Lineare Algebra II

Vorlesung, gehalten im Sommersemester 1999
Sigrid Böge

Inhalt

1. Moduln über Hauptidealringen
2. Anwendungen des Invariantenteilersatzes
3. Verallgemeinerung der Jordanschen Normalform
4. Alternierende p-Linearformen
5. Graßmannalgebra
6. Pfaffsche Determinante
7. Projektive Geometrie
8. Doppelverhältnis
9. Projektive und affine Klassifikation der Quadriken
10. Projektive Erzeugung der Kegelschnitte nach Steiner
11. Resultate
12. Anwendung auf die elementare Geometrie der kubischen Kurven
13. Endliche Drehgruppen im $\mathbb{R}^3$

1. Moduln über Hauptidealringen

In Kap.12-15 haben wir viel mit Polynomen gerechnet und festgestellt: Zu je zwei Polynomen $f, g \neq 0$ gibt es genau ein normiertes Polynom d mit

a) f und g sind beide durch d teilbar
b) d läßt sich aus f und g kombinieren: $d = uf + vg$ mit geeigneten Polynomen u und v, was insbesondere zur Folge hat, daß jeder gemeinsame Teiler von f und g auch in d aufgeht.

Wir wollen jetzt für eine größere Klasse von Ringen, welche diese Eigenschaft mit dem Polynomring $K[X]$ über einem Körper K gemeinsam haben, den Satz 41 in einer abstrakten Form beweisen. Dabei wird nichts aus Kap.14 verwendet, der Beweis wird unabhängig davon, elegant und allgemeiner sein. Dafür hat er gegenüber Kap 14 den typischen Nachteil, daß er nicht "konstruktiv" ist, d.h. er gibt keinen Hinweis darauf, wie man die Invariantenteiler $\alpha_1, ..., \alpha_n$ (siehe Satz 3 unten) tatsächlich finden kann: dieses Defizit ist der Preis für den "höheren Standpunkt".

Im Folgenden sei stets A ein kommutativer ($\alpha\beta = \beta\alpha$) nullteilerfreier ($\alpha\beta = 0 \Rightarrow \alpha$ oder $\beta = 0$) Ring mit Eins.

Definition 1: Ein A-Modul M ist eine additive Gruppe, deren Elemente man distributiv mit den Elementen aus A multiplizieren kann:

$$\alpha(x+y) = \alpha x + \alpha y \text{ und } (\alpha+\beta)x = \alpha x + \beta x \text{ für } \alpha, \beta \in A, x, y \in M$$

Und es gilt

$$\alpha(\beta x) = (\alpha\beta)x \text{ und } 1 \cdot x = x \text{ für alle } \alpha, \beta \in A, x \in M$$

1.Beispiel: Jede abelsche Gruppe ist ein $\mathbb{Z}$-Modul vermöge

$$m \cdot x = x + x + ... + x \ \ (m \text{ mal }), \text{ falls } m > 0 \text{ und } m \cdot x = -|m| \cdot x \text{ falls } m < 0$$

2.Beispiel: Wenn A ein Körper ist, dann bedeutet A-Modul dasselbe wie Vektorraum über A

Definition 2: Ein Ideal I in A ist eine Teilmenge von A mit

$$I + I \subset I \text{ und } A \cdot I \subset I$$

Beispiele:
(1) $5\mathbb{Z}$ ist Ideal in $\mathbb{Z}$
(2) $\mathbb{Z}$ ist nicht Ideal in $\mathbb{Z}[i] = \{x + iy \in \mathbb{C} \mid x, y \in \mathbb{Z}\}$
(3) $I_a := \{f \in K[X] \mid f(a) = 0\}$ ($a \in K$ fest) ist Ideal in $K[X]$.
(4) $\{f \in K[X,Y] \mid f(0,0) = 0\}$ ist Ideal in $K[X,Y]$.

Definition 3: Ein Ideal I in A heißt Hauptideal, wenn es $\alpha \in I$ gibt mit $I = A\alpha$.

Von den Beispielen nach Definition 2 sind (1) und (3) Hauptideale. (4) nicht. (Was ist das α im Falle (3)?)

Definition 4: A heißt Hauptidealring, wenn in A jedes Ideal Hauptideal ist.

Satz 1. *Für jeden Körper K ist $K[X]$ Hauptidealring.*

Beweis: Sei $I \neq 0$ Ideal in $K[X]$. Unter allen Polynomen $\neq 0$ aus I sei f eines mit möglichst kleinem Grad. Sei $g \in I$ beliebig. Teile g mit Rest durch f: $g = qf + r$ mit $r = 0$ oder grad $r <$ grad f. Da f und g in I, ist auch r in I. Da grad f minimal, folgt $r = 0$: $g = q \cdot f$. Das beweist $I = K[X] \cdot f$.

Bemerkung: Hier sieht man den Unterschied der Betrachtungsweisen: Sind f und g gegebene Polynome, so bilden die Polynome $uf+vg$ mit $u, v \in K[X]$ ein Ideal I in $K[X]$. Daß dieses Hauptideal ist, bedeutet: es gibt $d \in I$ so, daß $I = K[X]d$, d.h. daß einerseits (nach Definition von I) d die Gestalt $uf+vg$ hat, und daß anderseits alle Polynome aus I (also f und g) Vielfache von d sind. Die bloße Existenz von d folgt wie oben in drei Zeilen aus dem Wohlordnungsprinzip der natürlichen Zahlen (unter den Polynomgraden in I gibt es einen kleinsten). Die Konstruktion von d geschieht mit Hilfe des Euklidischen Algorithmus. Der Beweis von Satz 1 gilt für jedes Ideal; der Euklidische Algorithmus zunächst für von zwei Polynomen erzeugte Ideale.

Satz 1'. *$\mathbb{Z}$ ist Hauptidealring.*

Beweis: Sei $I \neq 0$ ein Ideal in $\mathbb{Z}$. Unter allen Zahlen $\neq 0$ in I sei a die kleinste positive. Sei m in I beliebig. Teile m mit Rest durch a: $m = qa + r$, $0 \leq r < a$. Da m und a in I, muß auch r in I, und, da a minimal war, $= 0$ sein: $m = qa$. Das zeigt $I = \mathbb{Z}a$.

Jetzt sieht jeder, dass man denselben Beweis in jedem Ring führen kann, der eine Division mit Rest gestattet, z.B. in $\mathbb{Z}[i]$ (Übung).

Definition 5: Ein A-Modul M heißt endlich erzeugt, wenn es in ihm endlich viele Elemente $x_1, ..., x_n$ gibt mit $M = Ax_1 + ... + Ax_n$ (Vergleiche Kap.3, Def.5)

Definition 6: Ein endlich erzeugter A-Modul M heißt frei, wenn er eine Basis besitzt, d.h. daß jedes $x \in M$ eine *eindeutige* Darstellung $x = \alpha_1 x_1 + ... + \alpha_n x_n$ mit $\alpha_i \in A$ besitzt.

1.Bemerkung: Für die Definition 6 ist es nicht wichtig, daß M endlich erzeugt ist. Aber unser Hauptergebnis wird ohnehin nur in diesem Falle Sinn machen.

2.Bemerkung: Ist A ein Körper, so ist jeder A-Modul frei. (Jeder Vektorraum besitzt eine Basis).

Satz 2. *Sei A ein Hauptidealring und L ein freier A-Modul. Dann ist jeder A-Untermodul M von L frei.*

Beweis: Sei $x_1, ..., x_n$ eine Basis von L über A. Induktion nach n:
$n = 1$, $L = Ax_1$: $I := \{\lambda \in A \mid \lambda x_1 \in M\}$ ist ein Ideal in A, nach Voraussetzung $= \alpha A$ mit $\alpha \in I$. Jedes $y \in M$ ist eindeutig darstellbar als Vielfaches von αx_1.
$n > 1$: Die $\lambda \in A$, für die es ein Element $y \in M$ gibt mit letzter Komponente λ, d.h.

$$y = ?x_1 + ?x_2 + ... + ?x_{n-1} + \lambda x_n$$

bilden ein Ideal I in A. Wenn $I = 0$, dann ist $M \subset Ax_1 + ... + Ax_{n-1}$. Dieser Fall ist erledigt nach Induktionsannahme. Wenn $I \neq 0$, dann ist $I = A\alpha$ mit $0 \neq \alpha \in A$. Sei etwa α der letzte Koeffizient von $y = \eta_1 x_1 + ... + \eta_{n-1} x_{n-1} + \alpha x_n \in M$. Nun sei $x = \xi_1 x_1 + ... + \xi_n x_n \in M$ beliebig. Nach Definition von I ist $\xi_n \in I$, etwa $= \lambda\alpha$. Dann ist $x - \lambda y \in L_{n-1} := Ax_1 + ... + Ax_{n-1}$ und natürlich in M. Dies zeigt

$$M = Ay + (M \cap L_{n-1})$$

Diese Summe ist direkt (d.h. die Summanden haben Durschnitt 0), weil α, die letzte Komponente von y, nicht 0 ist. Nach Induktionsannahme ist $M \cap L_{n-1}$ frei. Nun ist auch M frei.

Satz 2 und sein Beweis zeigen: Fur jeden Untermodul M von L kann man eine Basis finden, die durch Dreieckssubstitution aus einer gegebenen (notfalls noch umzunumerierenden) Basis von L hervorgeht. Insbesondere: Besitzt L eine Basis aus n Vektoren, so besitzt jeder Untermodul von L eine Basis aus höchstens n Vektoren. Als nächstes zeigen wir: wenn man nicht nur die Basis von M passend sucht, sondern auch die von L geeignet abändert, dann kann man sogar eine Basis von M finden, die aus dieser geeigneten von L durch Diagonalsubstitution hervorgeht. Um den Beweis davon nicht zu unterbrechen, beweisen wir vorher

Lemma 1. *In einem Hauptidealring A gibt es in jeder nicht leeren Menge von Idealen ein maximales, das ist eines, welches in keinem anderen Ideal der Menge echt enthalten ist.*

Beweis: Sei $\mathfrak{M}$ eine nicht leere Menge von Idealen in A. Gäbe es darin kein maximales, so könnte man eine unendliche echt aufsteigende Kette

$$I_1 \subsetneq I_2 \subsetneq .....$$

von Idealen $I_j \in \mathfrak{M}$ finden. $I := \cup_{i=1}^{\infty} I_j$ wäre dann auch ein Ideal, also ein $A\alpha$. mit $\alpha \in I$. Dieses α läge, da in der Vereinigung, in irgendeinem der I_j. Dann wäre aber I und damit alle $I_k \subset I_j$.

Satz 3. *Sei A ein Hauptidealring und L ein endlich erzeugter freier A-Modul und M ein Untermodul von L. Dann gibt es eine Basis $e_1, ..., e_n$ von L und Elemente $\alpha_1, ..., \alpha_k$ $(k \leq n)$ von A so, daß $\alpha_1 e_1, ..., \alpha_k e_k$ eine Basis von M bilden, und daß überdies $\alpha_1 | \alpha_2 | .... | \alpha_k$.*

Beweis: Sei L^* der A-Modul aller A-linearen Abbildungen von L nach A (sogenannte Linearformen). Für jedes g in L^* ist $g(M) = \{g(x) | x \in M\}$ ein Ideal in A. Unter den Idealen $g(M)$ ($g \in L^*$) gibt es

ein maximales, etwa $I = f(M)$. Da A Hauptidealring ist, ist $I = A\alpha$ mit $\alpha \in I$, etwa $\alpha = f(m)$. $L^*(m)$ ist auch ein Hauptideal, etwa $= A \cdot g(m)$. Nun haben wir

$$f(M) = A\alpha = Af(m) \subset L^*(m) = Ag(m) = g(Am) \subset g(M) \tag{1}$$

Da $f(M)$ maximal war, steht überall $=$, also

$$f(M) = A\alpha = L^*(m)$$

L ist frei, besitzt also eine Basis $x_1, ..., x_n$ über A. Sei π_i die Projektion auf die i-te Komponente, also $\pi_i(\lambda_1 x_1 + ... + \lambda_n x_n) = \lambda_i$. Die π_i sind aus L^*, nach (1) ist also $\pi_i(m) = \gamma_i \alpha$ mit $\gamma_i \in A$. Das bedeutet $m = \gamma_1 \alpha x_1 + ... + \gamma_n \alpha x_n$. Man setzt $e = \gamma_1 x_1 + ... + \gamma_n x_n$. Dann ist $m = \alpha e$, und aus $f(m) = \alpha$ folgt $f(e) = 1$. Für jedes $x \in L$ gilt

$$x = f(x)\, e + (x - f(x)\, e)$$

Das zeigt: L und M besitzen direkte Zerlegungen

$$L = Ae \oplus Kern\ f \text{ und } M = Am \oplus (M \cap Kern\ f)$$

Nach Satz 2 ist Kern f wieder frei. Kern f läßt sich mit weniger als n Elementen erzeugen. Um das zu sehen, könnte man sich darauf berufen, dass A in seinem Quotientenkörper K und L in einem K-Vektorraum enthalten ist, und daß n die Dimension dieses K-Vektorraumes ist und die Hyperebene $f = 0$ die Kodimension 1 hat. Kennt man dies alles nicht, so kommt man vielleicht so am schnellsten zum Ziel: Nach der Bemerkung hinter Satz 2 kann man den Untermodul Kern f jedenfalls durch höchstens n Elemente y_j aufspannen, die aus $x_1, ..., x_n$, eventuell nach Umnumerierung, durch Dreieckssubstiution hervorgehen:

$$\begin{array}{lcl}
y_k & = & \beta_{1k}x_1 + ... + \beta_{kk}x_k \\
y_{k+1} & = & \beta_{1,k+1}x_1 + ... + \beta_{k+1,k+1}x_{k+1} \\
\vdots & & \\
y_n & = & \beta_{1n}x_1 + ... + \beta_{nn}x_n
\end{array}$$

mit $\prod \beta_{ii} \neq 0$. Wäre $k = 1$, so folgte aus $f(y_j) = 0$ und $\beta_{jj} \neq 0$ der Reihe nach $f(x_1) = f(x_2) = ... = f(x_n) = 0$, Widerspruch gegen $f \neq 0$.
Nach Induktionsannahme gibt es nun eine Basis $e_2, ..., e_n$ von Kern f und $\alpha_2 | \alpha_3 | .... | \alpha_k$ $(k \leq n)$ so, dass die $\alpha_i e_i$ eine Basis von $M \cap$ Kern f bilden. Wenn wir jetzt noch zeigen können, daß $\alpha | \alpha_2$, dann sind wir fertig. Dazu sei h eine beliebige Linearform auf Kern f. Durch $h(e) = 1$ setzt man sie auf L fort. Dann ist

$$h(M) = h(Am + (M \cap \text{ Kern } f)) = Ah(m) + h(M \cap \text{ Kern } f) = A\alpha + h(M \cap \text{ Kern } f) \supset A\alpha$$

Da $A\alpha$ maximal unter allen $h(M)$ war, folgt $h(M \cap$ Kern $f) \subset A\alpha$, und daher $\alpha_2 \in A\alpha$, qed.

Eine besonders kurze Anwendung des Beweisgedankens von Satz 3 ist: Jeder primitive Vektor in einem freien A-Modul L läßt sich zu einer Basis von L ergänzen. Dabei heißt ein Vektor x primitiv, wenn für jedes $y \in L$ aus $x \in Ay$ folgt, daß $y \in Ax$. Beweis: Ist $x_1, ..., x_n$ eine beliebige Basis von L und $x = \lambda_1 x_1 + ... + \lambda_n x_n$ primitiv, so sind die λ_i teilerfremd. Daß sich aus ihnen die 1 kombinieren läßt, bedeutet: es gibt eine Linearform f auf L mit $f(x) = 1$. Dann ist $L = Ax \oplus$ Kern f.

2. Anwendungen des Invariantenteilersatzes

In der ersten Anwendung ist $A = \mathbb{Z}$.

Definition: Sind $v_1, ..., v_n$ n linear unabhängige Vektoren des $\mathbb{R}^n$, so heißt $L = \mathbb{Z}v_1 + ... + \mathbb{Z}v_n$ das von $v_1, ..., v_n$ aufgespannte Gitter. Das Parallelotop

$$\{\sum_{i=1}^{n} \lambda_i v_i | 0 \leq \lambda_i < 1\}$$

heißt eine Fundamentalmasche des Gitters.

Natürlich besitzt das Gitter unendlich viele Basen und damit Fundamentalmaschen, aber diese haben alle dasselbe Volumen, nämlich den Absolutbetrag der Determinante der Spaltenvektoren $v_1, ..., v_n$. Illustration von Satz 3:

Gegeben das Gitter L im $\mathbb{R}^2$ mit Basis $\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}$ und das Untergitter M mit Basis $\begin{pmatrix}2\\1\end{pmatrix}, \begin{pmatrix}-1\\2\end{pmatrix}$.

Die Linearformen auf L sind die Zeilen (r, s) mit $r, s \in \mathbb{Z}$ vermöge $(r, s)\begin{pmatrix}x\\y\end{pmatrix} = rx + sy$. Die Gleichung (1) aus Kap.1 ist in diesem Falle erfülllt mit

$$(0,1)M = \mathbb{Z} = \mathbb{Z}(0,1)\begin{pmatrix}2\\1\end{pmatrix} = L^*\begin{pmatrix}2\\1\end{pmatrix}$$

also $\alpha = 1, e = m = \begin{pmatrix}2\\1\end{pmatrix}$. Die Zerlegung der $x \in L$ lautet

$$x = x_2 e + (x - x_2 e) = x_2\begin{pmatrix}2\\1\end{pmatrix} + \begin{pmatrix}x_1 - 2x_2\\0\end{pmatrix}, \text{ und}$$

$$M \cap \text{ Kern } f = \{\lambda\begin{pmatrix}2\\1\end{pmatrix} + \mu\begin{pmatrix}-1\\2\end{pmatrix} | \lambda + 2\mu = 0\} = \mathbb{Z}\begin{pmatrix}5\\0\end{pmatrix}$$

Die gesuchte Basis von L ist $e_1 = \begin{pmatrix}2\\1\end{pmatrix}, e_2 = \begin{pmatrix}1\\0\end{pmatrix}$, die Invariantenteiler sind $\alpha_1 = 1, \alpha_2 = 5$.

Rechts kann man 5 Fundamentalmachen von L in eine von M packen. Allgemein: wenn

$$e_1, ..., e_n \text{ Basis von } L \text{ und } \alpha_1 e_1, ..., \alpha_n e_n \text{ Basis von } M, \alpha_i > 0$$

so kann man $k := \prod_{i=1}^{n} \alpha_i$ Fundamentalmaschen von L in eine von M packen (und diese ist dadurch ausgefüllt). Man nennt k den Index von M in L, Bezeichnug: $k = (L : M)$. Er ist das Verhältnis der Volumina der Fundamentalmachen von M und L. Dieses Verhältnis ist

$$(L : M) = \frac{|\det(v_1, ..., v_n)|}{|\det(u_1, ..., u_n)|}$$

für jede Basis $v_1, ..., v_n$ von M bzw. $u_1, ..., u_n$ von L.

Noch etwas Geometrisches über Gitter:

Lemma 1. *(Blichfeldt) Sei L ein Gitter im $\mathbb{R}^n$ mit Fundamentalmasche F und B eine Teilmenge des $\mathbb{R}^n$, welche ein Volumen besitzt, das echt größer als das Volumen von F ist. Dann gibt es $x, y \in B$ mit $0 \neq x - y \in L$.*

Beweis:

$$\mathbb{R}^n = \cup_{a \in L}(a + F), \quad \text{daher } B = \cup_{a \in L}(B \cap (a + F))$$

und die Vereinigungen sind disjunkt. Aus der Translationsinvarianz des Volumens folgt

$$Vol(B) = \sum_{a \in L} Vol(B \cap (a + F)) = \sum_{a \in L} Vol((B - a) \cap F)$$

Das Letzte wäre $= Vol(\cup_{a \in L}(F \cap (B - a)) \leq Vol(F)$, wenn diese Vereinigung disjunkt wäre. Da aber nach Voraussetzung $Vol(B) > Vol(F)$, kann die Vereinigung nicht disjunkt sein, und es gibt $a \neq b$ in L mit $(F \cap (B - a)) \cap (F \cap (B - b)) \neq \phi$. Ist etwa $x - a = y - b$ mit $x, y \in B$, so folgt $0 \neq x - y = a - b \in L$.

Dieses Lemma dient zum Beweis des Minkowskischen Gitterpunktsatzes:

Satz 4. *Sei L ein Gitter mit Fundamentalmasche F und S eine symmetrische konvexe Menge mit $Vol(S) > 2^n Vol(F)$. Dann enthält S einen von 0 verschiedenen Gitterpunkt.*

Beweis: Nach dem Lemma gibt es $x, y \in \frac{1}{2}S$ mit $0 \neq x - y \in L$

$$S \text{ symmetrisch } \Rightarrow 2x \text{ und } -2y \in S$$

$$S \text{ konvex } \Rightarrow \frac{1}{2}(2x + (-2y)) = x - y \in S$$

Also ist $0 \neq x - y \in L \cap S$.

Ist zum Beispiel die Fläche der Fundamentalmasche eines ebenen Gitters gleich p, so enthält die Kreisscheibe vom Radius $\sqrt{2p}$ einen von 0 verschiedenen Gitterpunkt, weil $2\pi > 4$.

2. Anwendung: Sei G eine endlich erzeugte abelsche Gruppe und $g_1, ..., g_n$ Erzeugende von G. Wir schreiben die Gruppenoperation in G als $+$. Die Elemente von G sind also alle $m_1 g_1 + m_2 g_2 + ... + m_n g_n$ mit $m_i \in \mathbb{Z}$. Natürlich ist diese Darstellung nicht eindeutig. Im Gegenteil: normalerweise ist

$$L := \{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{Z} \mid x_1 g_1 + x_2 g_2 + ... + x_n g_n = 0 \text{ in } G \}$$

nicht 0. Nach Definition ist L ein Untergitter in $\mathbb{Z}^n$. Nach Satz 3 gibt es eine Basis $u_1, ..., u_n$ von $\mathbb{Z}^n$ und $\alpha_1, ..., \alpha_k \in \mathbb{Z}$ mit $\alpha_1 | ... | \alpha_k$ $(k \leq n)$, so dass $\alpha_1 u_1, ..., \alpha_k u_k$ eine Basis von L bilden. Ist $e_1, ..., e_n$ die Standardbasis des $\mathbb{R}^n$, so ist $u_i = \sum_{j=1}^n a_{ji} e_j$ mit einer ganzzahlligen und ganzzahlig umkehrbaren Matrix $A = (a_{ij})$. Daher bilden auch die $h_i = \sum_{j=1}^n a_{ji} g_j$ ein Erzeugendensystem von G. Nun ist für $\lambda_1, ..., \lambda_n \in \mathbb{Z}$

$$\sum_i \lambda_i h_i = 0 \Leftrightarrow \sum_{i,j} \lambda_i a_{ji} g_j = 0 \Leftrightarrow \sum_{i,j} \lambda_i a_{ji} e_j \in L \Leftrightarrow \sum_i \lambda_i u_i \in L \Leftrightarrow \lambda_i = 0 \text{ für } i > k \text{ und } \alpha_i | \lambda_i \text{ für } i \leq k$$

Die Elemente $g \in G$ sind in eindeutiger Darstellung gegeben durch

(1) $$g = \lambda_1 h_1 + ... + \lambda_n h_n \text{ mit } \lambda_i \in \mathbb{Z} \text{ für alle } i \text{ und } 0 \leq \lambda_i < \alpha_i \text{ für } i \leq k$$

denn wegen $\alpha_i h_i = 0$ kommt es bei den ersten k Koeffizienten genau auf den Rest modulo α_i an.

Definition: Eine additiv geschriebene Gruppe H heißt zyklisch, wenn es in ihr ein Element h gibt so daß jedes Element aus H ein Vielfaches mh $(m \in \mathbb{Z})$ von h ist. Ein solches h heisst ein erzeugendes Element von H.

Ist m die kleinste Zahl > 0 mit $mh = 0$, so ist $H = \{0, h, 2h, ..., (m-1)h\}$. Diese Gruppe bezeichnet man mit Z_m. Gibt es ein solches m nicht, so ist $H \simeq \mathbb{Z}$.

Beispiel: Die n-ten Einheitswurzeln in $\mathbb{C}$ bilden eine (multiplikative) zyklische Gruppe der Ordnung n, ein erzeugendes Element ist $e^{\frac{2\pi i}{n}}$. Die Uhr ist eine (additive) zyklische Gruppe der Ordnung 12.

(1) kann man auch so ausdrücken: Jedes h_i erzeugt eine zyklische Untergruppe von G. Diese ist $\simeq \mathbb{Z}$ für $i > k$ und $\simeq Z_{\alpha_i}$ für $i \leq k$. Die Elemente aus G entsprechen umkehrbar eindeutig den n-Tupeln $(x_1, ..., x_n)$ mit $x_i \in Z_{\alpha_i}$ bzw. $x_i \in \mathbb{Z}$. Das formuliert man als

Satz 5. *(Hauptsatz für endlich erzeugte abelsche Gruppen) Jede endlich erzeugte (additiv geschriebene) abelsche Gruppe ist eine direkte Summe von zyklischen Gruppen*

$$Z_{\alpha_1} \oplus .... \oplus Z_{\alpha_k} \oplus \mathbb{Z} \oplus .... \oplus \mathbb{Z} \tag{2}$$

wobei Z_{α_i} die zyklische Gruppe der Ordnung α_i ist und außerdem $\alpha_1|....|\alpha_k$ erreicht werden kann.

Da G abelsch ist, bilden die Elemente endlicher Ordnung eine Untergruppe von G. Diese heißt die Torsionsuntergruppe $T(G)$ von G. Aus (2) sieht man $T(G) = Z_{\alpha_1} \oplus .... \oplus Z_{\alpha_k}$. Außerdem folgt aus Satz 5

Satz 6. *Ist G abelsch und endlich erzeugt und ist die Torsion von G null, so ist G frei als $\mathbb{Z}$-Modul.*

Dies trifft insbesondere für jede endlich erzeugte Untergruppe des $\mathbb{R}^n$ zu: jede solche ist ein Gitter (möglicherweise in einem Unterraum kleinerer Dimension).

Satz 5 kann dazu dienen, alle Isomorphietypen von abelschen Gruppen gegebener Ordnung n aufzustellen. Dazu muß man alle Zerlegungen $n = \prod_{i=1}^{k} \alpha_i$ mit $\alpha_1|....|\alpha_k$ hinschreiben. Um zu sehen, daß die so erhaltenen Typen tatsächlich alle verschieden sind, beweist man

Satz 7. *$\alpha_1, ..., \alpha_k > 0$ mit $\alpha_1|....|\alpha_k$ sind durch $G = Z_{\alpha_1} \oplus .... \oplus Z_{\alpha_k}$ eindeutig bestimmt.*

Beweis: Sei p eine Primzahl und $\alpha = p^\mu u$ mit $p \nmid u$. In der zyklischen Gruppe $Z_\alpha = \{0, g, 2g, ..., (\alpha-1)g\}$ der Ordnung α zählen wir die Elemente ig, die von p^l annulliert werden:

$$p^l \cdot ig = 0 \Leftrightarrow \alpha | p^l i \Leftrightarrow \begin{cases} u|i & \text{falls } \mu \le l \\ p^{\mu-l}|i & \text{falls } \mu > l \end{cases}$$

Die Anzahl der $i \in \{0, 1, ..., \alpha - 1\}$ (und damit der $ig \in Z_\alpha$) mit $p^l ig = 0$ ist also

$$= \begin{cases} \frac{\alpha}{u} = p^\mu & \text{falls } \mu \le l \\ \frac{\alpha}{p^{\mu-l}u} = p^l & \text{falls } \mu \ge l \end{cases} \tag{1}$$

Sei $G(p^l)$ die von p^l annullierte Untergruppe von G. Nach (1) gilt

$$\frac{|Z_\alpha(p^{l+1})|}{|Z_\alpha(p^l)|} = \begin{cases} p & \text{wenn } l < \mu \\ 1 & \text{wenn } l \ge \mu \end{cases} \tag{2}$$

Daraus folgt

$$\frac{|G(p^{l+1})|}{|G(p^l)|} = \prod_{1 \le i \le k, l < \mu_i} p \quad = p^{N_l} \tag{3}$$

wobei N_l die Anzahl der i ist mit $\mu_i > l$. Wegen $\alpha_1|....|\alpha_k$ liegt damit fest, welche der α_i durch p^l teilbar sind, nämlich die letzten N_l. Man muß natürlich nur die Primzahlen p in Betracht ziehen, die in der Gruppenordnung aufgehen.

