

### Der Elementarteilersatz

Es sei  $R$  ein kommutativer unitärer Ring. Die Menge der quadratischen Matrizen  $M(m \times m, R)$  ist ein Ring. Wir bezeichnen mit  $E_m$  die Einheitsmatrix. Es seien  $i, j \in [1, m]$  zwei verschiedene Zahlen und es sei  $\lambda \in R$ . Wenn man zur  $i$ -ten Zeile von  $E_m$  das  $\lambda$ -fache der  $j$ -ten Zeile addiert, so erhält man eine neue Matrix  $E_{ij}(\lambda)$ . Wenn man zur  $j$ -ten Spalte von  $E_m$  das  $\lambda$ -fache der  $i$ -ten Spalte addiert, erhält man auch die Matrix  $E_{ij}(\lambda)$ . Diese Matrix hat den Eintrag  $\lambda$  in der Position  $(i, j)$ .

Wenn  $A$  eine beliebige Matrix ist, so bildet man

$$A' = E_{ij}(\lambda)A, \quad A'' = AE_{ij}(\lambda).$$

Dann entsteht  $A'$  aus  $A$  indem man zur  $i$ -ten Zeile von  $A$  das  $\lambda$ -fache der  $j$ -ten Zeile addiert. Die Matrix  $A''$  entsteht aus  $A$  indem man zur  $j$ -ten Spalte von  $A$  das  $\lambda$ -fache der  $i$ -ten Spalte addiert.

Eine Elementarmatrix ist eine der Matrizen  $E_{ij}(\lambda)$  für beliebige  $i, j$  und  $\lambda \in R$ . Elementarmatrizen sind invertierbar:

$$E_{ij}(\lambda)E_{ij}(-\lambda) = E_m = E_{ij}(-\lambda)E_{ij}(\lambda).$$

Deshalb ist auch jedes Produkt von Elementarmatrizen eine invertierbare Matrix. Die Determinante eines solchen Produkts ist gleich 1.

Es seien zwei verschiedene Zeilen  $z_i$  und  $z_k$  der Matrix  $A$  gegeben. Wenn man die beiden Zeilen vertauscht und eine der beiden Zeilen mit  $-1$  multipliziert, so nennen wir das einen orientierten Zeilentausch. Man kann ihn durch Multiplikation mit elementaren Matrizen von links realisieren. Entsprechend definiert man einen orientierten Spaltentausch. Man kann ihn durch Multiplikation mit elementaren Matrizen von rechts realisieren.

Wir bezeichnen mit  $GL(n, R) \subset M(n \times n, R)$  die Menge aller Matrizen  $A \in M(n \times n, R)$ , für die es eine Matrix  $B$  gibt, so dass  $A \cdot B = B \cdot A = E_n$ . Das sind genau die Matrizen  $A$ , so dass  $\det A \in R$  eine Einheit ist. Bezüglich der Multiplikation ist  $GL(n, R)$  eine Gruppe. Es sei

$$SL(n, R) = \{A \in GL(n, R) \mid \det A = 1\}.$$

**Satz 0.1** (Elementarteilersatz) *Es sei  $R$  ein Hauptidealring. Es sei  $A \in M(m \times n, R)$ . Dann gibt es Matrizen  $X \in SL(m, R)$  und  $Y \in SL(n, R)$ , so dass*

$$XAY = D,$$

wobei  $D$  höchstens an den Positionen  $(i, i)$  Einträge  $d_i$  hat, die von 0 verschieden sein können. Wenn  $d_1, \dots, d_r$  die von 0 verschiedenen Einträge bezeichnet, so gilt:

$$Rd_1 \supset Rd_2 \supset \dots \supset Rd_r. \quad (1)$$

Die Zahl  $r$  und die Ideale  $Rd_1, \dots, Rd_r$  hängen nur von  $A$  ab und nicht von der Wahl der Matrizen  $X$  und  $Y$ .

Genauer gilt: Es seien  $S \in GL(m, R)$  und  $T \in GL(n, R)$  Matrizen, so dass  $SAT = D'$ , wobei  $D'$  eine Matrix mit den diagonalen Einträgen  $d'_1, \dots, d'_r$ , von der gleichen Art wie  $D$  ist. Dann gilt  $r = r'$  und  $Rd'_i = Rd_i$ .

