

7 Ganzzahlige lineare Gleichungen und Moduln über euklidischen Ringen

7.1 Der Elementarteilalgorithmus

7.1.1 Matrizen über euklidischen Ringen

Sei (R, gr) ein Euklidischer Ring.

Definition

- (i) $GL_n(R) = (R^{n \times n})$ heißt *allgemeine lineare Gruppe* über R (GL = general linear)
- (ii) $1_n := 1_{GL_n(R)}$ ($n \times n$ -Einheitsmatrix)

Lemma 7.1

$GL_n(R) = \{U \in R^{n \times n} \mid \det U \in R^\times\}$
 (falls $R = \mathbb{Z}$, $U \in GL_n(\mathbb{Z}) \Leftrightarrow U \in \mathbb{Z}^{n \times n}, \det U = \pm 1$)

Beweis

- (i) $U \in (R^{n \times n})^\times \Leftrightarrow \exists V \in R^{n \times n}, VU = UV = 1_n \Rightarrow 1 = \det 1_n = \det(UV) = \underbrace{\det U}_{\in R} \cdot \underbrace{\det V}_{\in R} \Rightarrow \det U \in R^\times$
- (ii) Sei $U \in R^{n \times n}, \det U \in R^\times$. In LA I zeigt man für die Adjungierte $U^\#$ von U : $UU^\# = U^\#U = \det U \cdot 1_n$
 $U^\#$ wird aus $\det W$ gewonnen, wo W Untermatrizen von U sind, also $\det W \in R \Rightarrow U^\# \in R^{n \times n}, \det U \in R^\times \Rightarrow U^{-1} = \frac{1}{\det U} U^\# \in R^{n \times n} \Rightarrow U \in (R^{n \times n})^\times$ ■

Definition

$B = (b_{ij}) \in R^{m \times n}$, so sei $\text{ggT}(B) := \text{ggT}(b_{ij})$ ($i = 1, \dots, m$ und $j = 1, \dots, n$)

Lemma 7.2

$A \in R^{l \times m}, B \in R^{m \times n}$. Dann gilt:

- (i) $\text{ggT}(A) \mid \text{ggT}(AB), \text{ggT}(B) \mid \text{ggT}(AB)$
- (ii) $U \in GL_m(R), V \in GL_n(R)$, so ist $\text{ggT}(UBV) = \text{ggT}(B)$

Beweis

- (i) $A = (a_{ij}), B = (b_{kl}), d = \text{ggT}(A) \Rightarrow a_{ij} = d \cdot a'_{ij}, a'_{ij} \in R. AB = C = (c_{rs}), c_{rs} = \sum_{j=1}^m d_{rj} b_{js} = d \cdot \sum_j a'_{ij} \cdot b_{js} \Rightarrow \forall r, s : d \mid c_{rs} \Rightarrow d \mid \text{ggT}(C) = \text{ggT}(c_{rs} \mid r, s).$
 $\text{ggT}(B) = \text{ggT}(AB)$ genau so.
- (ii) $\text{ggT}(B) \mid \text{ggT}(UB) \mid \text{ggT}(U^{-1}(UB)) = \text{ggT}(B) \Rightarrow \text{ggT}(B) = \text{ggT}(UB).$
 $\text{ggT}(UB) = \text{ggT}((UB)V)$ genau so ■

Spezielle Matrizen:

E_{ij} „Matrizeneinheiten“, $E_{ij,kl} = \delta_{ik}\delta_{jl}$. Es steht in der i -ten Zeile und der j -ten Spalte eine 1.

Beispiel:
$$\begin{pmatrix} 0 & & & 0 \\ & \ddots & & \\ & & 1 & \\ & & & \ddots \\ 0 & & & & 0 \end{pmatrix}$$

Elementarmatrizen sollen folgende Matrizen genannt werden (in $R^{n \times n}$):

- 1.) *Additionsmatrizen*: $A_{ij}(b) = \underbrace{1_n}_{=E_n} + b \cdot E_{ij} (i \neq j).$

Beispiel:
$$\begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & b & \\ & & & \ddots \\ 0 & & & & 1 \end{pmatrix}$$

- 2.) *Vertauschungsmatrizen*: $V_{ij} = 1_n - E_{ii} - E_{jj} + E_{ij} + E_{ji}.$

Beispiel:
$$\begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & 0 & 1 & \\ & & 1 & 0 & \\ & & & & \ddots \\ 0 & & & & & 1 \end{pmatrix}$$

- 3.) „Einheitsdiagonalmatrizen“:

$$\text{diag}_j(\epsilon) = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \epsilon & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}, \epsilon \in R^\times$$

Laut LA: $\det A_{ij}(b) = 1, \det(V_{ij}) = -1 (i \neq j), \det \text{diag}_j(\epsilon) = \epsilon \Rightarrow$

Alle Elementarmatrizen sind in $GL_n(R)$

Weiter Matrizen besonderer Form:

Diagonalmatrizen: $D = \text{diag}(d_1, \dots, d_r, 0, \dots, 0)$ (in $R^{m \times n}$). Für $r = 0 : D = 0$.