Beispiel: $n = 360 = 2^3 \cdot 3^2 \cdot 5$. Die möglichen Zerlegungen mit der Teilbarkeitsbedingung sind

$$360 = 2 \cdot 180 = 2 \cdot 2 \cdot 90 = 3 \cdot 120 = 6 \cdot 60 = 2 \cdot 6 \cdot 30$$

Die Zahlen in der Tabelle geben an, wieviele Elemente des oben stehenden Typs von der in der linken Spalte stehenden p-Potenz annulliert werden.

	Z_{360}	$Z_2 \oplus Z_{180}$	$Z_2 \oplus Z_2 \oplus Z_{90}$	$Z_3 \oplus Z_{120}$	$Z_6 \oplus Z_{60}$	$Z_2 \oplus Z_6 \oplus Z_{30}$
2 |	2	4	8	2	4	8
4 |	4	8	8	4	8	8
8 |	8	8	8	8	8	8
3 |	3	3	3	9	9	9
9 |	9	9	9	9	9	9
5 |	5	5	5	5	5	5

3. Anwendung. V sei ein Vektorraum über einem Körper K und ϕ ein Endomorphismus von V. Wir machen V zu einem $K[X]$-Modul durch

$$f(X) \cdot v = f(\phi)(v) \text{ für } v \in V, f(X) \in K[X]$$

Sei $v_1, ..., v_n$ eine Basis von V über K. Dann bilden die v_i natürlich erst recht ein Erzeugendensystem von V über $K[X]$. Sei L der freie $K[X]$-Modul, der aus allen n-Tupeln $\begin{pmatrix} f_1(X) \\ \vdots \\ f_n(X) \end{pmatrix}$ mit $f_i(X) \in K[X]$ besteht. Wir bilden L auf V ab durch

$$\begin{pmatrix} f_1(X) \\ \vdots \\ f_n(X) \end{pmatrix} \mapsto f_1(\phi)v_1 + ... + f_n(\phi)v_n$$

Sei $M \subset L$ der Kern. Er besteht aus allen n-Tupeln von Polynomen mit $\sum_{i=1}^{n} f_i(\phi)v_i = 0$. Nach Satz 3 gibt es eine Basis $u_1, ..., u_n$ von L über $K[X]$ und Polynome $\alpha_1(X), ..., \alpha_k(X)$, $(k \leq n)$ mit $\alpha_1 | .... | \alpha_k$ und so, daß $\alpha_1 u_1, ..., \alpha_k u_k$ eine Basis von M bilden. Ist $u_i = \begin{pmatrix} u_{1i}(X) \\ \vdots \\ u_{ni}(X) \end{pmatrix}$, so ist die Matrix der $u_{ij}(X)$ invertierbar; denn aus den u_i läßt sich ja die Standardbasis der $\begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ wieder mit Koeffizienten aus $K[X]$ kombinieren. Daher bilden auch die

$$w_i = \sum_{j=1}^{n} u_{ji}(\phi)v_j \quad (1 \leq i \leq n)$$

ein Erzeugendensystem von V als $K[X]$-Modul; nämlich wenn $(b_{ij}(X))_{ij}$ die zu $(u_{ij}(X))_{ij}$ inverse Matrix ist, so ist

$$\sum_{j=1}^{n} b_{ji}(\phi)w_j = \sum_{j=1}^{n} b_{ji}(\phi) \sum_{l=1}^{n} u_{lj}(\phi)v_j = v_l$$

(indem man ϕ in die Polynomidentitäten $\sum u_{lj}(X)b_{ji}(X) = \delta_{jl}$ einsetzt.) Achtung! Die w_i bilden im allgemeinen keine Basis von V über K, sie können sogar teilweise gleich 0 sein! Mit den w_i gelten für alle $f_i(X)$ die Doppelpfeile

$$\sum_{i=1}^{n} f_i(\phi)w_i = 0 \Leftrightarrow \sum_{i=1}^{n}\sum_{j=1}^{n} f_i(\phi)u_{ji}(\phi)v_j = 0 \Leftrightarrow \sum_{i=1}^{n} f_i(X)u_i(X) \in M \Leftrightarrow \alpha_i(X) | f_i(X) \text{ für } i \leq k$$

$$\text{und } f_i(X) = 0 \text{ fuer } i > k \tag{1}$$

Für das Minimalpolynom f von ϕ gilt nun aber sicher $f(\phi)w_n = 0$. Also muß das n-Tupel $(0, ..., 0, f)$ die letzte Bedingung erfüllen. Wegen $f \neq 0$ kann nicht $k < n$ sein: es folgt $k = n$.
Sei nun d_i der Grad des Polynoms $f_i(X)$. Weil $\alpha_1 | .... | \alpha_n$, ist $d_1 \leq .... \leq d_n$. $d_i = 0$ bedeutet $w_i = 0$ nach (1). Für $d_i > 0$ folgt aus (1), daß $w_i, \phi w_i, ..., \phi^{d_i - 1} w_i$ linear unabhängig sind. Sie bilden eine Basis für den von w_i erzeugten Teilraum W_i (Definition auf Seite 5, Kap.14), und (1) zeigt auch, daß die Summe der W_i direkt (und $= V$) ist. Das Ergebnis ist

Satz 8. *V ist direkte Summe der ϕ-zyklischen Räume W_i. W_i wird von $\alpha_i(\phi)$ annulliert, aber von keinem Polynom kleineren Grades in ϕ. Das Minimalpolynom von ϕ ist α_n, und das charakteristische Polynom ist $\alpha_1(X) \cdot .... \cdot \alpha_n(X)$.*

Die letzte Aussage folgt daraus, daß in zyklischen Räumen das charakteristische Polynom gleich dem Minimalpolynom ist (Kap.14, Satz 44)

3. Verallgemeinerung der Jordanschen Normalform

Aus Satz 6 hatten wir in Kap.15 über $\mathbb{C}$ die Jordansche Normalform hergestellt. Diese sah so aus:

(1) $$J = \begin{pmatrix} J_\alpha & & & \\ & J_\beta & & \\ & & \ddots & \\ & & & J_\mu \end{pmatrix} \text{ mit } J_\alpha = \begin{pmatrix} \alpha & 1 & & 0 \\ & \alpha & \ddots & \\ & & \ddots & 1 \\ 0 & & & \alpha \end{pmatrix}$$

wobei die $\alpha, \beta, ..., \mu$ nicht verschieden zu sein brauchen. In

$$J_\alpha = \alpha \cdot \mathbf{1} + \begin{pmatrix} 0 & 1 & & 0 \\ & & \ddots & \\ & & & 1 \\ 0 & & & 0 \end{pmatrix}$$

sind die Summanden rechts miteinander vertauschbar, der erste ist diagonal und der zweite nilpotent. Setzt man die Kästchen J_α wie in (1) aneinander, so erhält man

(2) $$J = D + L, \;\; D \text{ diagonal }, L \text{ nilpotent}, \; LD = DL$$

Jede Matrix ist zu einer Matrix vom Typ J konjugiert (Kap.15, Satz 46). Aus (2) folgt: Jede Matrix $A \in M_n(\mathbb{C})$ ist zerlegbar in

$$A = S + N, \;\; S \text{ diagonalisierbar }, N \text{ nilpotent }, \; SN = NS$$

Diesen Satz wollen wir auf (fast) beliebige Grundkörper (statt $\mathbb{C}$) verallgemeinern. In Kap.11, Seite 4, sahen wir: die vernünftige Verallgemeinerung von diagonalisierbar ist

Definition: Ein Endomorphismus ϕ eines Vektorraumes V heißt halbeinfach, wenn es zu jedem ϕ-invarianten Unterraum U einen ϕ- *invarianten* Unterraum W gibt mit

$$V = U \oplus W$$

Satz 9. *ϕ ist halbeinfach genau dann, wenn das Minimalpolynom von ϕ Produkt verschiedener irreduzibler Faktoren ist.*

Beweis: " $\Rightarrow$ ": Sei ϕ halbeinfach und $f(X) = \prod_{i=1}^r p_i(X)^{\mu_i}$ das Minimalpolynom von ϕ. Zu zeigen ist: alle $\mu_i = 1$. Dazu sei $g(X) = \prod_{i=1}^r p_i(X)$ das Produkt der verschiedenen Primteiler von f und

$$U = \{x \in V \mid g(\phi)x = 0\}$$

U ist ϕ-invariant. Da ϕ halbeinfach ist, gibt es W mit $\phi W \subset W$ und $V = U \oplus W$. Jedenfalls ist nach Kap.12

$$V = \oplus V_i \text{ mit } V_i = \{x \in V \mid p_i(\phi)^{\mu_i} x = 0\} \text{ und entsprechend}$$

(1) $$W = \oplus W_i \text{ mit } W_i = \{x \in W \mid p_i(\phi)^{\mu_i} x = 0\} = W \cap V_i$$

Wäre auch nur ein einziges $\mu_i > 1$, so wäre $V \neq U$ und daher $W \neq 0$. Sei $0 \neq w \in W$. Schreibe $w = \sum_i w_i$ entsprechend (1). Für diejenigen i mit $w_i \neq 0$ sei s_i minimal mit $p_i(\phi)^{s_i} w_i = 0$. Man setzt $w^* = \sum p_i(\phi)^{s_i - 1} w_i$, wobei nur über die i mit $w_i \neq 0$ summiert wird. Nach Konstruktion ist $w^* \neq 0$ und in U. Aber da alle $\phi W_i \subset W_i$, ist $w^* \in W$, Widerspruch gegen $W \cap U = 0$.
" $\Leftarrow$ " Sei $g(X) = p_1(X) \cdot .... \cdot p_r(X)$ mit verschiedenen irreduziblen p_i das Minimalpolynom von ϕ und U ein ϕ-invarianter Unterraum. Man hat

$$V = \oplus V_i \text{ mit } V_i = \{x \in V \mid p_i(\phi)x = 0\} \text{ und } U = \oplus U_i \text{ mit } U_i = U \cap V_i$$

Wenn man in jedem V_i ein invariantes W_i finden kann mit $U_i \oplus W_i = V_i$, dann leistet $W = \oplus W_i$ das Verlangte: $V = U \oplus W$. Also genügt es, die Behauptung zu beweisen für $r = 1, g = p$ irreduzibel:
Wenn $U = V$, ist nichts zu zeigen. Sonst sei $x \in V$, $x \notin U$ und W_0 der kleinste ϕ-invariante Unterraum von V, der x enthält. Er besteht aus allen $h(\phi)x$ mit $h(X) \in K[X]$.

1. Fall: $p|h$. Dann ist $h(\phi) = 0$.
2. Fall: $p \not| h$. Da p irreduzibel, gibt es $u(X), v(X)$ mit $up + vh = 1$. Dann ist $x = v(\phi)h(\phi)x$. Da $x \notin U$ und $\phi U \subset U$, kann $h(\phi)x$ nicht in U liegen. Das zeigt $W_0 \cap U = 0$. Also ist $W_0 + U = W_0 \oplus U$. Sollte dies gleich V sein, sind wir fertig. Sonst fährt man fort mit $W_0 \oplus U$ statt U. Nach endlich vielen Schritten ist V erschöpft, und man hat $W_0 \oplus ..... \oplus W_k =: W$ mit $U \oplus W = V$.

Um den die Jordansche Normalform verallgemeinernden Zerlegungssatz zu beweisen, brauchen wir ein Lemma über Polynome:

Lemma 1. *Sei $g(X) \in K[X]$ teilerfremd zu seiner Ableitung $g'(X)$. Dann gibt es eine Folge von Polynomen $u_1, u_2, ...$ so daß*

$$g(X + \sum_{i=1}^{k-1} u_i g^i) \text{ durch } g^k \text{ teilbar ist für } k = 1, 2, ...$$

Beweis: Für $k = 1$ ist das richtig (leere Summe =0). Seinen $u_1, ...u_{k-1}$ bekannt und

$$g(X + \sum_{i=1}^{k-1} u_i g^i) = g(X)^k \cdot \Phi(X)$$

Man setzt zur Abkürzung $\sum_{i=1}^{k-1} u_i g^i = \Psi$. Da $(g, g') = 1$, gibt es Polynome v und w mit $vg + wg' = 1$. Für jedes Polynom u gilt (Taylorsche Formel)

$$g(X + \Psi + ug^k) = g(X + \Psi) + g'(X + \Psi)ug^k + R, \tag{1}$$

wobei der Rest $R(X)$ durch g^{2k}, also wegen $k \geq 1$ erst recht durch g^{k+1} teilbar ist. Man setze $u_k(X) = -\Phi(X) \cdot w(X + \Psi)$. Mit Benutzung der Induktionsannahme wird

$$g(X + \Psi) + g'(X + \Psi)ug^k = g^k\Phi - g'(X + \Psi)\Phi(X)w(X + \Psi)g^k =$$

$$g^k\Phi \cdot (1 - g'(X + \Psi)w(X + \Psi)) = g^k\Phi v(X + \Psi)g(X + \Psi)$$

und das ist durch g^{k+1} (sogar durch g^{2k}) teilbar. Mit dieser Wahl von $u = u_k$ haben wir nach (1) den Induktionsbeweis vollendet.

Beispiele:

1. Für Polynome ersten Grades $g(X) = X - a$ genügt $u_1 = -1$ und $u_i = 0$ für $i \geq 2$. Denn $g(X - g) = X - g - a = 0$.
2. $g(X) = X^2 + 1$. Damit $g(X + ug)$ durch g^2 teilbar ist, muß man u so wählen, daß $1 + 2Xu$ durch $X^2 + 1$ teilbar ist, also z.B. $u = \frac{1}{2}X$: dann wird nämlich

$$g(X + ug) = (X + ug)^2 + 1 = X^2 + 2Xug + u^2g^2 + 1 = g \cdot (1 + 2Xu) + u^2g^2 = g^2 \cdot (1 + u^2)$$

Bemerkung:

* Wir haben halbeinfache Endomorphismen dadurch gekennzeichnet, daß ihr Minimalpolynom nur einfache Faktoren hat.
* Im Beweis des Lemmas haben wir aber vorausgesetzt, daß das Polynom g teilerfremd zu seiner Ableitung ist.

Ist das dasselbe?
Sei $g(X) = \prod_i p_i(X)^{k_i}$ mit verschiedenen irreduziblen Polynomen $p_1, ..., p_r$. Frage:

$$\text{Wann ist } ggT(g, g') = 1 \Longleftrightarrow \text{ alle } k_i = 1?$$

Zu $\Leftarrow$: Wenn auch nur ein einziges $k_i > 1$, so ist $g = p_i^2 \cdot h$ mit einem gewissen Polynom h, und p_i ist gemeinsamer Teiler von g und $g' = 2p_i p_i' h + p_i^2 h'$.
Zu $\Rightarrow$: Jeder irreduzible Teiler von g ist eines der p_i. Wenn g und g' einen nicht konstanten gemeinsamen Teiler besitzen, dann muß g' durch eines der p_i teilbar sein, etwa durch p_1. In

$$g' = p_1' p_2 ....p_r + p_1 p_2' ....p_r + ... + p_1 ....p_{r-1} p_r'$$

sind der zweite bis letzte Summand durch p_1 teilbar. Damit g' durch p_1 teilbar ist, muß also p_1' durch p_1 teilbar sein. Das geht aus Gradgründen nur, wenn $p_1' = 0$ ist. Ist nun $p_1(X) = X^k + ... + c_0$, $(k \geq 1)$, so ist $p_1'(X) = kX^{k-1} + ... + c_1$. Ist K ein Körper, in dem $k \neq 0$ ist, so ist mit Sicherheit $p_1' \neq 0$. Ein Körper, in dem alle natürlichen Zahlen ungleich 0 sind, heißt ein Körper mit Chatakteristik 0. Ergebnis: Wenn K ein Körper mit Charakteristik 0 ist, dann hat jedes irreduzible Polynom eine von 0 verschiedene Ableitung, und der Doppelpfeil ist richtig.

Satz 10. *K habe die Charakteristik 0 und V sei ein Vektorraum über K mit Endomorphismus ϕ. Dann besitzt ϕ eine Zerlegung $\phi = s + n$ mit*
* *s halbeinfach*
* *n nilpotent*
* *n und s sind Polynome in ϕ, insbesondere $ns = sn$.*

Beweis: Sei $f(X) = \prod_{i=1}^{r} p_i(X)^{k_i}$ das Minimalpolynom von ϕ und $g(X) = p_1(X)....p_r(X)$, die p_i verschieden. Da jetzt der Doppelpfeil gilt, ist g teilerfremd zu g'. Sei k das größte der k_i. Nach dem Lemma 1 gibt es Polynome $u_1, u_2, ..., u_{k-1}$ so, daß $g(X + \sum_{i=1}^{k-1} u_i(X) g(X)^i)$ durch g^k teilbar ist. Dann ist es erst recht durch f teilbar, etwa $= f(X)h(X)$. Man setzt

$$n = -\sum_{i=1}^{k-1} u_i(\phi) g(\phi)^i \text{ und } s = \phi - n$$

Dann ist $n^k = 0$, weil $\sum_i u_i(X) g(X)^i$ durch g teilbar ist, und $g(s) = 0$, also s halbeinfach nach Satz 9.
Zusatz: Die Zerlegung $\phi = s + n$ mit den Bedingungen
* s ist halbeinfach
* n ist nilpotent
* $sn = ns$

ist eindeutig.
Beweis falls $K \subset \mathbb{C}$: Sei $s_1 + n_1 = \phi = s + n$, wobei $s+n$ die im Beweis von Satz 10 in Gestalt von Polynomen in ϕ gefundenen Endomorphismen sind und s_1, n_1 irgendwelche anderen, die die drei Bedingungen oben erfüllen. Da s_1 mit n_1 und damit mit ϕ vertauschbar ist, ist es auch mit s vertauschbar. Aus demselben Grunde ist n_1 mit n vertauschbar. Daher ist $n - n_1$ auch nilpotent. Über $\mathbb{C}$ können wir die halbeinfachen Endomorphismen diagonalisieren, und zwar, da sie vertauschbar sind, simultan. Dann ist auch ihre Differenz diagonalisiert, m.a.W. die Differenz zweier vertauschbarer halbeinfacher Endomorphismen ist halbeinfach. Nun ist $s - s_1 = n_1 - n$ gleichzeitig halbeinfach und nilpotent, also gleich 0 (das Minimalpoynom hat nur einfache Faktoren und ist ein Teiler von X^k, also $= X$.)
Ein anderer Beweis, der nicht $K \subset \mathbb{C}$, aber natürlich $K \supset \mathbb{Q}$, benutzt, wurde in den Übungen gegeben.

Die Voraussetzung über die Charakteristik von K ist wesentlich. Für gewisse Körper kann man
* Matrizen finden, die sich nicht gemäß Satz 10 zerlegen lassen
* Halbeinfache vertauschbare Matrizen finden, deren Summe nicht halbeinfach ist.

4. Alternierende p-Linearformen

Sei K ein Körper und V ein n-dimensionaler Vektorraum über K.

Definition: Eine Funktion F auf $V \times ..... \times V$ (p-mal) heißt p-Linearform, wenn für jedes $i = 1, 2, ..., p$ gilt: Sind $a_1, ..., a_{i-1}, a_{i+1}, ...a_p$ beliebige, aber dann festgehaltene Vektoren aus V, dann ist die Funktion

$$f(x) = F(a_1, ..., a_{i-1}, x, a_{i+1}, ..., a_p) \text{ eine Linearform auf } V$$

Eine 1-Linearform ist einfach eine Linearform, für $p = 2$ sagt man Bilinearform.

Definition: Die p-Linearform F heißt alternierend, wenn $F(x_1, ..., x_p) = 0$ sobald zwei der Argumente x_i übereinstimmen.

Durch "Polarisieren" folgt daraus sofort $F(...., x, ..., y, ...) = -F(..., y, ..., x, ...)$.

Satz 11. *Ist F eine alternierende p-Linearform, so ist $F(x_1, ..., x_p) = 0$ sobald $x_1, ..., x_p$ linear abhängig sind.*

Beweis: Sei $\lambda_1 x_1 + ... + \lambda_p x_p = 0$, nicht alle $\lambda_i = 0$, z.B. $\lambda_1 \neq 0$. Dann ist

$$F(x_1, ..., x_p) = F(-\sum_{i=2}^{p} \frac{\lambda_i}{\lambda_1} x_i, x_2, ..., x_p) = -\sum_{i=2}^{p} \frac{\lambda_i}{\lambda_1} F(x_i, x_2, ..., x_p)$$

In jedem Summanden stimmen zwei Argumente überein, also sind sie alle =0.

Folgerung: Ist F eine von 0 verschiedene p-Linearform, so ist $p \leq n$.

Beispiel: $p = n$. Die Determinante ist bis auf Vielfache die einzige alternierende p-Linearform. Genauer: Sei $V = K^n$ und F eine alternierende n-Linearform auf K^n. Dann gibt es eine Konstante c, so daß für alle $x_i = \begin{pmatrix} x_{1i} \\ \vdots \\ x_{ni} \end{pmatrix}$

$$F(x_1, ..., x_n) = c \cdot \begin{vmatrix} x_{11} & \dots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \dots & x_{nn} \end{vmatrix} \quad \text{(Kap.7)}$$

Wir behandeln zuerst $p = 2$. In Kap.8 haben wir uns mit symmetrischen Bilinearformen beschäftigt. Die alternierenden bilden gewissermaßen ein Gegenstück dazu:

$$F \text{ symmetrisch } \iff F(x, y) = F(y, x)$$

$$F \text{ alternierend } \implies F(x, y) = -F(y, x)$$

Ist K ein Körper, in dem $2 \neq 0$ ist (z.B. ein Körper, der $\mathbb{Q}$ enthält), so kann in der zweiten Zeile auch ein Doppelpfeil geschrieben werden, und jede Bilinearform ist Summe einer symmetrischen und einer alternierenden:

$$F(x, y) = \frac{1}{2}(F(x, y) + F(y, x)) + \frac{1}{2}(F(x, y) - F(y, x))$$

Klassifikation der alternierenden Bilinearformen

Dies ist viel leichter als für die symmetrischen Bilinearformen.

Definition: F (oder auch V) heißt nicht ausgeartet, wenn es zu $x \neq 0$ ein y gibt mit $F(x, y) \neq 0$.

Lemma 1. *Ist $R = \{x \in V \mid F(x, y) = 0 \text{ für alle } y\}$, so ist $V = R \oplus W$ mit einem nicht ausgearteten Raum W.*

Beweis: Nach dem Basisergänzungssatz gibt es jedenfalls W mit $V = R \oplus W$. Wir zeigen, daß jedes solche W nicht ausgeartet ist. Nämlich: Sei $0 \neq x \in W$. Dann ist $x \notin R$, und folglich gibt es $z \in V$ mit $F(x, z) \neq 0$. Schreibe $z = y + r$ mit $y \in W$ und $r \in R$. Dann ist $0 \neq F(x, z) = F(x, y) + F(x, r) = F(x, y)$.

Satz 12. *Sei V ein Vektorraum über dem Körper K mit einer nicht ausgearteten alternierenden Bilinearform F. Dann besitzt V eine Basis $u_1, ..., u_k, v_1, ..., v_k$ mit*

$$F(u_i, u_j) = F(v_i, v_j) = 0 \text{ und } F(u_i, v_j) = \delta_{ij} \text{ für alle } i, j$$

Insbesondere ist $n = 2k$ gerade.

Beweis: Sei $u_1 \neq 0$ beliebig in V. Da V nicht ausgeartet, gibt es $v_1 \in V$ mit $F(u_1, v_1) = 1$. Sei H_1 der von u_1 und v_1 aufgespannte zweidimensionale Teilraum. (Er ist tatsächlich zweidimensional, weil $F(u_1, v_1) \neq 0$, aber $F(u_1, u_1) = 0$). Für beliebige $x \in V$ schreibt man

$$x = (F(x, v_1)u_1 - F(x, u_1)v_1) + (x - F(x, v_1)u_1 + F(x, u_1)v_1) \tag{1}$$

Die erste Klammer ist in H_1, die zweite in

$$W_1 := \{y \in V \mid F(y, u_1) = F(y, v_1) = 0\}$$

und (1) zeigt $V = H_1 \oplus W_1$. Der Raum W_1 ist nicht ausgeartet. Fährt man mit W_1 statt V fort, so erhält man schließlich eine Basis wie gewünscht.

Übersetzung in Matrizen: Sei F eine alternierende Bilinearform auf K^n und $F(e_i, e_j) = a_{ij}$ für die Standardbasis e_i des K^n. Dann ist $a_{ij} = -a_{ji}$, und F ist durch die a_{ij} bestimmt; denn für $x = \sum_i x_i e_i$ und $y = \sum_i y_i e_i$ ist

$$F(x, y) = \sum_{ij} x_i a_{ij} y_j = x' A y$$

Definition: Eine Matrix A mit $A' = -A$ heißt schiefsymmetrisch.

Die alternierenden Bilinearformen F auf K^n entsprechen umkehrbar eindeutig den schiefsymmetrischen Matrizen $A \in M_n(K)$ vermöge

$$F(x, y) = x' A y, \text{ und}$$

$$F \text{ nicht ausgeartet } \Leftrightarrow x' A y = 0 \text{ für alle } x \text{ nur für } y = 0 \Leftrightarrow Ay = 0 \text{ nur für } y = 0 \Leftrightarrow A \text{ invertierbar}$$

Folgerung aus Satz 12:
a) Ist $A = -A'$ invertierbar, so ist die Zeilenzahl von A gerade.
b) Ist $A = -A'$, so ist die Determinante $|A|$ eine Quadratzahl.
Beweis: a) ist nach dem Vorhergehenden klar, man sieht es aber auch aus $|A| = |A'| = |-A| = (-1)^n |A|$.
b) Lassen wir den Fall $|A| = 0$ beiseite. Nach Satz 12 besitzt K^n eine Basis, deren Formenwertmatrix

$$B = \begin{pmatrix} I & \dots & 0 \\ & \ddots & \\ 0 & \dots & I \end{pmatrix} \text{ ist mit } I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Sind $t_i = \sum t_{ji} e_j$ diese Basisvektoren, so ist $B = T' A T$. Da $|B| = 1$, folgt $|A| = |T|^{-2}$.
Später werden wir eine Funktion von A kennenlernen, deren Quadrat die Determinante ist.

