

## Invariantentheorie

### Vorlesung 1

Wir beginnen mit einigen typischen Beispielen zur Invariantentheorie.

#### Dreieckskongruenzen

BEISPIEL 1.1. Wir betrachten Dreiecke im  $\mathbb{R}^2$ . Die Ebene  $\mathbb{R}^2$  sei mit dem Standardskalarprodukt versehen, so dass wir Längen, Winkel und Flächeninhalte zur Verfügung haben. Eine *affine Isometrie* (oder eine *Kongruenz*) der Ebene ist eine Abbildung

$$\mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

der Form

$$P \mapsto AP + v,$$

wobei  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  eine lineare Isometrie ist, also durch eine orthogonale Matrix beschrieben wird, und wobei  $v \in \mathbb{R}^2$  ein (Verschiebungs)-Vektor ist. In Koordinaten liegt also die Abbildung

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$$

vor. Orthogonal bedeutet, dass die Spaltenvektoren eine Orthonormalbasis bilden. Im zweidimensionalen bedeutet dies, dass entweder  $A$  eine Drehmatrix

$$A = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$$

oder eine *gespiegelte Drehmatrix* (oder *uneigentliche Drehmatrix*)

$$A = \begin{pmatrix} \cos \alpha & \sin \alpha \\ \sin \alpha & -\cos \alpha \end{pmatrix}$$

ist. Zu den ebenen Kongruenzen gehören insbesondere *Verschiebungen*, *Achsenpiegelungen*, *Punktspiegelungen* und *Drehungen*, die auch aus der Schule bekannt sind. Diese Abbildungen erhalten allesamt das Skalarprodukt, Längen, Winkel (aber ohne die Orientierung) und Flächeninhalte.

Unter einem *Dreieck* in der Ebene verstehen wir einfach ein Tupel aus drei Punkten der Ebene, also ein geordnetes Tripel  $(P_1, P_2, P_3)$  mit  $P_i = (x_i, y_i)$ . Die Dreieckspunkte sind also geordnet und wir erlauben auch *degenerierte* (oder *ausgeartete*) Dreiecke, beispielsweise können die Punkte *kolinear* sein oder auch zusammenfallen. Eine Kongruenz  $g$  überführt ein Dreieck  $\Delta$  in ein neues Dreieck, und zwar ist das Bilddreieck durch

$$g(\Delta) = g(P_1, P_2, P_3) = (g(P_1), g(P_2), g(P_3))$$

definiert. Zwei Dreiecke  $\Delta_1$  und  $\Delta_2$  heißen *geordnet kongruent*, wenn es eine Kongruenz gibt, die das eine Dreieck in das andere überführt (bei einer nicht geordneten Kongruenz kann man noch die Nummerierung der Punkte ändern). Die (geordnete) Kongruenz von Dreiecken ist eine Äquivalenzrelation. Unter einer Kongruenz bleiben diejenigen Größen eines Dreiecks erhalten, die generell unter einer Kongruenz erhalten bleiben, also der Flächeninhalt, die Länge der Seiten, und daraus abgeleitete Größen wie der Umfang des Dreiecks, die Länge der kleinsten Seite, usw., dagegen werden andere Größen des Dreiecks verändert, seine Lage im Raum, die Koordinaten seiner Punkte.

Da ein Dreieck durch die Koordinaten seiner Eckpunkte vollständig beschrieben wird, müssen alle dem Dreieck zugeordneten Größen als eine Funktion der sechs Koordinaten  $(x_1, y_1, x_2, y_2, x_3, y_3)$  ausdrückbar sein. Eine Größe ist also einfach eine zunächst beliebige Funktion

$$\mu: \mathbb{R}^6 \longrightarrow \mathbb{R}, \Delta \longmapsto \mu(\Delta),$$

(man kann auch andere Wertebereiche zulassen). Man sagt, dass eine solche Funktion *nur von der Kongruenzklasse abhängt* oder *invariant* unter der Kongruenz ist, wenn für jedes Dreieck  $\Delta \in \mathbb{R}^6$  und jede Kongruenz  $g$  die Gleichheit

$$\mu(\Delta) = \mu(g(\Delta))$$

gilt. Eine solche invariante Funktion nennt man auch eine *innere Größe* des Dreiecks, da sie nicht von der Lage des Dreiecks in der Ebene abhängt (wobei man sowohl die invariante Funktion als auch den Wert einer solchen an einem bestimmten Dreieck als innere Größe bezeichnet).

