Begriffe

Faser: Es sei $f : M \to N$ eine Abbildung von Mengen. Es sei $n \in N$. Die Menge $f^{-1}(\{n\}) \subset M$ nennt man die Faser in n. (Skript Seite 119).

Parallel: Zwei Vektoren v und w heißen parallel, wenn für einen Punkt $A \in \mathbb{A}$, die Punkte $A, A + v, A + w$ auf einer Geraden liegen.

Dies gilt dann auch, wenn man A durch irgendeinen anderen Punkt ersetzt.

Sätze

16.10.2012

Elemente von $\mathcal{S}_n = \mathrm{Aut}([1, n])$ heißen Permutationen. Spezielle Permutationen sind Transpositionen und Zyklen. (Vergl. Skript S.124 - 126.)

Satz E 1 *Jede Permutation ist Produkt elementfremder Zyklen.*

Satz E 2 *Es sei $\Gamma \subset \mathbb{Z}$ eine Untergruppe der additiven Gruppe der ganzen Zahlen. Dann gibt es eine Zahl $d \geq 0$, so dass*

$$\Gamma = \mathbb{Z}d.$$

18.10.2012

Satz E 3 *Es sei $(G, \cdot)$ eine Gruppe mit dem neutralen Element e_G. Es sei $g \in G$ ein Element. Dann gibt es eine ganze Zahl $d \geq 0$ mit folgender Eigenschaft:*

Wenn $d = 0$, so sind alle Potenzen g^n, für $n \in \mathbb{Z}$ verschieden.

Wenn $d > 0$, so gilt $g^n = e_G$ genau dann, wenn $d|n$ (lies: d teilt n). Allgemeiner gilt für ganze Zahlen m und n die Gleichung $g^n = g^m$ genau dann, wenn $d|n - m$.

Satz E 4 *Es sei V der Vektorraum der Translationen des Raumes $\mathbb{A}$ und es sei W der Vektorraum der Translationen einer Ebene $E \subset \mathbb{A}$.*

Es sei $\pi : \mathbb{A} \to E$ eine Parallelprojektion.

Dann gibt es genau einen Homomorphismus von Gruppen $\check{\pi} : V \to W$, so dass für alle $v \in V$ und $P \in \mathbb{A}$:

$$\pi(P + v) = \pi(P) + \check{\pi}(v).$$

23.10.2012

Satz E 5 *Es sei $\mathbb{E}$ die Ebene und es seien W die Vektoren der Ebene. Es seien $u, v \in W$ zwei Vektoren, die nicht parallel sind. Dann kann man jeden Vektor $w \in W$ schreiben:*

$$w = \xi u + \eta v, \quad \xi, \eta \in \mathbb{R}.$$

Die Zahlen ξ und η sind eindeutig bestimmt und heißen die Koordinaten des Vektors. Die Zuordnung κ, die w auf $(\xi, \eta) \in \mathbb{R}^2$ abbildet, ist ein Homomorphismus von Gruppen

$$\kappa : W \to \mathbb{R}^2.$$

κ ist bijektiv.

25.10.2012

Es seien $A, B, C \in \mathbb{E}$ drei Punkte der Ebene $\mathbb{E}$, die nicht auf einer Geraden liegen. Wir sagen, dass $(\lambda, \mu, \tau) \in \mathbb{R}^3$ baryzentrische Koordinaten des Punktes $S \in \mathbb{E}$ sind, wenn

1. $\lambda + \mu + \tau \neq 0$,
2. S ist der Schwerpunkt der gewichteten Punkte (A, λ), (B, μ), (C, τ).

Dann ist für einen beliebigen Punkt $\mathfrak{O}$ die folgende Gleichung erfüllt:

$$(\lambda + \mu + \tau)\overrightarrow{\mathfrak{O}S} = \lambda\overrightarrow{\mathfrak{O}A} + \mu\overrightarrow{\mathfrak{O}B} + \tau\overrightarrow{\mathfrak{O}S}.$$

Wir schreiben $\tilde{S} = (\lambda, \mu, \tau)$, um anzudeuten, dass wir baryzentrische Koordinaten des Punktes S betrachten. Für jedes $a \in \mathbb{R}$, $a \neq 0$, sind auch $a\tilde{S} := (a\lambda, a\mu, a\tau)$ baryzentrische Koordinaten von S und umgekehrt sind

beliebige baryzentrische Koordinaten von S von der Form $a\tilde{S}$. Die Zahl $\lambda+\mu+\tau$ nennen wir das Gewicht der baryzentrischen Koordinaten $\tilde{S}$.