Alternierende p-Linearformen, $p \geq 2$

Seien $v_1, ..., v_n \in V$ und F eine alternierende p-Linearform auf V. Für alle $a_{ij} \in K$ ist

$$F(\sum_{i=1}^{n} a_{i1} v_i, ..., \sum_{i=1}^{n} a_{ip} v_i) =$$

$$\sum_{1 \leq i_1 < ... < i_p \leq n} a_{i_1 1} .... a_{i_p p} F(v_{i_1}, ..., v_{i_p}) \text{ da } F \text{ multilinear}$$

$$= \sum_{i_\nu verschieden} a_{i_1 1} .... a_{i_p p} F(v_{i_1}, ..., v_{i_p}) \text{ da } F \text{ alternierend}$$

$$= \sum_{1 \le i_1 < ... < i_p \le n} \sum_{\sigma \in S_p} sig\,(\sigma) a_{i_{\sigma(1)} 1} .... a_{i_{\sigma(p)} p} F(v_{i_1}, ..., v_{i_p})$$

$$= \sum_{1 \le i_1 < ... < i_p \le n} \begin{vmatrix} a_{i_1 1} & \dots & a_{i_1 p} \\ \vdots & & \\ a_{i_p 1} & \dots & a_{i_p p} \end{vmatrix} F(v_{i_1}, ..., v_{i_p}) \text{ nach Definition der Determinante in Kap.7}$$

Beispiel $p = 2$:

$$F(\sum_{i=1}^{n} a_{i1} v_i, \sum_{i=1}^{n} a_{i2} v_i) = \sum_{1 \le i_1, i_2 \le n} a_{i_1 1} a_{i_2 2} F(v_{i_1}, v_{i_2}) = \sum_{1 \le i_1 < i_2 \le n} (a_{i_1 1} a_{i_2 2} - a_{i_2 1} a_{i_1 2}) F(v_{i_1}, v_{i_2})$$

$$= \sum_{1 \le i_1 < i_2 \le n} \begin{vmatrix} a_{i_1 1} & a_{i_1 2} \\ a_{i_2 1} & a_{i_2 2} \end{vmatrix} F(v_{i_1}, v_{i_2})$$

1.Anwendung: (Gramsche Formel) Sei

$$A = \begin{pmatrix} a_{11} & \dots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{np} \end{pmatrix}, \quad X = \begin{pmatrix} x_{11} & \dots & x_{1p} \\ \vdots & & \vdots \\ x_{n1} & \dots & x_{np} \end{pmatrix} \quad \text{und } n \ge p$$

Dann ist $A'X$ eine p-reihige quadratische Matrix. Seien $x_1, ..., x_p$ die Spalten von X.
Behauptung : $F(x_1, ..., x_p) = |A'X|$ ist eine alternierende p-Linearform.
Beweis: Die Spalten von $A'X$ sind $A'x_1, ..., A'x_p$. Für feste u_j ist

$$F(u_1, ..., u_{i-1}, x, u_{i+1}, ..., u_p) = |A'u_1, ..., A'x, ..., A'u_p|$$

Dies ist linear in $A'x$ (Kap.7), und $A'x$ ist linear in x. Also ist die rechte Seite linear in x. Ist $x_i = x_j$ und $i \ne j$, so hat $A'X$ zwei gleiche Spalten, und ihre Determinante ist 0.
Nun können wir (1) anwenden:

$$(2) \qquad |A'X| = F(x_1, ..., x_p) = \sum_{1 \le i_1 < .... < i_p \le n} \begin{vmatrix} x_{i_1 1} & \dots & x_{i_1 p} \\ \vdots & & \vdots \\ x_{i_p 1} & \dots & x_{i_p p} \end{vmatrix} F(e_{i_1}, ..., e_{i_p})$$

wobei die e_j die Standardbasisvektoren im K^n sind. Nach Definition ist

$$F(e_{i_1}, ..., e_{i_p}) = |A'e_{i_1}, ..., A'e_{i_p}|$$

$A'e_{i_\nu}$ ist die i_ν te Spalte der Matrix A', also $= \begin{pmatrix} a_{i_\nu 1} \\ \vdots \\ a_{i\nu p} \end{pmatrix}$, und $F(e_{i_1}, ..., e_{i_p})$ ist die Determinante dieser Spalten. Dies in (2) eingesetzt ergibt, wenn man noch der Schönheit halber B statt X schreibt

Satz 13. *(Gramsche Formel) Für $A = A_{n,p}$ und $B = B_{n,p}$ gilt*

$$|A'B| = \sum_{1 \le i_1 < ... < i_p \le n} \begin{vmatrix} a_{i_1 1} & \dots & a_{i_1 p} \\ \vdots & & \\ a_{i_p 1} & \dots & a_{i_p p} \end{vmatrix} \cdot \begin{vmatrix} b_{i_1 1} & \dots & b_{i_1 p} \\ \vdots & & \\ b_{i_p 1} & \dots & b_{i_p p} \end{vmatrix}$$

Die Einträge der Matrix $A'A$ sind die p^2 Skalarprodukte der Spaltenvektoren a_i von A miteinander. Die Matrix $A'A$ nennt man die Gramsche Matrix der Vektoren $a_1, ..., a_p$. Ist $K = \mathbb{R}$, so ist ihre Determinante das Quadrat des Volumens des von $a_1, ..., a_p$ aufgespannten Parallelotops. Nach der Gramschen Formel ist dies

$$|A'A| = \sum_{1 \le i_1 < ... < i_p \le n} \begin{vmatrix} a_{i_1 1} & \dots & a_{i_1 p} \\ \vdots & & \vdots \\ a_{i_p 1} & \dots & a_{i_p p} \end{vmatrix}^2$$

Beispiel: $n = 3$, $p = 2$. Man nimmt zwei Vektoren $x, y \in \mathbb{R}^3$ und für A die 3×2-Matrix mit den Spalten x und y .Das Quadrat der Fläche F des von x und y aufgepannten Parallelogramms ist

$$F^2 = \begin{vmatrix} x'x & x'y \\ y'x & y'y \end{vmatrix} \text{ oder anders bezeichnet } = \begin{vmatrix} (x,x) & (x,y) \\ (x,y) & (y,y) \end{vmatrix} =$$

$$(x,x)(y,y) - (x,y)^2 = |x|^2 \cdot |y|^2 (1 - \cos^2 \alpha) = (|x| \cdot |y| \sin \alpha)^2$$

wobei α der Winkel zwischen x und y ist. Die zweireihigen Unterdeterminanten von A sind die Komponenten des Kreuzprodukts $x \times y$. Die Gramsche Formel besagt für diesen Fall

$$\begin{vmatrix} (x,x) & (x,y) \\ (x,y) & (y,y) \end{vmatrix} = |x \times y|^2$$

zusammen mit obigem

$$|x \times y| = |x| \cdot |y| \cdot |\sin \alpha|$$

2. Anwendung: (Laplacescher Entwicklungssatz) Wir betrachten die Determinante einer $n \times n$-Matrix unter Festhalten ihrer letzten $n - p$ Spalten als alternierende p-Linearform ihrer ersten p Spalten:

$$\begin{vmatrix} x_{11} & \dots & x_{1p} & a_{1,p+1} & \dots & a_{1n} \\ \vdots & & & & & \vdots \\ x_{n1} & \dots & x_{np} & a_{n,p+1} & \dots & a_{nn} \end{vmatrix} = F(x_1, ..., x_p)$$

Die Formel (1) sagt

$$F(x_1, ..., x_p) = \sum_{1 \le i_1 < ... < i_p \le n} \begin{vmatrix} x_{i_1 1} & \dots & x_{i_1 p} \\ \vdots & & \vdots \\ x_{i_p 1} & \dots & x_{i_p p} \end{vmatrix} \cdot F(e_{i_1}, ..., e_{i_p})$$

Diesmal ist $F(e_{i_1}, ..., e_{i_p})$ die Determinante der Matrix, deren erste p Spalten $e_{i_1}, ..., e_{i_p}$ und deren letzte Spalten $a_{p+1}, ..., a_n$ sind. Dies ist eine alternierende $(n-p)$-Linearform $G_{i_1,....,i_p}(a_{p+1}, ..., a_n)$ und aus demselben Grunde gleich

$$\sum_{1 \le j_1 < ... < j_{n-p} \le n} \begin{vmatrix} a_{j_1,p+1} & \dots & a_{j_1 n} \\ \vdots & & \vdots \\ a_{j_{n-p},p+1} & \dots & a_{j_{n-p} n} \end{vmatrix} \cdot G_{i_1,...,i_p}(e_{j_1}, ..., e_{j_{n-p}})$$

Hierin ist $G_{i_1,...,i_p}(e_{j_1}, ..., e_{j_{n-p}})$ die Determinante der Matrix, deren erste p Spalten $e_{i_1}, ..., e_{i_p}$ und deren letzte $n - p$ Spalten $e_{j_1}, ..., e_{j_{n-p}}$ sind. Damit diese Determinante nicht 0 ist, müssen $j_1, ..., j_{n-p}$ gerade die Indices sein, die von $i_1, ..., i_p$ übrig gelassen werden. Die Matrix mit den Spalten $e_{i_1}, ..., e_{i_p}, e_{j_1}, ..., e_{j_{n-p}}$ entsteht durch Permutation der Spalten aus der Einheitsmatrix, und ihre Determinante ist gleich dem Vorzeichen dieser Permutation. Wir bezeichnen diese mit $\sigma_{i_1 ... i_p}$ und ihr Vorzeichen mit $\epsilon_{i_1 ... i_p}$.

Beispiel: $n = 5$: $i_1, i_2, i_3 = 2,3,5$ und $j_1, j_2 = 1,4$. $\sigma_{i_1 ... i_p}$ ist die Permutation, die 2,3,5,1,4 in die natürliche Reihenfolge bringt. Man kann sie durch 4 Transpositionen bewirken, ihr Vorzeichen ist also =1.

Damit das Ergebnis hübscher aussieht, numerieren wir die von $i_1, ..., i_p$ übrig gelassenen Indices nicht $j_1, ..., j_{n-p}$, sondern $j_{p+1}, ..., j_n$. Damit erhalten wir

Satz 14. *(Laplacescher Entwicklungssatz)*

$$|A| = \sum_{1 \le i_1 < \ldots < i_p \le n} \epsilon_{i_1 \ldots i_p} \begin{vmatrix} a_{i_1 1} & \ldots & a_{i_1 p} \\ \vdots & & \vdots \\ a_{i_p 1} & \ldots & a_{i_p p} \end{vmatrix} \cdot \begin{vmatrix} a_{j_{p+1}, p+1} & \ldots & a_{j_{p+1} n} \\ \vdots & & \vdots \\ a_{j_n, p+1} & \ldots & a_{j_n n} \end{vmatrix}$$

Entwicklung nach den ersten p Spalten

Analoges folgt durch Stürzen für die Zeilen.

Beispiel:

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 5 & 6 \\ 7 & 8 & 9 & 1 \\ 0 & 0 & 2 & 3 \end{vmatrix} = \epsilon_{13} \begin{vmatrix} 1 & 2 \\ 7 & 8 \end{vmatrix} \cdot \begin{vmatrix} 5 & 6 \\ 2 & 3 \end{vmatrix} = -(8-14) \cdot (15-12) = 18$$

weil alle andern zweireihigen Teilmatrizen, die man aus den ersten beiden Spalten bilden kann, eine Nullzeile haben.

5. Graßmannalgebra

Etwas allgemeiner als in Kap.4 wollen wir nicht nur alternierende p-Linear*formen* betrachten, sondern p-lineare Abbildungen mit Werten in irgendeinem anderen Vektorraum W (über demselben Körper):

$$F: \overbrace{V \times V \times ... \times V}^{p-mal} \longrightarrow W, \ p\text{-linear und alternierend}$$

Wieder haben wir

$$F(\sum_{i=1}^{n} a_{i1}e_i, ..., \sum_{i=1}^{n} a_{ip}e_i) = \sum_{1 \le i_1 < ... < i_p \le n} \begin{vmatrix} a_{i_1 1} & \dots & a_{i_1 p} \\ \vdots & & \vdots \\ a_{i_p 1} & \dots & a_{i_p p} \end{vmatrix} F(e_{i_1}, ..., e_{i_p}) \tag{1}$$

Dies zeigt: wenn $e_1, ..., e_n$ eine Basis von V bilden, dann ist die Abbildung F durch Angabe der $\binom{n}{p}$ Bildvektoren $F(e_{i_1}, ..., e_{i_p})$ festgelegt. Umgekehrt: Gibt man $\binom{n}{p}$ beliebige Vektoren $w_{i_1 ... i_p} \in W$ vor, so ist vermöge (1) durch $F(e_{i_1}, ..., e_{i_p}) = w_{i_1 ... i_p}$ eine alternierende p-lineare Abbildung definiert.
Beweis: Jede Determinante auf der rechten Seite ist eine p-lineare alternierende Funktion ihrer Spalten und damit von den Vektoren $\sum_{i=1}^{n} a_{ij}e_i, \quad (j = 1, ..., p)$ auf der linken Seite.
Wir beschreiben diesen Tatbestand mit Hilfe eines sogenannten universellen Objekts: Wir nehmen $\binom{n}{p}$ Symbole, die wir mit e_I bezeichnen, wobei I alle p-elementigen Teilmengen der Menge $\{1, 2, ..., n\}$ durchläuft. Das sind gerade $\binom{n}{p}$ Stück. Diese e_I ernennen wir zur Basis eines Vektorraumes, den wir mit $\wedge^p V$ bezeichnen. Nach dem oben Gesagten (mit $\wedge^p V$ statt W) gibt es genau eine p-lineare alternierende Abbildung F von $V \times ..... \times V$ in $\wedge^p V$ mit

$$F(e_{i_1}, ..., e_{i_p}) = e_I \text{ für alle Folgen } 1 \le i_1 < ... < i_p \le n \tag{2}$$

In (2) soll I die Teilmenge von $\{1, 2, ..., n\}$ sein, die aus den Ziffern $i_1, ..., i_p$ besteht.
Bezeichnung: Das Bild irgend eines p-Tupels $x_1, ..., x_p$ unter F wird mit $x_1 \wedge x_2 \wedge ... \wedge x_p$ bezeichnet. Dann ist $e_{i_1} \wedge ... \wedge e_{i_p}$ gerade gleich e_I. Nach (1) ist, wenn $x_i = \sum_{j=1}^{n} x_{ji}e_j$,

$$x_1 \wedge .... \wedge x_p = \sum_{1 \le i_1 < ... < i_p \le n} \begin{vmatrix} x_{i_1 1} & \dots & x_{i_1 p} \\ \vdots & & \vdots \\ x_{i_p 1} & \dots & x_{i_p p} \end{vmatrix} e_{i_1} \wedge ... \wedge e_{i_p} \tag{3}$$

Satz 15. *$\wedge^p V$ hat die folgende "universelle Abbildungseigenschaft": Ist W ein beliebiger K-Vektorraum und F eine alternierende p-lineare Abbildung von $V \times ... \times V$ nach W, dann gibt es genau eine lineare Abbildung f von $\wedge^p V$ nach W mit*

$$F(x_1, ..., x_p) = f(x_1 \wedge ... \wedge x_p) \tag{4}$$

Beweis: Da die e_I eine Basis von $\wedge^p V$ bilden, gibt es genau eine lineare Abbildung f von $\wedge^p V$ in W mit $f(e_I) = F(e_{i_1}, ..., e_{i_p})$ für alle $I = \{i_1, ..., i_p\}$, $1 \le i_1 < ... < i_p \le n$. Vergleich von (1) mit (3) zeigt (4).

Sei noch einmal F die durch (2) definierte p-lineare Abbildung von $V \times .... \times V$ nach $\wedge^p V$. Sei $u_1, ..., u_n$ irgendeine andere Basis von V. Dann ist $e_i = \sum_{j=1}^{n} a_{ji}u_j$ mit gewissen $a_{ji} \in K$. Formel (1) zeigt, daß die $e_{i_1} \wedge ... \wedge e_{i_p} = F(e_{i_1}, ..., e_{i_p})$ Linearkombinationen der $F(u_{i_1}, ..., u_{i_p}) = u_{i_1} \wedge ... \wedge u_{i_p}$ sind.

Folgerung 1. *Für jede Basis $u_1, ..., u_n$ von V bilden die $u_{i_1} \wedge ... \wedge u_{i_p}$ mit $1 \le i_1 < ... < i_p \le n$ eine Basis von $\wedge^p V$.*

Folgerung 2.

$$x_1, ..., x_p \in V \text{ linear abhängig} \iff x_1 \wedge ... \wedge x_p = 0$$

Beweis: Wenn $x_1, ..., x_p$ linear abhängig sind, dann ist $F(x_1, ..., x_p) = 0$ für jede p-lineare alterniernde Abbildung F, insbesondere ist $x_1 \wedge ... \wedge x_p = 0$. Umgekehrt: simd sie linear unabhängig, so ergänze man sie zu einer Basis $x_1, ..., x_n$ von V. Dann ist $x_1 \wedge ... \wedge x_p$ einer der $\binom{n}{p}$ Basisvektoren $x_{i_1} \wedge ... \wedge x_{i_p}$ und bestimmt nicht 0.

Jetzt bilden wir

$$K \oplus V \oplus \wedge^2 V \oplus ... \oplus \wedge^n V =: E$$

E ist ein Vektorraum über K der Dimension

$$1 + n + \binom{n}{2} + ... + \binom{n}{n} = 2^n$$

Wir wollen sehen, daß E (in noch zu erklärender Weise) eine "Algebra" ist.

Definition: Eine Algebra A über einem Körper K ist ein (endlich-dimensionaler) Vektorraum zusammen mit einer bilinearen Abbildung

$$A \times A \longrightarrow A,$$

die man Multiplikation nennt und mit $a \cdot b$ oder einfach ab oder auch manchmal noch anders bezeichnet. Bilinear bedeutet

$$(\lambda a + \mu b) \cdot c = \lambda ac + \mu bc \text{ und } a \cdot (\lambda b + \mu c) = \lambda ab + \mu ac$$

also die distributiven Gesetze plus der Forderung $(\lambda a) \cdot b = \lambda(ab) = a \cdot \lambda b$. Ist $ea = ae = a$ für alle $a \in a$, so nennt man e das (!) Einselement von A und sagt, A sei eine Algebra mit Eins. In diesem Falle bettet man K in A ein vermöge $\lambda \mapsto \lambda e$, identifiziert K mit seinem Bild und schreibt 1 statt e. Die Bedingung $a \cdot \lambda b = \lambda ab$ bedeutet dann, daß die Elemente aus K mit allen Elementen aus A vertauschbar sind.

1. Beispiel: $A = L$ ein Oberkörper von K
2. Beispiel: $A = M_n(K)$. Hier ist e die Einheitsmatrix

Man kann auch so sagen: Eine Algebra über K ist eine Ring, der gleichzeitig ein (endlich-dimensionaler) Vektorraum über K ist, wobei für die Multiplikation $*$ in der Algebra bzw. $\cdot$ mit Skalaren gilt

$$(\lambda \cdot a) * b = \lambda \cdot (a * b) = a * (\lambda \cdot b)$$

Natürlich läßt man $*$ und $\cdot$ weg, wenn man einmal weiß, was gemeint ist.

Nun stellen wir uns $y_1, ..., y_p \in V$ fest und $x_1, ..., x_p$ variabel in V vor. Die Abbildung

$$V \times .... \times V \longrightarrow \wedge^{p+q} V$$

$$(x_1, ..., x_p) \mapsto x_1 \wedge .... \wedge x_p \wedge y_1 \wedge ... \wedge y_q$$

ist p-linear und alternierend. Nach der universellen Abbildungseigenschaft gibt es genau eine *lineare* Abbildung

$$R : \wedge^p V \to \wedge^{p+q} V \text{ mit } R(x_1 \wedge ... \wedge x_p) = x_1 \wedge ... \wedge x_p \wedge y_1 \wedge ... \wedge y_q$$

Betrachten wir umgekehrt $x_1, ..., x_p$ als fest und $y_1, ..., y_q$ als variabel, so erhalten wir eine *lineare* Abbildung

$$L : \wedge^q V \to \wedge^{p+q} V \text{ mit } L(y_1 \wedge ... \wedge y_q) = x_1 \wedge ... \wedge x_p \wedge y_1 \wedge ... \wedge y_q$$

Das bedeutet: Es gibt eine wohldefinierte Abbildung

$$M : \wedge^p V \times \wedge^q V \longrightarrow \wedge^{p+q} V$$

$$(*) \qquad \text{mit } M(x_1 \wedge ... \wedge x_p, y_1 \wedge ... \wedge y_q) = x_1 \wedge ... \wedge x_p \wedge y_1 \wedge ... \wedge y_q,$$

und M ist bilinear.

1. Bemerkung: Ist $p+q>n$, so kommt 0 raus, die Bilder liegen also in $k \oplus V \oplus .... \oplus \wedge^n V = E$.

2. Bemerkung: Damit klar ist, warum das gemacht wurde: $x_1 \wedge ... \wedge x_p \wedge y_1 \wedge ... \wedge y_q$ sieht nur so aus, als ob es nur von $x_1 \wedge ... \wedge x_p$ und $y_1 \wedge ... \wedge y_q$ abhinge. Aber es ist nach Definition das Bild des $(p+q)$-Tupels $(x_1, ..., y_q)$ unter der in (2) definierten $(p+q)$-linearen Abbildung von $V \times ... \times V$ ($(p+q)$-mal) nach $\wedge^{p+q} V$. Das oben gegebene Argument zeigt, daß es tatsächlich nur von $x_1 \wedge ... \wedge x_p$ und $y_1 \wedge ... \wedge y_q$ und nicht wirklich von dem p-bzw. q-Tupel abhängt. Beachte, daß es verschiedene p-Tupel mit gleichem Dachprodukt gibt, zum Beispiel ist $x \wedge y = x \wedge (x+y)$ für alle $x, y \in V$.

(*) zeigt, daß E eine Algebra ist mit der Multiplikation $\wedge$. Sie ist assoziativ, aber nicht kommutativ, zum Beispiel ist

$$u \wedge v = (-1)^{pq} v \wedge u \text{ für alle } u \in \wedge^p V \text{ und } v \in \wedge^q V$$

Definition: E heißt die Graßmannsche Algebra von V.

In Verallgemeinerung der 2. Bemerkung gilt für Vektoren x_i und y_i aus V

Satz 16. *Ist* $x_1 \wedge ... \wedge x_p \neq 0$, *so sind folgende Aussagen äquivalent*

(i) *Es gibt* $\rho \in K$, $\rho \neq 0$ *mit* $x_1 \wedge ... \wedge x_p = \rho y_1 \wedge .... \wedge y_p$

$x_1, ..., x_p$ *spannen denselben* p*-dimensionalen Unterraum von* V *auf wie* $y_1, ..., y_p$

Beweis: " $\Leftarrow$ ": Wenn $x_i = \sum_{i=1}^{p} a_{ji} y_j$, so ist

$$x_1 \wedge ... \wedge x_p = \begin{vmatrix} a_{11} & \dots & a_{1p} \\ \vdots & & \vdots \\ a_{p1} & \dots & a_{pp} \end{vmatrix} \cdot y_1 \wedge ... \wedge y_q$$

" $\Rightarrow$ ": Ist $0 \neq x_1 \wedge ... \wedge x_p = \rho y_1 \wedge ... \wedge y_q$, so multipliziert man die Gleichung (zum Beispiel von rechts) mit y_i und erhält 0. Nach Folgerung 2 zu Satz 15 sind $x_1, ..., x_p, y_i$ linear abhängig. Da $x_1, ..., x_p$ linear unabhängig sind, liegt y_i in dem von $x_1, ..., x_p$ aufgespannten Teilraum. Dasselbe gilt für alle i. Die Voraussetzung ist symmetrisch in den x und den y. Also liegen auch alle x_i in dem von $y_1, ..., y_p$ aufgespannten Teilraum,womit der Satz bewiesen ist.

Anwendungen: Nach Satz 16 entsprechen die p-dimensionalen Teilräume von V umkehrbar eindeutig gewissen eindimensionalen Teilräumen von $\wedge^p V$ vermöge

$$< x_1, ..., x_p > \longleftrightarrow < x_1 \wedge ... \wedge x_p >$$

Ist $e_1, ..., e_n$ eine vorgegebene Basis von V, so ist

$$x_1 \wedge .... \wedge x_p = \sum_{1 \leq i_1 < ... < i_p \leq n} \begin{vmatrix} x_{i_1 1} & \dots & x_{i_1 p} \\ \vdots & & \vdots \\ x_{i_p 1} & \dots & x_{i_p p} \end{vmatrix} e_{i_1} \wedge .... \wedge e_{i_p}$$

Die $\binom{n}{p}$ Unterdeterminanten in dieser Summe heißen die Plückerschen Koordinaten des Teilraums $< x_1, , , .x_p >$. Offensichtlich sind sie nur bis auf einen gemeinsamen Faktor bestimmt.

$\wedge^p V$ besteht aus *allen* Linearkombinationen der $e_{i_1} \wedge .... \wedge e_{i_p}$. Nicht alle werden i.a. auf diese Weise von p-dimensionalen Unterräumen herkommen.

Definition: Eine p-Vektor z heißt zerlegbar, wenn es Vektoren $x_1, ..., x_p \in V$ gibt mit $z = x_1 \wedge ... \wedge x_p$.

Wir suchen ein Kriterium für Zerlegbarkeit. Dazu brauchen wir die

Operation des Dualraums V^* auf der Graßmannalgebra:

Sei f eine Linearform auf V.
$p=1$: Für $x \in V$ ist $f(x) \in K$.

$p = 2$: Die Abbildung

$$b : V \times V \to V, \text{ definiert durch } b(x,y) = f(x)y - f(y)x$$

ist bilinear und alternierend. Nach der universellen Abbildungseigenschaft gibt es eine lineare Abbildung

$$f^{\wedge 2} : \wedge^2 V \to V \text{ mit } f^{\wedge 2}(x \wedge y) = f(x)y - f(y)x$$

Verallgemeinerung: Für $2 \leq p \leq n$ betrachten wir die Abbildung

$$(x_1, ..., x_p) \mapsto \sum_{i=1}^{p} (-1)^{i-1} f(x_i) x_1 \wedge ...\hat{i}... \wedge x_p$$

wobei $\hat{i}$ bedeutet, daß in dem Dachprodukt $x_1 \wedge ... \wedge x_p$ der i-te Faktor weggelassen wird. Die eben erklärte Abbildung ist p-linear und alternierend. Daher gibt es genau eine lineare Abbildung $f^{\wedge p}$ von $\wedge^p V$ nach $\wedge^{p-1} V$ mit

$$f^{\wedge p}(x_1 \wedge ... \wedge x_p) = \sum_{i=1}^{p} (-1)^{i-1} f(x_i) x_1 \wedge ...\hat{i}... \wedge x_p$$

Da wir immer die Argumente $x_1 \wedge ... \wedge x_p$ dazuschreiben, entsteht kein Mißverständnis, wenn wir einfach f statt $f^{\wedge p}$ schreiben. Wir können das auch so sehen: Wir haben die lineare Abbildung f, die auf V gegeben war, auf die Graßmannalgebra fortgesetzt.

Regel: Für $u \in \wedge^p V$ und $v \in \wedge^q V$ gilt

$$f(u \wedge v) = f(u) \wedge v + (-1)^p u \wedge f(v)$$

Beweis: Das folgt aus der Definition, indem man die Summe von 1 bis $p+q$ aufspaltet in die Summe von 1 bis p und von $p+1$ bis $p+q$ und aus der zweiten $(-1)^p$ ausklammert.

Wir können nun zwei solche Abbildungen f hintereinander anwenden:

$$f(g(x_1 \wedge ... \wedge x_p) = f(\sum_{i=1}^{p} (-1)^{i-1} g(x_i) x_1 \wedge ...\hat{i}... \wedge x_p) = \sum_{i=1}^{p} (-1)^{i-1} g(x_i) f(x_1 \wedge ...\hat{i}... \wedge x_p)$$

$$= \sum_{i=1}^{p} (-1)^{i-1} g(x_i) \{ \sum_{j=1}^{i-1} (-1)^{j-1} f(x_j) x_1 \wedge ...\hat{j}...\hat{i}... \wedge x_p + \sum_{j=i+1}^{p} (-1)^{j} f(x_j) x_1 \wedge ...\hat{i}...\hat{j}... \wedge x_p \ \}$$

$$= \sum_{j<i} (-1)^{i+j} [g(x_i) f(x_j) - g(x_j) f(x_i)] x_1 \wedge ...\hat{j}...\hat{i}... \wedge x_p$$

Das zeigt $f \circ f = 0$ und allgemeiner

$$f \circ g_1 \circ ... \circ g_k \circ f = -g_1 \circ f \circ ... \circ g_k \circ f = (-1)^k g_1 \circ ... \circ g_k \circ f \circ f = 0$$

Daher ist (bei fest gedachten $x_1, ..., x_p$) die Abbildung

$$(f_1, ..., f_q) \mapsto f_1(f_2(...(f_q(x_1 \wedge ... \wedge x_p))....) \text{ von } V^* \times .... \times V^* \text{ nach } \wedge^{p-q}$$

q-linear und alternierend. Wieder nach der universellen Abbildungseigenschaft gibt es eine lineare Abbildung L von $\wedge^q V^*$ nach $\wedge^{p-q} V$ mit

$$L(f_1 \wedge ... \wedge f_q) = f_1(f_2(...(f_q(x_1 \wedge .... \wedge x_p))....))$$

Lassen wir nun wieder beide Seiten variabel, so erhalten wir eine bilineare Abbildung

$$\wedge^q V^* \times \wedge^p V \longrightarrow \wedge^{p-q} V$$

(Für $p<q$ wird sinngemäß die rechte Seite gleich 0 gesetzt.) Es ist vernünftig, die Abbildung $f_1 \circ ... \circ f_q$ von $\wedge^p V$ nach $\wedge^{p-q} V$ mit $f_1 \wedge ... \wedge f_q$ zu bezeichnen.