Beispiel:
$$\begin{pmatrix} d_1 & & & 0 \\ & \ddots & & \\ & & d_r & \\ 0 & & & 0 \\ & & & & \ddots \end{pmatrix}$$

Bemerkung: Eine Matrix $B \in R^{n \times n}$ heie in „Elementarteilerform“ $\Leftrightarrow B = \text{diag}(d_1, \dots, d_r, 0, \dots, 0), d_1, \dots, d_r$ normiert und $d_r \neq 0$ und $d_1 \mid d_2 \mid \dots \mid d_r$ (dann $d_1 = \text{ggT}(B)$)

Eine Elementaroperation (ausgebt auf $B \in R^{m \times n}$) ist eine der folgenden Operationen:
Zu Γ Elementarmatrix bilde $B' = \Gamma B$ oder $B' = B\Gamma$ und setze wieder $B := B'$.

Liste:

Zeilenoperationen	bewirkt
$B \rightarrow B := B' = A_{ij}(b) \cdot B$	Addition des b -fachen der j -ten Zeile von B zur i -ten
$B \rightarrow B := B' = V_{ij} \cdot B$	Vertauschen der i -ten mit der j -ten Zeile
$B \rightarrow B := B' = \text{diag}_j(\epsilon) \cdot B$	Multiplikation der j -ten Zeile mit ϵ
Spaltenoperationen	bewirkt
$B \rightarrow B := B' = B \cdot A_{ij}(b)$	Addition der i -ten Spalte $\cdot b$ zur j -ten
$B \rightarrow B := B' = B \cdot V_{ij}$	Vertauschen der i -ten mit der j -ten Spalte
$B \rightarrow B := B' = B \cdot \text{diag}_j(\epsilon)$	Multiplikation der j -ten Spalte mit ϵ

Jeder Algorithmus der eine Matrix A durch eine endliche Folge von Elementaroperationen in Elementarteilerform berfhrt, heit *Elementarteileralgorithmus*.

Vorschlag:

Bearbeite Tripel $(U, B, V) \in GL_m(R) \times R^{m \times n} \times GL_n(R)$ beginnend mit $(1_m, A, 1_n)$, so dass immer $B = UAV$ ist.

Elementaroperationen hier $(U, B, V) \rightarrow (U, B, V) := (\underbrace{\Gamma U}_{=U'}, \underbrace{\Gamma B}_{=B'}, \underbrace{V}_{=V'})$ (Zeilenoperation) oder

$(U, B, V) \rightarrow (U, B, V) := (\underbrace{U}_{=U'}, \underbrace{B\Gamma}_{=B'}, \underbrace{V\Gamma}_{=V'})$ (Spaltenoperation).

Bedingung okay: $\underbrace{\Gamma U A V}_{U' A' V'} = \Gamma B = B'$, ebenso $U A V \Gamma = B\Gamma = B'$

Ziel: Steure die Operationen so, dass nach endlich vielen Elementaroperationen ein (U, B, V) entsteht, mit $B =: D$ eine Elementarteilerform, also $A = UDV$.

Falls man so einen Algorithmus hat, so beweist das:

Satz 7.3 (Elementarteilersatz)

Sei R ein euklidischer Ring, $m, n \in \mathbb{N}_+$, $A \in R^{m \times n}$

- (i) Dann gibt es ein $U \in GL_m(R), V \in GL_n(R)$ und $D \in R^{m \times n}$, D in Elementarform, derart, dass $\underline{A = UDV}$
- (ii) D ist durch A eindeutig bestimmt

Zur Eindeutigkeit (Beweis-Skizze):

$d_1 = \text{ggT}(D) = \text{ggT}(UDV) = \text{ggT}(A)$. Man kann zeigen: $d_1 \cdot \dots \cdot d_j$ ist der ggT der Determinanten aller $j \times j$ -Untermatrizen von A .

Bemerkung: 1.) $A \in R^{m \times n}$, so $\det A = \det U \det D \det V$. Dann zur Berechnung von $\det A$ benutzt werden.

