# Vorlesung Lineare Algebra II

SoSe '20 hhu
K. Halupczok

## §2: Normalformentheorie

## l8: Der Euklidische Algorithmus

eukl. Algo

**Stichworte:** Grad eines Polynoms, Polynom-Division mit Rest, Teilbarkeit, ggT, teilerfremd, Satz von Bézout = Darstellbarkeit des ggT als L.K., Berechnung der Bézout-Koeffizienten

---

Wir erarbeiten hier noch weitere Ergebnisse über $K[T]$, inwieweit man Polynome durch andere "teilen" kann und mit einer sukzessiven Polynomdivision mit Rest den größten gemeinsamen Teiler zweier Polynome berechnen kann. ~"Euklidischer Algo"

8.1. **Def.:** Ist $p = \sum_{i=0}^{n} a_i T^i \in K[T]$, so heißt $m := \max\{i; a_i \neq 0\}$ der **Grad von $p$**, Kurz: $\deg(p) = m$ für "Degree". (Vgl. Def. L8.13 in LA I).
Weiter heißt $a_m$ der **höchste Koeffizient / Leitkoeffizient** von $p$.
Ist er 1, so heißt $p$ **normiert**.
Ist $p = 0$, d.h. das **Nullpolynom**, in dem alle Koeffizienten $= 0$ sind, so setzen wir $\deg(0) = -\infty$.

8.2. **Bem.:** Für den Grad gelten die Regeln: $\deg(p+q) \leq \max(\deg(p), \deg(q))$,
$\deg(p \cdot q) = \deg(p) + \deg(q)$
(natürlich auch in Sonderfällen, wenn z.B. $p = 0$ ist. Genau dafür wurde die Setzung $\deg(0) = -\infty$ gemacht).
Die Wiederholung aus LA I, L8.25 ist dieser wichtige Satz über die **Polynomdivision:**

8.3. **Satz (Division mit Rest):** Zu je zwei Polynomen $p_1, p_2$ (mit $p_2 \neq 0$) gibt es eindeutig bestimmte Polynome $q, r$ mit $\deg(r) < \deg(p_2)$, so dass $p_1 = q p_2 + r$ gilt.

8.4. **Bsp.:** $(T^3 - T + 1) : (T+2) = T^2 - 2T + 3$, Rest $-5$

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

Rest $= -3$

Also: $\underbrace{T^3 - T + 1}_{p_1} = \underbrace{(T^2 - 2T + 3)}_{\text{Quotient } q} \cdot \underbrace{(T+2)}_{p_2} \underbrace{- 5}_{r}$

$(T^3 - T + 1) : (T + 2) = T^2 - 2T + 3$ Rest $-5$

$-(T^3 + 2T^2)$

$-2T^2 - T + 1$

$-(-2T^2 - 4T)$

$3T + 1$

$-(3T + 6)$

$-5$

↳ genau wie für LA I, L 8.25, dort L 8.27.

8.5 **Bew.:** • Ist $\deg(p_1) < \deg(p_2)$, setze $q := 0$, $r := p_1$. Sei also $\deg(p_1) =: m_1 \geq m_2 := \deg(p_2)$, und $p_1 = \sum_{i=0}^{m_1} \alpha_i T^i$, $p_2 = \sum_{i=0}^{m_2} \beta_i T^i$, wo $\alpha_{m_1} \neq 0 \neq \beta_{m_2}$. Setzen $q_1 := \frac{\alpha_{m_1}}{\beta_{m_2}} \cdot T^{m_1 - m_2}$ und $r_1 := p_1 - q_1 p_2$. Dann ist $p_1 = q_1 p_2 + r_1$ und $\deg(r_1) \leq m_1 - 1 < \deg(p_1)$, da wir gerade den nächsten Koeff. annuliert haben. Fertig, wenn $\deg(r_1) < \deg(p_2)$. Andernfalls können wir mit $r_1$ statt $p_1$ dieselbe Konstruktion nochmal machen und erhalten $q_2, r_2$ mit $\deg(r_2) < \deg(r_1)$ so, dass $r_1 = q_2 p_2 + r_2$. Dann ist $p_1 = q_1 p_2 + r_1 = q_1 p_2 + q_2 p_2 + r_2 = (q_1 + q_2) p_2 + r_2$ mit $\deg(r_2) \leq \deg(p_1) - 2$. Wir iterieren dies, bis schließlich bei einem $k$-ten Schritt der dann erhaltene Rest $r_k$ die Ungleichung $\deg(r_k) < \deg(p_2)$ erfüllt. Dann fertig.