Bemerkung: Von $f(f(z))=0$ gilt auch die "Umkehrung": Wenn $z \in \wedge^p V$ und $f(z)=0$, dann gibt es $u \in \wedge^{p+1} V$ mit $z=f(u)$ (Aufgabe 23).

1. Beispiel: $p=q=2$:

$$(f \wedge g)(x \wedge y) = f(g(x)y - g(y)x) = g(x)f(y) - g(y)f(x) = \begin{vmatrix} g(x) & g(y) \\ f(x) & f(y) \end{vmatrix}$$

2. Beispiel: $p=3, q=2$:

$$(f \wedge g)(x \wedge y \wedge z) = f(g(x)y \wedge z - g(y)x \wedge z + g(z)x \wedge y) = \begin{vmatrix} g(x) & g(y) \\ f(x) & f(y) \end{vmatrix} \cdot z - \begin{vmatrix} g(x) & g(z) \\ f(x) & f(z) \end{vmatrix} \cdot y + \begin{vmatrix} g(y) & g(z) \\ f(y) & f(z) \end{vmatrix} \cdot x$$

Anwendung zur Beschreibung zerlegbarer p-Vektoren:

Zu $\in \wedge^p V$ bezeichne

$$V_z = \{x \in V \mid z \wedge x = 0\}$$

Lemma 1. *Sei $0 \neq z \in \wedge^p V$. Stets gilt dim $V_z \leq p$, und dim $V_z = p$ genau dann, wenn z zerlegbar.*

Beweis: Seien $x_1, ..., x_q \in V_z$ linear unabhängig. Man ergänzt sie zu einer Basis von V. Nach Folgerung 1 aus Satz 15 ist

$$z = \sum_{1 \leq i_1 < ... < i_p \leq n} \alpha_{i_1 ... i_p} x_{i_1} \wedge ... \wedge x_{i_p} \text{ mit gewissen } \alpha_{i_1 ... i_p} \in K$$

$z \wedge x_i = 0$ für $i = 1, ..., q$ bedeutet, daß $\alpha_{i_1 ... i_p} = 0$, wenn $i \notin \{i_1, ..., i_p\}$. Daraus folgt $q \leq p$. Ist $q=p$, so folgt $z = \alpha_{1...p} x_1 \wedge ... \wedge x_p$. Ist umgekehrt z zerlegbar, also $= x_1 \wedge ... \wedge x_p$ mit $x_i \in V$, so gehören alle x_i zu V_z. Da $z \neq 0$, sind sie linear unabhängig. Also ist dim $V_z gleq p$. Da wir $\leq$ schon wissen, folgt dim $V_z = p$.

Lemma 2. *Sei $0 \neq z \in \wedge^p V$. Dann sind unter den Vektoren $(f_1 \wedge ... \wedge f_{p-1})z$ (sie liegen alle in V!) p linear unabhängige, wenn die f_i alle Linearformen auf V durchlaufen.*

Beweis: Sei $e_1, ..., e_n$ eine Basis von V und

$$z = \sum_{1 \leq i_1 < ... < i_p \leq n} \alpha_{i_1 ... i_p} e_{i_1} \wedge .... \wedge e_{i_p}$$

Da $z \neq 0$, sind nicht alle α null; oE sei $\alpha_{1...p} \neq 0$. Jetzt nehmen wir für f_i die Linearform mit $f_i(e_j) = 1$, falls $i=j$, und =0, falls $i \neq j$. Dann ist

$$f_1(e_{i_1} \wedge .... \wedge e_{i_p}) = \begin{cases} e_{i_2} \wedge ... \wedge e_{i_p} & \text{wenn } i_1 = 1 \\ 0 & \text{sonst} \end{cases}$$

$$(f_2 \wedge f_1)(e_{i_1} \wedge .... \wedge e_{i_p}) = \begin{cases} e_{i_3} \wedge ... \wedge e_{i_p} & \text{wenn } i_1 = 1 \text{ und } i_2 = 2 \\ 0 & \text{sonst} \end{cases}$$

$$\vdots$$

Wendet man also $f_{p-1} \wedge ... \wedge f_1$ auf z an, so fallen alle Summanden weg, für die $\{i_1, ..., i_{p-1}\} \neq \{1, ..., p-1\}$ ist, und das Ergebnis ist

$$(f_{p-1} \wedge ... \wedge f_1)z = \alpha_{1...p} e_p + \sum_{j>p} \alpha_{1,...,p-1,j} e_j$$

Läßt man statt f_p aus den $f_1, ..., f_p$ ein anders f_j $(j \leq p)$ weg, so erhält man

$$(f_p \wedge ... \hat{j} ... \wedge f_1)z = \pm \alpha_{1...p} e_j + \sum_{k>p} \alpha_{1...\hat{j}...pk} e_k \tag{1}$$

Die p Vektoren, die auf der rechten Seite von (1) für $j = 1, ..., p$ entstehen, sind linear unabhängig.

Mit Hilfe der soeben bewiesenen Lemmata 1 und 2 beweisen wir das Kriterium

Satz 17. *Sei* $0 \neq z \in \wedge^p V$. *Genau dann ist* z *zerlegbar, wenn*

$$F(z) \wedge z = 0 \text{ für alle } F \in \wedge^{p-1} V^*$$

Beweis: " $\Leftarrow$ ": Lemma 2 liefert p linear unabhängige Vektoren in V_z, und nach Lemma 1 ist z damit zerlegbar.
" $\Rightarrow$ ": Sei $z = x_1 \wedge ... \wedge x_p$. Aus der Definition der Fortsetzung der Linearformen f auf die Graßmannalgebra folgt, daß nach Anwendung von $p-1$ Linearformen hintereinander eine Linearkombination der x_i herauskommt. Diese wird bei $\wedge z$ annulliert.

Beispiel: $p = 2, n = 4$: $z = \sum_{i<j} a_{ij} e_i \wedge e_j$
Wir hatten die Regeln $f(z) \wedge z + z \wedge f(z) = f(z \wedge z)$ und $f(z) \wedge z = z \wedge f(z)$ (beachte $p = 2$!). Also ist $f(z) \wedge z = 0$ für alle f gleichbedeutend mit $f(z \wedge z) = 0$ für alle f, d.h. mit $z \wedge z = 0$.

$$z \wedge z = \sum_{i<j} \sum_{k<l} a_{ij} a_{kl} e_i \wedge e_j \wedge e_k \wedge e_l$$

Summiert werden muß über alle Paare $i < j$, und für $k < l$ müssen die übrig bleibenden Indices genommen werden. Ist σ die Permutation, die $ijkl$ in 1234 überführt, so ist $e_i \wedge e_j \wedge e_k \wedge e_l = \operatorname{sig} \sigma \cdot e_1 \wedge e_2 \wedge e_3 \wedge e_4$. Das ergibt

$$z \wedge z = 2(a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23})\, e_1 \wedge e_2 \wedge e_3 \wedge e_4$$

z ist zerlegbar genau dann, wenn die sogenannte Plückerrelation

$$a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23} = 0$$

erfüllt ist.

6. Pfaffsche Determinante

Sei $e_1, ..., e_n$ die Standardbasis des $\mathbb{R}^n$ und $n = 2m$ gerade. Jede andere Orthonormalbasis $u_1, ..., u_n$ geht daraus hervor durch

$$u_i = Ue_i = \sum_{j=1}^{n} u_{ji} e_j \text{ mit } U'U = \mathbf{1}$$

Für jede Matrix $A \in M_n(\mathbb{R})$ gilt in $\wedge^2 V$

$$\sum_{i=1}^{n} u_i \wedge Au_i = \sum_{i,j,k=1}^{n} u_{ji} e_j \wedge Au_{ki} e_k = \sum_{j,k=1}^{n} (\sum_{i=1}^{n} u_{ki} u_{ji}) e_j \wedge Ae_k = \sum_{j=1}^{n} e_j \wedge Ae_j$$

Also ist

$$\Omega := \sum_{i=1}^{n} e_i \wedge Ae_i$$

unabhängig von der Wahl der Orthonormalbasis.

Multpliziert man Ω m-mal äußerlich mit sich selbst, so erhält man einen n-Vektor. Dieser ist proportional zu $e_1 \wedge .... \wedge e_n$. Das Dachprodukt $e_1 \wedge .... \wedge e_n$ wird bei Basiswechsel mit der Determinante der Übergangsmatrix multipliziert, es bleibt also ungeändert bei allen Substitutionen mit Determinante 1. Man nennt eine Basis des $\mathbb{R}^n$ rechts oder positiv orientiert, wenn sie aus der Standardbasis durch eine Substitution mit positiver Determinante hervorgeht.

Definition: Die durch

$$\frac{1}{2^m m!} \Omega \wedge .... \wedge \Omega \ (m \text{ mal }) = Pf(A) \cdot e_1 \wedge .... \wedge e_n$$

definierte Zahl $Pf(A)$ heißt die Pfaffsche Determinante von A. Sie ändert sich nicht, wenn man $e_1, ..., e_n$ durch irgend eine andere rechts orientierte Orthonormalbasis ersetzt.

Bevor wir den Satz über die Pfaffsche Determinante einer schiefsymmetrischen Matrix beweisen, müssen wir die letztere präparieren:

Satz 18. *A sei eine reelle schiefsymmetrische Matrix mit $|A| \neq 0$. Dann gibt es eine Basis $u_1, v_1, ..., u_m, v_m$ des $\mathbb{R}^n$ ($n = 2m$) und reelle Zahlen $\alpha_1, ..., \alpha_m$ mit*

$$Au_i = \alpha_i v_i \text{ und } Av_i = -\alpha_i u_i \text{ für } i = 1, ..., m$$

Beweis: A^2 ist reell und symmetrisch und hat daher lauter reelle Eigenwerte. Sei β ein Eigenwert von A^2 und $A^2 u = \beta u$, $u \neq 0$. Sei $Au = v$. Es gilt $v'u = u'A'u = -u'Au = -u'v = -v'u$, also $v'u = 0$. Weiter $v'v = u'A'Au = -u'A^2 u = -u'\beta u = -\beta u'u$. Wegen $|A| \neq 0$ ist β nicht 0 und nun $-\beta > 0$. Daher gibt es reelles α mit $\alpha^2 = -\beta$. Man setzt $v_1 = \frac{1}{\alpha} v$. Dann ist

$$v_1' v_1 = \frac{1}{\alpha^2} v'v = -\frac{1}{\beta} v'v = u'u, \quad Au = v = \alpha v_1 \text{und } Av_1 = \frac{1}{\alpha} Av = \frac{1}{\alpha} A^2 u = -\alpha u$$

Multipliziert man u und v_1 mit demselben geeigneten Faktor, so erhält man (mit neuer Bezeichnung) ein orthonormiertes Paar u, v mit $Au = \alpha v$ und $Av = -\alpha u$. Das Orthokomplement von $< u, v >$ im $\mathbb{R}^n$ wird bei A in sich abgebildet:

$$x'u = x'v = 0 \Rightarrow (Ax)'u = x'A'u = -x'Au = -x'\alpha v = 0, \text{ genau so } (Ax)'v = 0$$

Im Orthokomplement von $< u, v >$ sucht man nun ein zweites orthonormiertes Paar u_2, v_2 und α_2 mit $Au_2 = \alpha_2 v_2$ und $Av_2 = -\alpha_2 u_2$ usw., bis man den ganzen $\mathbb{R}^n$ durch solche (zueinander senkrechten) Paare aufgespannt hat.

Mit Hilfe von Satz 18 beweisen wir

Satz 19. *Ist A schiefsymmetrisch, so ist*

$$|A| = Pf(A)^2$$

Beweis: Da Ω sich nicht ändert, wenn man zu einer anderen Orthonormalbasis übergeht, nimmt man zweckmäßig die A angepaßte Basis aus Satz 18. Dann erhält man

$$\Omega = \sum_{i=1}^{m} u_i \wedge Au_i + \sum_{i=1}^{m} v_i \wedge Av_i = \sum_{i=1}^{m} u_i \wedge \alpha_i v_i + \sum_{i=1}^{m} v_i \wedge (-\alpha_i u_i) = 2\sum_{i=1}^{m} \alpha_i \cdot (u_i \wedge v_i)$$

Die m-te äußere Potenz hiervon ist

$$2^m \alpha_1 ....\alpha_m (\sum_{i=1}^{m} u_i \wedge v_i) \wedge .... \wedge (\sum_{i=1}^{m} u_i \wedge v_i) = 2^m \alpha_1 ....\alpha_m \sum_{\sigma \in S_m} u_{\sigma(1)} \wedge v_{\sigma(1)} \wedge ..... \wedge u_{\sigma(m)} \wedge v_{\sigma(m)}$$

$$= 2^m m!\, \alpha_1 ....\alpha_m \; u_1 \wedge v_1 \wedge .... \wedge u_m \wedge v_m$$

weil die Faktoren im Dachprodukt paarweise vertauscht werden, um die zuletzt hingeschriebene Reihenfolge zu erreichen, also beim Vertauschen kein Vorzeichen aufgenommen wird. Daraus folgt

$$Pf(A) = \pm \alpha_1 ....\alpha_m$$

($\pm$, weil wir nicht darüber nachgedacht haben, wie die Orthonormalbasis aus Satz 18 orientiert ist). Anderseits ist $|A| = \alpha_1^2 .....\alpha_m^2$, also $|A| = Pf(A)^2$.

7. Projektive Geometrie

Motivation:

1. Zwei verschiedene Geraden $ax+by=1$ und $cx+dy=1$ schneiden sich im Punkt $x_s=\frac{d-b}{ad-bc}$, $y_s=\frac{a-c}{ad-bc}$, falls $ad\neq bc$, und nicht, falls $ad=bc$.
2. Die Ellipse oder Hyperbel $ax^2+by^2=1$ $(ab\neq 0)$ und die Gerade $x=y$ schneiden sich im Komplexen in zwei Punkten, falls $a+b\neq 0$, und nicht, falls $a+b=0$.
3. Zwei Ellipsen oder Hyperbeln mit Achsen parallel zu den Koordinatenachsen

$$ax^2+by^2=\alpha x+\beta y+\mu \text{ und } cx^2+dy^2=\gamma x+\delta y+\nu$$

in der reellen Ebene können so liegen:

Zunächst kann die Verschiedenheit der Anzahl der Schnittpunkte damit erklärt werden, dass diese nicht reell und deshalb auf der Zeichnung nicht zu sehen sind. Läßt man komplexe Lösungen zu, so hat man, falls $ad\neq bc$, im allgemeinen 4 Schnittpunkte. Dagegen haben zwei Kreise immer höchstens zwei gemeinsame Punkte: Sind sie gegeben durch

$$I:\ x^2+y^2=ax+by+c \text{ und } II:\ x^2+y^2=dx+ey+f$$

so ist ihr Schnitt derselbe wie der von I und $I-II$, also eines Kreises mit $(a-d)x+(b-e)y+(c-f)=0$. Ist $a=d$ und $b=e$ aber $c\neq f$, so ist der Schnitt leer. Sonst ist der Schnitt der beiden Kreise gleich dem Schnitt eines von ihnen mit einer Geraden, besteht also (im Komplexen) aus 2 Punkten.

Also selbst wenn man in allen Polynomgleichungen komplexe Lösungen zuläßt, "fehlen" Punkte. Die projektive Geometrie wird diese "im Unendlichen" finden.

Man setzt

$$x = \frac{x_1}{x_0} \text{ und } y = \frac{x_2}{x_0}, \text{ zunächst } x_0 \neq 0 \tag{1}$$

Natürlich sind x_0, x_1, x_2 nicht durch x und y bestimmt, sondern

$$\text{Paare } (x,y) \longleftrightarrow \text{ Tripel } (x_0,x_1,x_2) \text{ mit } x_0 \neq 0 \text{ bis auf einen gemeinsamen Faktor } \neq 0$$

x_0, x_1, x_2 heißen homogene Koordinaten. Rechnen wir noch einmal die Beispiele, jetzt in den homogenen Koordinaten:

1. Die Gleichungen zweier verschiedener paralleler Geraden werden zu

$$ax_1 + bx_2 = cx_0 \text{ und } ax_1 + bx_2 = dx_0 \text{ wobei } c \neq d$$

   und bekommen die gemeinsame Lösung $(0, b, -a)$, die bis auf einen Faktor ungleich 0 bestimmt ist.
2. Die Geradengleichung $x_1 = x_2$ und die Hyperbelgleichung $x_1^2 - x_2^2 = x_0^2$ bekommen die gemeinsame Lösung $(0,1,1)$.
3. Je zwei Kreise

$$x_1^2 + x_2^2 = ax_1x_0 + bx_2x_0 + cx_0^2 \text{ und } x_1^2 + x_2^2 = dx_1x_0 + ex_2x_0 + fx_0^2$$

   haben $(0,1,i)$ und $(0,1,-i)$ gemeinsam.

Im Hinblick auf (1) nennt man diese neuen Lösungen mit $x_0 = 0$ unendlich fern. Durch Hinzunahme der Fernpunkte erhält man also für

1. je zwei verschiedene Geraden genau einen Schnittpunkt (K beliebig)
2. eine Gerade und einen Kegelschnitt, der nicht in ein diese Gerade enthaltendes Geradenpaar entartet ist, genau zwei Schnittpunkte (wobei der Berührpunkt doppelt gezählt werden muß, wenn die Gerade Tangente ist). ($k = \mathbb{C}$)
3. Zwei Kegelschnitte, die nicht so entarten, daß sie eine Gerade gemeinsam haben, vier Schnittpunkte (mit Vielfachheiten gezählt).

Das sind Spezialfälle des Satzes von Bézout, der in der komplexen projektiven Ebene gilt: Zwei Kurven vom Grad n bzw. m, die keine gemeinsame Komponente haben, schneiden sich in $n \cdot m$ Punkten, wenn man diese mit den richtigen Vielfachheiten zählt. Die Hauptschwierigkeit beim Beweis dieses Satzes besteht darin, diese Vielfachheiten zu definieren.

Nach diesen Vorbetrachtungen die genaue

Definition: Sei V ein Vektorraum der Dimension $n+1$ über dem Körper K. Die Menge aller eindimensionalen Unterräume von V heißt der zu V gehörige n-dimensionale projektiver Raum $P(V)$.

Seine Elemente (das sind sie eindimensionalen Unterräume von V) heißen Punkte. Allgemeiner: ist U ein $(k+1)$-dimensionaler Untervektorraum von V und $k \geq 0$, so heißt

$$\bar{U} := \{< u > \mid 0 \neq u \in U\}$$

ein k-dimensionaler Unterraum von $P(V)$. Offenbar ist

$$\bar{U} \cap \bar{W} = \{< x > \mid 0 \neq x \in U \cap W\} = \overline{U \cap W}.$$

$$\overline{U+W} = \{< x > \mid 0 \neq x \in U + W\} \text{ heißt der Verbindungsraum}$$

von $\bar{U}$ und $\bar{W}$ und wird mit $\bar{U} \vee \bar{W}$ bezeichnet. Zwei Räume $\bar{U}$ und $\bar{W}$ mit $U \cap W = 0$ nennt man windschief. Dann ist $\bar{U} \cap \bar{W} = \phi$. Dem leeren Unterraum von $P(V)$ teilen wir die Dimension -1 zu, dann können wir ohne Fallunterscheidung rechnen:

$$\dim(\bar{U} \vee \bar{W}) = \dim \overline{U+W} = \dim(U+W) - 1 = \dim U + \dim W - \dim(U \cap W) - 1$$

$$= \dim \bar{U} + \dim \bar{W} - \dim(\bar{U} \cap \bar{W})$$

Die eindimensionalen projektiven Unterräume heißen Geraden, die $(n-1)$-dimensionalen Hyperebenen. Auf den beiden Aussagen im Falle $n = 2$

1. Je zwei Geraden in der projektiven Ebene schneiden sich in genau einem Pukt
2. Durch je zwei Punkte der projektiven Ebene geht genau eine Gerade.

beruht das Dualitätsprinzip der ebenen projektiven Geometrie:

Ersetzt man in einer richtigen Aussage über Punkte und Geraden

* *Punkt durch Gerade*
* *Gerade durch Punkt*
* *Schneiden durch Verbinden*
* *Verbinden durch Schneiden*

so erhält man wieder eine richtige Aussage.

Einführung von Koordinaten: $P_0, ..., P_{n+1}$ seien $n+2$ Punkte in $P(V)$, von denen keine $n+1$ in einer Hyperebene liegen. Ist $P_i =< v_i >$ mit $v_i \in V$, so sind also $v_0, v_1, ..., v_n$ linear unabhängig und bilden eine Basis von V. Jeder Vektor $v \in V$ ist eine Linearkombination $\lambda_0 v_0 + ... + \lambda_n v_n$, aber da man v_i durch ein beliebiges Vielfaches ungleich 0 ersetzen kann, ohne P_i zu ändern, sind die λ_i durch Vorgabe von $P_0, ..., P_n$ überhaupt nicht festgelegt. Aber: in $v_{n+1} = \sum_{i=0}^{n} \gamma_i v_i$ sind alle $\gamma_i \neq 0$, weil sonst die übrigen v_i linear abhängig wären, also die übrigen P_i in einer Hyperebene lägen entgegen der Voraussetzung. Ersetzt man v_i durch $\gamma_i v_i$, so erhält man

(1) eine Basis $v_0, ..., v_n$ mit $< v_i >= P_i$ und $< v_0 + v_1 + ... + v_n >= P_{n+1}$

Behauptung: Sind zu gegebenen Punkten $P_0, ..., P_{n+1}$ Vektoren aus V gewählt mit (1), so sind in $P =< \lambda_0 v_0 + ... + \lambda_n v_n >$ die λ_i durch P bis auf einen gemeinsamen Faktor bestimmt.
Beweis: Angenommen, es seien auch w_i mit (1) gewählt und $P =< \mu_0 w_1 + ... + \mu_n w_n >$. Dann gibt es Zahlen α_i, β, γ, alle nicht 0, mit

$$w_i = \alpha_i v_i, \quad \sum_{i=0}^{n} w_i = \beta \sum_{i=0}^{n} v_i \text{ und } \sum_{i=0}^{n} \mu_i w_i = \gamma \sum_{i=0}^{n} \lambda_i v_i$$

Daraus folgt $\alpha_i = \beta$ und $\mu_i \alpha_i = \gamma \lambda_i$ für alle i, also $\beta \mu_i = \gamma \lambda_i$ für alle i.

Definition: Die bis auf einen gemeinsamen Faktor ungleich 0 durch P bestimmten Zahlen $\lambda_0, ..., \lambda_n$ nennt man die homogenen Koordinaten von P in bezug auf das Koordinatensystem $P_o, ..., P_{n+1}$. Die Punkte $P_0, ..., P_n$ heißen die Ecken des Koordinatensystems, P_{n+1} der Einheitspunkt.
Ein Koordinatensystem ist also gegeben durch eine Basis von V mit der zusätzlichen Festlegung, welcher Punkt die Koordinaten 1,1,...,1 haben soll.

Man zeichnet eine Hyperebene $\bar{H}$ in $P(V)$ aus und legt das Koordinatensystem so, daß diese die Gleichung $x_0 = 0$ bekommt. Für einen Punkt $P \notin \bar{H}$ kann man die homogenen Koordinaten so normieren, daß $x_0 = 1$. Danach sind $x_1, ..., x_n$ durch P bestimmt:

$$P(V) \setminus \bar{H} \longleftrightarrow \{(1, x_1, ..., x_n) \mid x_i \in K\} \longleftrightarrow K^n$$

In diesem Sinne schreibt man

$$P(V) = K^n \cup \bar{H}$$

Man nennt $\bar{H}$ die Fernhyperebene und $P(V) \setminus \bar{H}$ einen affinen Teil von $P(V)$.

Projektivitäten: V und W seien Vektorräume über K und ϕ eine lineare Abbildung von V nach W. Wenn $v \in V$ und $\phi v \neq 0$, dann spannt ϕv einen eindimensionalen Unterraum von V auf, $< \phi v >$ ist also ein Punkt des projektiven Raumen $P(W)$. Dieser hängt nur von $< v >$ ab. ϕ induziert also eine Abbildung

$$\bar{\phi} : P(V) \setminus \overline{Kern\, \phi} \longrightarrow P(W)$$

Satz 20. *ϕ und ψ seien lineare Abbildungen von V nach W mit gleichem Kern Z, dim Bild $\phi \geq 2$. Dann gilt*

$$\bar{\phi} = \bar{\psi} \Longleftrightarrow \text{ es gibt } \alpha \in K^* \text{ mit } \psi = \alpha\phi$$

Beweis: Zu $x \in V$, $x \notin Z$, gibt es $\lambda_x \in K^*$ mit $\psi x = \lambda_x \phi x$. Seien $x, y \in V$ derart, daß ihre Bilder $\phi x, \phi y$ linear unabhängig sind. Dann ist

$$\lambda_x \phi x + \lambda_y \phi y = \psi x + \psi y = \psi(x+y) = \lambda_{x+y}\phi(x+y) = \lambda_{x+y}\phi x + \lambda_{x+y}\phi y$$

Es folgt $\lambda_x = \lambda_{x+y} = \lambda_y$. Sind ϕx und ϕy linear abhängig, so wählt man $z \in V$ so, daß ϕx und ϕz linear unabhängig sind und schließt wie oben $\lambda_x = \lambda_z = \lambda_y$.

Ab jetzt sei Kern $\phi = 0$ und dim V = dim W. Dann ist ϕ bijektiv und damit auch $\bar{\phi}$. Da ϕ Unterräume auf Unterräume abbildet und $\bar{\phi}\bar{U} = \overline{\phi U}$, tut das auch $\bar{\phi}$.

Definition 1: Die durch bijektive lineare Abbildungen von V nach W induzierten Abbildungen von $P(V)$ nach $P(W)$ heißen Projektivitäten.

Definition 2: V und V' seien Vektorräume über K bzw. K'. Eine Abbildung σ von $P(V)$ nach $P(V')$ heißt eine Kollineation, wenn

1. dim V = dim $V' \geq 3$
2. σ bijektiv
3. Falls $A, B, C \in P(V)$ auf einer Geraden liegen, dann auch $\sigma A, \sigma B, \sigma C$. Man sagt: kollineare Punkte gehen in kollineare Punkte über.

dim $V \geq 3$ wird gefordert, weil sonst die dritte Bedingung gar nichts mehr aussagt. Jede Projektivität ist eine Kollineation (mit $K = K'$.) Das wollen wir so weit wie möglich umkehren: Es liege der Sachverhalt von Definition 2 vor. Mit $L, L_1, ...$ usw. bezeichnen wir eindimensionale Teilräume von V.

1. Schritt: Wir zeigen durch Induktion nach r:

$$L \subset L_1 + ... + L_r \Rightarrow \sigma L \subset \sigma L_1 + ... + \sigma L_r$$

Beweis: $r = 1$ ist trivial, ebenso $L = L_r$. Sei $r > 1$ und $L \neq L_r$. Dann ist $L =< x + y >$ mit $y \in L_r$ und $0 \neq x \in L_1 + ... + L_{r-1}$. Nach 3. in Definition 2 ist $\sigma L \subset \sigma < x > + \sigma L_r$ und nach Induktionsannahme ist $\sigma < x > \subset \sigma L_1 + ... + \sigma L_{r-1}$. Daraus folgt die Behauptung.

