

## Vorlesung Lineare Algebra II

SoSe'20 hhu

K. Halupczok

### §2: Normalformentheorie

#### l8: Der Euklidische Algorithmus

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. Daf.: Ist  $p = \sum_{i=0}^n \alpha_i T^i \in K[T]$ , so heißt  $m := \max \{ i; \alpha_i \neq 0 \}$  der Grad von  $p$ , kurz:  $\deg(p) = m$  für "Degree". (Vgl. Def. L8.19 in LA I). Weiter heißt  $\alpha_m$  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  $p_1 = q \cdot p_2 + r$  gilt.

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

$$\begin{array}{r} -(T^3 + 2T^2) \\ \hline -T^2 - 2T^2 - 4T \\ \hline -3T + 1 \\ \hline -3 \end{array}$$

Also:  $\frac{T^3 - T + 1}{T + 2} = \underbrace{(T^2 - 2T + 2)}_{\text{Quotient } q} \cdot \underbrace{(T + 2)}_{P_2} - \underbrace{-3}_{r = -3}$

genau wie für LAI, L8.25, dort L8.27.

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  $q_1 := \frac{\alpha_{m_1}}{\beta_{m_2}} T^{m_1-m_2}$  und  $r := p_1 - q_1 p_2$ . Dann ist  $p_1 = q_1 p_2 + r$ , und  $\deg(r) \leq m_1 - 1 < \deg(p_1)$ , da wir gerade den nächsten Koeff. annuliert haben. Fertig, wenn  $\deg(r) < \deg(p_2)$ . 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  $(q_1 - q_2) p_2 = r_2 - r_1$ .

$\overbrace{\text{grad} \geq \deg(p_2)}$   $\overbrace{\text{grad} < \deg(p_2)}$  falls  $q_1 \neq q_2$   $\square$ .

Also:  $q_1 = q_2$  und  $r_1 = r_2$ .  $\square$

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:  $p = \text{ggT}(p_1, \dots, p_m)$ , 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  $p_2 | p_1$  für "p<sub>2</sub> teilt p<sub>1</sub>", d.h.  $p_2 | p_1 : \Leftrightarrow \exists q : p_1 = p_2 q$ .

8.7. Bsp.:  $(T-1) | (T^3-1)$ , da  $\frac{(T^3-1)}{(T-1)} = T^2 + T + 1$ , geht restlos auf.

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

normiert

→ ohne Rest

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

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

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  $p_{m+1} \neq 0$ , so sei  $p_{m+2}$  der bei der Division von  $p_m$  (geteilt) durch  $p_{m+1}$  auftretende Rest, d.h. 
$$p_m = p_{m+1} \cdot q_m + p_{m+2} \quad \text{mit } \deg(p_{m+2}) < \deg(p_{m+1}),$$
 für  $m = 1, 2, 3, \dots$

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

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

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

Dann haben wir

$$\begin{aligned} p_1 &= p_2 \cdot q_1 + p_3 \\ p_2 &= p_3 \cdot q_2 + p_4 \\ &\vdots && \vdots \end{aligned}$$

$$p_{m-2} = p_{m-1} \cdot q_{m-2} + p_m \quad \leftarrow \text{letzter Rest } \neq 0,$$

$$p_{m-1} = p_m \cdot q_{m-1} \quad \leftarrow \text{geht restlos auf.}$$

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

Weiter:  $p_m | p_{m-2}$ , 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  $p_m | p_{m-3}, \dots$  Die Fortsetzung / Iteration dieses Schusses

zeigt dann  $p_m | p_2$  und  $p_m | p_1$ , 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. Polynom  $s_1, s_2$  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.  $d | p_3$ .

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

Durch Fortsetzung / Iteration dieses Schusses folgt:  $d | p_m$ .

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

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

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:

$$\begin{array}{r}
 15T^6 - 17T^5 - 11T^4 + 7T^3 + 19T^2 + 20T + 2 = (15T^4 - 2T^3 + 2T^2 - 8T) \cdot (T^2 - T - 1) + p_3 \\
 -(15T^6 - 2T^5 + 2T^4 - 8T^3) \\
 \hline
 -15T^5 - 13T^4 + 15T^3 + 19T^2 \\
 -(-15T^5 + 2T^4 - 2T^3 + 8T^2) \\
 \hline
 -15T^4 + 17T^3 + 11T^2 + 20T \\
 -(-15T^4 + 2T^3 - 2T^2 + 8T) \\
 \hline
 15T^3 + 13T^2 + 12T + 2 \quad \leftarrow \text{Rest} = : p_3, \text{ dann } \deg p_3 < \deg p_2 = 4
 \end{array}$$

Mit dem eben erhaltenen Rest  $p_3 := 15T^3 + 13T^2 + 12T + 2$  führen wir die Division "P<sub>2</sub> geteilt durch P<sub>3</sub>" durch, um den nächsten Rest P<sub>4</sub> zu erhalten:

$$\begin{array}{r}
 15T^4 - 2T^3 + 2T^2 - 8T = (15T^3 + 13T^2 + 12T + 2) \cdot (T - 1) + p_4 \\
 -(15T^4 + 13T^3 + 12T^2 + 2T) \\
 \hline
 -15T^3 - 10T^2 - 10T \\
 -(-15T^3 - 13T^2 - 12T - 2) \\
 \hline
 3T^2 + 2T + 2 \quad \leftarrow \text{Rest} = : p_4, \text{ dann } \deg p_4 < \deg p_3 = 3
 \end{array}$$

Wenn man nun mit dem jetzt erhaltenen Rest P<sub>4</sub> noch einen Schritt weiter rechnet, erhält man den Rest P<sub>5</sub> = 0. Laut Satz 8.8 ist dann P<sub>4</sub> = ggT(P<sub>1</sub>, P<sub>2</sub>).