• Die Eindeutigkeit folgt so: Sei $p_1 = q_1 p_2 + r_1$ und $p_1 = q_2 p_2 + r_2$ mit $\deg(r_i) < \deg(p_2)$ für $i = 1, 2$. Dann ist $\underbrace{(q_1 - q_2) p_2}_{\text{Grad} \geq \deg(p_2)} = \underbrace{r_2 - r_1}_{\text{Grad} < \deg(p_2)}$ falls $q_1 \neq q_2$ ↯.

Also: $q_1 = q_2$ und $r_1 = r_2$. □

8.6 **Def.:** Ein Polynom $p_2$ teilt ein Polynom $p_1$, wenn ein Polynom $q$ existiert mit $p_1 = p_2 q$. Ein Polynom $p$ heißt ein gemeinsamer Teiler von $p_1, \dots, p_m$, wenn $p$ jedes $p_i$ teilt. Ein Polynom $p$ heißt ein größter gemeinsamer Teiler von $p_1, \dots p_m$, in Zeichen: $p = \mathrm{ggT}(p_1, \dots, p_m)$, falls

1.) $p$ gemeinsamer Teiler von $p_1, \dots, p_m$ und

2.) jeder gemeinsame Teiler von $p_1, \dots, p_m$ auch $p$ teilt.

Polynome heißen teilerfremd, wenn (bis auf Normierung) 1 ihr größter gemeinsamer Teiler ist.

→ Abkürzung: schreiben $p_2 \mid p_1$ für "$p_2$ teilt $p_1$", d.h. $p_2 \mid p_1 :\Leftrightarrow \exists q : p_1 = p_2 q$.

8.7 **Bsp.:** $(T-1) \mid (T^3 - 1)$, da $(T^3 - 1) : (T-1) = T^2 + T + 1$, geht restlos auf.

$$\begin{array}{r} -(T^3 - T^2) \\ \hline T^2 - 1 \\ -(T^2 - T) \\ \hline T - 1 \\ -(T - 1) \\ \hline 0 \end{array}$$

← ohne Rest

• $\mathrm{ggT}(T-1, T^3-1) = \overbrace{T-1}^{\text{normiert}}$, aber auch $= 1 - T$ oder $= 2 - 2T$

Ein ggT ist nicht eindeutig bestimmt, bzw. "bis auf Normierung" eindeutig bestimmt.

$$(T^n - 1) : (T - 1) = T^{n-1} + T^{n-2} + \ldots + T + 1$$

$$\begin{array}{r} -(T^n - T^{n-1}) \\ \hline T^{n-1} - 1 \\ -(T^{n-1} - T^{n-2}) \\ \hline T^{n-2} - 1 \\ \vdots \\ T^2 - 1 \\ -(T^2 - T) \\ \hline T - 1 \\ -(T - 1) \\ \hline 0 \end{array}$$

$$\sum_{i=0}^{n-1} x^i = \frac{x^n - 1}{x - 1}, \quad x \neq -1$$

$$ggT(2^3 \cdot 3^4 \cdot 11^2,\ 2^2 \cdot 3^2 \cdot 5) = 2^2 \cdot 3^2$$

$$ggT(12345,\ 113) = ?$$

Den ggT kann man (wie auch für $\mathbb{Z}$) mit dem euklidischen Algorithmus berechnen, und i.a. sogar sehr schnell (was wir hier nicht zeigen):