Der Flächeninhalt (vergleiche Aufgabe 1.1; man verschiebe den Eckpunkt  $(x_3, y_3)$  des Dreiecks in den Nullpunkt und betrachte dann die daran anliegenden Seiten als Vektoren) des Dreiecks wird durch

$$\begin{aligned} \mu(\Delta) &= \frac{1}{2} \left| \det \begin{pmatrix} x_1 - x_3 & x_2 - x_3 \\ y_1 - y_3 & y_2 - y_3 \end{pmatrix} \right| \\ &= \frac{1}{2} |(x_1 - x_3)(y_2 - y_3) - (y_1 - y_3)(x_2 - x_3)| \\ &= \frac{1}{2} |x_1 y_2 - x_2 y_1 - x_1 y_3 + x_3 y_1 - x_3 y_2 + x_2 y_3| \end{aligned}$$

gegeben. Aufgrund der inhaltlichen Interpretation als Flächeninhalt eines Dreiecks muss es sich um eine innere Größe handeln. Dies lässt sich aber auch numerisch überprüfen. Um den Rechenaufwand zu minimieren, sind folgende einfache Vorüberlegungen sinnvoll:

- Wenn eine Funktion  $\mu$  invariant ist, so ist auch jede Funktion invariant, die nur von dieser Funktion abhängt; wenn also der Ausdruck  $\nu(\Delta) = x_1 y_2 - x_2 y_1 - x_1 y_3 + x_3 y_1 - x_3 y_2 + x_2 y_3$  unter einer bestimmten Kongruenz invariant ist, so ist insbesondere auch der Betrag davon unter dieser Kongruenz invariant.

• Da man jede Kongruenz als Hintereinanderschaltung von besonders einfachen Kongruenzen schreiben kann, nämlich von Verschiebungen, Drehungen und eventuell einer Spiegelung an der  $x$ -Achse, genügt es, die Invarianz unter diesen erzeugenden Kongruenzen zu zeigen.

Betrachten wir also diese speziellen Kongruenzen. Bei einer Verschiebung  $g$  um den Vektor  $(w, z)$  ist

$$\begin{aligned}\nu(g(\Delta)) &= \nu(x_1 + w, y_1 + z, x_2 + w, y_2 + z, x_3 + w, y_3 + z) \\ &= \det \begin{pmatrix} x_1 - w - (x_3 - w) & x_2 - w - (x_3 - w) \\ y_1 - z - (y_3 - z) & y_2 - z - (y_3 - z) \end{pmatrix} \\ &= \det \begin{pmatrix} x_1 - x_3 & x_2 - x_3 \\ y_1 - y_3 & y_2 - y_3 \end{pmatrix} \\ &= \nu(\Delta).\end{aligned}$$

Für eine Drehung  $D$  um den Winkel  $\alpha$  und einen Vektor  $v \in V$  und die zugehörige Verschiebung  $V_v$  gilt  $V_{-D(v)} \circ D \circ V_v = D$ . Da wir die Invarianz unter einer Verschiebung schon bewiesen haben, können wir annehmen, dass der dritte Eckpunkt der Nullpunkt ist, dass also  $(x_3, y_3) = (0, 0)$  ist. Damit ist aufgrund des Determinantenmultiplikationssatzes

$$\begin{aligned}\nu(D(\Delta)) &= \det \left( \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} \right) \\ &= \det \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \det \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} \\ &= \det \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} \\ &= \nu(\Delta).\end{aligned}$$