2. Schritt. Sei $v_1, ..., v_n$ eine Basis von V und $L' \subset V'$. Da σ surjektiv, ist $L' = \sigma L \subset \sigma(< v_1 > + ... < v_n >) \subset \sigma < v_1 > + ... + \sigma < v_n >$. Dies zeigt: wenn $< v_i' >= \sigma < v_i >$, dann wird V' von den v_i' aufgespannt, wegen dim V = dim V' bilden die v_i' eine Basis von V'.

3. Schritt: Sei $\lambda \in K$. Nach 1. ist $\sigma < v_1 + \lambda v_2 > \subset < v_1' > + < v_2' >$, aber $\neq < v_2' >$, da σ injektiv. Daher gibt es genau ein $\lambda' \in K'$ mit $\sigma < v_1 + \lambda v_2 >=< v_1' + \lambda' v_2' >$. Die Abbildung $\lambda \mapsto \lambda'$ von K nach K' ist injektiv. Man normiert v_2' so, daß $\sigma < v_1 + v_2 >=< v_1' + v_2' >$, das bedeutet $1' = 1$. Natürlich ist $0' = 0$.

4. Schritt: Wie in 3. definieren wir eine injektive Abbildung $\lambda \mapsto \lambda''$ von K nach K'' durch $\sigma < v_1 + \lambda v_3 >=< v_1' + \lambda'' v_3' >$, wieder mit $1'' = 1$. Hier wird dim $V \geq 3$ benutzt. Wir zeigen $\lambda' = \lambda''$:

$$\text{Aus } < \lambda v_2 - \lambda v_3 > \subset < v_2 > + < v_3 > \text{ und } \subset < v_1 + \lambda v_2 > + < v_1 + \lambda v_3 >$$

$$\text{folgt } \sigma < \lambda v_2 - \lambda v_3 > \subset < v_2' > + < v_3'' > \text{ und } \subset < v_1' + \lambda' v_2' > + < v_1' + \lambda'' v_3' >$$

Die einzige Möglichhkeit, einen Vektor auf beide Weisen zu kombinieren, ist

$$\sigma < \lambda v_2 - \lambda v_3 >=< \lambda' v_2' - \lambda'' v_3' >$$

Dies ist aus demselben Grunde

$$= \sigma < v_2 - v_3 >=< 1' v_2' - 1'' v_3' >$$

Aus $1' = 1 = 1''$ folgt $\lambda' = \lambda''$.

5. Schritt: Wir haben $\sigma < v_1 + \lambda v_i > = < v_1' + \lambda' v_i' >$ für $i = 2, ..., n$ und zeigen jetzt durch Induktion

$$\sigma < v_1 + \lambda_2 v_2 + ... + \lambda_r v_r > = < v_1' + \lambda_2' v_2' + ... + \lambda_r' v_r' >$$

Die Verankerung $r = 2$ ist Schritt 4. Für $r > 2$ ist $< v_1 + \lambda_2 v_2 + ... + \lambda_r v_r >$

$$\subset < v_1 + ... + \lambda_{r-1} v_{r-1} > + < v_r > \text{ und } \subset < v_1 + \lambda_r v_r > + < v_2 > + ... + < v_{r-1} >$$

Nach der Induktionsannahme bzw. nach Schritt 1 folgt daraus $\sigma < v_1 + \lambda_2 v_2 + ... + \lambda_r v_r >$

$$\subset < v_1' + \lambda_2' v_2' + ... + \lambda_{r-1}' v_{r-1}' > + < v_r' > \text{ und } \subset < v_1' + \lambda_r' v_r' > + < v_2' > + ... + < v_{r-1}' >$$

Die einzigen Vektoren, die sich auf beide Weisen kombinieren lassen, liegen in

$$< v_1' + \lambda_2' v_2' + ... + \lambda_r' v_r' >$$

6. Schritt: Die Vektoren, deren erste Komponente 0 ist, erreicht man so:

$$< \lambda_2 v_2 + ... + \lambda_n v_n > \subset < v_1 + \lambda_2 v_2 + ... + \lambda_n v_n > + < v_1 > \text{ und } \subset < v_2 > + ... + < v_n >$$

Nach dem 5. bzw. ersten Schritt folgt daraus

$$\sigma < \lambda_2 v_2 + ... + \lambda_n v_n > \subset < v_1' + \lambda_2' v_2' + ... + \lambda_n' v_n' > + < v_1' > \text{ und } \subset < v_2' > + ... + < v_n' >$$

Der Durchschnitt der letzten beiden Räume ist

$$< \lambda_2' v_2' + ... + \lambda_n' v_n' >$$

7. Schritt: Jetzt wird gezeigt, daß die Abbildung $\lambda \mapsto \lambda'$ ein Isomorphismus von K auf K' ist:

a) Nach 6. haben die $< \sum_i \lambda_i v_i >$ mit $\lambda_1 = 0$ auch Bilder mit $\lambda_1' = 0$. Da σ surjektiv ist, muß $< v_1' + \mu v_2' >$ Bild eines $< v_1 + \lambda v_2 >$ sein, d.h. $\mu = \lambda'$ und $'$ ist surjektiv. In Schritt 3 sahen wir bereits, daß $'$ injektiv ist.

b) Einerseits ist

$$\sigma < v_1 + (\lambda + \mu) v_2 + v_3 > \subset \sigma < v_1 + \lambda v_2 > + \sigma < \mu v_2 + v_3 > = < v_1' + \lambda' v_2' > + < \mu' v_2' + v_3' >$$

$$\text{und anderseits } = < v_1' + (\lambda + \mu)' v_2' + v_3' >$$

Daraus folgt $(\lambda + \mu)' = \lambda' + \mu'$.

c) Einerseits ist

$$\sigma < v_1 + \lambda\mu v_2 + \lambda v_3 > \subset \sigma < v_1 > + \sigma < \mu v_2 + v_3 > = < v_1' > + < \mu' v_2' + v_3' >$$

$$\text{und anderseits } = < v_1' + (\lambda\mu)' v_2' + \lambda' v_3' >$$

Daraus folgt $(\lambda\mu)' = \lambda'\mu'$.

8. Schritt: Man definiert eine Abbildung ϕ von V nach V' durch

$$\phi(\sum_{i=1}^{n} \lambda_i v_i) = \sum_{i=1}^{n} \lambda_i' v_i'$$

Dann gilt

a) $\sigma < v > = < \phi v >$ für alle $v \in V$, $v \neq 0$.

b) ϕ ist bijektiv

c) $\phi(u + v) = \phi(u) + \phi(v)$ und $\phi(\lambda v) = \lambda' \phi(v)$ für alle $u, v \in V$, $\lambda \in K$.

Definition: Seien K und K' Körper und $\lambda \mapsto \lambda'$ ein Isomorphismus von K auf K'. Eine Abbildung eines K-Vektorraumes V in einen K'-Vektorraum V' mit c) heißt semilinear bezüglich $'$.

Wir haben bewiesen

Satz 21. *(Fundamentalsatz der projektiven Geometrie)* V *und* V' *seien Vektorräume gleicher Dimension über* K *bzw.* K' *und* σ *eine Kollineation von* $P(V)$ *auf* $P(V')$. *Dann gibt es einen Isomorphismus* $'$ *von* K *auf* K' *und eine bezüglich* $'$ *semilineare bijektive Abbildung* ϕ *von* V *auf* V' *, so daß*

$$\sigma < v >=< \phi v > \text{ für alle } v \in V,\ v \neq 0$$

Spezialfall: $K = K'$, und K besitzt außer der Identität keine Automorphismen. (Dies gilt z.B. für $K = \mathbb{Q}$ und $K = \mathbb{R}$.) Dann ist jede Kollineation eine Projektivität.

Häufig benutzt wird

Satz 22. *Eine Projektivität* σ *ist durch die Bilder von* $n+2$ *Punkten, von denen keine* $n+1$ *in einer Hyperebene liegen, bestimmt. Umgekehrt gibt es zu je zwei solchen* $(n+2)-$*Tupeln eine Projektivität, die das eine in das andere überführt.*

Beweis: Wir machen die $n+2$ Punkte zu Ecken und Einheitspunkt eines Koordinatensystems in $P(V)$, ebenso deren Bilder in $P(V')$. Da σ durch eine lineare Abbildung induziert wird, geht der Punkt aus $P(V)$ mit den homogenen Koordinaten $\lambda_0, ..., \lambda_n$ in den Punkt aus $P(V')$ mit denselben Koordinaten über. Also ist σ durch die Bilder dieser $n+2$ Punkte bestimmt, und umgekehrt wird durch diese Vorschrift eine Projektivität von $P(V)$ auf $P(V')$ erklärt, die die Punkte wie verlangt abbildet.

Die Projektivitäten eines projektiven Raumes $P(V)$ auf sich bilden eine Gruppe, bezeichnet mit $PGL(V)$. Ist $V = K^{n+1}$, so bezeichnet man $P(V)$ mit $P^n(K)$ und die Gruppe seiner Projektivitäten mit $PGL(n+1, K)$. Nach Definition ist $PGL(V)$ das Bild von $GL(V)$ unter $\phi \mapsto \bar{\phi}$, und $\bar{\phi} = id$ genau dann, wenn $\phi \in K^* \cdot id$. Diesen Sachverhalt beschreibt man (für die Matrizengruppe $GL(n+1, K)$) durch

$$K^* \hookrightarrow GL(n+1, K) \longrightarrow PGL(n+1, K)$$

Spezielle Projektivitäten:

Definition: Eine Projektivität eines projektiven Raumes auf sich, die eine Hyperebene punktweise festläßt, heißt Perspektivität.

Sei $n = \dim P(V) \geq 2$ und $\bar{H}$ die von σ punktweise festgelassene Hyperebene, H der zugehörige n-dimensionale Untervektorraum von V. Da die σ induzierende lineare Abbildung ϕ nur bis auf einen Faktor bestimmt ist und auf H (wegen $n \geq 2$) Vielfaches der Eins ist, ist oE $\phi x = x$ für alle $x \in H$. Ist $\phi \neq id$, so ist dim Bild $(\phi - 1) = 1$, also $(\phi - 1)V =< s >$ mit $0 \neq s \in V$. Für den Punkt $S =< s >$ in $P(V)$ folgt daraus
(1) Für alle $P \in P(V)$ sind P, σP und S kollinear.

Definition: $\bar{H}$ heißt die Achse und S das Zentrum der Perspektivität.

Behauptung: Eine Perspektivität ist durch ihre Achse, das Zentrum, sowie einen Punkt P und sein Bild bestimmt. (Figur 1-4)
Beweis: Sei $Q \notin \bar{H}$ und nicht auf $P \vee S$. Die Verbindungsgerade $P \vee Q$ schneide $\bar{H}$ in F. Dann ist $\sigma P \vee \sigma Q = \sigma(P \vee Q) = \sigma(P \vee F) = \sigma P \vee F$, also liegt σQ auf $\sigma P \vee F$. Anderseits liegt σQ auf $Q \vee S$. Die beiden Geraden $Q \vee S$ und $\sigma P \vee F$ liegen in einer Ebene (nämlich $P \vee Q \vee S$) und sind verschieden, haben also genau einen Schnittpunkt. Dieser ist σQ.

Für eine Perspektivität gibt es zwei Möglichkeiten: das Zentrum kann auf der Achse liegen oder nicht. Im ersten Falle heißt sie eine Translation, im zweiten eine Dilatation. Bei geeigneter Koordinatenwahl werden die Translationen durch elementare Matrizen und die Dilatationen durch Diagonalmatrizen beschrieben. Da man durch solche Matrizen die volle $GL(n, K)$ erzeugen kann, folgt

Satz 23. *Jede Projektivität ist eine Hintereinanderausführung von Perspektivitäten.*

Anwendung: Gegeben seien zwei Dreiecke ABC und $A'B'C'$, so daß die Verbindungsgeraden entsprechender Ecken durch einen Punkt S gehen. (Figur 5)
Sei $(A \vee B) \cap (A' \vee B') = P$ und $(A \vee C) \cap (A' \vee C') = Q$ und $g = P \vee Q$. Dann sei π die Perspektivität mit Zentrum S und Achse g, welche A in A' abbildet. πB liegt auf $\pi A \vee P$ und auf $B \vee S$, also ist $\pi B = B'$. Genauso folgt $\pi C = C'$. Dann müssen sich aber $B \vee C$ und $\pi B \vee \pi C$ auch auf der Achse g treffen. Das ist der

Satz 24. *(Satz des Desargues) Gehen die Verbindungsgeraden entsprechender Ecken von zwei Dreiecken durch einen Punkt (perspektive Lage der Dreiecke), so liegen die Schnittpunkte entsprechender Seiten auf einer Geraden.*

Dualisiert man diesen Satz, so erhält man gerade seine logische Umkehrung.

8. Doppelverhältnis

Auf K ist das Teilverhältnis von c in Bezug auf a und b ($a \neq b \neq c \neq a$) erklärt durch

$$TV(a,b,c) = \frac{c-a}{c-b}$$

Das Doppelverhältnis ist das Verhältnis von zwei Teilverhältnissen:

$$DV(a,b,c,d) = \frac{c-a}{c-b} \cdot \frac{d-b}{d-a} \tag{1}$$

Dabei ist wieder vorausgesetzt, daß die vier Zahlen paarweise verschieden sind. Um das Doppelverhältnis auf der projektiven Geraden zu erklären, benutzt man homogene Koordinaten:

Definition: Für vier verschiedene Punkte $A = (a_0, a_1)$, B, C, $D = (d_0, d_1)$ ist das Doppelverhältnis erklärt durch

$$DV(ABCD) = \frac{(c_1a_0 - c_0a_1)\cdot(d_1b_0 - d_0b_1)}{(c_1b_0 - c_0b_1)\cdot(d_1a_0 - d_0a_1)} = \frac{\begin{vmatrix} a_0 & c_0 \\ a_1 & c_1 \end{vmatrix} \cdot \begin{vmatrix} b_0 & d_0 \\ b_1 & d_1 \end{vmatrix}}{\begin{vmatrix} b_0 & c_0 \\ b_1 & c_1 \end{vmatrix} \cdot \begin{vmatrix} a_0 & d_0 \\ a_1 & d_1 \end{vmatrix}} \tag{2}$$

Aus der Darstellung durch Determinanten sieht man sofort die wichtigste Eigenschaft des Doppelverhältnisses:

Satz 25. *Das Doppelverhältnis ist invariant bei Projektivitäten.*

Spezialfälle:

1. Legt man das Koordinatensystem so, daß $A = (1,0)$, $B = (0,1)$, $D = (1,1)$, so ist für den Punkt $C = (1,c)$
$$DV(ABCD) = c$$
2. Für den Fernpunkt $\infty = (0,1)$ ist
$$DV(ABC\infty) = \frac{(a_0c_1 - a_1c_0)\cdot b_0}{(b_0c_1 - b_1c_0)\cdot a_0} = \frac{c-a}{b-a}$$ das Teilverhältnis von A, B, C
3. Ist $DV(AB\infty D) = -1$, so ist D der Mittelpunkt der Strecke AB.

Es gibt 24 Permutationen von $ABCD$. An der Definition sieht man, daß das Doppelverhältnis sich bei den Permutationen id, $(AB)(CD)$, $(AC)(BD)$ und $(AD)(BC)$ der sogenannten Kleinschen Vierergruppe nicht ändert. Also kann es höchstens 6 verschiedene Werte annehmen. Sei $DV(ABCD) = \lambda$. Durch eine Projektivität, die ja DV nicht ändert, kann man dafür sorgen, daß ∞ unter den vier Punkten nicht vorkommt. Dann können wir mit den Koordinaten a, b, c, d aus (1) rechnen:

$$\lambda = \frac{(c-a)(d-b)}{(c-b)(d-a)} = \frac{[(c-b)-(a-b)][(d-a)-(b-a)]}{(c-b)(d-a)} =$$

$$1 - (a-b)\frac{(d-a)-(c-b)+(a-b)}{(c-b)(d-a)} = 1 - \frac{(a-b)(d-c)}{(c-b)(d-a)} = 1 - DV(ACBD), \text{ also}$$

$$DV(ACBD) = 1 - \lambda$$

Aus der Definition (2) ist offenkundig, daß bei Vertauschen von A und B und Festhalten von C und D das Doppelverhältnis λ in seinen Kehrwert $\frac{1}{\lambda}$ übergeht. Mit λ kommen also auch $\frac{1}{\lambda}$ und $1-\lambda$ vor, dadurch erhalten wir tatsächlich die sechs im allgemeinen verschiedenen Werte

$$\lambda,\ \frac{1}{\lambda},\ 1-\lambda,\ \frac{1}{1-\lambda},\ \frac{\lambda-1}{\lambda},\ \frac{\lambda}{\lambda-1}$$

Bei besonderer Lage der vier Punkte können diese Werte natürlich teilweise zusammenfallen.

1. Wenn $2 \neq 0$ in K, dann fallen für $\lambda = -1$ je zwei der Werte zusammen, und man erhält -1, $\frac{1}{2}$ und 2. Diesen Fall nennt man harmonische Lage.
2. Ist K ein Körper, der eine primitive 6. Einheitswurzel ζ enthält, so fallen für $\lambda = \zeta$ je 3 der Werte zusammen, und man erhält ζ und $\bar{\zeta} = \zeta^{-1} = 1 - \zeta$. Diesen Fall nennt man die äquianharmonische Lage.

g und h seien zwei Geraden in $P^2(K)$ und S ein Punkt, der weder auf g noch auf h liegt. Die Abbildung, die jedem Punkt $P \in g$ den Punkt $h \cap (P \vee S)$ zuordnet, ist eine Projektivität von g auf h; denn wir betrachten einfach die Perspektivität π in $P^2(K)$ mit Zentrum S und irgendeiner Achse, die weder mit g noch mit h zusammenfällt und durch $F = g \cap h$ geht, und die einen beliebig aber fest gewählten Punkt $C \in g$ auf $h \cap (S \vee C)$ abbildet. Das Bild πP eines beliebigen Punktes $P \in g$ liegt dann auf $S \vee P$ und auf $\pi C \vee F = h$, ist also $= h \cap (S \vee P)$ (Figur 1)

Umgekehrt: Ist π eine Projektivität von g auf h, bei der $F = g \cap h$ fest bleibt, so entsteht π auf diese Weise: Sei $F =< f > \neq < a >= A \in g$. f und a bilden eine Basis des Vektorraumes $U \subset K^3$ mit $g = P(U) \subset P^2(K)$. Da π durch eine lineare Abbildung ϕ induziert wird, ist $\pi < \lambda f + \mu a > = - < \phi(\lambda f + \mu a) > = < \lambda f + \mu \phi a >$ wegen $\pi F = F$, also oE $\phi f = f$. Das zeigt, daß alle Verbindungsgeraden $P \vee \pi P$ durch $< a - \phi a >$ gehen.

Anwendung: Gegeben seien vier Geraden, von denen keine drei durch einen Punkt gehen. Sie bilden ein sogenanntes Vierseit und schneiden sich in $\binom{4}{2} = 6$ Punkten. Auf jeder Seite liegen 3 der 6 Punkte, jeder Punkt ist also mit 4 anderen durch eine Seite verbunden, also mit einem nicht. Die 3 noch fehlenden Verbindungsgeraden von Ecken heißen die Diagonalen des Vierseits.

Satz 26. *Auf jeder der drei Diagonalen eines Vierseits liegen die Schnittpunkte mit den beiden anderen Diagonalen harmonisch zu den beiden auf der Diagonalen liegenden Ecken. (Figur 2)*

Beweis: Bei Projektion der Geraden $A \vee C$ aus dem Zentrum H auf die Gerade $G \vee C$ geht das Quadrupel $ABCD$ auf $EGCF$. Dieses geht bei Projektion aus S auf die Gerade $A \vee B$ nach $BACD$. Wegen der Invarianz des Doppelverhältnisses folgt

$$\lambda := DV(ABCD) = DV(EGCF) = DV(BACD) = \frac{1}{\lambda}$$

Daraus folgt $\lambda^2 = 1$, und da $\lambda = 1$ ausgeschlossen ist, muß $\lambda = -1$ sein.

Spezialfall: Die Diagonalen $A \vee B$ und $G \vee E$ sind parallel, das heißt C ist der Fernpunkt von beiden. $DV(ABCD) = -1$ bedeutet dann, daß D der Mittelppunkt der Verbindungsstrecke von A und B ist. Mit Hilfe der Figur vom Vierseit kann man nur mit dem Lineal eine gegebene Strecke halbieren, falls zu dieser eine Parallele gezeichnet vorliegt (oder umgekehrt zu einer halbierten Strecke durch jeden gegebenen Punkt eine Parallele zeichnen).

9. Projektive und affine Klassifikation der Quadriken

Sei $A = A' \in M_{n+1}(K)$. Mit $x'Ax = 0$ ist auch $(\lambda x)'A(\lambda x) = 0$ für alle $\lambda \in K$. Daher ist durch $x'Ax = 0$ eine Teilmenge des $P^n(K)$ definiert.

Definition:

$$\mathfrak{Q} = \{P =< x >\in P^n(K) \mid x'Ax = 0\}$$

heißt eine Quadrik, für $n = 2$ ein Kegelschnitt.

Wir wollen diese klassifizieren, und zwar

a) komplex projektiv, indem wir alle Projektivitäten aus $PGL(n+1, \mathbb{C})$ zulassen
b) reell projektiv, indem wir $K = \mathbb{R}$ setzen und alle Projektivitäten aus $PGL(n+1, \mathbb{R})$ zulassen
c) reell affin, indem wir $K = \mathbb{R}$ setzen und nur Affinitäten (s.u.) zulassen.

Genauer wollen wir die Matrizen A bis auf einen Faktor, d.h. die zu A gehörigen "Polaritäten" (s.u.) klassifizieren. Diesen entsprechen die Quadriken umkehrbar eindeutig über $\mathbb{C}$, aber i.a. nicht über beliebigen Körpern, z.B. nicht über $\mathbb{R}$.

Satz 27. *Sind* $A = A'$ *und* $B = B'$ *in* $M_{n+1}(\mathbb{C})$ *und gilt*

$$x'Ax = 0 \Longleftrightarrow x'Bx = 0$$

dann gibt es eine Zahl $\rho \neq 0$ *mit* $B = \rho A$.

Beweis: Ist $x'Ax = 0$ für alle x, so ist $0 = (x+y)'A(x+y) = 2x'Ay$ fúr alle x und y, also $A = 0$ und genauso $B = 0$. Ist das nicht der Fall, so sei $e \in \mathbb{C}^{n+1}$ und $e'Ae \neq 0$. Indem man A und B um einen Faktor abändert, kann man annehmen, daß $e'Ae = e'Be = 1$ ist. Für alle $x \in \mathbb{C}^{n+1}$ und alle komplexen Zahlen λ gilt

$$(x + \lambda e)'A(x + \lambda e) = 0 \Leftrightarrow (x + \lambda e)'B(x + \lambda e) = 0$$

Die beiden quadratischen Polynome in λ

$$\lambda^2 + 2\lambda x'Ae + x'Ax \text{ und } \lambda^2 + 2\lambda x'Be + x'Bx$$

haben also dieselben Nullstellen und damit nach Vieta dieselben Koeffizienten. Daraus folgt $x'Ax = x'Bx$ für alle x und damit $x'Ay = x'By$ für alle x, y, also $A = B$.

1. Bemerkung: Dies ist ein Spezialfall des Hilbertschen Nullstellensatzes: Ist f null auf dem gemeinsamen Nullstellengebilde von $g_1, ..., g_k$, so läßt sich eine Potenz von f aus den g_i kombinieren: $f^s = u_1 g_1 + ... + u_k g_k$ mit $u_i \in \mathbb{C}[X_0, ..., X_n]$.

2. Bemerkung: Über anderen Körpern als $\mathbb{C}$ ist die Behauptung falsch, zum Beispiel haben alle positiv definiten reellen Matrizen A dieselben Lösungen von $x'Ax = 0$, nämlich $x = 0$.

Definition: Sei $A = A' \in M_{n+1}(K)$ und $|A| \neq 0$. Dann wird bei festem $P =< p >\in P^n(K)$ durch $p'Ax = 0$ eine Hyperebene definiert. Sie heißt die Polare von P. Umgekehrt gibt es zu jeder Hyperebene $a'x = 0$ genau einen Punkt $P =< p >$, dessen Polare sie ist, nämlich $p = A^{-1}a$. Er heißt ihr Pol. $P =< p >$ und $Q =< q >$ heißen polar zueinander, wenn $p'Aq = 0$.

Definition: Eine Hyperebene, die ihren Pol P enthält, heißt Tangentialhyperebene im Punkte P an die Quadrik. P heißt der Berührungspunkt.

Die Tangentialhyperebene in P enthält mit jedem Punkt $Q \neq P$ auch die Verbindungsgerade $P \vee Q$: aus $p'Ap = 0$ (P auf Quadrik) und $p'Aq = 0$ (Q polar zu P) folgt $(\lambda p + \mu q)'Ap = 0$, d.h. $< \lambda p + \mu q >$ polar zu P für alle λ, μ.

Definition: Ist die Matrix A nicht invertierbar, so heißt der durch $Ax = 0$ definierte projektive Unterraum die Spitze der Quadrik.

Eine Quadrik ohne Spitze heißt nicht ausgeartet. Es bedeutet, daß die Matrix A den Rang $n+1$ hat.

Zur Klassifikation:

a) komplex projektiv: Zu $A = A' \in M_{n+1}(\mathbb{C})$ gibt es $T \in GL(n+1,\mathbb{C})$, so daß $T'AT$ eine Diagonalmatrix mit Nullen und Einsen ist. Jede Quadrik läßt sich transformieren auf

$$x_0^2 + x_1^2 + ... + x_r^2 = 0, \;\; 0 \leq r \leq n$$

Alle Quadriken, deren Spitze dieselbe Dimension hat, sind projektiv äquivalent (lassen sich durch eine Projektivität ineinander überführen).

b) reell projektiv: Zu $A = A' \in M_{n+1}(\mathbb{R})$ gibt es nach dem Sylvesterschen Trägheitssatz $T \in GL(n+1,\mathbb{R})$ mit

$$T'AT = \begin{pmatrix} \mathbf{1}_p & & \\ & -\mathbf{1}_q & \\ & & \mathbf{0} \end{pmatrix}$$

und p und q sind durch A bestimmt. Da man die Gleichung der Quadrik mit -1 multiplizieren kann, ohne die Quadrik zu ändern, kann man die Gleichung immer so schreiben, daß die Zahl der Minuseinsen nicht größer ist als die der Einsen. Man erhält alle Typen, jeden genau einmal, in der Gestalt

$$x_0^2 + ... + x_r^2 - x_{r+1}^2 - .... - x_{r+s}^2 = 0, \;\; r+1 \geq s, \;\; r+s \leq n$$

Beispiel: Die nicht ausgearteten Quadriken im dreidimensionalen reellen projektiven Raum sind

(a) $$x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0 \quad (\text{ leer })$$

(b) $$x_0^2 + x_1^2 + x_2^2 - x_3^2 = 0 \quad (\text{ Ellipsoid })$$

(c) $$x_0^2 + x_1^2 - x_2^2 - x_3^2 = 0 \quad (\text{ Hyperboloid })$$

Wir beweisen, daß (c) relle Geraden trägt. Genauer:

Satz 28. *Auf der Quadrik (c) gibt es zwei Scharen von Geraden. Je zwei Geraden derselben Schar sind windschief, je zwei Geraden aus verschiedenen Scharen schneiden sich in genau einem Punkt. Durch jeden Punkt der Quadrik geht von jeder Schar genau eine Gerade.*

Beweis: Durch

$$\begin{aligned} z_0 &= x_0 + x_2, & z_2 &= x_3 + x_1 \\ z_1 &= x_0 - x_2, & z_3 &= x_3 - x_1 \end{aligned}$$

kann man das Hyperboloid (c) auf

(c') $$z_0 z_1 - z_2 z_3 = 0$$

transformieren. Eine Gerade im dreidimensionalen projektiven Raum wird durch Nullsetzen von zwei Linearformen beschrieben. Offenbar liegen alle Geraden

(I) $$\begin{aligned} \alpha z_0 + \beta z_2 &= 0 \\ \alpha z_3 + \beta z_1 &= 0 \end{aligned}, \quad (\alpha,\beta) \neq (0,0)$$

auf (c'); denn (I) ist ein lineares Gleichungssystem mit nicht trivialer Lösung (α,β), dessen Koeffizientendeterminante die linke Seite von (c') ist. Ebenso liegen alle Geraden

(II) $$\begin{aligned} \gamma z_0 + \delta z_3 &= 0 \\ \gamma z_2 + \delta z_1 &= 0 \end{aligned} \quad (\gamma,\delta) \neq (0,0)$$

auf (c').

a) Sind (α, β) und (α', β') nicht proportional, so folgt aus

$$\begin{array}{rcrcl} \alpha z_0 & + & \beta z_2 & = & 0 \\ \alpha' z_0 & + & \beta' z_2 & = & 0 \end{array}$$

daß $z_0 = z_2 = 0$. Genauso folgt aus der zweiten Gleichung in (I), daß $z_1 = z_3 = 0$. Also haben zwei verschiedene Systeme (I) nur die Lösung $z = 0$ gemeinsam, zwei verschieden Geraden (I) also keinen Punkt.
b) Gegeben seien eine Gerade (I) und eine Gerade (II) mit den Parametern $\alpha.\beta$ bzw. γ, δ. Als gemeinsame nicht triviale Lösung von (I) und (II) sieht man sofort $(-\beta\delta, -\alpha\gamma, \alpha\delta, \beta\gamma)$. Und diese ist bis auf einen Faktor einzig, weil die vierreihige Koeffizientenmatrix von (I) und (II) zusammen den Rang 3 hat.
c) Sei g eine Gerade auf (c'). Sie trifft die Ebene $x_0 = 0$ in einem Punkt mit $x_2 = 0$ oder $x_3 = 0$. Sei etwa $< (0, \alpha, 0, \beta) > \in g$ und $P =< (p_0, p_1, p_2, p_3) > \in g$ mit $p_0 \neq 0$. Dann besteht g aud allen $< (\lambda p_0, \lambda p_1 + \mu\alpha, \lambda p_2, \lambda p_3 + \mu\beta) >$. Da g ganz auf (c') liegt, folgt $p_0 p_1 = p_2 p_3$ und $p_0\alpha = p_2\beta$. Alle Punkte auf g erfüllen

$$\alpha x_0 - \beta x_2 = 0 \text{ und } \alpha x_3 - \beta x_1 = \alpha(\lambda p_3 + \mu\beta) - \beta(\lambda p_1 + \mu\alpha) = \frac{p_3}{p_0}(\alpha p_0 - \beta p_2) = 0$$

Also ist g eine Gerade der Schar I. Der Fall $g \cap \{x_0 = 0\} =< (0, \alpha, \beta, 0) >$ liefert $g \in$ II. Also gibt es keine weiteren Geraden auf dem Hyperboloid außer denen der beiden Scharen I und II.