8.8. **Satz (Euklidischer Algorithmus):** Seien $p_1, p_2 \in K[T] \setminus \{0\}$, führen sukzessive, d.h. fortlaufend, eine Division mit Rest durch:

Ist $p_{n+1} \neq 0$, so sei $p_{n+2}$ der bei der Division von $p_n$ (geteilt) durch $p_{n+1}$ auftretende Rest, d.h. $\boxed{p_n = p_{n+1} \cdot q_n + p_{n+2}}$ mit $\deg(p_{n+2}) < \deg(p_{n+1})$, für $n = 1, 2, 3, \ldots$

Ist dann $m$ der größte Index mit $p_m \neq 0$, so ist $p_m = ggT(p_1, p_2)$, d.h. der letzte Rest $\neq 0$ ist größter gemeinsamer Teiler von $p_1$ und $p_2$.

**Bew.:** • OE sei $\deg(p_1) \geq \deg(p_2)$. Laut Satz 8.3 (Div. mit Rest) haben wir dann $\deg p_1 \geq \deg p_2 > \deg p_3 > \deg p_4 > \ldots$ Der Algorithmus bricht jedenfalls ab.

• Sei nun $p_m$ der letzte nichtverschwindende Rest bei dieser Kette von Divisionen. Dann haben wir

$$\begin{aligned}
p_1 &= p_2 \cdot q_1 + p_3 \\
p_2 &= p_3 \cdot q_2 + p_4 \\
&\vdots \\
p_{m-2} &= p_{m-1} \cdot q_{m-2} + p_m && \leftarrow \text{letzter Rest} \neq 0, \\
p_{m-1} &= p_m \cdot q_{m-1} && \leftarrow \text{geht restlos auf.}
\end{aligned}$$

Damit ist $p_m \mid p_{m-1}$, denn mit $s_{m-1} := q_{m-1}$ gilt $p_{m-1} = s_{m-1} p_m$.

Weiter: $p_m \mid p_{m-2}$, denn $p_{m-2} = p_{m-1} \cdot q_{m-2} + p_m = \underbrace{(s_{m-1} q_{m-2} + 1)}_{=: s_{m-2}} p_m$,

weiter $p_m \mid p_{m-3}$, ... Die Fortsetzung/Iteration dieses Schlusses zeigt dann $p_m \mid p_2$ und $p_m \mid p_1$, d.h. $p_m$ ist gemeinsamer Teiler von $p_1$ und $p_2$.

• Ist nun $d$ (irgend) ein gemeinsamer Teiler von $p_1$ und $p_2$, so ex. Polynome $s_1, s_2$ mit $p_1 = s_1 d$, $p_2 = s_2 d$. Dann ist $p_3 = p_1 - p_2 q_1 = s_1 d - s_2 d q_1$, also $p_3 = (s_1 - s_2 q_1) \cdot d$, d.h. $d \mid p_3$.

Wenden wir dies auf $p_2, p_3$ an, folgt wie eben $d \mid p_4$, dann $d \mid p_5$ usw.

Durch Fortsetzung/Iteration dieses Schlusses folgt: $d \mid p_m$.

• Also gilt: 1.) $p_m \mid p_1$, $p_m \mid p_2$, 2.) $d \mid p_1$, $d \mid p_2 \Rightarrow d \mid p_m$.

Nach Def. von "ggT" folgt also $p_m = ggT(p_1, p_2)$. □

8.9 **Bsp.:** Zeigen eukl. Algo für $p_1 = 15T^6 - 17T^5 - 11T^4 + 7T^3 + 19T^2 + 20T + 2$
und $p_2 = 15T^4 - 2T^3 + 2T^2 - 8T$.