**Beweis:** Wir betrachten die Menge aller Matrizen der Form:

$$B = XAY.$$

wobei  $X \in SL(m, R)$  und  $Y \in SL(n, R)$ . Wir betrachten die Menge aller Ideale der Form  $Ra$ , wobei  $a$  ein Eintrag in irgendeiner der Matrizen  $B$  ist. Dann gibt es nach noetherscher Induktion ein in dieser Menge maximales Ideal  $Ru$ . Wir können nach orientiertem Zeilen oder Spaltentausch annehmen, dass  $u$  in der Position  $(1, 1)$  steht und dass dies in der Matrix  $A$  passiert.

Wir behaupten, dass alle Einträge in der ersten Zeile bzw. Spalte von  $A$  durch  $u$  teilbar sind. Angenommen wir haben in Position  $(2, 1)$  ein Element  $v$ , das nicht durch  $u$  teilbar ist:

$$A = \begin{pmatrix} u & \dots \\ v & \dots \\ & \dots \end{pmatrix},$$

Es sei  $w$  der *g.g.T* von  $u$  und  $v$ . Dann gibt es eine Gleichung

$$au + bv = w$$

wobei  $w|u$  und  $w|v$  und  $Ru \subsetneq Rw$ . Wir betrachten die invertierbare  $2 \times 2$ -Matrix

$$\check{X} = \begin{pmatrix} a & b \\ -v/w & u/w \end{pmatrix}$$

Dann ist auch

$$X = \begin{pmatrix} \check{X} & \mathbf{0} \\ \mathbf{0} & E_{m-2} \end{pmatrix}$$

invertierbar und hat die Determinante 1. Das Produkt  $XA$  hat an der Position  $(1, 1)$  den Eintrag  $w$ . Da  $\det X = 1$  und  $Ru \subsetneq Rw$  widerspricht das der Wahl von  $Ru$ . Also gilt  $u|v$ .

Genauso sehen wir, dass alle Einträge in der ersten Zeile und Spalte von  $A$  durch  $u$  teilbar sein müssen. Nach Zeilen- und Spaltenscherungen kann man annehmen, dass

$$A = \begin{pmatrix} u & 0 \\ 0 & C \end{pmatrix},$$

wobei  $C$  ein kleineres Format hat als  $A$ .

Wenn man eine Zeile (bzw.) Spalte von  $C$  zur ersten Zeile (bzw.) Spalte von  $A$  addiert, sieht man aus den obigen Überlegungen, dass auch alle Einträge von  $C$  durch  $u$  teilbar. Die Behauptung folgt durch Induktion nach dem Format von  $A$ , indem man die Induktionsvoraussetzung auf  $(1/u)C$  anwendet.

Wir beweisen jetzt die Eindeutigkeit. Die Zahl  $r$  ist der Rang der Matrix  $A$  über dem Quotientenkörper von  $R$ . Es sei  $B = SAT$  wobei  $S \in \text{GL}(m, R)$  und  $T \in \text{GL}(n, R)$ . Wir bezeichnen mit  $I_A$  das Ideal welches von allen Einträgen der Matrix  $A$  erzeugt wird. Wir zeigen, dass

$$I_A = I_B.$$

In der Tat, die Gleichung  $B = SAT$  zeigt, dass die Einträge von  $B$  Linearkombinationen der Einträge von  $A$  sind. Daher gilt  $I_B \subset I_A$ . Die umgekehrte Inklusion folgt aus  $S^{-1}AT^{-1} = B$ . Insbesondere folgt, dass  $I_A = Rd_1$  nur von  $A$  abhängt.