Zu jedem S gibt es daher eindeutig bestimmte baryzentrische Koordinaten (λ,μ,τ) vom Gewicht 1, d.h. $\lambda+\mu+\tau=1$. Das sind die normierten baryzentrische Koordinaten von S.

Wenn wir drei reelle Zahlen (λ',μ',τ') haben, so sind das genau dann die baryzentrischen Koordinaten eines Punktes, wenn das Gewicht $\lambda'+\mu'+\tau'$ nicht 0 ist.

Wenn $a\in\mathbb{R}$, so schreiben wir

$$a(\lambda,\mu,\tau):=(a\lambda,a\mu,a\tau)$$

Wir addieren zwei Koordinaten, indem wir sie als Elemente der Gruppe $\mathbb{R}^3$ auffassen:

$$(\lambda_1,\mu_1,\tau_1)+(\lambda_2,\mu_2,\tau_2)=(\lambda_1+\lambda_2,\mu_1+\mu_2,\tau_1+\tau_2)$$

Satz E 6 *Es seien $S,T\in\mathbb{E}$ zwei verschiedene Punkte. Es seien $\tilde{S}$ bzw. $\tilde{T}$ beliebig gewählte baryzentrische Koordinaten von S bzw. T und $a,b\in\mathbb{R}$ beliebig gewählte reelle Zahlen, so dass das Gewicht von*

$$a\tilde{S}+b\tilde{T}\in\mathbb{R}^3 \tag{1}$$

nicht 0 ist. Dann sind (1) die baryzentrischen Koordinaten eines Punktes auf der Geraden ST.

Umgekehrt sind beliebige baryzentrische Koordinaten $\tilde{P}$ eines Punktes P der Geraden ST von der Form (1):

$$\tilde{P}=a\tilde{S}+b\tilde{T}.$$

30.10.2012

Satz E 7 *Es seien $P,Q\in\mathbb{E}$ zwei verschiedene Punkte. Wir wählen baryzentrische Koordinaten $\tilde{P}$ und $\tilde{Q}$, die das gleiche Gewicht haben. Es sei P' ein weiterer Punkt und es seien $\tilde{P}'$ baryzentrische Koordinaten von P'.*

Die Punkte auf der Parallelen zu PQ durch P' sind genau die Punkte, deren baryzentrische Koordinaten die Form

$$a\tilde{P}'+b(\tilde{Q}-\tilde{P}),\quad a,b\in\mathbb{R},\ a\neq 0$$

haben.

Beweis: Die baryzentrischen sind bezüglich der gewählten Punkte A, B, C gemeint. Wir wählen zusätzlich einen beliebigen Punkt $\mathfrak{O}$.

Es sei $\tilde{P} = (\lambda, \mu, \tau) \in \mathbb{R}^3$ und es sei $\tilde{Q} = (\xi, \eta, \nu) \in \mathbb{R}^3$. Nach Voraussetzung gilt

$$\lambda + \mu + \tau = \xi + \eta + \nu \neq 0.$$

Man setzt $g = \lambda + \mu + \tau$. Wenn man alle baryzentrischen Koordinaten durch g teilt, so kann man annehmen, dass

$$\lambda + \mu + \tau = \xi + \eta + \nu = 1.$$

Ein Punkt auf der Parallelen zu PQ durch P' hat die Form:

$$Q' = P' + t\overrightarrow{PQ}, \tag{2}$$

wobei $t \in \mathbb{R}$ jede reelle Zahl sein kann.