Für die Divisionen mit Rest $p_1 = p_2 q_1 + p_3$, $p_2 = p_3 q_2 + p_4$, $p_3 = p_4 q_3 + p_5$, ... erhalten wir:

$15T^6 - 17T^5 - 11T^4 + 7T^3 + 19T^2 + 20T + 2 = (15T^4 - 2T^3 + 2T^2 - 8T) \cdot (T^2 - T - 1) + \underbrace{p_3}_{\text{Rest}}$

$-(15T^6 - 2T^5 + 2T^4 - 8T^3)$
$-15T^5 - 13T^4 + 15T^3 + 19T^2$
$-(-15T^5 + 2T^4 - 2T^3 + 8T^2)$
$-15T^4 + 17T^3 + 11T^2 + 20T$
$-(-15T^4 + 2T^3 - 2T^2 + 8T)$
$15T^3 + 13T^2 + 12T + 2$ ← Rest $=: p_3$, denn $\deg p_3 < \deg p_2 = 4$

Mit dem eben erhaltenen Rest $p_3 := 15T^3 + 13T^2 + 12T + 2$ führen wir die Division "$p_2$ geteilt durch $p_3$" durch, um den nächsten Rest $p_4$ zu erhalten:

$15T^4 - 2T^3 + 2T^2 - 8T = (15T^3 + 13T^2 + 12T + 2) \cdot (T - 1) + p_4$

$-(15T^4 + 13T^3 + 12T^2 + 2T)$
$-15T^3 - 10T^2 - 10T$
$-(-15T^3 - 13T^2 - 12T - 2)$
$3T^2 + 2T + 2$ ← Rest $=: p_4$, denn $\deg p_4 < \deg p_3 = 3$

Wenn man nun mit dem jetzt erhaltenen Rest $p_4$ noch einen Schritt weiter rechnet, erhält man den Rest $p_5 = 0$. Laut Satz 8.8 ist dann $p_4 = ggT(p_1, p_2)$.

8.10. **Bem.:** Der eukl. Algo ist immer in Ringen durchführbar, die eine Division mit Rest zulassen (und deswegen "euklidischer Ring" heißen). Das ist auch für $\mathbb{Z}$ möglich:

$p_1 = p_2 \cdot q_1 + p_3$, **Bsp.:** $12378 = 3054 \cdot 4 + 162$ → $p_3 < p_2$
$p_2 = p_3 \cdot q_2 + p_4$ $3054 = 162 \cdot 18 + 138$ → $p_4 < p_3$
$p_3 = p_4 \cdot q_3 + p_5$ $162 = 138 \cdot 1 + 24$ ⋮
⋮ $138 = 24 \cdot 5 + 18$
letzter Rest $\neq 0$ sei $p_m$ ⇝ $p_m = ggT(p_1, p_2)$ $24 = 18 \cdot 1 + 6$ → $p_7 < p_6$ ⇝ $p_7 = 6 = ggT(12378, 3054)$.
$18 = 6 \cdot 3 + 0$ $p_8 = 0$

ges.: $ggT(p_1, p_2) = ?$

$p_1 = p_2 \cdot q_1 + p_3$,
$p_2 = p_3 \cdot q_2 + p_4$
$p_3 = p_4 \cdot q_3 + p_5$
⋮
⋮
$p_{m-2} = p_{m-1} q_{m-2} + p_m$
$p_{m-1} = p_m \cdot q_{m-1} + 0$

$p_m$: letzter Rest $\neq 0$

letzter Rest $\neq 0$ sei $p_m \rightsquigarrow p_m = ggT(p_1, p_2)$

$p_1 = 12378, \quad p_2 = 3054$

Bsp.:
$12378 = 3054 \cdot 4 + 162 \rightarrow p_3 < p_2$
$3054 = 162 \cdot 18 + 138 \rightarrow p_4 < p_3$
$162 = 138 \cdot 1 + 24$
$138 = 24 \cdot 5 + 18$
$24 = 18 \cdot 1 + 6 \rightsquigarrow p_7 < p_6$ ← $p_7 = 6 \neq 0$
$18 = 6 \cdot 3 + 0$ ← $p_8 = 0$