Wir fassen die Multiplikation mit  $A$  als lineare Abbildung auf  $A : R^n \rightarrow R^m$ . Die Matrixkoeffizienten der linearen Abbildung  $\wedge^t A : \wedge^t R^n \rightarrow \wedge^t R^m$  sind die  $t \times t$ -Unterdeterminanten von  $A$  (siehe unten). Die Gleichung  $B = XAY$  induziert ein kommutatives Diagramm

$$\begin{array}{ccc} \wedge^t R^n & \xrightarrow{\wedge^t A} & \wedge^t R^m \\ \wedge^t Y \uparrow & & \downarrow \wedge^t X \\ \wedge^t R^n & \xrightarrow{\wedge^t B} & \wedge^t R^m \end{array}$$

Daraus folgt, dass das Ideal  $I_A^t$ , welches von den  $t \times t$ -Unterdeterminanten von  $A$  erzeugt wird, gleich dem Ideal  $I_B^t$  ist, welches von den  $t \times t$ -Unterdeterminanten von  $B$  erzeugt wird. Also ist  $I_A^t = R(d_1 \cdot \dots \cdot d_t)$ . Daraus folgt die Eindeutigkeit. *Q.E.D.*

Die Behauptung über die Unterdeterminanten sieht man so. Die Standardform  $\langle , \rangle: R^n \times R^n \rightarrow R$  induziert

$$\langle , \rangle_t: \quad \wedge^t R^n \quad \times \quad \wedge^t R^n \quad \rightarrow \quad R \\ v_1 \wedge \dots \wedge v_t \quad \times \quad w_1 \wedge \dots \wedge w_t \quad \mapsto \quad \det(\langle v_i, w_j \rangle)$$

Wenn  $e_1, \dots, e_n$  die Standardbasis von  $R^n$  ist, so ist  $e_{i_1} \wedge \dots \wedge e_{i_t}$ , für  $i_1 < \dots < i_t \leq n$  eine selbstduale Basis von  $\wedge^t R^n$  bzgl. der symmetrischen Form  $\langle , \rangle_t$ . Wir bezeichnen die entsprechende Basis von  $\wedge^t R^n$  mit  $f_{j_1} \wedge \dots \wedge f_{j_t}$ . Dann sind die Koeffizienten der Matrix von  $\wedge^t A$  bezüglich dieser Basen

$$\langle Ae_{i_1} \wedge \dots \wedge Ae_{i_t}, f_{j_1} \wedge \dots \wedge f_{j_t} \rangle_t = \det(\langle Ae_{i_k}, f_{j_l} \rangle_t).$$

Rechts stehen genau die  $t \times t$ -Unterdeterminanten der Matrix  $A$ .

**Definition 0.2** *Es sei  $A \in M(m \times n, R)$ . Dann nennen wir die Ideale  $Rd_i$ ,  $i = 1, \dots, r$  aus (1) die Elementarteiler von  $A$ .*

**Corollary 0.3** *Zwei Matrizen  $A, B \in M(m \times n, R)$  haben genau dann die gleichen Elementarteiler, wenn es Matrizen  $S \in GL(m, R)$  und  $T \in GL(n, R)$  gibt, so dass  $SAT = B$ .*

**Beweis:** Das ist klar.

Wir geben zwei Anwendungen.

**Satz 0.4** *Es sei  $R$  ein Hauptidealring. Es sei  $u \in R$ , so dass  $Ru \neq R$ . Dann ist die kanonische Abbildung*

$$\mathrm{SL}(n, R) \rightarrow \mathrm{SL}(n, R/uR)$$

*surjektiv.*

**Beweis:** Im Fall  $n = 1$  gibt es nichts zu beweisen. Es sei  $\bar{A} \in \mathrm{SL}(n, R/u)$ . Wir wählen eine Matrix  $A \in M(n \times n, R)$ , die bei der Abbildung  $M(n \times n, R) \rightarrow M(n \times n, R/uR)$  auf  $\bar{A}$  abgebildet wird. Dann finden wir Matrizen  $X, Y \in \mathrm{SL}(n, R)$ , so dass  $XAY = D$  wie im Satz 0.1. Es folgt, dass  $\bar{D} \in \mathrm{SL}(n, R/uR)$  und daher kann  $D$  keine Nullen auf der Diagonalen haben. Die Diagonalelemente  $t_i$ ,  $i = 1, \dots, n$  sind relativ prim zu  $u$ , da sie auf Einheiten in  $R/uR$  abgebildet werden. Wir erhalten

