)^{e_1} \cdots (T - \gamma_s)^{e_s}$$

mit paarweise verschiedenen $\gamma_i \in K$ und mit natürlichen Zahlen $e_i \in \mathbb{N}_1$.

Wir wenden die Überlegungen des letzten Abschnitts mit $g_i = (T - \gamma_i)^{e_i}$ an. Wir betrachten also für jedes i den Unterraum

$$U_{\gamma_i} = \{v \in K^n \mid (A - \gamma_i I_n)^{e_i} v = 0\},$$

man nennt ihn den *Hauptraum* zum Eigenwert γ_i.

Alle Unterräume U_{γ_i} sind A-invariant und es ist

$$K^n = \bigoplus_{i=1}^s U_{\gamma_i}.$$

Wählen wir Basen der Unterräume U_{γ_i}, so erhalten wir eine Basis von K^n und bezüglich dieser Basis hat A eine Matrizendarstellung der Form

$$\begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & A_s \end{bmatrix},$$

dabei ist A_i eine Matrizendarstellung der Einschränkung der Abbildung $u \mapsto Au$ auf U_{γ_i}.

Nach Definition von U_{γ_i} ist die Einschränkung der Abbildung $u \mapsto Au$ auf U_{γ_i} eine Abbildung g_i mit $(g_i - \gamma_i \cdot 1)^{e_i} = 0$. Es bleibt also die Aufgabe, Endomorphismen f eines endlich-dimensionalen Vektorraums zu beschreiben, für die $(f - \gamma \cdot 1)^e = 0$ für ein $\gamma \in K$ und $e \in \mathbb{N}_1$ gilt.

Satz. *Sei V ein n-dimensionaler Vektorraum, sei $\gamma \in K$. Sei $f\colon V \to V$ ein Endomorphismus mit $(f - \gamma \cdot 1)^e = 0$. Dann gibt es eine Partition λ von n, so daß f bezüglich einer geeigneten Basis von V die Matrix-Darstellung $\gamma I_n + J(\lambda)$ hat.*

Die Matrizen, die wir hier betrachten, haben also die Form $\gamma I_n + J(\lambda)$; hier als typisches Beispiel wieder der Fall $\lambda = (5,4,2,2,1,1)$:

$$\gamma I_{15} + J((5,4,2,2,1,1)) = \begin{bmatrix} \gamma & 1 & & & & & & & & & & & & & \\ & \gamma & 1 & & & & & & & & & & & & \\ & & \gamma & 1 & & & & & & & & & & & \\ & & & \gamma & 1 & & & & & & & & & & \\ & & & & \gamma & & & & & & & & & & \\ & & & & & \gamma & 1 & & & & & & & & \\ & & & & & & \gamma & 1 & & & & & & & \\ & & & & & & & \gamma & 1 & & & & & & \\ & & & & & & & & \gamma & & & & & & \\ & & & & & & & & & \gamma & 1 & & & & \\ & & & & & & & & & & \gamma & & & & \\ & & & & & & & & & & & \gamma & 1 & & \\ & & & & & & & & & & & & \gamma & & \\ & & & & & & & & & & & & & \gamma & 1 \\ & & & & & & & & & & & & & & \gamma \end{bmatrix}$$

Satz. *Sei K ein Körper. Sei $A \in M(n \times n, K)$ eine Matrix, deren charakteristisches Polynom in Linearfaktoren zerfällt. Dann gibt es paarweise verschiedene Elemente $\gamma_1, \ldots, \gamma_s \in K$ und zu jedem γ_i eine Partition $\lambda^{(i)}$, so daß A ähnlich zur Matrix $\bigoplus_i \big(\gamma_i I_{n_i} + J(\lambda^{(i)})\big)$ ist.*

Ist A ähnlich zur Matrix $\bigoplus_{i=1}^{s} \big(\gamma_i I_{n_i} + J(\lambda^{(i)})\big)$, wobei $\gamma_1, \ldots, \gamma_s$ paarweise verschiedene Elemente aus K sind, jedes $\lambda^{(i)}$ eine Partition von n_i ist, für $1 \le i \le s$ (mit $\sum_i n_i = n$), so sind die γ_i die Eigenwerte von A, die Vielfachheit von $T - \gamma_i$ in χ_A ist n_i, die Vielfachheit von $T - \gamma_i$ in μ_A ist $\lambda^{(i)}_1$.