Haben:
$ggT(12378, 3054) = 6$

---

$p_3 = p_4 \cdot q_3 + p_5$

$15T^3 + 13T^2 + 12T + 2 = (3T^2 + 2T + 2) \cdot (5I + 1) + 0$

$-(15T^3 + 10T^2 + 10T)$

$3T^2 + 2T + 2$

$-(3T^2 + 2T + 2)$

$0$

$p_4$ = letzter Rest $\neq 0$
$\rightsquigarrow p_4 = ggT(p_2, p_1)$

$0 =: p_5$

Der euklidische Algorithmus liefert nun auch eine geschlossene Darstellung/Formel für den ggT wie folgt.

**8.11 Satz** (Darstellung des ggT als "Linear"kombination / Satz von Bézout):

Sind $p_1, p_2 \in K[T]$ und $d = ggT(p_1, p_2)$, so ex. $s_1, s_2 \in K[T]$ mit

$$\boxed{d = s_1 p_1 + s_2 p_2}$$

Sind insb. $p_1, p_2$ teilerfremd, so ex. eine Darstellung $1 = s_1 p_1 + s_2 p_2$.

**Bew.:** Sei $d := p_m$ der letzte im euklidischen Algorithmus 8.8 Rest $\neq 0$, also $d = ggT(p_1, p_2)$, und wir haben eine Darstellung $d = p_m = p_{m-2} - q_{m-2} p_{m-1}$, das ist eine "Linear-"Kombination von $p_{m-2}$ und $p_{m-1}$.
Anstelle $p_{m-1}$ setzen wir darin jetzt $p_{m-1} = p_{m-3} - q_{m-3} p_{m-2}$ ein und können so $p_{m-1}$ eliminieren. Dann erhalten wir

$$\begin{aligned} d = p_m &= p_{m-2} - q_{m-2} \cdot (p_{m-3} - q_{m-3} p_{m-2}) \\ &= (-q_{m-2}) \cdot p_{m-3} + (1 + q_{m-2} q_{m-3}) \cdot p_{m-2}, \end{aligned}$$

also eine "Linear-"Kombination von $p_{m-3}$ und $p_{m-2}$.
Dies wird wieder fortgesetzt/iteriert, bis nur noch eine "Linear-"Kombination von $p_1$ und $p_2$ auftritt, wie zu zeigen war. □

**8.12 Def.:** Die Koeffizienten $s_1$ und $s_2$, die in der Darstellung des ggT hier vorkommen, nennt man Bézout-Koeffizienten. Sie sind nicht eindeutig bestimmt.

Man kann sie durch sukzessives Durchgehen "von unten nach oben" in einem eukl.-Algo-Rechenschema explizit berechnen:

**8.13 Bsp.:** Die Algn. in 8.10, in umgekehrter Reihenfolge:

$24 = 18 \cdot 1 + 6$
$138 = 24 \cdot 5 + 18$
$162 = 138 \cdot 1 + 24$
$3054 = 162 \cdot 18 + 138$
$12378 = 3054 \cdot 4 + 162$

$(ggT(12378, 3054) = 6)$

Schreiben der (6) als Linearkombination:

$6 = 24 - 18$
$= 24 - (138 - 5 \cdot 24) = 6 \cdot 24 - 138$
$= 6 \cdot (162 - 1 \cdot 138) - 138 = 6 \cdot 162 - 7 \cdot 138$
$= 6 \cdot 162 - 7 \cdot (3054 - 18 \cdot 162) = 132 \cdot 162 - 7 \cdot 3054$
$= 132 \cdot (12378 - 4 \cdot 3054) - 7 \cdot 3054$
$= \underbrace{132}_{s_1} \cdot 12378 + \underbrace{(-535)}_{s_2} \cdot 3054.$

Reste einsetzen

(ü) Rechnen Sie im Bsp. 8.9 nach, dass $p_4 = (-T+1) p_1 + (T^3 - 2T^2 + 2) p_2$ gilt.