Es seien $(\xi', \eta', \nu') \in \mathbb{R}$ normierte baryzentrische Koordinaten des Punktes Q', d.h. $\xi' + \eta' + \nu' = 1$ und

$$\overrightarrow{\mathfrak{O}Q'} = \xi'\overrightarrow{\mathfrak{O}A} + \eta'\overrightarrow{\mathfrak{O}B} + \nu'\overrightarrow{\mathfrak{O}C}.$$

Aus der Gleichung (2) erhalten wir:

$$\overrightarrow{\mathfrak{O}Q'} = \overrightarrow{\mathfrak{O}P'} + t(\overrightarrow{\mathfrak{O}Q} - \overrightarrow{\mathfrak{O}P}). \tag{3}$$

Die rechte Seite dieser Gleichung formen wir mit Hilfe der baryzentrischen Koordinaten um und erhalten:

$$\begin{aligned}\overrightarrow{\mathfrak{O}Q'} &= \lambda'\overrightarrow{\mathfrak{O}A} + \mu'\overrightarrow{\mathfrak{O}B} + \tau'\overrightarrow{\mathfrak{O}C} \\ &\quad + t(\xi\overrightarrow{\mathfrak{O}A} + \eta\overrightarrow{\mathfrak{O}B} + \nu\overrightarrow{\mathfrak{O}C} - \lambda\overrightarrow{\mathfrak{O}A} - \mu\overrightarrow{\mathfrak{O}B} - \tau\overrightarrow{\mathfrak{O}C}) \\ &= (\lambda' + t(\xi - \lambda))\overrightarrow{\mathfrak{O}A} + (\mu' + t(\eta - \mu))\overrightarrow{\mathfrak{O}B} + (\tau' + t(\nu - \tau))\overrightarrow{\mathfrak{O}C}.\end{aligned}$$

Es gilt:

$$(\lambda' + t(\xi - \lambda)) + (\mu' + t(\eta - \mu)) + (\tau' + t(\nu - \tau)) = 1$$

Daher sind

$$((\lambda' + t(\xi - \lambda)), (\mu' + t(\eta - \mu)), (\tau' + t(\nu - \tau))) = \tilde{P}' - t(\tilde{Q} - \tilde{P})$$

die normierten baryzentrischen Koordinaten von Q'. $Q.E.D.$

Bemerkung: Wenn man die Sätze 6 und 7 vergleicht, so kann man zu der Ansicht kommen, dass $\tilde{Q} - \tilde{P}$ in Satz 7 die Koordinaten des unendlichen fernen Punktes der Geraden PQ sind. Das tut man in der projektiven Geometrie.

Corollary 8 *Es seien S, P, P', Q, Q' verschiedene Punkte, so dass jeweils S, P, P' und S, Q, Q' auf einer Geraden liegen. Dann kann man baryzentrische Koordinaten $\tilde{S}, \tilde{P}, \tilde{P}', \tilde{Q}, \tilde{Q}' \in \mathbb{R}^3$ finden, so dass*

$$\tilde{S} + \tilde{P} + \tilde{P}' = 0, \quad \tilde{S} + \tilde{Q} + \tilde{Q}' = 0.$$

Dann gilt

$$\tilde{P} - \tilde{Q} = \tilde{Q}' - \tilde{P}' \in \mathbb{R}^3. \tag{4}$$

Wenn das Gewicht von $\tilde{P} - \tilde{Q}$ nicht 0 ist, so sind $\tilde{P} - \tilde{Q}$ die baryzentrischen Koordinaten des Schnittpunktes der Geraden PQ und $P'Q'$. Ist dagegen das Gewicht von $\tilde{P} - \tilde{Q}$ null, so sind die Geraden PQ und $P'Q'$ parallel.

Satz E 9 *(Satz von Desargues) Es seien PQR und $P'Q'R'$ zwei Dreiecke. Wir nehmen an, dass alle aufgeführten Punkte verschieden sind. Die drei Geraden PP', QQ' und RR' mögen alle verschieden sein und sich in einem gemeinsamen Punkt S treffen, der von den Eckpunkten der Dreiecke verschieden ist.*

Wir nehmen an, dass sich
die Geraden PQ und $P'Q'$ in einem Punkt X schneiden,
die Geraden QR und $Q'R'$ in einem Punkt Y schneiden,
die Geraden RP und $R'P'$ in einem Punkt Z schneiden.

Dann liegen die Punkte X, Y, Z auf einer Geraden.