Für die Spiegelung  $S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  ist schließlich

$$\nu(S(\Delta)) = \nu \left( \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x_1 - x_3 & x_2 - x_3 \\ y_1 - y_3 & y_2 - y_3 \end{pmatrix} \right) = -\nu(\Delta).$$

Die Funktion  $\nu$  ist also nicht invariant unter der Spiegelung, wohl aber ihr Betrag oder das Quadrat davon (letzteres gilt über jedem Körper). Die Funktion  $\nu$  (oder  $\nu^2$  oder  $|\nu|$ ) enthält auch die Information, ob das Dreieck ausgeartet ist oder nicht, nämlich genau dann, wenn  $\nu$  den Wert 0 annimmt.

Betrachten wir die Seitenlängen. Da wir mit geordneten Dreiecken arbeiten, sind (für  $i \neq j$ ) die Seitenlängen

$$L_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$$

invariant unter Kongruenzen (sie sind nicht invariant unter Umnummerierungen, da diese ja beispielsweise  $L_{12}$  in  $L_{13}$  überführen). Der Ausdruck  $U = L_{12} + L_{13} + L_{23}$ , also der Umfang, ist invariant unter den Kongruenzen, aber auch unter Umnummerierungen.

Die Invarianz der Seitenlängen ist ein Spezialfall der Invarianz der Skalarprodukte. Isometrien erhalten das Skalarprodukt, dies ist ihre definierende Eigenschaft. Zu  $i \neq j$  (und  $k$  die dritte Zahl aus  $\{1, 2, 3\}$ ) sei

$$\begin{aligned} S_{ij} &:= \left\langle \begin{pmatrix} x_i - x_k \\ y_i - y_k \end{pmatrix}, \begin{pmatrix} x_j - x_k \\ y_j - y_k \end{pmatrix} \right\rangle \\ &= (x_i - x_k)(x_j - x_k) + (y_i - y_k)(y_j - y_k) \\ &= x_i x_j - x_i x_k - x_j x_k + x_k^2 + y_i y_j - y_i y_k - y_j y_k + y_k^2. \end{aligned}$$

Das ist also das Skalarprodukt der beiden vektoriellen Seiten, die am Eckpunkt  $P_k$  anliegen. Diese Funktionen sind invariant unter geordneten Kongruenzen. Die Invarianz der Winkel (an einer bestimmten Ecke) zwischen zwei Dreiecksseiten folgt direkt aus der Invarianz der Skalarprodukte der zwei Seiten.

Es gibt eine Reihe von elementargeometrischen Sätzen, die besagen, dass ein Dreieck bis auf Kongruenz durch die Angabe gewisser Größen bestimmt ist, z.B. durch die Angabe der drei Seitenlängen oder die Angabe eines Winkels und der Längen der beiden anliegenden Seiten. Betrachten wir die drei Längen als Abbildung (die wir die *Längenabbildung* nennen)

$$L: \mathbb{R}^6 \longrightarrow \mathbb{R}^3, \Delta \longmapsto (L_{12}(\Delta), L_{13}(\Delta), L_{23}(\Delta)).$$

Zwei Dreiecke sind genau dann kongruent, wenn ihre Werte unter der Abbildung  $L$  übereinstimmen. Die Faser der Abbildung über einem Längentupel  $\ell_1, \ell_2, \ell_3$  besteht aus allen geordneten Dreiecken, deren Seitenlängen gleich  $\ell_i$  sind. Die Abbildung ist nicht surjektiv, da das Längentupel eines Dreiecks in  $\mathbb{R}_{\geq 0}^3$  liegt und die Dreiecksungleichung  $\ell_1 \leq \ell_2 + \ell_3$  (und Permutationen davon) erfüllen muss (über einem algebraisch abgeschlossenen Körper ist die Abbildung aber surjektiv). Wenn  $\mu: \mathbb{R}^6 \rightarrow \mathbb{R}$  irgendeine invariante Funktion ist, so ist diese auf den Kongruenzklassen, also den Fasern von  $L$ , konstant, und somit gibt es eine eindeutig bestimmte Funktion  $\tilde{\mu}: \mathbb{R}^3 \rightarrow \mathbb{R}$  mit  $\mu = \tilde{\mu} \circ L$ . In einem gewissen Sinn beschreiben die  $L_{ij}$  sämtliche invarianten Funktionen.