2.) Idee für LGS: Für $A = D$ in Elementarteilerform kann Lösung unmittelbar abgelesen werden \Rightarrow Lösung für A wird mittels Rücktransformation ermittelt.

LGS:

$xA = b, A \in R^{m \times n}, b \in R^{1 \times n}$ (Zeile) ist gegeben. Gesucht „Lösung“ $x \in R^{1 \times m}$ (Zeile). (LA oft $Ax = b$ mit Spalten, $Ax = b \Leftrightarrow x^T A^T = b^T$)

Besser: Information über die Lösungsmenge: $\mathcal{L}(A, B) = \{x \in R^m = R^{1 \times m} \mid xA = b\}$

Antwort sehr leicht, falls $A = D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}$ in Elementarteilerform. $y = (y_1, \dots, y_m) \in$

$$\mathcal{L}(D, c), c = (c_1, \dots, c_n) \Leftrightarrow yD = \underbrace{(y_1 d_1, \dots, y_r d_r, 0, \dots, 0)}_{n\text{-Stück}} \stackrel{!}{=} (c_1, \dots, c_n)$$

Lösbarkeitsbedingung (notwendig und hinreichend): $\mathcal{L}(D, C) \neq \emptyset \Leftrightarrow c_{r+1} = c_{r+1} = \dots c_n = 0$
und $d_1 \mid c_1, d_2 \mid c_2, \dots, d_r \mid c_r$

Falls Bedingung erfüllt, so hat man die „spezielle Lösung“ (wo $c_j = d_j y_j$, Bezeichnung $y_j = d_j^{-1} c_j$).

$$y \stackrel{(0)}{=} (d_1^{-1} c_1, \dots, d_r^{-1} c_r, 0, \dots, 0).$$

Die „allgemeine“ Lösung hat die Form:

$$y = y_0 + \sum_{j=r+1}^n a_j e_j, e_j = (0, \dots, 0, 1, 0, \dots, 0) \text{ Einheitsvektor, } a_j \in R$$

$$\begin{aligned} y \in \mathcal{L}(D, c) &\Leftrightarrow yD = c \text{ (auch } y_0 D = c) \\ &\Leftrightarrow (y - y_0)D = 0 \\ &\Leftrightarrow z = (y - y_0) \text{ ist Lösung des zugehörigen homogenen Systems} \\ &zD = 0, \text{ d.h. von der Form } \sum_{j=r+1}^n a_j e_j \end{aligned}$$

Es muss $z_j d_j = 0$, also $z_0 = 0$ für $j = 1, \dots, r$ gelten.

Man transformiert $xA = b$ wie folgt auf Diagonalform: $xA = b \Leftrightarrow \underbrace{xU^{-1}}_y \underbrace{UAV}_D = \underbrace{bV}_c = 0$.

$yD = c$, wo $c = bV$ und $y = xU^{-1}$, also $x = yU$ ist.

$$\underline{\mathcal{L}(A, b) = \mathcal{L}(D, bV) \cdot U}$$

$$(U, B, V) \in GL_m(R) \times R^{m \times n} \times GL_n(R), B = UAV.$$

Elementarteilalgorithmus Idee: Falls $B \neq 0$, so setze

$$gr(B) = \min\{gr(b_{ij}, i = 1, 2, \dots, m, j = 1, 2, \dots, n, b_{ij} \neq 0)\}.$$

Wenn es gelingt durch Elementaroperationen von B nach B' überzugehen, so dass $gr(B') < gr(B)$, so ist man induktiv fertig.

Zuerst benötigen wir einen Unteralgorithmus: ggTnachVorn(A):

Er soll zu einem $0 \neq A \in R^{m \times n}$ (U_1, B_1, V_1) mit $U_1 \in GL_m(R)$, $v_1 \in GL_n(R)$, $b_1 = U_1 A V_1$ gilt, wobei

$$B = \left(\begin{array}{c|c} d_1 & 0 \\ \hline 0 & A' \end{array} \right), \quad d_1 = \text{ggT}(A).$$

Skizze:

0. Initialisierung: $(U, B, V) := (1_m, A, 1_n)$.
1. Bestimme (k, l) mit $gr(b_{kl} = gr(B)$.
2. Fall I: Es gibt eine Zeile i mit $B_{kl} \nmid b_{il}$. Division mit Rest: $b_{ij} = qb_{kl} + r$. Addiere $(-q)$ -faches der k -ten Zeile. Das ergibt B' mit $b'_{il} = b_{il} - qb_{kl} = r$. Induktiv sind wir fertig, denn: $gr(r) < gr(b_{kl}) = gr(B)$. Weiter bei Schritt 1.
3. Fall II: Es gibt eine Spalte j mit $b_{kl} \nmid b_{kj}$. Genau wie bei Schritt 2, nur mit Spaltenoperationen erhalten wir $b_{kj} = q'b_{kl} + r'$. Addieren wir nun das $(-q')$ -fache der l -ten Spalte auf die j -te Spalte, erhalten wir B' mit $gr(B') < gr(B)$.
4. Fall III: $b_{kl} \mid b_{il}$ und $b_{kl} \mid b_{kj}$, $\forall i, j$ aber $\exists(i, j)$ mit $b_{kl} \nmid b_{ij}$. $b_{il} = q''b_{kl}$, $i \neq k, l \neq j$. Addiere $(1 - q'')$ -faches der k -ten Zeile zur i -ten hinzu:

$$b'_{il} = \underbrace{b_{ij}}_{q'b_{kl}} + (1 - q'')b_{kl} = b_{kl}$$

$$b'_{ij} = b_{ij} + (1 - q'')b_{kl} \implies b_{kl} = b'_{il} \nmid b'_{ij} \text{ (wegen } b_{kl} \nmid b_{ij}, b_{kl} \mid b_{kl})$$
 Fall II liegt vor mit i -ter statt k -ter Zeile. $B := B'$, $(k, l) := (i, l)$, weiter bei Schritt 3.
5. $\forall i, j : b_{kl} \mid b_{ij}$ (letzter möglicher Fall). Vertausche k -te und 1. Zeile und l -te und j -te Spalte. Entsteht b mit $0 \neq b_{11} \mid b_{ij} \forall i, j \implies b_{11}$ ist ein ggT, $\implies \exists \epsilon \in R^\times : d_1 = \epsilon b_{11} = \text{ggT}(B) \stackrel{\text{Lemma 2}}{=} \text{ggT}(A) \implies$ Multipliziere 1. Zeile mit ϵ : Es entsteht Matrix mit $b_{11} = d_1 = \text{ggT}(A)$. Wie bei Gaußalgorithmus erzeugt man jetzt in der ersten Spalte und ersten Zeile Nullen außer bei b_{11} . Jetzt hat man (U, B, V) mit $A = UBV$ und $B = \left(\begin{array}{c|c} d_1 & 0 \\ \hline 0 & A' \end{array} \right)$. Ausgabe: $(U_1, B_1, V_1) := (U, B, V)$

Klar: Man kann genauso mit A' weitermachen: Braucht: $d_n = \text{ggT}(A) = \text{ggT}(B_1) \mid \text{ggT}(A')$. Im Detail:

ELT(A) :

- (1) Falls $A \neq 0$, Ausgabe: $(1_m, A, A_n)$.
- (2) Anderfalls liefert ggTnachVorn(A) (U_1, B_1, V_1) wie oben: Falls $n = 1$ oder $M = 1$, so fertig. Ausgabe $(U, D, V) := (U_1, B_1, V_1)$. Falls $m, n > 1$ und $A' = 0$, so wieder fertig. Ausgabe wie

oben.

Falls $A' \neq 0$, so liefert $\text{ELT}(A')$ (U', D', V') mit $U'D'V' = A'$ und

$$\begin{aligned} & U_1 \left(\begin{array}{c|c} 1 & 0 \\ 0 & U' \end{array} \right) \left(\begin{array}{c|c} d_1 & 0 \\ 0 & D' \end{array} \right) \left(\begin{array}{c|c} 1 & 0 \\ 0 & V' \end{array} \right) V_1 \\ &= U_1 B = \left(\begin{array}{c|c} d_1 & 0 \\ 0 & \underbrace{U'D'V'}_{=A'} \end{array} \right) V_1 \\ &= U_1 B_1 V_1 \\ &= A \end{aligned}$$

Ausgabe (U, D, V) mit U, D, V passend wie in obiger Formel.

Einschub Beispielrechnung (folgt vielleicht später, hab' grade keine Lust, die zwei DinA4-Blätter abzutippen)

7.2 Ganzzahlige Lösungen eines ganzzahligen linearen Gleichungssystems

Betrache LGS $xA = B$, gegeben $a \in R^{m \times n}$, $b \in R^{1 \times n}$.

Gesucht: $\mathcal{L}(A, B) = \{x \in R^{1 \times m} = R^m : xA = b\}$

Elementarteilersatz: $A = UDV$, $D = \text{diag}(d_1, d_2, \dots, d_r, 0, \dots)$ in Elementarteilerform. $U \in GL_m(R)$, $V \in GL_n(R)$. Gesehen: $\mathcal{L}(A, b) = \mathcal{L}(D, bV)U$. $c := bV = (c_1, c_2, \dots, c_n)$.