Affine reelle Klassifikation In Kap.7 hatten wir den n-dimensionalen projektiven Raum als Vereinigung des K^n mit einer Hyperebene geschrieben, welche die Fernebene genannt wurde. K^n hieß affiner Teil des projektiven Raumes.

Definition: Eine Projektivität, die die Fernebene in sich abbildet, heißt Affinität.

Üblicherweise hat die Fernebene die Gleichung $x_0 = 0$. Eine Affinität muß auch den affinen Teil $x_0 \neq 0$ in sich abbilden. Sei sie etwa gegeben durch

$$(1) \qquad x_i' = \sum_{i=0}^{n} a_{ij} x_j$$

Wenn $x_0 = 0$ gleichbedeutend ist mit $x_0' = 0$, sind $a_{01} = ... = a_{0n} = 0$, und aus (1) wird

$$\begin{array}{rcl} x_0' & = & a_{00} x_0 \qquad , \qquad a_{00} \neq 0 \\ x_i' & = & \sum_{j=0}^{n} a_{ij} x_j \quad = \quad a_{i0} x_0 + \sum_{j=1}^{n} a_{ij} x_j \quad \text{für } i = 1, ..., n \end{array}$$

In affinen Koordinaten liest sich das

$$\frac{x_i'}{x_0'} = \frac{a_{i0}}{a_{00}} + \sum_{j=1}^{n} \frac{a_{ij}}{a_{00}} \cdot \frac{x_i}{x_0} \quad \text{für } i = 1, ..., n$$

Eine Affinität ist also eine lineare Transformation der affinen Koordinaten, gefolgt von einer Schiebung. Die Schiebungen sind die Affinitäten, die die Fernebene nicht nur als Ganzes, sondern elementweise festlassen.

"Reelle affine Klassifikation" der Quadriken bedeutet, daß man zwei Quadriken im $P^n(\mathbb{R})$ als äquivalent ansieht, wenn sie durch eine Affinität auseinander hervorgehen, und daß man für jede Äquivalenzklasse einen Vertreter durch eine (möglichst einfache) Gleichung angibt. Dies geschieht nun, indem man erst gröbere, dann feinere Unterscheidungsmerkmale berücksichtigt, die sich offensichtlich durch eine Affinität nicht beseitigen lassen, und das Koordinatensystem geeignet wählt. Wir führen das für $n = 3$ vollständig durch, gucken aber vorher, welche nicht ausgearteten Typen es für $n = 2$ gibt. Die allgemeine Kegelschnittgleichung lautet

$$(1) \qquad x' A x = a_{00} x_0^2 + 2a_{01} x_0 x_1 + 2a_{02} x_0 x_2 + a_{11} x_1^2 + 2a_{12} x_1 x_2 + a_{22} x_2^2 = 0$$

1. Der Pol der Ferngerade ist endlich. Wir legen ihn nach (100). Dann wird aus (1)

$$a_{00} x_0^2 + a_{11} x_1^2 + 2a_{12} x_1 x_2 + a_{22} x_2^2 = 0$$

Durch

$$T\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_0 \\ t_{11}x_1 + t_{12}x_2 \\ t_{21}x_1 + t_{22}x_2 \end{pmatrix}$$

wird dies nach Sylvester auf

$$x_0^2 \pm x_1^2 \pm x_2^2 = 0$$

gebracht. Es gibt 3 wesentlich verschiedene Vorzeichenverteilungen:
a) $x_0^2 + x_1^2 + x_2^2 = 0$, der Kegelschnitt ist leer
b) $x_0^2 + x_1^2 - x_2^2 = 0$, Hyperbel
c) $x_0^2 - x_1^2 - x_2^2 = 0$, Ellipsse

2. Die Ferngerade enthält ihren Pol (ist Tangente an den Kegelschnitt). Dann wird aus (1)

$$x_0 \cdot (a_{00}x_0 + 2a_{01}x_1 + 2a_{02}x_2) + a_{11}x_1^2 = 0$$

mit $a_{02} \neq 0$ wegen Rang $A = 3$. Durch

$$x_0' = x_0, \quad x_1' = x_1, \quad x_2' = 2a_{02}x_2 + 2a_{01}x_1 + a_{00}x_0$$

wird daraus (oE $a_{11} = -1$)

$$x_1^2 = x_0x_2 \qquad \text{Parabel}$$

Die drei nicht leeren (nicht ausgearteten) Kegelschnitte unterscheiden sich dadurch, ob sie die Ferngerade in 2, 0 oder einem Punkt treffen.

Jetzt kommt die Klassifikation für $n = 3$:

Rang $A = 4$:

1. Der Pol der Fernebene ist endlich. Dann legt man ihn in (1000). Nun ist $x'Ay = 0$ erfüllt für $x = (1000)$ und alle y mit $y_0 = 0$. Das bedeutet

$$A = \begin{pmatrix} a_{00} & 0 & 0 & 0 \\ 0 & & & \\ 0 & & B & \\ 0 & & & \end{pmatrix}$$

Jede Transformation vom Typ $\begin{pmatrix} 1 & 0 \\ 0 & T \end{pmatrix}$ ist eine Affinität. Also kann man auf die Teilmatrix B den Sylvesterschen Trägheitssatz anwenden und sie auf Diagonalgestalt transformieren. Dadurch erhält die Quadrik die Gleichung

$$a_0x_0^2 + a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0, \quad \text{alle } a_i = \pm 1$$

a) alle $a_i > 0$ (oder alle < 0) : Die Gleichung ist

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0, \quad \text{die Quadrik ist leer}$$

b) Die Quadrik ist nicht leer, enthält aber keine Fernpunkte. Dann lautet die Gleichung

$$x_1^2 + x_2^2 + x_3^2 = x_0^2, \quad \text{die Quadrik ist ein Ellipsoid}$$

c) Die Quadrik hat Fernpunkte, trägt aber keine Geraden. Aus der Fernebene $x_0 = 0$ wird eine Ellipse ausgeschnitten, die Gleichung wird

$$x_1^2 + x_2^2 + x_0^2 = x_3^2, \quad \text{zweischaliges Hyperboloid}$$

d) Jetzt ist bis auf Äquivalenz noch eine Vorzeichenverteilung übrig, nämlich

$$x_0^2 + x_1^2 - x_2^2 - x_3^2 = 0, \quad \text{einschaliges Hyperboloid}$$

Dies ist die einzige Quadrik ohne Spitze, die Geraden trägt. Sie schneidet ebenfalls aus der Fernebene eine Ellipse aus.

Beide Typen von Hyperboloiden entstehen durch Drehung einer Hyperbel. Offenbar kann man eine Hyperbel um eine Symmetrieachse so drehen, daß eine zusammenhängende Fläche entsteht (einschaliges Hyperboloid) und um eine dazu senkrechte, so daß eine aus zwei Teilen bestehende Fläche entsteht (zweischaliges Hyperboloid).

2. Der Pol der Fernebene liegt auf ihr, d.h. die Fernebene ist Tangentialebene.

Solche Quadriken nennt man Paraboloide. Wir machen den Pol der Fernebene zu (0001). Dadurch wird die Matrix A zu

$$A = \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & 0 \\ a_{20} & a_{21} & a_{22} & 0 \\ a_{30} & 0 & 0 & 0 \end{pmatrix}$$

Da A den Rang 4 hat, ist $a_{03} \neq 0$ und $a_{11}a_{22} - a_{12}^2 \neq 0$. Jede Transformation

$$\begin{array}{lcl} x_0' &=& x_0 \\ x_1' &=& t_{11}x_1 + t_{12}x_2 \\ x_2' &=& t_{21}x_2 + t_{22}x_2 \\ x_3' &=& a_{00}x_0 + 2a_{01}x_1 + 2a_{02}x_2 + 2a_{03}x_3 \end{array}$$

mit invertierbarem T ist eine Affinität, und nach Sylvester kann man durch geeignetes T den Mittelteil von A zu $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$ machen. Dann erhalten wir für die Quadrik eine Gleichung $x_0x_3 = \pm x_1^2 \pm x_2^2$.

a) $x_0x_3 = x_1^2 + x_2^2$ elliptisches Paraboloid
b) $x_0x_3 = x_1^2 - x_2^2$ hyperbolisches Paraboloid

Es gibt also 6 Typen nicht ausgearteter Quadriken im $P^3(\mathbb{R})$: vier Typen von Mittelpunktsquadriken (Pol der Fernebene endlich), wenn man die sogenannte nullteilige Quadrik, die gar keine reellen Punkte besitzt, mitzählt, und zwei Paraboloide.

Rang $A = 3$

Diese Quadriken haben eine Spitze, die aus genau einem Punkt besteht.

1. Die Spitze ist endlich. Dann legen wir sie nach (1000). Nach Definition von Spitze bedeutet das, daß die erste Spalte der Matrix A verschwindet. In den Koordinaten x_1, x_2, x_3 können wir jede Projektivität anwenden (und x_0 dabei festlassen). Nach dem Sylvesterschen Trägheitssatz finden wir

a) $x_1^2 + x_2^2 + x_3^2 = 0$ Die Quadrik besteht nur aus ihrer Spitze (1000).
b) $x_1^2 + x_2^2 - x_3^2 = 0$ Dies ist ein Kegel, dessen Spitze der Nullpunkt des affinen Koordinatensystems ist.

2. Die Spitze liegt auf der Fernebene. Wir machen sie zu (0001). Das bedeutet, daß in der Matrix A die letzte Spalte verschwindet. Die Restmatrix hat den Rang 3, und die affine Klassifikation der (nicht ausgearteten) Kegelschnitte liefert

a) $x_0^2 + x_1^2 + x_2^2 = 0$. Die Quadrik hat keinen endlichen Punkt, sie besteht nur aus ihrer unendlich fernen Spitze.
b) $x_1^2 + x_2^2 = x_0^2$ elliptischer Zylinder
c) $x_1^2 - x_2^2 = x_0^2$ hyperbolischer Zylinder
d) $x_0x_1 - x_2^2 = 0$ parabolischer Zylinder

Rang $A = 2$

Jetzt ist die Spitze eine Gerade. Jedenfalls trifft sie die Fernebene, man muß unterscheiden, ob sie ganz auf ihr liegt oder nicht.

1. Die Spitze ist eine unendlich ferne Gerade. Dann wählen wir die Koordinaten so, daß sie von (0001) und (0010) aufgespannt wird. Dadurch werden die letzten beiden Spalten von A zum Verschwinden gebracht. Die Quadrik erhält die Gleichung $a_{00}x_0^2 + 2a_{01}x_0x_1 + a_{11}x_1^2 = 0$, und die zweireihige Matrix dieser Koeffizienten a_{ij} hat Rang 2. Ist sie positiv oder negativ definit, so hat die Quadrik keine Punkte mit $x_0 \neq 0$, besteht also nur aus der unendlich fernen Geraden. Ist sie indefinit, so ist die linke Seite der Gleichung das Produkt von zwei Linearformen, die wegen Rang A=2 linear unabhängig sind. In diesem Falle besteht die Quadrik aus den beiden Ebenen, die durch Nullsetzen dieser Linearformen entstehen. Eine der beiden Ebenen kann die Fernebene sein. Ist keine die Fernebene, so sind sie parallel, denn ihre Schnittgerade ist die unendlich ferne Spitze.

2. Die Spitze liegt nicht ganz auf der Fernebene. Dann spannen wir sie durch (1000) und (0100) auf. Dadurch verschwinden die ersten beiden Spalten der Matrix A. Wieder gilt: Ist die verbleibende Matrix definit, so besteht die Quadrik nur aus ihrer Spitze. Sonst besteht sie aus zwei Ebenen, die aber in diesem Falle nicht parallel sind, sondern sich in der (nunmehr endlichen) Spitze schneiden.

Rang $A = 1$. Dann ist die Quadrik eine Ebene, welche die Fernebene sein kann oder nicht.

Zusammen finden wir also 19 Typen, wenn wir den trivialen Fall, daß $A = 0$ und die "Quadrik" der ganze Raum ist, nicht mitzählen:

Rang A	Gleichung	Gebilde	Schnitt mit der Fernebene
4	$x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0$	leer	leer
4	$x_0^2 = x_1^2 + x_2^2 + x_3^2$	Ellipsoid	leer
4	$x_1^2 + x_2^2 + x_0^2 = x_3^2$	zweischaliges Hyperboloid	Ellipse
4	$x_0^2 + x_1^2 - x_2^2 - x_3^2 = 0$	einschaliges Hyperboloid	Ellipse
4	$x_1^2 + x_2^2 = x_0x_3$	elliptisches Paraboloid	Punkt
4	$x_1^2 - x_2^2 = x_0x_3$	hyperbolisches Paraboloid	Geradenpaar
3	$x_1^2 + x_2^2 + x_3^2 = 0$	Punkt	leer
3	$x_1^2 + x_2^2 = x_3^2$	Kegel	Ellipse
3	$x_0^2 + x_1^2 + x_2^2 = 0$	leer	Punkt
3	$x_1^2 + x_2^2 = x_0^2$	elliptischer Zylinder	Punkt
3	$x_1^2 - x_2^2 = x_0^2$	hyperbolischer Zylinder	Geradenpaar
3	$x_0x_1 = x_2^2$	parabolischer Zylinder	Gerade
2	$x_0^2 + x_1^2 = 0$	leer	Gerade
2	$x_0x_1 = 0$	Ebene	Ebene
2	$x_0^2 - x_1^2 = 0$	Paar paralleler Ebenen	Gerade
2	$x_2^2 + x_3^2 = 0$	Gerade	Punkt
2	$x_2^2 - x_3^2 = 0$	Paar sich schneidender Ebenen	Geradenpaar
1	$x_0^2 = 0$	leer	Ebene
1	$x_1^2 = 0$	Ebene	Gerade

10. Projektive Erzeugung der Kegelschnitte nach Steiner

In diesem Kapitel werden wir vorübergehend mit $g, h, f...$ manchmal sowohl Linearformen auf K^3 als auch die Geraden mit Gleichung $g = 0$ usw. bezeichnen, also einfach "die Gerade g" sagen statt "die Gerade mit der Gleichung $g = 0$" . Sonst wird der Text zu umständlich, und Mißverständnisse sind ausgeschlossen.
Vorbemerkung: Sei $Z \in P^2(K)$ und g und h zwei verschiedenen Geraden durch Z. Dann hat jede Gerade durch Z eine Gleichung der Form $\lambda g + \mu h = 0$ mit $\lambda, \mu \in K$, die bis auf euinen gemeinsamen Faktor bestimmt sind; denn sind f, g und h drei Geraden durch einen Punkt, so sind die drei Zeilen ihrer Koeffizienten linear abhängig.

Definition: Die Menge aller Geraden durch Z heißt das Geradenbüschel durch Z.

Wählt man aus dem Büschel $\mathfrak{B}$ zwei feste Geraden g und h aus, so entsprechen die sämtlichen Geraden aus $\mathfrak{B}$ umkehrbar eindeutig den Punkten von $P^1(K)$ vermöge

$$\mathfrak{B} \ni \{\lambda g + \mu h\} \longleftrightarrow <(\lambda, \mu)> \in P^1(K) \tag{1}$$

Diese Entsprechung hat auch eine geometrische Bedeutung: Sei l irgendeine Geade, die nicht durch Z geht, und $P = g \cap l$, $Q = h \cap l$. Man normiert g und h so, daß eine beliebig vorgegebene Gerade e durch Z die Gleichung $g + h = 0$ bekommt.

Nimmt man jetzt das Koordinatensystem mit P und Q als Ecken $(1,0)$ bzw. $(0,1)$ und $E := l \cap e$ als Einheitspunkt, so schneidet die allgemeine Büschelgerade $\lambda g + \mu h$ die Gerade l im Punkt mit den Koordinaten λ, μ; denn aus $g(P) = h(Q) = (g + h)(P + Q) = 0$ folgt $g(Q) + h(P) = 0$ und dann

$$(\lambda g + \mu h)(P + Q) = \lambda^2 g(P) + \lambda\mu(g(Q) + h(P)) + \mu^2 h(Q) = 0$$

Nachdem man nun nach Festlegung dreier Geraden g, h und $g + h$ das Büschel umkehrbar eindeutig auf die projektive Gerade abgebildet hat, ist klar, was man unter einer Projektivität zwischen zwei Büscheln verstehen soll: Ist ein zweites Büschel auf analoge Weise auf $P^1(K)$ abgebildet, so gibt jede Projektivität von $P^1(K)$ Anlaß zu einer Bijektion zwischen den Büscheln, in Formeln:
$\mathfrak{B}_1$ bestehe aus allen Geraden mit Gleichungen $\lambda g + \mu h = 0$, $(\lambda, \mu) \neq (0,0)$ und g und h fest. Ebenso bestehe $\mathfrak{B}_2$ aus allen Geraden $\rho f + \sigma k = 0$.

Definition: Eine durch

$$\begin{array}{rcrcl} \rho & = & \alpha\lambda & + & \beta\mu \\ \sigma & = & \gamma\lambda & + & \delta\mu \end{array} \quad \text{mit } \alpha\delta - \beta\gamma \neq 0$$

gegebene Bijektion zwischen den beiden Büscheln heißt eine Projektivität.

Nun sei $\mathfrak{K}$ ein Kegelschnitt, der nicht zu einem Geradenpaar entartet ist, $P \notin \mathfrak{K}$ und g die Polare von P sowie R und S die Schnittpunkte von g mit $\mathfrak{K}$. Man legt das Koordinatensystem so, daß

$$R = (100), \quad S = (010) \text{ und } P = (001)$$

In der Kegelschnittgleichung $\sum a_{ij} x_i x_j = 0$ wird dadurch $a_{00} = a_{11} = a_{02} = a_{12} = 0$, und nach Normierung erhält $\mathfrak{K}$ die Gleichung $x_o x_1 = x_2^2$.

Satz 29. *Ordnet man jeder von der Tangente an $\mathfrak{K}$ in R und von $R \vee S$ verschiedenen Geraden g des Büschels durch R die Verbindungsgerade $S \vee Y$ zu, wobei Y der Schnittpunkt $\neq R$ von g mit $\mathfrak{K}$ ist, so erhält man eine Projektivität von dem Büschel durch R auf das Büschel durch S, wenn man noch die Tangente in R auf $R \vee S$ und $R \vee S$ auf die Tangente in S abbildet.*

Beweis: Jede Gerade durch R hat eine Gleichung $a_1x_1 + a_2x_2 = 0$, a_1, a_2 nicht beide 0. Der Punkt $Y = (a_1^2, a_2^2, -a_1a_2)$ liegt auf g und $\mathfrak{K}$ und ist $\neq S$, wenn $a_1 \neq 0$. In diesem Falle ist $Y \vee S$ die Gerade

$$\begin{vmatrix} x_0 & 0 & a_1^2 \\ x_1 & 1 & a_2^2 \\ x_2 & 0 & -a_1a_2 \end{vmatrix} = -a_1a_2x_0 - a_1^2x_2 = 0, \text{ also } a_2x_0 + a_1x_2 = 0$$

Die Gerade $a_1x_1 + a_2x_2 = 0$ geht also über in $a_2x_0 + a_1x_2 = 0$, und das ist in der Tat eine Projektivität.Die Grenzfälle

$$\begin{aligned} a_1 = 0, &\quad g = R \vee S, \quad g' = S \vee P \\ a_2 = 0, &\quad g = R \vee P, \quad g' = R \vee S \end{aligned}$$

ordnen sich nachträglich ein wie angegeben.
In der Sprache der alten Geometer: Ein Kegelschnitt wird aus je zweien seiner Punkte durch die Strahlen projektiv zugeordneter Büschel gesehen.

Umkehrung: Seien zwei Büschel $\mathfrak{B}_1$ und $\mathfrak{B}_2$ gegeben und eine Projektivität von $\mathfrak{B}_1$ auf $\mathfrak{B}_2$. Seien $g, h \in \mathfrak{B}_1$ und $g', h' \in \mathfrak{B}_2$, und die Projektivität möge der Geraden $\lambda g + \mu h = 0$ aus dem ersten die Gerade $\lambda g' + \mu h' = 0$ aus dem zweiten Büschel zuordnen. Der Schnittpunkt erfüllt das System

$$\begin{array}{rcrcl} \lambda g & + & \mu h & = & 0 \\ \lambda g' & + & \mu h' & = & 0 \end{array} \tag{2}$$

Da λ, μ nicht beide 0, folgt aus (2), daß

$$\begin{vmatrix} g & h \\ g' & h' \end{vmatrix} = gh' - hg' = 0$$

Dies ist eine quadratische Gleichung für die Koordinaten des Schnittpunkts:

Satz 30. *Die Schnittpunkte projektiv zugeordneter Geraden aus zwei Büscheln liegen auf einem Kegel-- schnitt.*

Zusatz: Der durch die Projektivität π zwiscchen den Büscheln durch R und S bestimmte Kegelschnitt ist genau dann ausgeartet, wenn für die Verbindungsgerade $g = R \vee S$ gilt $\pi g = g$.
Beweis: Man spanne die Büschel auf durch g und eine andere Gerade h bzw. durch πg und πh. Ist $\pi g = g$, so ist $g \cdot \pi h - \pi g \cdot h = g \cdot (\pi h - h)$ zerfallend. Umgekehrt: Man wählt die Koordinaten so, daß $R = (100)$ und $S = (010)$. Die Gerade g hat die Gleichung $x_2 = 0$, und für h nimmt man $x_1 = 0$. Das Büschel durch S wird aufgespannt von $x_0 = 0$ und $x_2 = 0$. Ist $\pi g = \alpha x_0 + \beta x_2$ und $\pi h = \gamma x_0 + \delta x_2$, so bekommt der durch π bestimmte Kegelschnitt die Gleichung

$$x_2 \cdot (\gamma x_0 + \delta x_2) - x_1 \cdot (\alpha x_0 + \beta x_2) = -\alpha x_0 x_1 + \gamma x_0 x_2 - \beta x_1 x_2 + \delta x_2 = 0$$

Die zugehörige Koeffizientenmatrix hat die Determinante $-\frac{\alpha}{4} \cdot (\alpha\delta - \beta\gamma)$. Da $\alpha\delta - \beta\gamma \neq 0$, ist die Determinante 0 (d.h. der Kegelschnitt ausgeartet) genau dann, wenn $\alpha = 0$. Und das bedeutet genau $\pi g = g$.

Die Sätze 29 und 30 beinhalten die "projektive Erzeugung der Kegelschnitte nach Steiner".

1. Anwendung:

Satz 31. *Durch 5 verschiedene Punkte geht genau ein Kegelschnitt. Dieser ist nicht ausgeartet genau dann, wenn keine 3 der 5 Punkte auf einer Geraden liegen.*

Beweis: Der letzte Zusatz ist klar.
Seien nun zuerst 5 Punkte A, B, C, D, E gegeben. Man bilde das Büschel durch A projektiv ab auf das Büschel durch B, indem man $A \vee C$ auf $B \vee C$ und $A \vee D$ auf $B \vee D$ und $A \vee E$ suf $B \vee E$ abbildet. Nach Satz 22 und mit (1), Seite 1, gibt es genau eine Projektivität, die das leistet. Nach Satz 30 liegen die Schnittpunkte zugeordneter Geraden auf einem Kegelschnitt. Dieser enthält die gegebenen 5 Punkte. Umgekehrt: Jeder Kegelschnitt durch A, B, C, D, E besteht nach Satz 29 aus den Schnittpunkten projektiv zugeordneter Geraden aus zwei Büscheln durch zwei beliebige Punkte auf ihm, z.B. durch A und B. Diese Projektivität wird aber durch C, D, E bestimmt. Also gibt es nur einen Kegelschnitt durch die 5 Punkte.

Bemerkung: Ein Kreis kann definiert werden als Kegelschnitt, der durch die unendlich fernen Punkte $(0, 1, i)$ und $(0, 1, -i)$ geht. Er ist also durch 3 weitere Punkte bestimmt (Umkreis).

2. Anwendung:

Satz 32. *(Pascal) Ist ein Sechseck einem Kegelschnitt einbeschrieben, so liegen die 3 Schnittpunkte der Paare von Gegenseiten auf einer Geraden.*

Beweis: Die Ecken werden mit 1,....,6 numeriert. Der Seite $1 \vee 2$ gegenüber liegt die Seite $4 \vee 5$, usw. Die Behauptung ist also, daß die 3 Punkte

$$(1 \vee 2) \cap (4 \vee 5), \quad (2 \vee 3) \cap (5 \vee 6) \text{ und } (3 \vee 4) \cap (6 \vee 1)$$

auf einer Geraden liegen. Statt $1 \vee 2$ schreiben wir kurz 12. Da die Punkte auf einem Kegelschnitt liegen, sind die Geraden $14, 12, 16, 13$ aus dem Büschel durch 1 den Geraden $54, 52, 56, 53$ aus dem Büschel durch 5 projektiv zugeordnet. Daher sind ihre Schnittpunkte $4IQ3$ mit der Geraden 34 den Schnittpunkten der entsprechenden Geraden aus dem andern Büschel mit der Geraden 23 projektiv zugeordnet. Dies sind $J2P3$. Bei dieser Projektivität von 34 auf 23 bleibt 3 fest. Nach Kap.8, Seite 2 (Figur 1) ist sie eine Perspektivität. Deren Zentrum ist $4J \cap I2 \cap PQ$, d.h. $4J \cap I2$ liegt auf PQ. Da $J \in 45$, ist $4J = 45$, und da $I \in 12$, ist $2I = 12$. Also ist $R := 12 \cap 45 \in PQ$: die Punkte P, Q, R sind kollinear.