Beweis: Man findet baryzentrische Koordinaten $\tilde{S}, \tilde{P}, \tilde{P}', \tilde{Q}, \tilde{Q}', \tilde{R}, \tilde{R}' \in \mathbb{R}^3$, so dass die folgenden Gleichungen gelten:

$$\begin{aligned} \tilde{S} + \tilde{P} + \tilde{P}' &= 0 \\ \tilde{S} + \tilde{Q} + \tilde{Q}' &= 0 \\ \tilde{S} + \tilde{R} + \tilde{R}' &= 0. \end{aligned}$$

Daraus ergeben sich die Gleichungen:

$$\begin{aligned} \tilde{P} - \tilde{Q} &= \tilde{Q}' - \tilde{P}' \\ \tilde{Q} - \tilde{R} &= \tilde{R}' - \tilde{Q}' \\ \tilde{R} - \tilde{P} &= \tilde{P}' - \tilde{R}'. \end{aligned} \tag{5}$$

Da wir vorausgesetzt haben, dass die Geraden PQ und $P'Q'$ nicht parallel sind, ist nach Korollar 8 das Gewicht von $\tilde{P} - \tilde{Q}$ nicht 0 und $\tilde{X} := \tilde{P} - \tilde{Q}$ sind

baryzentrische Koordinaten des Schnittpunktes der Geraden PQ und $P'Q'$. Genauso finden wir baryzentrische Koordinaten der Punkte Y und Z:

$$\tilde{Y} = \tilde{Q} - \tilde{R}, \quad \tilde{Z} = \tilde{R} - \tilde{P}.$$

Es ergibt sich:

$$\tilde{X} + \tilde{Y} + \tilde{Z} = (\tilde{P} - \tilde{Q}) + (\tilde{Q} - \tilde{R}) + (\tilde{R} - \tilde{P}) = 0.$$

Daraus folgt nach Satz 6, dass die Punkte X, Y, Z auf einer Geraden liegen. $Q.E.D.$

6.11.2012

Wikipedia "Matrizenrechnung" (bis Einheitsmatrix).

Formale Definitionen: Ringe, Körper, Moduln (siehe Wikipedia: "Ringtheorie" (davon nur die Definition bis zum Begriff "Unterring")), "Körper (Mathematik)" (bis "Verallgemeinerungen: Schiefkörper"), "Modul (Mathematik)" (nur bis "Abelsche Gruppe") "Vektorraum" (bis "alternative Definition").

lineare Hülle, lineare Unabhängigkeit (Skript S.1-3)

8.11.2012

Der Austauschsatz (Skript Satz 4). $\dim K^n = n$, wo $K^n = M(n \times 1, K)$.

Es sei K ein Körper und es sei $(a_{ij}) \in M(m \times n, K)$ eine Matrix. Wir suchen Elemente $x_1, \ldots, x_n \in K$, so dass die folgenden Gleichungen erfüllt sind:

$$\begin{array}{c} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = 0 \\ \ldots \\ a_{m1}x_1 + a_{22}x_2 + \ldots + a_{mn}x_n = 0 \end{array} \tag{6}$$

Satz E 10 *Es sei in dem Gleichungssystem (6) $n > m$, d.h. es gibt mehr Unbekannte als Gleichungen. Dann gibt es Elemente $x_1, \ldots, x_n \in K$, die nicht alle gleich Null sind, so dass die Gleichungen (6) erfüllt sind.*

4.12.2012

Über die Spur

Es sei V ein endlich erzeuter Vektorraum. Wir fixieren eine Basis $v_1, \ldots, v_d$. Es sei $\hat{v}_1, \ldots, \hat{v}_d$ die duale Basis. Wir definieren die Spur eines Endomorphismus $\phi : V \to V$ wie folgt:

$$\text{Spur}(\phi) = \sum_{i=1}^{d} \hat{v}_i(\phi(v_i)). \tag{7}$$

Das ist eine lineare Abbildung von Vektorräumen:

$$\text{Spur} : \text{Hom}(V, V) \to K$$

Es sei $w \in V$ und es sei $\tilde{w} : K \to V$ die lineare Abbildung, welche $1 \in K$ auf w abbildet. Es sei $\ell : V \to K$ eine lineare Abbildung. Wir betrachten den Endomorphismus

$$\tilde{w} \circ \ell : V \to V.$$

Lemma 11 *Es gilt:*

$$\text{Spur}(\tilde{w} \circ \ell) = \ell(w).$$

Zum Beweis benutzen wir die folgenden einfachen Formeln:

$$\ell = \sum_{i=1}^{d} \ell(v_i)\hat{v}_i, \quad w = \sum_{i=1}^{d} \hat{v}_i(w)v_i.$$