## Symmetrische Polynome

DEFINITION 1.2. Es sei  $K$  ein Körper. Ein Polynom  $f \in K[X_1, \dots, X_n]$  heißt *symmetrisch*, wenn für jede Permutation  $\sigma \in S_n$  die Gleichheit

$$f = f^\sigma$$

besteht, wobei  $f^\sigma$  aus  $f$  entsteht, indem man überall in  $f$  die Variable  $X_i$  durch  $X_{\sigma(i)}$  ersetzt.<sup>1</sup>

<sup>1</sup>Wenn man die durch eine Permutation induzierte lineare Abbildung

$$K^n \longrightarrow K^n, e_i \longmapsto e_{\sigma(i)},$$

betrachtet, so ist es natürlicher, die  $i$ -te Variable  $X_i$ , die ja die  $i$ -te Projektion von  $K^n$  auf  $K$  bezeichnet, auf  $X_i \circ \sigma$ , also auf  $X_{\sigma^{-1}(i)}$ , abzubilden.

BEISPIEL 1.3. Bei  $n = 1$  sind alle Polynome symmetrisch, da dort allein die Identität vorliegt. Bei  $n = 2$  sind die Konstanten und beispielsweise  $x + y, xy, 5 + x + y, 3x + 3y + x^2y^2$  symmetrische Polynome. Bei  $n = 3$  sind  $x + y + z, xy + xz + yz, xyz, x^4 + y^4 + z^4$  typische Beispiele.

Die Summe und das Produkt von symmetrischen Polynomen ist wieder symmetrisch, daher bilden die symmetrischen Polynome einen Unterring des Polynomrings.

DEFINITION 1.4. Das  $i$ -te *elementarsymmetrische Polynom* in  $n$  Variablen ist das Polynom (mit  $i = 1, \dots, n$ )

$$E_i := \sum_{1 \leq k_1 < \dots < k_i \leq n} X_{k_1} \cdots X_{k_i}.$$

Die elementarsymmetrischen Polynome treten in folgender Situation auf.

BEMERKUNG 1.5. Wir betrachten das Produkt

$$(T + X_1) \cdots (T + X_n)$$

in  $K[X_1, \dots, X_n, T] = K[X_1, \dots, X_n][T]$ . Wenn man dieses Produkt ausmultipliziert, so erhält man ein (normiertes) Polynom in  $T$  vom Grad  $n$ , wobei die Koeffizienten selbst Polynome aus  $K[X_1, \dots, X_n]$  sind. Da man beim Ausmultiplizieren alles mit allem multiplizieren muss, gilt

$$(T + X_1) \cdots (T + X_n) = T^n + E_1 T^{n-1} + \dots + E_n T^0,$$

wobei  $E_i$  gerade das  $i$ -te elementarsymmetrische Polynom bezeichnet. Ein Polynom in  $T$  mit den Nullstellen  $-X_i$  besitzt also die elementarsymmetrischen Polynome als Koeffizienten.

Mit Hilfe der elementarsymmetrischen Polynome kann man nun einfach alle symmetrischen Polynome in eindeutiger Form schreiben. Dies ist der Inhalt des *Hauptsatzes über symmetrische Polynome*. Für den Beweis benötigen wir den Begriff der *gradlexikographischen Ordnung*.