Man nennt eine Matrix der Form $\bigoplus_i \big(\gamma_i I_{n_i} + J(\lambda^{(i)})\big)$ eine *Jordan'sche Normalform.*

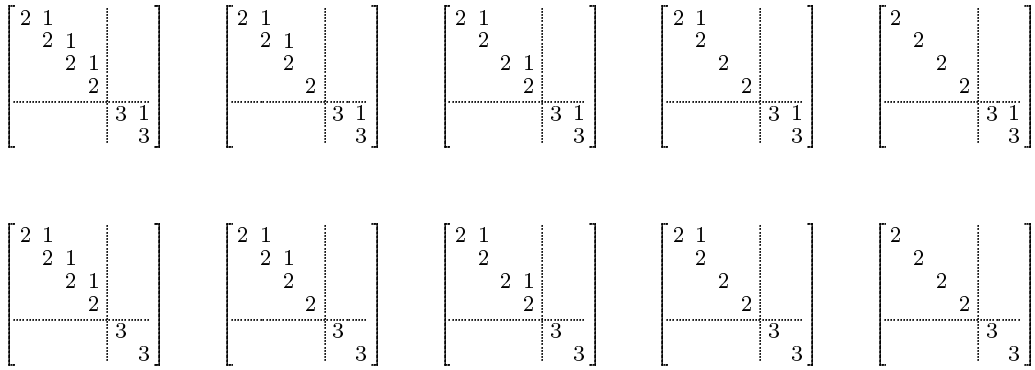
Eindeutigkeit. Vertauscht man die einzelnen Blöcke $\gamma_i I_{n_i} + J(\lambda^{(i)})$ untereinander, so erhält man eine zur gegebenen Matrix ähnliche Matrix. Bis auf derartige Vertauschungen ist die Jordan'sche Normalform eindeutig: *Sind zwei Matrizen $\bigoplus_i \big(\gamma_i I_{n_i} + J(\lambda^{(i)})\big)$ und $\bigoplus_i \big(\delta_i I_{n_i} + J(\nu^{(i)})\big)$ ähnlich, so gibt es eine Permutation σ mit $\gamma_i = \delta_{\sigma(i)}$ und $\lambda^{(i)} = \nu^{(\sigma(i))}$.* Dies folgt zum Beispiel daraus, daß man zu jedem Eigenwert γ_i die zugehörige Partition $\lambda^{(i)}$ wie folgt berechnen kann:

Verfahren zur Bestimmung der Jordan'schen Normalform. Sei $\gamma = \gamma_i$ ein Eigenwert von A. Wie sieht die zugehörige Partition $\lambda = \lambda^{(i)}$ aus? Betrachte die Matrizen der Form

$$\gamma I_n - A,\ (\gamma I_n - A)^2,\ (\gamma I_n - A)^3,\ \ldots$$

Sei r_i der Rang der Matrix $(\gamma I_n - A)^i$ für $i \geq 1$ und $r_0 = n$ (dies ist natürlich gerade der Rang der Matrix $(\gamma I_n - A)^0 = I_n$). *Es ist* $(r_0 - r_1, r_1 - r_2, \dots)$ *die zu* λ *duale Partition.*

Hier alle Jordan'schen Normalformen von Matrizen mit charakteristischem Polynom $(T-2)^4(T-3)^2$:



Folgerung. *Sei* K *ein Körper. Sei* $A \in M(n \times n, K)$ *eine Matrix, deren charakteristisches Polynom in Linearfaktoren zerfällt. Dann läßt sich* A *als Summe einer diagonalisierbaren Matrix* A' *und einer nilpotenten Matrix* A''*, mit* $A'A'' = A''A'$ *schreiben.*

Beweis: Wir wissen, daß A zu einer Matrix der Form $B = \bigoplus_i \big(\gamma_i I_{n_i} + J(\lambda^{(i)})\big)$ ähnlich ist, es gibt also eine invertierbare Matrix S mit $A = S^{-1}BS$. Wir können $B = B' + B''$ schreiben mit $B' = \bigoplus_i \gamma_i I_{n_i}$ und $B'' = \bigoplus_i J(\lambda^{(i)})$. Die Matrix B' ist eine Diagonalmatrix, B'' ist nilpotent, und man sieht leicht, daß $B'B'' = B''B'$ gilt. Setze $A' = S^{-1}A'S$ und $A'' = S^{-1}B''S$. Dann ist A' diagonalisierbar, A'' nilpotent, und es ist

$$A'A'' = S^{-1}B'SS^{-1}B''S = S^{-1}B'B''S = S^{-1}B''B'S = A''A'.$$

Warnung: Ob ein Polynom in Linearfaktoren zerfällt oder nicht, ist davon abhängig, welchen Körper man als Grundkörper betrachtet. *Ist* f *ein Polynom, so gibt es einen endlichen Erweiterungskörper, über dem* f *in Linearfaktoren zerfällt.* (Algebra I) Jeder Körper ist einbettbar in einen "algebraisch abgeschlossenen" Körper: in ihm zerfällt jedes Polynom in Linearfaktoren (Algebra I). Arbeiten wir mit dem Körper $\mathbb{R}$ der reellen Zahlen, und ist $f \in \mathbb{R}[T]$, so zerfällt f über dem Körper $\mathbb{C}$ der komplexen Zahlen in Linearfaktoren (dies ist der schon öfters erwähnte "Fundamentalsatz der Algebra").