11. Resultante

Seien f und $g \in K[X]$. Wenn f und g einen nicht trivialen gemeinsamen Teiler p besitzen, etwa $f = v \cdot p$ und $g = u \cdot p$, dann ist $uf - vg = 0$. Umgekehrt kann man aus dem Bestehen einer Gleichung $uf - vg = 0$, u und $v \neq 0$, nicht unbedingt schließen, daß f und g einen nicht konstanten gemeinsamen Teiler besitzen; es ist ja z.B. stets $fg - gf = 0$. Wenn man aber zusätzlich verlangt, daß grad $u <$ grad g, dann folgt aus $g|uf$ und dem Satz über die eindeutige Primfaktorzerlegung in $K[X]$, daß g und f einen gemeinsamen Teiler besitzen müssen. Genauso genügt es, grad $v <$ grad f vorauszusetzen. Schreiben wir also

$$f(X) = a_0X^m + a_1X^{m-1} + ... + a_{m-1}X + a_0 \text{ und}$$

$$g(X) = b_0X^n + b_1X^{n-1} + ... + b_{n-1}X + b_n, \text{ wobei } a_0, b_0 \text{ nicht } \underline{\textit{beide}}\ 0$$

so ist die Existenz von Polynomen

$$u(X) = u_0X^{n-1} + ... + u_{n-1} \text{ und } v(X) = v_0X^{m-1} + ... + v_{m-1}$$

die nicht 0 sind (aber natürlich nicht notwendig vom Grad $n-1$ bzw. $m-1$) mit

$$uf - vg = 0 \tag{1}$$

gleichbedeutend damit, daß f und g nicht teilerfremd sind. (1) bedeutet für die Koeffizienten von u und v das lineare Gleichungssystem

$$\begin{array}{lllllllllll}
a_0u_0 & & & & & & = & b_0v_0 & & & \\
a_1u_0 & + & a_0u_1 & & & & = & b_1v_0 & + & b_0v_1 & \\
\vdots & & & & & & & & & & \\
a_ku_0 & + & \ldots & + & a_0u_k & & = & b_kv_0 & + & \ldots & + \quad b_0v_k \\
\vdots & & & & & & & & & & \\
 & & & & a_mu_{n-1} & = & & & & b_nv_{m-1} &
\end{array} \tag{2}$$

Dieses besitzt genau dann eine nicht triviale Lösung u_i, v_j, wenn die Determinante aus seinen Koeffizienten 0 ist. Man schreibt sie üblicherweise gestürzt auf:

Definition: Die Determinante

$$R = \begin{vmatrix}
a_0 & a_1 & \ldots & a_m & & & \\
 & a_0 & \ldots & & a_m & & \\
 & & \ddots & & & \ddots & \\
 & & & a_0 & & & a_m \\
b_0 & b_1 & \ldots & b_n & & & \\
 & b_0 & \ldots & & b_n & & \\
 & & \ddots & & & \ddots & \\
 & & & b_0 & & & b_n
\end{vmatrix} \tag{3}$$

heißt die Resultante der Polynome f und g.

Wir haben gesehen:

Satz 33. *f und g seien wie oben, a_0, b_0 nicht beide 0. Genau dann haben f und g einen nicht trivialen gemeinsamen Teiler, wenn die Resultante (3) null ist.*

Beispiel: $f(X) = X^2 + a_1X + a_2$, $g(X) = X + b_1$.

$$R = \begin{vmatrix} 1 & a_1 & a_2 \\ 1 & b_1 & 0 \\ 0 & 1 & b_1 \end{vmatrix} = b_1^2 - a_1b_1 + a_2 = f(-b_1)$$

$R = 0$ ist die zu erwartende Bedingung, daß f an der (einzigen) Nullstelle von g verschwinden muß.

Von der einschränkenden Bedingung $(a_0, b_0) \neq (0,0)$ kann man sich durch Homogenisierung befreien: Man setzt $X = \frac{X_1}{X_0}$ und

$$F(X_0, X_1) = X_0^m F(X) = a_0 X_1^m + a_1 X_0 X_1^{m-1} + ... + a_m X_0^m \text{ und } G(X_0, X_1) = b_0 X_1^n + ... + b_n X_0^n$$

Ist $f(X) = p(X) \cdot v(X)$ und $0 <$ grad $p =: k < m$, so ist $F(X_0, X_1) = X_0^k p(X) \cdot X_0^{m-k} v(X)$ in zwei homogene Faktoren k-ten bzw. $(m-k)$-ten Grades zerlegt. Umgekehrt: Ist $F(X_0, X_1) = P(X_0, X_1) \cdot V(X_0, X_1)$ und P und V homogen vom Grade k bzw. $m-k$, so ist $f(X) = F(1, X) = P(1, X)V(1, X)$ entweder eine echte Zerlegung von f, oder $P(1, X)$ oder $V(1, X)$ ist konstant. Das bedeutet $P = X_0^k$ oder $V = X_0^{m-k}$. Daher haben F und G genau dann einen gemeinsamen Faktor, wenn f und g dies tun oder wenn sie beide durch X_0 teilbar sind. Das letzte ist gleichbedeutend mit $a_0 = b_0 = 0$. In diesem Falle ist trivialerweise die Resultante 0. Für die homogenen Polynome F und G haben wir also ausnahmslos

Satz 33'. *F und G haben genau dann einen nicht trivialen gemeinsamen Teiler, wenn die Resultante R aus (3) null ist.*

Offenbar ist R ein homogenes Polynom $(m+n)$-ten Grades in den a_i, b_j. Wir brauchen mehr:

Definition: $w(a_0^{i_0} a_1^{i_1} .... a_m^{i_m} b_0^{j_0} b_1^{j_1} .... b_n^{j_n}) = 0 \cdot i_0 + 1 \cdot i_1 + ... + m \cdot i_m + 0 \cdot j_0 + 1 \cdot j_1 + ... + n \cdot j_n = \sum_{\mu=1}^{m} \mu i_\mu + \sum_{\nu=1}^{n} \nu j_\nu$ heißt das Gewicht des Monoms $a_0^{i_0} \cdot .... \cdot b_n^{j_n}$.

Definition: ein Polynom in den a_i, b_j heißt isobar, wenn alle Monome gleiches Gewicht haben.

Satz 34. *Die Resultante ist ein isobares Polynom vom Gewicht nm in den a_i, b_j.*

Beweis: Die Einträge r_{ij} in der Resultante sind

$$r_{ij} = \begin{cases} a_{j-i} & \text{wenn } 0 \leq j-i \leq m \\ 0 & \text{sonst} \end{cases} \quad \text{in den Zeilen } i = 1, ..., n$$

$$r_{ij} = \begin{cases} b_{j-i+n} & \text{wenn } 0 \leq j-i+n \leq n \\ 0 & \text{sonst} \end{cases} \quad \text{in den Zeilen } i = n+1, ..., n+m \tag{4}$$

Wir entwickeln R nach den ersten n Zeilen (Laplace). Dazu müssen wir zuerst alle Unterdeterminanten

$$\begin{vmatrix} r_{1,i_1} & \dots & r_{1,i_n} \\ \vdots & & \\ r_{n,i_1} & \dots & r_{n,i_n} \end{vmatrix} = \sum_{\sigma \in S_n} \pm r_{\sigma(1)i_1} ..... r_{\sigma(n)i_n}$$

bestimmen. Die Terme in der Summe sind 0 oder haben das Gewicht

$$(i_1 - \sigma(1)) + ... + (i_n - \sigma(n)) = i_1 + ... + i_n - 1 - 2 - .... - n$$

denn $\sigma(1), ..., \sigma(n)$ sind wieder genau die Zahlen 1,2,...,n. Dieses Gewicht hängt nicht von σ, sondern nur von $i_1, ..., i_n$ ab.
Analog haben die aus den letzten m Zeilen gebildeten Unterdeterminanten das Gewicht

$$(j_1 + n - \sigma(1)) + ... + (j_m + n - \sigma(m)) = j_1 + ... + j_m + nm - \sigma(1) - .... - \sigma(m)$$

Diesmal sind $\sigma(1), ..., \sigma(m)$ die Zahlen $n+1, ..., n+m$ in irgendeiner Reihenfolge.
Bezeichnet Δ die oberen und Δ' die unteren Unterdeterminanten, so wird nach dem Laplaceschen Entwicklungssatz

$$R = \sum \pm \Delta_{i_1 ... i_n} \Delta'_{j_1 ... j_m}$$

wobei $i_1,...i_n,j_1,...j_m$ zusammen genau alle Zahlen von 1 bis $n+m$ sind. Daher ist

$$w(\Delta_{i_1...i_n}\Delta'_{j_1...j_m}) = i_1+...+i_n-1-...-n+j_1+...+j_m+nm-(n+1)-...-(n+m)$$
$$= i_1+...+i_n+j_1+...j_m-1-...-n-(n+1)-...-(n+m)+nm = nm$$

Alle Summanden im Laplaceschen Entwicklungssatz und damit die Determinante R haben also das Gewicht nm.

Eine weitere wichtige Eigenschaft der Resultante ist, wenn $R \neq 0$, eine unmittelbare Anwendung der Cramerschen Regel. Da wir die Formel unabhängig von $R \neq 0$ haben wollen, gucken wir noch einmal genauer: $(\tilde{r}_{ij})_{i,j}$ sei die Adjunkte der Matrix $(r_{ij})_{i,j}$ aus (4). Das System (offensichtlich richtiger Gleichungen)

$$\begin{array}{rcccccccccc}
X^{n-1}f(X) & = & a_0X^{m+n-1} & + & a_1X^{m+n-2} & + & .... & + & a_mX^{n-1} & & \\
X^{n-2}f(X) & = & & & a_0X^{m+n-2} & + & & & & + & a_mX^{n-2} \\
\vdots & & & & & & \ddots & & & & \\
f(X) & = & & & & & a_0X^m & + & ... & + & a_m \\
X^{m-1}g(X) & = & b_0X^{m+n-1} & + & b_1X^{m+n-2} & + & .... & + & b_nX^{m-1} & & \\
X^{m-2}g(X) & = & & & b_0X^{m+n-2} & + & & & & + & b_nX^{m-2} \\
\vdots & & & & & & \ddots & & & & \\
g(X) & = & & & & & b_0X^n & + & ... & + & b_n
\end{array}$$

lautet kurz so:

$$X^{n-k}F(X) = \sum_{j=1}^{n+m} r_{kj}X^{n+m-j} \quad (k=1,....,n)$$

$$X^{m-k}g(X) = \sum_{j=1}^{n+m} r_{n+k,j}X^{n+m-j} \quad (k=1,....,m)$$

Man multipliziert die k-te Gleichung mit $\tilde{r}_{lk}$ und summiert über k. Auf der rechten Seite erhält man wegen der für alle Matrizen A gültigen Gleichung $\tilde{A}\cdot A = |A|\cdot\mathbf{1}$ einfach $R\cdot X^{n+m-l}$ und auf der linken

$$\sum_{k=1}^{n}\tilde{r}_{lk}X^{n-k}f(X) + \sum_{k=1}^{m}X^{m-k}\tilde{r}_{l,n+k}g(X),$$

also eine Kombination von $f(X)$ und $g(X)$. Speziell für $l=m+n$ erhält man

Satz 35. *Die Resultante R läßt sich aus f und g kombinieren:*

$$R = u(X)f(X)+v(X)g(X) \tag{5}$$

Die Koeffizienten der Polynome u und v sind Polynome in den Koeffizienten a_i und b_j von f und g.

Der letzte Zusatz folgt aus der Herleitung und ist für die Anwendung wichtig. Man kann ihn auch in folgendem Zusammenhang sehen: Aus I,Kap.12 wissen wir, daß man aus teilerfremden Polynomen f und g in $K[X]$ die 1 kombinieren kann. Haben nun zum Beispiel f und g ganzzahlige Koeffizienten, so wird man zur Kombination der 1 i.a. Polynome u und v mit rationalen Koeffizienten benötigen. Der Zusatz in Satz 35 besagt, daß man die Zahl R sogar mit $u,v \in \mathbb{Z}[X]$ kombinieren kann. Oder: die Koeffizienten von f und g seien ihrerseits Polynome in irgendwelchen anderen Variablen $Y_1,...,Y_s$. Dann ist die Resultante kraft ihrer Definition auch ein Polynom in den Y_i. Und die Koeffizienten von u und v in Satz 35 sind dann auch Polynome in den Y_i.

Ab jetzt sei $K=\mathbb{C}$. Dann haben zwei Polynome (in einer Variablen) genau dann einen nicht trivialen gemeinsamen Faktor, wenn sie eine gemeinsame Nullstelle besitzen. $F(X_0,X_1,X_2)$ und $G(X_0,X_1,X_2)$ seien homogen vom Grade m bzw. n. Man sortiert nach Potenzen von X_2

$$F(X_0,X_1,X_2) = a_0X_2^m + a_1(X_0,X_1)X_2^{m-1} + ... + a_m(X_0,X_1)$$

Dabei sind die $a_i(X_0, X_1)$ homogen von Grade i in X_0 und X_1. Man legt das Koordinatensystem so, daß der Punkt (001) nicht auf der Kurve $F = 0$ liegt. Dann ist $a_0 \neq 0$. Unter derselben Voraussetzung für G ist

$$G(X_0, X_1, X_2) = b_0 X_2^n + b_1(X_0, X_1) X_2^{n-1} + ... + b_n(X_0, X_1) \text{ mit } b_0 \neq 0$$

Von F und G, aufgefaßt als Polynome in X_2, berechnen wir die Resultante. Sie ist ein Polynom in X_0 und X_1: $R = R(X_0, X_1)$. Nach Satz 34 ist sie ein isobares Polynom vom Gewicht mn in den a_i und den b_j. Da a_i und b_j homogen vom Grade i bzw. j in X_0 und X_1 sind, folgt: $R = R(X_0, X_1)$ ist ein homogenes Polynom vom Grade mn in X_0, X_1. Angenommen, F und G haben eine gemeinsame Nullstelle (x_0, x_1, x_2). Dann haben die Polynome $f(X) = F(x_0, x_1, X)$ und $g(X) = G(x_0, x_1, X)$ in X die gemeinsame Nullstelle x_2. Aus Satz 33 folgt $R(x_0, x_1) = 0$. Umgekehrt: Zu jeder Nullstelle (x_0, x_1) von R gibt es x_2, so daß (x_0, x_1, x_2) gemeinsame Nullstelle von F und G ist.

1. Fall: $R(X_0, X_1)$ ist das Nullpolynom. Nach (5) ist $uF + vG = 0$. Dabei sind u, v Polynome mit einem Grad in X_2, der $< n$ bzw. $< m$ ist. Daher ist sicher F kein Teiler von v. Aber F teilt vG. Benutzt man, daß in $K[X_0, X_1, X_2]$ der Satz von der eindeutigen Primfaktorzerlegung gilt, so kann man daraus schließen, daß F und G einen nicht konstanten gemeinsamen Teiler besitzen, d.h. daß die Kurven $F = 0$ und $G = 0$ eine gemeinsame Teilkurve haben. Will man sich ohne jenen Satz behelfen, so benutzt man die (uns bekannte) eindeutige Primfaktorzerlegung in $L[X_2]$, wo L der Körper der rationalen Funkionen in X_0 und X_1 ist. Damit folgt: es gibt $p \in L[X_2]$, mit grad $p > 0$, oE p normiert, und mit $p|F$, $p|G$. Die Koeffizienten von p sind rationale Funktionen in X_0 und X_1, und durch Multiplikation mit dem Hauptnenner werden daraus Polynome in X_0, X_1. Facit: es gibt $h(X_0, X_1) \neq 0$ so, daß $hp =: q \in K[X_0, X_1, X_2]$ als Polynom in X_2 nicht konstant ist und den höchsten Koeffizienten h hat, und $q|Fh$, $q|Gh$ in $K[X_0, X_1, X_2]$. Da $h \neq 0$, gibt es unendlich viele (x_0, x_1) mit $h(x_0, x_1) \neq 0$. Zu jedem solchen gibt es, da $K = \mathbb{C}$, ein x_2 mit $q(x_0, x_1, x_2) = 0$. Dann ist (x_0, x_1, x_2) Nullstelle von F und von G, und wir sehen auf diese Weise wenigstens, daß F und G unendlich viele gemeinsame Nullstellen besitzen.

2. Fall: R ist nicht das Nullpolynom. R ist homogen vom Grade mn und über $\mathbb{C}$ in ein Produkt von Linearformen zerlegbar:

$$R(X_0, X_1) = \prod_{i=1}^{nm} (\alpha_i X_0 - \beta_i X_1), \quad (\alpha_i, \beta_i) \neq (0,0)$$

(dehomogenisiere und zerlege das Polynom in einer Variablen in Linearfaktoren, es ist ja $K = \mathbb{C}$, und homogenisiere wieder). Zu jeder Nullstelle (β, α) von R gehört eine (aber höchstens endlich viele) gemeinsame Nullstelle (β, α, γ) von F und G. Angenommen, zu (β, α) gehören zwei verschiedene $\gamma \neq \gamma'$. Dann liegt der Punkt (001) auf der Verbindungsgeraden der beiden gemeinsamen Nullstellen (β, α, γ) und (β, α, γ'). Da wir in dem Fall sind, wo es nur endlich viele solche gibt, können wir uns das Koordinatensystem so gelegt denken, daß keine der Verbindungsgeraden von zwei gemeinsamen Nullstellen durch den Punkt (001) geht. Dann gehört zu jeder Nullstelle der Resultante genau eine gemeinsame Nullstelle von F unf G. Da alle $(\beta_i, \alpha_i) \neq (0,0)$, sind die so gewonnenen Nullstellen von (000) verschieden und definieren einen Punkt in $P^2(\mathbb{C})$: Die Kurven $F = 0$ und $G = 0$ haben sicherlich einen gemeinsamen Punkt. Da R vom Grade mn ist, gibt es höchstens mn verschiedene Nullstellen (β_i, α_i), und zu jeder gehört genau eine gemeinsame Nullstelle von F und G. Wir haben bewiesen:

Satz 36. *(halber Satz von Bézout): Zwei Kurven $F = 0$ und $G = 0$ vom Grade m bzw. n (> 0) in $P^2(\mathbb{C})$ haben stets einen gemeinsamen Punkt. Falls sie nur endlich viele Punkte gemeinsam haben, so höchstens mn.*

Illustration: F und G seien zwei quadratische Formen, für die (001) nicht Nullstelle ist. Dann sind sie oE

$$F = X_2^2 + a_1 X_2 + a_2 \quad \text{und } G = X_2^2 + b_1 X_2 + b_2$$

wobei die a_i und b_i Formen i-ten Grades in X_0, X_1 sind. Die Resultante bezüglich X_2 ist

$$R = \begin{vmatrix} 1 & a_1 & a_2 & 0 \\ 0 & 1 & a_1 & a_2 \\ 1 & b_1 & b_2 & 0 \\ 0 & 1 & b_1 & b_2 \end{vmatrix}$$

Nach kurzer Rechnung findet man

$$R = (a_2 - b_2)^2 + (a_1 - b_1)(a_1 b_2 - a_2 b_1) \tag{1}$$

Die a_i, b_j sind als Formen in 2 Unbestimmten Produkte von Linearformen (siehe oben). Ist $R = 0$, so zeigt (1), daß $a_2 - b_2$ ein Vielfaches von $a_1 - b_1$ ist, etwa $= (a_1 - b_1) \cdot L$ mit einer Linearform L. Nach kurzer Rechnung folgt aus (1)

$$0 = (a_1 - b_1)^2 \cdot (L^2 - a_1 L + a_2)$$

Es gibt zwei Möglichkeiten: $a_1 = b_1$, woraus auch $a_2 = b_2$ und damit $F = G$ folgt. Oder $L^2 - a_1 L + a_2 = 0$. Dann findet man durch Einsetzen

$$F = X_2^2 + a_1 X_2 + a_1 L - L^2 = (X_2 + L)(X_2 - L + a_1) \text{ und } G = (X_2 + L)(X_2 - L + b_1)$$

Jetzt sieht man deutlich, daß F und G, falls $R = 0$, einen Faktor gemeinsam haben und daher die Kegelschnitte $F = 0$ und $G = 0$ mindestens eine gemeinsame Gerade. (Der Fall kann also nur eintreten, wenn sie in ein Geradenpaar entarten).

12. Anwendung auf die elementare Geometrie der kubischen Kurven.

Sei $F(X_0, X_1, X_2)$ ein homogenes Polynom 3. Grades (man sagt auch "kubische Form"). An die homogenen Koordinaten sind wir inzwischen so gewöhnt,daß wir die spitzen Klammern $< >$ bei der Bezeichnung der Punkte des projektiven Raumes von nun an weglassen.

Definition:

$$\mathfrak{C} := \{P = (x_0, x_1, x_2) \in P^2(K) \mid F(x_0, x_1, x_2) = 0\}$$

heißt eine (ebene) kubische Kurve.

Wenn F zerlegbar ist, so sind die beiden Faktoren auch homogen. Ist $F = L_1 L_2 L_3$ Produkt von 3 Linearformen, so ist $\mathfrak{C}$ Vereinigung der 3 Geraden $L_i = 0$. Ist F Produkt einer Linearform und einer nicht zerfallenden quadratischen Form, so ist $\mathfrak{C}$ Vereinigung einer Geraden und eines Kegelschnitts.

Ab jetzt wird vorausgesetzt, daß F irreduzibel ist. Man nennt dann auch die Kurve $\mathfrak{C}$ irreduzibel.

Eulersche Identität: Für jedes homogene Polynom m-ten Grades in n Unbestimmten gilt

$$\sum_{i=0}^{n} X_i \frac{\partial F}{\partial X_i} = m \cdot F$$

Beweis: Für jedes Monom $M = X_0^{k_0} .... X_n^{k_n}$ gilt

$$X_i \frac{\partial M}{\partial X_i} = k_i M$$

Wegen $\sum_{i=0}^{n} k_i =$ grad $M = m$ folgt die Behauptung durch Summation über i.

Definition: Ein Punkt $P \in \mathfrak{C}$ heißt singulär, wenn alle drei partiellen Ableitungen von F an der Stelle P null sind.

Beispiel: Für $F = X_1^3 - X_0 X_2^2$ ist (100) singulär.
Eine nicht zerfallende kubische Kurve hat nur endlich viele Singularitäten; denn wenn die quadratischen Formen $\frac{\partial F}{\partial X_i}$ unendlich viele gemeinsame Nullstellen haben, spalten sie nach Kap.11 einen gemeinsamen Linearfaktor ab oder fallen zusammen. Nach der Eulerschen Identität zerfällt F.

Wir setzen ab jetzt voraus, daß die kubische Kurve keinen singulären Punkt besitzt. Dann hat sie in jedem Punkt eine wohlbestimmte Tangente, nämlich die Gerade mit der Gleichung

$$\sum_{i=0}^{2} \frac{\partial F}{\partial X_i}(P) x_i = 0$$

Die partiellen Ableitungen $\frac{\partial F}{\partial X_i}$ werden zur Abkürzung mit F_i bezeichnet.

Definition: Der Polarkegelschnitt des Punktes $P = (p_0, p_1, p_2)$ besteht aus den Nullstellen der quadratischen Form $\sum_{i=0}^{2} p_i F_i$.

Definition: Ein Punkt P auf $\mathfrak{C}$ heißt Wendepunkt, wenn die Tangente in P keinen Punkt außer P mit der Kurve gemeinsam hat.

Satz 37. *$P \in \mathfrak{C}$ ist Wendepunkt genau dann, wenn der Polarkegelschnitt von P entartet.*

Beweis: Wir legen das Koordinatensystem so, daß $P = (100)$, die Tangente $\mathfrak{T}$ in P die Gleichung $x_2 = 0$ hat, und $(001) \notin \mathfrak{C}$. Dann schreiben wir wieder F in der Form

$$F = a_0 X_2^3 + a_1 X_2^2 + a_2 X_2 + a_3, \quad a_i \text{ homogen vom Grade } i \text{ in } X_0, X_1 \text{ und } a_0 \neq 0$$

Dann ist

$$F_i(P) = \frac{\partial a_3}{\partial X_i}(1,0) \text{ für } i = 0,1 \text{ und } F_2(P) = a_2(1,0)$$

Daß die Tangente in P die Gleichung $x_2 = 0$ haben soll, bedeutet

$$a_2(1,0) \neq 0 \text{ und } a_3 = X_1^2(c_2X_0 + c_3X_1)$$

$\mathfrak{T} \cap \mathfrak{C}$ besteht aus den Punkten mit $x_2 = 0$ und $a_3(x_0, x_1) = 0$. Dies gilt einzig und allein für P genau dann, wenn $\underline{c_2 = 0}$.

Nun betrachten wir den Polarkegelschnitt im Punkte P:

$$F_0(x_0, x_1, x_2) = 0$$

Schreibt man

$$a_1 = aX_0 + bX_1, \quad a_2 = cX_0^2 + 2dX_0X_1 + eX_1^2$$

so ist

$$F_0 = aX_2^2 + X_2(2cX_0 + 2dX_1) + c_2X_1^2$$

Die Koeffizientenmatrix dieser quadratischen Form ist

$$\begin{pmatrix} 0 & 0 & c \\ 0 & c_2 & d \\ c & d & a \end{pmatrix}$$

Wegen $c = a_2(1,0) \neq 0$ ist sie singulär, also der Kegelschnitt entartet, genau dann, wenn $\underline{c_2 = 0}$. Damit ist die Gleichwertigkeit der beiden Bedingungen in Satz 37 erkannt.

Durch mehrfache Anwendung der Eulerschen Identität schreiben wir die Gleichung des Polarkegelschnitts um:

$$(1) \qquad \sum_{i=0}^{2} p_iF_i = \sum_{i=0}^{2} p_i(\frac{1}{2}\sum_{j=0}^{2} X_jF_{ij}) = \frac{1}{2}\sum_{i,j,k=0}^{2} p_iX_jX_kF_{ijk} = \frac{1}{2}\sum_{j,k=0}^{2} F_{jk}(P)X_jX_k$$

(1) zeigt die Koeffizientenmatrix des Polarkegelschnitts.

Folgerung: Der Polarkegelschnitt von P ist genau dann entartet, wenn die Determinante

$$H = \begin{vmatrix} F_{00} & F_{01} & F_{02} \\ F_{10} & F_{11} & F_{12} \\ F_{20} & F_{21} & F_{22} \end{vmatrix}$$

an der Stelle P den Wert 0 hat.

Die F_{ij} sind Linearformen, die Determinante also ein homogenes Polynom dritten Grades in X_0, X_1, X_2.

Definition: Die kubische Kurve mit der Gleichung $H = 0$ heißt die Hesse-Kurve von $\mathfrak{C}$.

Aus Satz 37 folgt

Satz 38. *Die Wendepunkte von $\mathfrak{C}$ sind genau die Schnittpunkte von $\mathfrak{C}$ mit ihrer Hesse-Kurve.*

Nach Kap.11 (Resultante) gibt es also mindestens einen Wendepunkt.