Wir finden

$$\text{Spur}(\tilde{w} \circ \ell) = \sum_{i=1}^{d} \hat{v}_i(\ell(v_i)w) = \sum_{i=1}^{d} \ell(v_i)\hat{v}_i(w) = \ell(\sum_{i=1}^{d} \hat{v}_i(w)v_i) = \ell(w).$$

Man sieht leicht, dass die Definition (7) linear in ϕ ist. Es sei $u_1, \ldots, u_d$ eine weitere Basis und $\hat{u}_1, \ldots \hat{u}_d$ die duale Basis. Wir setzen $\phi(u_i) = w_i$. Dann hat man die Gleichung

$$\phi = \sum_{i=1}^{d} \tilde{w}_i \circ \hat{u}_i.$$

Wenn man die Spur von dieser Gleichung nimmt, so sieht man, dass die Definition (7) unabhängig von der Wahl der Basis $u_1, \ldots, u_d$ ist.

4.12.2012

Elementare Matrizen

Es seien $k, l \in [1, m]$ zwei verschiedene natürliche Zahlen. Es sei $\lambda \in K$. Dann definieren wir die Matrix $E_{kl}(\lambda) = (\epsilon_{ij}) \in M(m \times m, K)$ als die Matrix mit den folgenden Einträgen

$$\begin{aligned} &\epsilon_{ii} = 1, && \text{für } i \in [1, m] \\ &\epsilon_{kl} = 1, \\ &\epsilon_{ij} = 0, && \text{für } i \neq j, \text{ und } (i, j) \neq (k, l). \end{aligned}$$

Wir nennen $E_{kl}(\lambda)$ eine Elementarmatrix. Wenn wir hervorheben wollen, dass die Elementarmatrix die Größe $m \times m$ haben soll, schreiben wir $E_{kl}^{(m)}(\lambda)$.

Wir bezeichnen mit $e_1, \ldots, e_n \in K^n$ die Standardvektoren. Dann kann man die Definition auch schreiben:

$$E_{kl}(\lambda)e_i = e_i, \quad E_{kl}(\lambda)e_l = e_l + \lambda e_k.$$

Auf den linken Seiten der Gleichungen steht Matrixmultiplikation.

Schließlich kann man $E_{kl}(\lambda)$ auch so definieren: Es ist die Matrix die man aus der Einheitsmatrix durch die folgende Scherung erhält:

$$(k\text{-te Zeile}) := (k\text{-te Zeile}) + \lambda(l\text{-te Zeile}). \tag{8}$$

Es sei $A \in M(m \times n, K)$ eine Matrix. Es sei $A' \in M(m \times n, K)$ die Matrix, welche man aus A durch die Zeilenoperation (8) erhält. Dann gilt:

$$A' = E_{kl}(\lambda)A.$$

Es gibt auch Spaltenscherungen. Das bedeutet, dass man zur l-ten Spalte einer Matrix B ein Vielfaches einer anderen Spalte addiert. Wir schreiben das:

$$(l\text{-te Spalte}) := (l\text{-te Spalte}) + \lambda(k\text{-te Spalte}) \tag{9}$$

Es sei $B \in M(p \times m, K)$. Es sei B' die Matrix, die man aus B durch die Spaltenscherung (9) erhält. Dann gilt

$$B' = BE_{kl}(\lambda)$$

Man erhält also $E_{kl}(\lambda)$ auch, indem man auf die Einheitsmatrix die Spaltenoperation (9) anwendet.

24.1.2013

Polynome

Es sei K ein unendlicher Körper. Die Menge $\mathrm{Abb}(K,K)$ aller Abbildungen der Menge K in die Menge K ist ein (kommutativer) Ring, denn man kann zwei Funktionen $f, g \in \mathrm{Abb}(K,K)$ addieren und multiplizieren:

$$(f+g)(\lambda) = f(\lambda) + g(\lambda), \quad (fg)(\lambda) = f(\lambda)g(\lambda),$$

für alle $\lambda \in K$.