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:

$$P_1 = P_2 \cdot q_1 + P_3, \quad \text{Bsp.: } 12378 = 3054 \cdot 4 + 162 \rightarrow P_3 < P_2$$

$$P_2 = P_3 \cdot q_2 + P_4 \quad 3054 = 162 \cdot 18 + 138 \rightarrow P_4 < P_3$$

$$P_3 = P_4 \cdot q_3 + P_5 \quad 162 = 138 \cdot 1 + 24$$

$$P_4 = P_5 \cdot q_4 + P_6 \quad 138 = 24 \cdot 5 + 18$$

$$P_5 = P_6 \cdot q_5 + P_7 \quad 24 = 18 \cdot 1 + 6 \rightarrow P_7 < P_6 \rightarrow P_7 = 6 = \text{ggT}(12378, 3054)$$

$$\text{Letzter Rest } \neq 0 \text{ sei } P_m \rightarrow P_m = \text{ggT}(P_1, P_2)$$

$$18 = 6 \cdot 3 + \underline{\underline{0}} \quad P_8 = 0$$

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

### 8.11. Satz (Darstellung des ggT als Linearkombination / Satz von Bézout):

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

mit

$$d = s_1 p_1 + s_2 p_2.$$

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  $d = \text{ggT}(p_1, p_2)$ , 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.  $\square$

### 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" im eukl.-Algo-Rechenschema explizit berechnen:

8.13. Bsp.: • Die Qtg. in 8.10, in umgekehrter Reihenfolge:

$\begin{array}{rcl} 24 & = & 18 \cdot 1 + 6 \\ 138 & = & 24 \cdot 5 + 18 \\ 162 & = & 138 \cdot 1 + 24 \\ 3054 & = & 162 \cdot 18 + 138 \\ 12378 & = & 3054 \cdot 4 + 162 \end{array}$	<p>Schreibe der 6 als Linearkombination:</p> $\begin{aligned} 6 &= 24 - 18 \\ &= 24 - (138 - 5 \cdot 24) = 6 \cdot 24 - 138 \\ &= 6 \cdot (162 - 1 \cdot 138) - 138 = 6 \cdot 162 - 7 \cdot 138 \\ &= 6 \cdot 162 - 4 \cdot (3054 - 18 \cdot 162) = 132 \cdot 162 - 4 \cdot 3054 \\ &= 132 \cdot (12378 - 4 \cdot 3054) - 4 \cdot 3054 \\ &\xrightarrow{\text{restle einsetzen}} \underline{\underline{s_1}} = 132 \cdot 12378 + (\underline{-535}) \cdot 3054. \end{aligned}$
--	--

(u) 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,  $q_1, q_2, \dots$  sei mit  $q_0, q_1, q_2, \dots$  durchnumeniert.
- Dann werden rekursiv definiert:  $c_{-2} = 0, c_{-1} = 1, c_{m+2} = c_m + c_{m+1} \cdot q_{m+2}$ ,

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

Das kann man in einer Tabelle machen, im Bsp. oben: ( $p_1 = 12348, p_2 = 3054$ )

$m$	-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)

andet mit letzter aufgehende  
 Division,  
 (muss eigentlich  
 nicht mehr  
 eingetragen werden)

hier stehen die Bézout-Koeff.  $\uparrow$   
 bis aufs Vorzeichen

(aber Punkt  
 vor Strich beachten!)

Anfangswerte

$$\text{d.h. wir haben } \pm 6 = 535 \cdot 3054 - 132 \cdot 12348$$

Die Probe ergibt, dass "-6" herauskommt auf der r.v. Also ist  $6 = \frac{s_2}{p_2} \cdot p_2 + \frac{s_1}{p_1} \cdot p_1$

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

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

$$\begin{aligned}
 & 84 : 49 = 1 \quad q_1 \\
 & 49 : 35 = 1 \quad q_2 \\
 & 35 : 14 = 2 \quad q_3 \\
 & 14 : 7 = 2 \text{ (Rest 0)} \quad q_4 \\
 & \text{(letzter Rest } \neq 0, \text{ ist } = \text{ggT}(133, 84))
 \end{aligned}$$

$$\rightarrow \text{z.B. } p_4 = 7 \text{ Haben } 8 \cdot 84 - 5 \cdot 133 = 7. \checkmark$$

8.16. Das Polynom-Bsp. in 8.9:  $m \mid -2 \mid -1 \mid 0 \mid 1$   
 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	$T^2 - T - 1$	$\frac{1 + (T^2 - T - 1) \cdot (T - 1)}{= T^3 - 2T^2 + 2}$
$d_m$	1	0	1	$T - 1$

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