Satz 7.4 (LGS-Satz)

Mit diesen Voraussetzungen und Bezeichnungen gilt:

- (1) $\mathcal{L}(A, b) \neq \emptyset \iff d_i \mid c_i, i = 1, 2, \dots, r, c_{r+1} = c_{r+2} = \dots = c_n = 0$.
- (2) Lösung des homogenen Systems $xA = 0$:
 $\mathcal{L}(A, 0) = \mathcal{L}(D, 0)U = \bigoplus_{j=r+1}^m R(e_j U)$. e_j ist der j -te Einheitsvektor in R^m . Das heißt, eine R -Basis von $\mathcal{L}(A, 0)$ ist gegeben durch Basis $b_{r+1}, b_{r+2}, \dots, b_m$, mit $b_j = e_j U$, also die j -te Zeile von U ist. Falls $m \leq r$, so $\mathcal{L}(A, 0) = 0$, d-h- jede Lösung $y \in \mathcal{L}(A, 0)$ hat eindeutige Darstellung $y = \sum_{j=r+1}^m a_j b_j$, $a_j \in R$.
- (3) Falls das LGS lösbar ist, so erhält man die allgemeine Lösung x aus einer speziellen Lösung x_0 in der Form $x = x_0 + y$, $y \in \mathcal{L}(A, 0)$. Man kann wählen: $x_0 = (d_1^{-1}c_1, d_2^{-1}c_2, \dots, d_r^{-1}c_r, 0, \dots, 0)$.

Beweis

Alles schon bewiesen...

Bemerkungen:

- (1) Ist $A \in R^{n \times n}$, so gilt

$$A \in GL_n(R) \iff D = 1_n$$

(2) Jedes $U \in GL_n(R)$ ist Produkt von Elementarmatrizen.

Beweis

(1) $A = UDV$, $U, V \in GL_n(R)$. $D \in GL_n(R) \iff n = r, d_1, \dots, d_n = 1 \implies D = 1_n$

(2) $A \in GL_n(R) \iff D = 1_n \implies A = UV \implies$ Behauptung ■

Freunde der Algebra mögen beachten, dass für ein R -Modul M die selben Axiome wie für einen Vektorraum gelten, nur dass R ein Ring statt einem Körper ist. Das \mathbb{Z} -Modul ist (fast) das selbe wie eine (additive) abelsche Gruppe. Die Hauptneuheit ist, dass man im Allgemeinen in M eine R -Basis hat.

Ein Beispiel dazu ist mit $R = \mathbb{Z}$ das Modul $M = (\mathbb{Z}/2\mathbb{Z}, +)$. Wäre die Basis die leere Menge, so wäre $M = 0$, Widerspruch. Ist nun b ein Element der Basis, so wären alle $z \cdot b$, $z \in \mathbb{Z}$ verschieden, also $\#M = \infty$, was auch ein Widerspruch ist.

In der Algebra zeigt man leicht: Ist $M = \langle u_1, \dots, u_m \rangle = \{ \sum_{i=1}^m \alpha_i u_i \mid \alpha_i \in R \}$, so existiert ein $A \in R^{m \times n}$ mit $M \cong R^n / R^m \cdot A$. Klar: $A = UDV$ wie im Elementarsatz, also $R^m = R^m \cdot U$, $R^n = V \cdot R^n$

$$\begin{aligned} \implies M &\cong R^n / R^m U D V \\ &= R^n V / R^m D V \\ &\cong R^n / R^m D \\ &= (R \oplus \dots \oplus R) / (R d_1 \oplus \dots \oplus R d_r \oplus 0 \oplus \dots \oplus 0) \\ &\cong R / R d_1 \oplus \dots \oplus R / R d_r \oplus R \oplus \dots \oplus R \end{aligned}$$

Damit ist die Struktur bestimmt. So kann die Eindeutigkeit von D auch bewiesen werden.

Ist $R = \mathbb{Z}$, so ist $(\mathbb{Z}/d\mathbb{Z}, +)$ zyklisch, erzeugt von $1 + d\mathbb{Z} = \bar{1}$, \mathbb{Z} sowieso zyklisch.

Als Ergebnis haben wir: Jede endlich erzeugbare abelsche Gruppe ist direktes Produkt zyklischer Gruppen.

Die R -lineare Abbildung $R^l \rightarrow R^k$ beschreibung durch Darstellungsmatrizen in $R^{l \times k}$. Der Elementarteiler-Algorithmus liefert Mittel Kern(f) und Bild(f) explizit zu beschreiben.