Man nennt $P \in \mathrm{Abb}(K,K)$ ein Polynom (= Polynomfunktion), wenn Elemente $a_n, \ldots, a_1, a_0 \in K$ existieren, so dass

$$P(\lambda) = a_n\lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_1\lambda + a_0 \quad \text{für alle } \lambda \in K.$$

Die Menge aller Polynome ist ein Teilring von $\mathrm{Abb}(K,K)$. Wir bezeichnen mit $T : K \to K$ die Funktion $T(\lambda) = \lambda$. Den Ring der Polynome bezeichnen wir mit $K[T]$.

Dann können wir das Polynom P schreiben:

$$P = a_nT^n + a_{n-1}T^{n-1} + \ldots + a_1T + a_0. \tag{10}$$

Hier versteht man unter a_0 die konstante Funktion $a_0(\lambda) = a_0$. Es gilt $T^m(\lambda) = \lambda^m$ für jede natürliche Zahl m. Die Funktionen $1, T, T^2, T^3, \ldots$ sind linear unabhängig (siehe Skript Seite 49). Es sei $P \neq 0$. Dann hat P eine eindeutige Darstellung (10) mit $a_n \neq 0$. Wir nennen a_n den *höchsten Koeffizienten* von P. Wir definieren

$$\deg P = n \quad \deg 0 = -\infty$$

Für zwei Polynome P, Q:

$$\deg(P+Q) \leq \max\{\deg P, \deg Q\}, \quad \deg(PQ) = \deg P + \deg Q.$$

Man überlege, was passiert, wenn $P = 0$.

Wenn P eine Darstellung (10) besitzt, so dass $a_n = 1$, so nennen wir P ein *unitäres* Polynom.

Satz E 12 *Es seien P und Q Polynome. Es sei $Q \neq 0$.*

Dann existieren eindeutig bestimmte Polynome A, R, so dass

$$P = QA + R, \quad \deg R < \deg Q.$$

(siehe Übungszettel 8).

Definition 13 *Eine Teilmenge $I \subset K[T]$ des Polynomrings heißt ein* Ideal, *wenn die folgenden Eigenschaften erfüllt sind:*

1. $0 \in I$.
2. *Wenn $P \in I$, so gilt auch $-P \in I$.*
3. *Wenn $P, Q \in I$, so gilt $P + Q \in I$.*
4. *Wenn $P \in I$ und $A \in K[T]$, so gilt $AP \in I$.*

Hier ist Punkt 2 eine Folge von Punkt 4. Eine Teilmenge I ist genau dann ein Ideal, wenn $I \subset K[T]$ ein K-Untervektorraum ist und wenn $TI \subset I$.

Es sei $D \in K[T]$. Dann ist die folgende Menge eine Ideal

$$I = \{AD \mid A \in K[T]\}$$

Solche Ideale heißen Hauptideale. Wir schreiben $I = K[T]D$. Wenn $P \in K[T]D$, so heißt D ein Teiler von P. in Zeichen $D|P$. Wenn D' ein weiteres Polynom ist, so dass $I = K[T]D'$, so folgt $D|D'$ und $D'|D$. Dann gibt es ein $c \in K$ mit $c \neq 0$, so dass

$$D' = cD$$

Wenn $I \neq 0$ ein Hauptideal ist, gibt es daher ein eindeutig bestimmtes unitäres Polynom D, so dass $I = K[T]D$.

Theorem 14 *(Hauptidealsatz) Jedes Ideal $I \subset K[T]$ ist ein Hauptideal.*

Es seien P, Q zwei Polynome. Dann ist die folgende Menge eine Ideal:

$$I = \{AP + BQ \mid A, B \in K[T]\}.$$

Nach dem Hauptidealsatz existiert also ein $D \in K[T]$, so dass $I = K[T]D$. Insbesondere folgt

$$D|P \text{ und } D|Q.$$

Uns interessieren nur die Fälle, wo P oder Q nicht null ist. Dann ist auch $D \neq 0$. Da $D \in I$ ist, gibt es eine Darstellung

$$D = AP + BQ.$$

Man sieht, dass D die folgende Eigenschaft hat:

- Es sei $E \in K[T]$ ein Polynom, so dass $E|P$ und $E|Q$. Dann folgt $E|D$.