Anleihe: Wir nehmen einmal an, daß wir zwei Wendpunkte $P \neq Q$ auf $\mathfrak{C}$ haben. Wir wollen zeigen, daß auf der Verbindungsgeraden $P \vee Q$ noch ein dritter Wendepunkt liegt: Die Tangente in P (man nennt sie Wendetangente) trifft nach Definition $\mathfrak{C}$ nur in P, der Punkt Q liegt also nicht auf ihr. Genauso liegt P nicht auf der Wendetangente durch Q. Die beiden Wendetangenten schneiden sich also in einem Punkt $S \neq P, Q$. Man legt das Koordinatensystem so, daß

$$P = (100), \quad Q = (010), \quad S = (001)$$

Wir schreiben F wieder in der Form

$$F(X_0, X_1, X_2) = a_0 X_2^3 + a_1 X_2^2 + a_2 X_2 + a_3$$

mit $a_0 \neq 0$ wegen $S \notin \mathfrak{C}$. Die Wendetangente in P hat die Gleichung $x_1 = 0$, also ist P der einzige Kurvenpunkt mit $x_1 = 0$. Das bedeutet $F(X_0, 0, X_2) = X_2^3$. Genauso ist Q der einzige Kurvenpunkt mit $x_0 = 0$. Das bedeutet $F(0, X_1, X_2) = X_2^3$. Für die Koeffizienten a_i heißt das

$$a_1(X_0, 0) = a_2(X_0, 0) = a_3(X_0, 0) = 0 \text{ und } a_1(0, X_1) = a_2(0, X_1) = a_3(0, X_1) = 0$$

Daher ist

$$a_1 = 0,\ a_2 = cX_0X_1,\ a_3 = X_0X_1(aX_0 + bX_1) \text{ mit Konstanten } a, b, c \text{ also}$$

$$F = X_2^3 + X_0X_1(aX_0 + bX_1 + cX_2) \tag{1}$$

wobei wir oE a_0 zu 1 gemacht haben.
Die Verbindungsgerade von P und Q hat die Gleichung $x_2 = 0$. Sie schneidet $\mathfrak{C}$ außer in P und Q noch in $(b, -a, 0) =:$R. Wir berechnen die Tangente an $\mathfrak{C}$ in R:

$$F_0 = 2aX_0X_1 + bX_1^2 + cX_1X_2,\ F_1 = aX_0^2 + 2bX_0X_1 + cX_0X_2,\ F_2 = 3X_2^2 + cX_0X_1$$

Hierin die Koordinaten von R eingesetzt ergibt

$$F_0(R)X_0 + F_1(R)X_1 + F_2(R)X_2 = -a^2bX_0 - ab^2X_1 - abcX_2$$

Wegen $ab \neq 0$ folgt daraus für die Tangente in R die Gleichung

$$ax_0 + bx_1 + cx_2 = 0$$

Wie man an (1) sieht, ist der einzige gemeinsame Punkt dieser Geraden mit der Kurve $\mathfrak{C}$ der Punkt R. Also ist R Wendepunkt. Damit ist bewiesen:

Satz 39. *Die Verbindungsgerade von zwei Wendepunkten auf der Kurve schneidet die Kurve in einem dritten Wendepunkt.*

Eine kleine Rechnung zeigt, daß die Hessekurve von (1) gegeben ist durch die kubische Form

$$H = 18c^2X_2^3 - 24cX_2^2(aX_0 + bX_1 + cX_2) - 24X_2(a^2X_0^2 + abX_0X_1 + b^2X_1^2) + 2c^2X_0X_1(aX_0 + bX_1 + cX_2)$$

Wegen $ab \neq 0$ ist H nicht proportional zu F, und da F irreduzibel ist, haben F und G auch keinen gemeinsamen Teiler kleineren Grades. Benutzt man (ohne Beweis), daß dann die Resultante von F und H (in bezug auf X_2) nicht das Nullpolynom (in X_0 und X_1) ist, so folgt aus Kap. 11, daß es höchstens 9 Wendepunkte gibt. In Wahrheit gibt es genau 9.

Schlußbemerkung zur Bedeutung von Satz 39: Man erklärt eine Verknüpfung zwischen den Punkten der Kurve auf folgende Weise: Man zeichnet zuerst einen Wendepunkt aus und nennt ihn $\mathfrak{O}$. Für zwei beliebige Punkte P, Q schneidet die Verbindungsgerade $P \vee Q$ (die Tangente, falls $P = Q$) die Kurve in einem wohlbestimmten dritten Punkt R (der nicht unbedingt von P und Q verschieden zu sein braucht). Die Gerade $R \vee \mathfrak{O}$ schneidet die Kurve wiederum in einem weiteren Punkt. Dieser wird mit $P \oplus Q$ bezeichnet. Man kann nun aus Schließungssätzen der algebraischen Geometrie oder mit Hilfe der Funktionentheorie beweisen, daß $\oplus$ assoziativ ist! Das ist nicht so leicht aber fundamental. Auf diese Weise bilden die Punkte auf der Kurve eine abelsche Gruppe mit $\mathfrak{O}$ als Null. Nach Konstruktion liegen 3 Punkte der Kurve genau dann auf einer Geraden, wenn in dieser Gruppe ihre Summe null ist. Die Wendepunkte sind genau die P mit $3P = P \oplus P \oplus P = 0$, die sogenannten Dreiteilungspunkte der Kurve! Satz 39 sagt: wenn $3P = 0$ und $3Q = 0$, dann ist auch $3(-P - Q) = 0$.

13. Endliche Drehgruppen im $\mathbb{R}^3$

G sei eine endliche Gruppe, bestehend aus n Drehungen im $\mathbb{R}^3$, $n > 1$. Jede Drehung hat eine Achse; diese trifft die Einheitssphäre $|x| = 1$ in zwei Punkten, den sogenannten Polen der Drehung. Sie sind die einzigen Punkte auf der Einheitssphäre, die bei der Drehung fest bleiben. Sei P die Menge aller Pole von Drehungen $\sigma \neq 1$ aus G. Wenn p Pol von σ ist, dann ist τp Pol von $\tau\sigma\tau^{-1}$; denn aus $\sigma p = p$ folgt $\tau\sigma\tau^{-1}(\tau p) = \tau p$. Deshalb vertauscht G die Pole. Die jetzt folgende Analyse beruht auf dem Studium von G als Permutationsgruppe von P.

Zu jedem $p \in P$ betrachten wir die *Bahn* von p

$$B_p = \{\sigma p \mid \sigma \in G\}$$

sowie den *Stabilisaor* von p

$$F_p = \{\sigma \in G \mid \sigma p = p\}$$

Liegt q in der Bahn von p, so ist die Bahn von q dieselbe wie die von p. Zwei Bahnen sind entweder disjunkt oder fallen zusammen. Deshalb ist P in Bahnen eingeteilt:

$$P = B_1 \cup B_2 \cup ..... \cup B_k, \quad B_i \cap B_j = \phi \text{ für } i \neq j$$

Die Anzahl der Elemente in einer Bahn nennt man auch deren Länge.

Lemma 1. *Sei p ein Pol, B seine Bahn und F sein Stabilisator. Dann gilt*

$$|F| \cdot |B| = n \quad (= |G|)$$

Beweis: B besteht aus allen σp mit $\sigma \in G$. Rein optisch wären das n Stück, aber die sind ja nicht alle verschieden. Sondern

$$\sigma p = \tau p \Leftrightarrow \tau^{-1}\sigma p = p \Leftrightarrow \tau^{-1}\sigma \in F \Leftrightarrow \sigma \in \tau F$$

Das zeigt, daß immer genau je $|F|$ verschiedene Elemente aus G denselben Punkt in der Bahn liefern, also $|B| = \frac{|G|}{|F|}$.

Das Lemma zeigt insbesondere, daß die Stabilisatoren von Polen aus derselben Bahn immer gleich viele Elemente besitzen. Für die i-te Bahn bezeichnen wir diese Anzahl mit n_i. Ist m_i die Länge von B_i, so besagt das Lemma also $m_i n_i = n$ für $i = 1, ..., k$.

Nun zählen wir auf 2 Weisen:

$$\sum_{1 \neq \sigma \in G} \; \sum_{p \in P, \sigma p = p} 1 = \sum_{1 \neq \sigma \in G} 2 = 2 \cdot (n-1)$$

Summieren wir dieselbe Summe in der anderen Reihenfolge, so kommt

$$\sum_{p \in P} \; \sum_{1 \neq \sigma \in G, \sigma p = p} 1 = \sum_{i=1}^{k} \; \sum_{p \in B_i} \; \sum_{1 \neq \sigma \in G, \sigma p = p} 1 = \sum_{i=1}^{k} m_i(n_i - 1)$$

Dies ergibt die Beziehung

$$\sum_{i=1}^{k} m_i(n_i - 1) = 2(n-1)$$

Dividiere durch $n = m_i n_i$

$$\sum_{i=1}^{k} (1 - \frac{1}{n_i}) = 2 \cdot (1 - \frac{1}{n}) \tag{1}$$

Wir ordnen die n_i so an, daß $n_1 \le n_2 \le .... \le n_k$. Natürlich sind sie alle ≥ 2.

$$n_i \ge 2 \Rightarrow 1 - \frac{1}{n_i} \ge \frac{1}{2} \Rightarrow \frac{k}{2} \le \sum_{i=1}^{k}(1 - \frac{1}{n_i}) = 2(1 - \frac{1}{n}) < 2$$

$$n_i \le n \Rightarrow 1 - \frac{1}{n_i} \le 1 - \frac{1}{n} \Rightarrow k(1 - \frac{1}{n}) \ge \sum_{i=1}^{k}(1 - \frac{1}{n_i}) = 2(1 - \frac{1}{n})$$

Aus beidem zusammen folgt $2 \le k < 4$, also $k = 2$ oder 3.

$k = 2$: Die Gleichung (1) besagt $\frac{1}{n_1} + \frac{1}{n_2} = \frac{2}{n}$. Da $n_i \le n$, ist das nur möglich für $n_1 = n_2 = n$. Es gibt 2 Bahnen, beide bestehend aus $m_i = \frac{n}{n_i} =$ einem Punkt. Es gibt nur zwei Pole, also nur eine Drehachse. G besteht aus Drehungen um eine feste Achse. Diese bilden eine zyklische Gruppe. Als ersten möglichen Typ erhalten wir also

$$G = Z_n \text{ zyklisch von der Ordnung } n$$

$k = 3$: Die Gleichung (1) wird zu

$$1 + \frac{2}{n} = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3}$$

Daraus sieht man sofort, daß die n_i nicht alle ≥ 3 sein können, das kleinste, also n_1, muß =2 sein. Für n_2 und n_3 behalten wir die Bedingung

$$\frac{1}{2} + \frac{2}{n} = \frac{1}{n_2} + \frac{1}{n_3}$$

Eine Lösung bietet sich an: $n_2 = 2$, $n = 2n_3$. Wir haben drei Bahnen, je zwei mit $\frac{n}{2}$ Polen und eine mit 2 Polen p und q. Der Stabilisator F von p besteht aus Drehungen um die Achse durch p und ist daher zyklisch. Da p und q zusammen eine Bahn bilden, müssen die Elemente aus G entweder p und q vertauschen oder beide festlassen. Es gibt $\sigma \in G$ mit $\sigma p = q$. Dann ist $G = F \cup \sigma F$, die Elemente aus F lassen p und q fest, und die Elemente aus σF vertauschen die beiden. Für alle $\tau \in \sigma F$ geht die Drehachse nicht durch p, aber τ^2 (welches ja dieselbe Drehachse wie τ hat) läßt p fest. Daraus folgt $\tau^2 = 1$. Die Gruppe G hat nun die folgende Struktur:

$$G = F \cup \sigma F,\ F \text{ zyklisch},\ \tau^2 = 1 \text{ für alle } \tau \in \sigma F$$

Eine solche Gruppe heißt Diedergruppe der Ordnung $n(= 2n_3)$. Die Ordnung ist stets gerade.

Nun suchen wir die restlichen Möglichkeiten. Wir haben $n_1 = 2 < n_2 \le n_3$. Man sieht sofort, daß n_2 nicht 4 oder größer sein kann. Also $n_2 = 3$. Wir haben die ganzzahligen Lösungen von

$$\frac{1}{6} = \frac{1}{n_3} - \frac{2}{n} \text{ mit } 3 \le n_3 \mid n \tag{2}$$

zu suchen. Wir setzen $n = tn_3$ und erhalten aus (2) die Bedingung $n_3 = 6 \cdot (1 - \frac{2}{t})$. Sie zeigt, daß t ein Teiler von 12 sein muß. Wegen $n_3 \ge 3$ kommen nur die Teiler 4, 6 und 12 in Frage. Das ergibt $n_3 = 3$, 4 oder 5 entsprechend $n = 12$, 24 bzw. 60.

n	n_1	n_2	n_3	m_1	m_2	m_3
12	2	3	3	6	4	4
24	2	3	4	12	8	6
60	2	3	5	30	20	12

$\underline{n = 12}$: Die Bahnen haben die Längen 6, 4, 4. Sei B eine Bahn mit 4 Polen. Die Drehungen aus G permutieren diese 4 Pole, und nur die Identität läßt alle 4 Pole fest, weil jede Drehung $\ne 1$ außer ihren beiden Polen keinen Punkt auf der Sphäre festläßt. Wir können also G als eine Gruppe von Permutationen von 4 Objekten, also als eine Untergruppe von S_4, auffassen. Die einzige Untergruppe der Ordnung 12

in S_4 ist die Untergruppe A_4 der geraden Permutationen. Wer es nicht glaubt, argumentiert so: Wegen $n_2 = n_3 = 3$ enthält G zwei Stabilisatoren der Ordnung 3, also mindestens 4 Elemente mit Ordnung 3. Als Permutationen sind das Dreierzyklen. G enthält also mindestens etwa $(abc), (acb) = (abc)^{-1}, (xyz)$ und (xzy) mit $z \notin \{abc\}$, d.h. in G müssen 2 Permutaionen vom Typ (abc) und (abd) vorkommen. Dann sind $(abc)(abd) = (ac)(bd)$ und $(abc)(ac)(bd)(abc)^{-1} = (ba)(cd)$ in G, und damit enthält G die Kleinsche Vierergruppe V_4. Diese erzeugt zusammen mit jedem Dreierzyklus die A_4. Also ist $G = A_4$.

$\underline{n = 24}$: Wir haben Stabilisatoren der Ordnungen 2, 3, 4 und dementsprechend Bahnen B_1, B_2, B_3 der Länge 12, 8 und 6. Mit p liegt auch $-p$ in B_2; denn die Pole in B_1 und B_3 gehören nicht zu Drehungen der Ordnung 3. Daher besteht B_2 aus 4 Paaren $(p_i, -p_i)$, $(i = 1, ..4)$, und G permutiert diese 4 Paare (d.h. die 4 Achsen durch diese 4 Polpaare). Wir wollen G mit der Gruppe S_4 aller Permutationen der 4 Achsen identifizieren. Dazu müssen wir zeigen:

$*$ kein Element außer 1 in G läßt alle 4 Achsen fest.

Beweis davon: Angenommen, es gäbe eine Drehung $\alpha \neq 1$ in G, etwa mit Pol a, so daß $\alpha p_i = \pm p_i$ für alle i. Dann ist $\alpha^2 p_i = p_i$ für 4 verschiedene i, also $\alpha^2 = 1$. Dann ist ord $\alpha \neq 3$, also $a \notin B_2$ und folglich von allen p_i verschieden. Daher kommt nur das Minuszeichen in Frage: $\alpha p_i = -p_i$ für alle i. Daraus folgt $a \perp p_i$; denn $(a, p_i) = (\alpha a, p_i) = (a, \alpha p_i) = -(a, p_i)$. Da die $\pm p_i$ eine Bahn bilden, gilt dasselbe für alle σa, $\sigma \in G$: $(\sigma a, p_i) = (a, \sigma^{-1} p_i) = (a, \pm p_j) = 0$. Da unter den p_i mindestens zwei linear unabhängige vorkommen, sind alle σa proportional: $\sigma a = \pm a$ für alle $\sigma \in G$. Nun kommt endlich der Widerspruch: Sei $\sigma = \pi_1$ eine Drehung der Ordnung 3 mit Pol p_1. Wegen $p_1 \neq \pm a$ ist $\pi_1 a \neq a$, also nun $= -a$, und $a = \pi_1^3 a = (-1)^3 a = -a$.
Damit ist $*$ bewiesen, und wir können G als Untergruppe der symmetrischen Gruppe S_4 betrachten. Da G gerade 24=4! Elemente hat, ist $G = S_4$.

$\underline{n = 60}$: Die 3 Bahnen haben die Länge 30, 20 und 12, die zugehörigen Stabilisatoren die Ordnungen 2, 3 und 5. Sei B die Bahn der Länge 30 und $a \in B$. Der Stabilisator F_a von a hat 2 Elemente, besteht also aus der Identität und einer Drehung α um 180^o (um die Achse durch a).Der Stabilisator von $-a$ ist derselbe wie der von a, deshalb ist auch $-a \in B$ (die Stabilisatoren der Pole in den anderen Bahnen haben Ordnung 3 oder 5 und nicht 2). Daher gibt es $\beta \in G$ mit $\beta a = -a$. Dann haben α und β sicher verschiedene Achsen. Ist b Pol von β, so läßt β^2 sowohl a als auch $b \neq \pm a$ fest und ist deshalb =1. $\beta\alpha\beta^{-1}$ ist eine 180^o-Drehung um die Achse $< \beta a > = < -a >$, also $= \alpha$. Dann ist aber auch $\alpha\beta\alpha^{-1} = \beta$, d.h. $\alpha b = \pm b$. Plus fällt aus; d.h. es gilt nicht nur $\beta a = -a$, sondern auch $\alpha b = -b$.

Die von α und β erzeugte Untergruppe $H \subset G$ ist beschrieben durch die Relationen

$$\alpha^2 = 1,\ \beta^2 = 1,\ \alpha\beta = \beta\alpha$$

Sie ist also die Kleinsche Vierergruppe, bestehend aus $1, \alpha, \beta$ und $\alpha\beta$.

Lemma 1. *Jede Drehung $\sigma \in G$, die mit α, β oder $\alpha\beta$ vertauschbar ist, gehört zu H.*

Beweis: Sei c Pol von $\alpha\beta$. Wie oben folgt $\alpha c = -c = \beta c$. Sei nun $\sigma \in G$.

$$\sigma\alpha\sigma^{-1} = \alpha \Rightarrow \sigma a = \pm a \Rightarrow \begin{cases} \sigma a = a \Rightarrow \sigma = 1 \text{ oder } \sigma = \alpha \\ \text{oder } \sigma a = \beta a \Rightarrow \beta\sigma = 1 \text{ oder } \alpha \end{cases}$$

In allen Fällen ist $\sigma \in H$. Da $\alpha b = -b$ und $\alpha c = -c$ ist, kann man denselben Schluß mit β und $\alpha\beta$ statt α machen.

Da a und b zur selben Bahn gehören, gibt es $\gamma \in G$ mit $\gamma a = b$. Dann ist $\gamma\alpha\gamma^{-1} = \beta$. Die Drehung $\delta := \gamma\beta\gamma^{-1}$ ist mit $\gamma\alpha\gamma^{-1}(= \beta)$ vertauschbar; nach dem Lemma 1 ist sie in H. Nach demselben Schluß ist $\gamma\delta\gamma^{-1} \in H$. Auf diese Weise permutiert γ die 3 Elemente α, β und $\alpha\beta$ und läßt dabei, weil $\notin H$, keines der 3 fest. D.h. γ permutiert die 3 zyklisch:

$$\gamma\alpha\gamma^{-1} = \beta,\ \gamma\beta\gamma^{-1} = \alpha\beta,\ \gamma\alpha\beta\gamma^{-1} = \alpha$$

Die Elemente α, β, γ erzeugen eine Untergruppe K der Ordnung 12 von G. An ihrer Erzeugung durch H und γ sieht man, daß sie isomorph zu A_4 ist.

Die Stabilisatoren aus der dritten Bahn haben Ordnung 5. Sie werden erzeugt von Drehungen der Ordnung 5. Sei σ eine solche. Die Nebenklassen

$$K,\ \sigma K,\ \sigma^2 K,\ \sigma^3 K,\ \sigma^4 K$$

sind disjunkt, und ihre Vereinigung ist G, weil sie zusammen $5 \cdot 12 = 60$ Elemente haben. Jede Nebenklasse τK für irgendein $\tau \in G$ ist eine von diesen 5; denn τ ist ja selbst ein $\sigma^j\kappa$ mit $\kappa \in K$, und damit ist $\tau K = \sigma^j \kappa K = \sigma^j K$. Also permutiert G die 5 Nebenklassen vermöge $\sigma^j K \mapsto \tau\sigma^j K$. Anders ausgedrückt: Man kann jedem Element $\tau \in G$ eine Permutaion $\pi = \pi_\tau$ der 5 Ziffern 0,1,2,3,4 zuordnen durch

$$\tau\sigma^j K = \sigma^{\pi_\tau(j)} K \quad \text{für } j = 0, ..., 4$$

Lemma 2. *Es gilt*
(a) $\pi_\tau \pi_\rho = \pi_{\tau\rho}$
(b) Die Abbildung $\tau \mapsto \pi_\tau$ *von* G *nach* S_5 *ist injektiv.*

Beweis: (a) rechnet man einfach nach. Zu (b): $\pi_\tau = id$ bedeutet $\tau\sigma^j K = \sigma^j K$ für alle j. Das wiederum bedeutet $\tau \in \sigma^j K \sigma^{-j}$ für alle j. Insbesondere ist $\tau \in K$. Die zu A_4 isomorphe Untergruppe K enthält nur Elemente der Ordnung 2 und 3.

1. $ord\,\tau = 2$: Alle Elemente von K mit Ordnung 2 liegen in H, und in H gibt es drei. Die $\sigma^j\tau\sigma^{-j}$ für $0 \le j \le 4$ sind also nicht alle verschieden: es gibt ein σ^r mit $0 < r < 4$, welches mit τ vertauschbar ist. Nach Lemma 1 müßte $\sigma^r \in H$ sein. Das geht nicht, weil σ^r Ordnung 5 hat.
2. $ord\tau = 3$: Nach Annahme sollen alle 5 Elemente $\sigma^i\tau\sigma^{-i}$ in K liegen. Dann liegen auch ihre Quadrate in K. Da K nur 8 Elemente der Ordnung 3 enthält (K ist isomorph zu A_4), können diese 10 nicht alle verschieden sein: Es gibt 2 Paare (i,k) und (j,l) mit

   $$\sigma^i\tau^k\sigma^{-i} = \sigma^j\tau^l\sigma^{-j} \text{ mit } 0 \le i,j < 5 \text{ und } 1 \le k,l \le 2 \text{ und } (i,k) \ne (j,l)$$

   Die Gleichung mit $i = j$ impliziert natürlich $k = l$. Also gibt es ein nicht durch 5 teilbares r und ein $k \in \{1,2\}$ mit

   $$\sigma^r\tau\sigma^{-r} = \tau^k$$

   Für die Pole $t, -t$ von τ gilt dann $\sigma^r t = \pm t$, also $\sigma^{2r} t = t$. Dann wäre t Pol sowohl von σ^{2r}, welches Ordnung 5 hat, als auch von τ, welches Ordnung 3 hat. Das ist unmöglich.

Nach Lemma 2 kann man nun G als Untergruppe der S_5 auffassen. Wie oben: benutzt man, daß die einzige Untergruppe von S_5 mit 60 Elementen die A_5 ist (das ist die sog. alternierende Gruppe, bestehend aus allen geraden Permutationen), so weiß man jetzt $G = A_5$. In der Tat ist dies richtig für alle n. Wer es noch nicht weiß, kann sich folgendes überlegen: Wäre $G \ne A_5$, so wäre das Signum der Permutation eine multiplikative Funktion ϵ auf G mit Werten in $\{\pm 1\}$, die den Wert -1 annimmt. Wegen $\sigma^5 = 1$ und $\gamma^3 = 1$ ist $\epsilon(\sigma) = \epsilon(\gamma) = 1$. Ferner ist $\epsilon(\alpha) = \epsilon(\gamma\alpha\gamma^{-1}) = \epsilon(\beta) = \epsilon(\gamma\beta\gamma^{-1}) = \epsilon(\alpha\beta) = \epsilon(\alpha) \cdot \epsilon(\beta)$. Daraus folgt $\epsilon(\alpha) = \epsilon(\beta) = 1$, und da α, β, γ und σ die Gruppe G erzeugen, ist doch $\epsilon = 1$ auf ganz G.

Damit haben wir bewiesen: Als endliche Drehgruppen im $\mathbb{R}^3$ kommen höchstens in Frage:

* Zyklische Gruppen der Ordnung n für jedes $n = 2, 3, 4....$
* Diedergruppen der Ordnung $2n$, $n \ge 2$
* Die alternierende Gruppe A_4

* Die symmetrische Gruppe S_4
* Die alternierende Gruppe A_5

Nun wollen wir alle diese auch tatsächlich realisieren:

1. Die Drehungen σ_k um eine feste Achse um die Winkel $\frac{2\pi}{n} \cdot k$ für $k = 0, 1, ..., n-1$ bilden eine zyklische Gruppe der Ordnung n.

2. Zu 1. nehme man eine 180^o-Drehung τ um eine zur Achse der σ_k senkrechte Achse hinzu. τ bewirkt in der zur Achse der σ_i senkrechten Ebene eine Spiegelung, und $\tau\sigma_k\tau = \sigma_k^{-1}$. Die von τ und den σ_k erzeugte Gruppe besteht aus den $2n$ Elementen σ_k und $\tau\sigma_k$. Sie ist die Diedergruppe der Ornung $2n$.

3. Ein Tetraeder gestattet Drehungen
   1. um 4 Achsen durch die Ecken und gegenüberliegenden Seitenmitten um 120^o bzw. 240^o
   2. um 3 Achsen durch gegenüberliegende Kantenmitten um 180^o.

Dabei erfahren die 4 Ecken des Tetraeders die Permutationen
   1. alle Dreierzyklen
   2. die Permutationen aus der Kleinschen Vierergruppe

Daher bilden die Drehungen des Tetraeders eine A_4.

4. Ein Würfel gestattet Drehungen
   1. um 3 Achsen durch gegenüberliegende Seitenmitten um 90^o, 180^o, und 270^o
   2. um 6 Achsen durch gegenüberliegende Kantenmiten um 180^o
   3. um die 4 Raumdiagonalen durch gegenüberliegende Ecken um 120^o und 240^o Zusammen mit der Identität erhalten wir

$$1 + 3 \cdot 3 + 6 + 4 \cdot 2 = 24 \text{ Drehungen}$$

   Bei jeder Drehung werden die 4 Raumdiagonalen permutiert, und keine Drehung $\neq 1$ läßt sie alle 4 fest. Also kann man G als Untergruppe der S_4 betrachten, und da G schon $24 = 4!$ Elemente hat, ist $G = S_4$.

Ein Ikosaeder hat 20 Seiten (lauter gleichseitige Dreiecke), 30 Kanten und 12 Ecken. Es gestattet Drehungen
   1. um 10 Achsen durch gegenüberliegende Seitenmitten um 120^o und 240^o
   2. um 15 Achsen durch gegenüberliegende Kantenmitten um 180^o
   3. um 6 Achsen durch gegenüberliegende Ecken um die Winkel $\frac{2\pi}{n} \cdot k$ mit $k = 1, 2, 3, 4$

Zusammen mit der Identität sind das

$$1 + 10 \cdot 2 + 15 + 6 \cdot 4 = 60 \text{ Drehungen}$$

Aus dem vorher Bewiesenen wissen wir nun bereits, daß diese Drehgruppe isomorph zur A_5 sein muß (sie hat mindestens 60 Elemente und andere Gruppen außer zyklischen und Diedergruppen mit so vielen Drehungen gibt es nicht). Nun wollen wir auch 5 Objekte finden, die von G permutiert werden! Man nehme ein Paar gegenüberliegender Kanten und stelle das Ikosaeder so (mit Mittelpunkt im Nullpunkt des Koordinatensystems) auf, daß sie in die x, y-Ebene fallen und parallel zur x-Achse sind. Dann gibt es ein weiteres solches Paar, welches parallel zur y-Achse und noch eines, welches parallel zur z-Achse ist. Die Mittelpunkte dieser Kanten bilden die Ecken eines Oktaeders. Nun hat das Ikosaeder 30 Kanten, und je 6 von ihnen bilden drei zueinander senkrechte Paare paralleler Kanten. Man kann dem Ikosaeder auf diese Weise 5 Oktaeder einbeschreiben. Wenn man das Ikosaeder betrachtet, sieht man, daß alle diese Oktaeder aus einem hervorgehen durch die Drehungen $\sigma, \sigma^2, ..., \sigma^5 = id$ um eine Achse vom Typ 3 oben. Es gibt keine Drehung $\neq 1$, die alle 5 Oktaeder in sich abbildet. Wir haben tatsächlich G als Permutationsgruppe auf 5 Objekten realisiert.