8.14. **Bem.:** • Der Satz von Bézout, d.h. die Darstellbarkeit des ggT als Linearkombination hat viele Anwendungen. Wir benötigen ihn für die Normalformentheorie.

• Die explizite Bestimmung laut Beweis, das "Rechnen von unten nach oben" der LK ist oft mühsam. In "Zahlentheorie" lernt man ein eleganteres Rechenschema kennen, das wir hier – ohne Beweis – nur angeben, wie es auch geht (es ist u.a. als "erweiterter euklidischer Algo" bekannt):

• Die Folge der Quotienten $q_1, q_2, \ldots$ sei mit $q_0, q_1, q_2, \ldots$ durchnummeriert.

• Dann werden rekursiv definiert: $c_{-2}=0,\ c_{-1}=1,\quad c_{m+2}=c_m+c_{m+1}\cdot q_{m+2}$,

$d_{-2}=1,\ d_{-1}=0,\quad d_{m+2}=d_m+d_{m+1}\cdot q_{m+2}$, $m=-2,-1,\ldots$

Das kann man in einer Tabelle machen, im Bsp. oben: ($p_1=12378, p_2=3054$)

| $m$ | -2 | -1 | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|---|
| $q_m$ | – | – | 4 | 18 | 1 | 5 | 1 | 3 |
| $c_m$ | 0 | 1 | 4 | 73 | 77 | 458 | 535 | (2063) |
| $d_m$ | 1 | 0 | 1 | 18 | 19 | 113 | 132 | (509) |

← endet mit letzter aufgehender Division, (muss eigentlich nicht mehr eingetragen werden)

Zelle = vorletzte Zelle + letzter Zelle mal $q$-Wert darüber (aber Punkt vor Strich beachten!)

Anfangswerte

hier stehen die Bézout-Koeff. bis aufs Vorzeichen ▽ 0

d.h. wir haben $\pm 6 = \underbrace{535}_{s_2}\cdot 3054 - \underbrace{132}_{s_1}\cdot 12378$

Die Probe ergibt, dass "−6" herauskommt auf der r.S. Also ist $6 = \underbrace{-535}_{s_2}\cdot p_2 + \underbrace{132}_{s_1}\cdot p_1$

8.15. **Ein anderes Bsp.:** $p_1=133, p_2=84$, Bestimmung der $q_i$:

$133:84=1$ $q_0$

$84:49=1$ $q_1$

$49:35=1$ $q_2$

$35:14=2$ $q_3$

$14:7=2$ (Rest 0) $q_4$

letzter Rest $\neq 0$, ist $=\mathrm{ggT}(133, 84)$

Tabelle:

| $m$ | -2 | -1 | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|---|---|
| $q_m$ | – | – | 1 | 1 | 1 | 2 | 2 |
| $c_m$ | 0 | 1 | 1 | 2 | 3 | 8 | 19 |
| $d_m$ | 1 | 0 | 1 | 1 | 2 | 5 | 12 |

$\rightsquigarrow$ zuletzt $p_4=7$ Haben $8\cdot 84 - 5\cdot 133 = 7$. ✓

8.16. **Das Polynom-Bsp. in 8.9:** der ggT war $p_4 = 3T^2+2T+2$

| $m$ | -2 | -1 | 0 | 1 |
|---|---|---|---|---|
| $q_m$ | – | – | $T^2-T-1$ | $T-1$ |
| $c_m$ | 0 | 1 | $T^2-T-1$ | $1+(T^2-T-1)\cdot(T-1) = T^3-2T^2+2$ |
| $d_m$ | 1 | 0 | 1 | $T-1$ |

$\rightarrow \pm p_4 = (T^3-2T^2+2)\cdot p_2 - (T-1)\cdot p_1$