Das eindeutig bestimmte unitäre Polynom D mit $I = K[T]D$ nenne wir den *größten gemeinsamen Teiler* der Polynome P und Q.

Definition 15 *Wir nennen ein Polynom P irreduzibel, wenn* $\deg P \geq 1$ *und wenn es keine Darstellung*

$$P = AB$$

gibt, wobei A und B Polynome sind für die $\deg A \geq 1$ *und* $\deg B \geq 1$.

Satz E 16 *Es sei P ein irreduzibles Polynom. Es seien A, B Polynome, so dass*

$$P|AB.$$

Dann gilt $P|A$ oder $P|B$.

Man nennt auf Grund dieser Eigenschaft irreduzible Polynome auch Primpolynome.

Es sei K ein (unendlicher) Körper und $K[T]$ der Polynomring. Das ist insbesondere ein K-Vetorraum. Es sei $I \subset K[T]$ ein Ideal. Da I insbesondere ein Untervektorraum von $K[T]$ ist, gibt es einen komplementären Untervektorraum $F \subset K[T]$:

$$I \oplus F = K[T].$$

Wir betrachten die parallele Projektion π längs I:

$$\begin{array}{rccl} \pi: & K[T] = I \oplus F & \to & F, \\ & P + R & \mapsto & R \end{array} \tag{11}$$

wobei $P \in I$ und $R \in F$. Die Fasern dieser Abbildung sind alle Mengen der Form $I + R$.

Expliziter kann man F und π so erhalten. Es sei $I = K[T]D$. Wir nehmen an, dass D folgende Form hat: $D = T^d + \alpha_{d-1}T^{d-1} + \ldots \alpha_1 T + \alpha_0, \quad \alpha_i \in K$ und $d \in \mathbb{Z}$, $d > 0$.

Es sei $Q \in K[T]$. Nach der Division mit Rest können wir schreiben:

$$Q = AD + R, \quad \deg R < d = \deg D.$$

Wir erhalten einen Homomorphismus von Vektorräumen

$$\pi : K[T] \to \mathcal{L}(1, T, \ldots, T^{d-1}) =: F$$

wenn wir $\pi(Q) = R$ definieren. Es folgt, dass $K[T] = I \oplus F$.

Wir kehren zur abstrakten Situation (11) zurück:

Satz E 17 *Es gibt eine eindeutig bestimmte Abbildung*

$$\begin{array}{rccc} \cdot_F : & F \times F & \to & F, \\ & (a,b) & \mapsto & a \cdot_F b \end{array}$$

so dass für alle $A, B \in K[T]$

$$\pi(A \cdot B) = \pi(A) \cdot_F \pi(B), \tag{12}$$

wobei hier auf der linken Seite die gewöhnliche Multiplikation von Polynomen steht.

Mit der Multiplikation $\cdot_F$ *wird die abelsche Gruppe* $(F, +)$ *ein Ring.*

Beweis: Es seien $a, b \in F$. Wir wählen Polynome $A, B \in K[T]$, so dass $\pi(A) = a$ und $\pi(B) = b$. Nach (12) sind wir gezwungen zu definieren:

$$a \cdot_F b := \pi(A \cdot B).$$

Damit diese Definition sinnvoll ist, darf das Element auf der rechten Seite nicht von der Wahl von A und B abhängen. Es seien A_1 und B_1 zwei weitere Polynome, so dass $\pi(A_1) = a$ und $\pi(B_1) = b$. Wir können schreiben:

$$A_1 = A + U, \quad B_1 = B + V, \quad \text{wo } U, V \in I.$$

Dann gilt:

$$A_1 \cdot B_1 = A \cdot B + (A_1 \cdot V + U \cdot B_1 + U \cdot V).$$

Da das Element in der Klammer zu I gehört, gilt

$$\pi(A \cdot B) = \pi(A_1 \cdot B_1).$$

Damit ist die Existenz und die Eindeutigkeit von $\cdot_F$ bewiesen.

Man muss noch zeigen, dass man einen Ring erhält. Das ist eine Übungsaufgabe. *Q.E.D.*