$$t_1 \cdot \dots \cdot t_{n-1} \cdot t_n = 1 + ru, \quad r \in R.$$

Das Element  $1 + ru$  ist eine Einheit in  $R/u^nR$ . Folglich finden wir  $t'_n$ , so dass die Bilder von  $t_n$  und  $t'_n$  in  $R/uR$  gleich sind und so dass

$$t_1 \cdot \dots \cdot t_{n-1} \cdot t'_n = 1 + au^n, \quad r \in R.$$

Wir betrachten die Matrix

$$\tilde{D} = \begin{pmatrix} t_1 & u & 0 & 0 & \dots & 0 & 0 \\ 0 & t_2 & u & 0 & \dots & 0 & 0 \\ & & & \dots & & & \\ & & & & & & \\ 0 & 0 & 0 & 0 & \dots & t_{n-1} & u \\ (-1)^n au & 0 & 0 & 0 & \dots & 0 & t'_n \end{pmatrix}$$

Wir sehen, dass  $\tilde{D} \in \text{SL}(n, R)$  und dass das Bild in  $\text{SL}(n, R/uR)$  die Matrix  $\bar{D}$  ist. Schließlich ist  $X^{-1}\tilde{D}Y^{-1} \in \text{SL}(n, R)$  und das Bild dieser Matrix in  $\text{SL}(n, R/uR)$  ist  $\bar{X}^{-1}\bar{D}\bar{Y}^{-1} = \bar{A}$ . Q.E.D.

**Bemerkung:** Im allgemeinen ist unter der Voraussetzungen von Satz 0.4 die Abbildung  $\text{GL}(n, R) \rightarrow \text{GL}(n, R/uR)$  nicht surjektiv. Es ist aber einfach zu sehen, dass dies richtig ist, wenn  $R$  lokal ist. In der Tat, es sei allgemeiner  $\pi : R \rightarrow S$  ein Surjektion lokaler Ringe, so dass  $\pi(\mathfrak{m}_R) \subset \mathfrak{m}_S$  für die maximalen Ideale. Dann ist  $\text{GL}(n, R) \rightarrow \text{GL}(n, S)$  surjektiv. In der Tat, es sei  $\bar{A} \in \text{GL}(n, R)$ . Eine beliebige Matrix  $A \in M(n \times n, R)$ , die auf  $\bar{A}$  abgebildet wird, liegt dann in  $\text{GL}(n, R)$ . Die Abbildung  $\text{SL}(n, R) \rightarrow \text{SL}(n, S)$  ist ebenfalls surjektiv. Es sei nämlich  $\det \bar{A} = 1$ . Daraus folgt  $1 - (\det A)^{-1} \in \text{Ker } \pi$ . Wenn man  $A$  mit der Diagonalmatrix  $\text{Diag} = (1, \dots, 1, \det A^{-1})$  multipliziert, erhält man eine Matrix in  $\text{SL}(n, R)$ , die auf  $\bar{A}$  abgebildet wird.

Es sei  $K$  ein Körper. Dann ist  $R = K[T]$  ein Hauptidealring. Für jedes Ideal  $\mathfrak{a} \subset K[T]$ ,  $\mathfrak{a} \neq 0$  gibt ein eindeutig bestimmtes unitäres Polynom (d.h. höchster Koeffizient = 1)  $f(T) \in K[T]$ , so dass  $\mathfrak{a} = f(T)K[T]$ . Mit den Bezeichnungen von Satz 0.1 gibt es eindeutig bestimmte unitäre Polynome  $\ell_i \in K[T]$ ,  $i = 1, \dots, r$ , so dass  $K[T]\ell_i = K[T]d_i$ . Man versteht unter den Elementarteilern von  $A$  oft auch die Polynome  $\ell_i$ .

Wir verändern die Notation. Es sei  $A \in M(n \times n, K)$  eine Matrix. Wir versehen  $K^n$  mit der Struktur eines  $K[T]$ -Moduls, indem wir definieren

$$T\underline{x} = A\underline{x}, \quad \underline{x} \in K^n.$$

Diesen  $K[T]$ -Modul bezeichnen wir mit  $V_A$ . Die Standardbasis von  $V_A = K^n$  als  $K$ -Vektorraum bezeichnen wir mit  $\bar{e}_i$ . Man nennt zwei Matrizen  $A, B \in$

$M(n \times n, K)$  ähnlich, wenn eine Matrix  $M \in \text{GL}(n, K)$  existiert, so dass  $MAM^{-1} = B$ . Aus der linearen Algebra ist bekannt, dass zwei Matrizen genau dann ähnlich sind, wenn die  $K[T]$ -Moduln  $V_A$  und  $V_B$  isomorph sind.

**Satz 0.5** (Frobenius) *Es sei  $K$  ein Körper. Es sei  $n$  eine natürliche Zahl. Es seien  $A, B \in M(n \times n, K)$  zwei Matrizen.*

*Die Matrizen  $A, B$  sind genau dann ähnlich, wenn die beiden Matrizen  $E_n T - A, E_n T - B \in M(n \times n, K[T])$  die gleichen Elementarteiler haben.*

Beweis: Es sei  $A = (a_{ij})$ , wobei  $a_{ij} \in K$ . Es sei  $e_i$  die Standardbasis des freien  $K[T]$ -Moduls  $K[T]^n$ . Es sei  $K[T]^n \rightarrow V_A$  der  $K[T]$ -Modulhomomorphismus, der durch  $e_i \mapsto \bar{e}_i$  definiert ist. Dann ist die folgende Sequenz exakt.

$$\begin{array}{ccccccc} 0 \rightarrow & K[T]^n & \xrightarrow{E_n T - A} & K[T]^n & \rightarrow & V_A & \rightarrow 0 \\ & e_i & \mapsto & T e_i - \sum_j a_{ji} e_j & & & \end{array}$$

Die Elemente  $T^t e_i$ ,  $t \in \mathbb{Z}_{\geq 0}$ ,  $i \in [1, n]$  sind eine Basis des  $K$ -Vektorraums  $K[T]^n$ . Man zeigt, dass der  $K$ -Vektorraum  $\sum_{i=1}^n K e_i$  ein Komplementärraum zum Bild von  $E_n T - A$  ist. Daraus folgt die Exaktheit.

Wir zeigen nur die Richtung, dass aus der Gleichheit der Elementarteiler die Ähnlichkeit folgt. Die Umkehrung ist nämlich einfach. Aus dem Korollar 0.3 folgt, dass es Matrizen  $X, Y \in \text{GL}(n, K[T])$  gibt, so dass  $X(E_n T - A)Y^{-1} = E_n T - B$ . Also hat man ein kommutatives Diagramm in der Kategorie der  $K[T]$ -Moduln.

$$\begin{array}{ccc} K[T]^n & \xrightarrow{E_n T - A} & K[T]^n \\ Y \downarrow & & \downarrow X \\ K[T]^n & \xrightarrow{E_n T - B} & K[T]^n \end{array}$$

Dann sind die Kokerne der horizontalen Pfeile nämlich  $V_A$  und  $V_B$  isomorph. *Q.E.D.*

**Satz 0.6** (über stabile Konjugation): *Es sei  $L/K$  ein Körpererweiterung. Es seien  $A, B \in M(n \times n, K) \subset M(n \times n, L)$  zwei Matrizen.*

*Wenn es eine Matrix  $\tilde{X} \in \text{GL}(n, L)$  gibt, so dass  $\tilde{X} A \tilde{X}^{-1} = B$ , so gibt es auch eine Matrix  $X \in \text{GL}(n, K)$ , so dass  $X A X^{-1} = B$ .*

**Beweis:** Wir müssen zeigen, dass die Elementarteiler der Matrizen  $E_n T - A$  und  $E_n T - B \in M(n \times n, K[T])$  die gleichen sind. Diese unitären Polynome  $d_{i,A}$  und  $d_{i,B} \in K[T]$  werden aber nach Voraussetzung gleich, wenn man sie als Polynome von  $L[T]$  ansieht. Also gilt  $d_{i,A} = d_{i,B}$  für  $i = 1, \dots, n$ . Nach dem Satz von Frobenius sind also die Matrizen  $A, B \in M(n \times n, K)$  ähnlich. *Q.E.D.*