DEFINITION 1.6. Es sei  $K$  ein Körper und  $K[X_1, \dots, X_n]$  der Polynomring über  $K$ . Die *gradlexikographische Ordnung* auf der Menge der Monome ist durch

$$X_1^{a_1} \cdots X_n^{a_n} \prec X_1^{b_1} \cdots X_n^{b_n},$$

falls der Grad von  $X_1^{a_1} \cdots X_n^{a_n}$ , (also  $\sum_{i=1}^n a_i$ ), kleiner als der Grad von  $X_1^{b_1} \cdots X_n^{b_n}$  ist, oder, bei gleichem Grad, wenn  $a_1 = b_1, \dots, a_k = b_k$ , aber  $a_{k+1} < b_{k+1}$  ist, gegeben.

Man verwendet also die Ordnung auf der Variablenmenge. Man vergleicht zwei Monome  $f$  und  $g$ , indem man zuerst den Grad miteinander vergleicht. Stimmt dieser überein, so vergleicht man die Exponenten der ersten Variable

der beiden Monome miteinander (man vergleicht also den „Anfangsbuchstaben“). Wenn es hier einen Größenunterschied gibt, so ist die Sache entschieden. Andernfalls schaut man sich den Exponenten der zweiten Variablen an, und so weiter. Dies führt zu einer totalen Ordnung auf der Menge der Monome. Zu einem Monom gibt es jeweils nur endlich viele Monome, die bezüglich dieser Ordnung kleiner sind. Daher kann man über diese Ordnung Induktion führen.

Zu einem Polynom  $f$  nennt man das Monom aus  $f$  (mit einem Koeffizienten  $\neq 0$ ) mit dem größten Exponententupel in der gradlexikographischen Ordnung das *Leitmonom* von  $f$ .

**SATZ 1.7.** *Jedes symmetrische Polynom  $F \in K[X_1, \dots, X_n]$  lässt sich eindeutig als Polynom in den elementarsymmetrischen Polynomen schreiben. D.h. es ist*

$$F = \sum_{\nu} a_{\nu} E^{\nu}$$

mit eindeutig bestimmten Koeffizienten  $a_{\nu} \in K$ .

*Beweis.* Wir führen Induktion über die gradlexikographische Ordnung. Zur Existenz. Es sei  $F$  ein symmetrisches Polynom. Es sei  $X_1^{a_1} \cdots X_n^{a_n}$  das Leitmonom von  $F$  (mit dem Koeffizienten  $c \neq 0$ ). Es ist  $a_{i+1} \leq a_i$  für alle  $i$ . Andernfalls nämlich betrachtet man die Permutation, die  $X_{i+1}$  und  $X_i$  vertauscht. Das resultierende Monom muss wegen der Symmetrie ebenfalls in  $F$  vorkommen, wäre aber größer in der gradlexikographischen Ordnung.

Wir betrachten das Polynom

$$G = F - c E_1^{a_1 - a_2} E_2^{a_2 - a_3} \cdots E_{n-1}^{a_{n-1} - a_n} E_n^{a_n}.$$

Dabei treten rechts die elementarsymmetrischen Polynome mit nichtnegativen Exponenten auf. Das Polynom rechts enthält ebenfalls  $X_1^{a_1} \cdots X_n^{a_n}$  als Leitmonom: Hierzu muss man sich die Monome in  $E_i$  klar machen. Das Leitmonom von  $E_i$  ist  $X_1 \cdots X_i$  und das Leitmonom von  $E_i^k$  ist  $(X_1 \cdots X_i)^k$  (das Leitmonom ist multiplikativ, siehe Aufgabe 1.10). Daher hat das Polynom rechts das Leitmonom

$$\begin{aligned} X_1^{a_1 - a_2} \cdot (X_1 X_2)^{a_2 - a_3} \cdots (X_1 \cdots X_{n-1})^{a_{n-1} - a_n} \cdot (X_1 \cdots X_n)^{a_n} \\ = X_1^{a_1} X_2^{a_2} \cdots X_{n-1}^{a_{n-1}} X_n^{a_n}. \end{aligned}$$

In der Differenz  $G$  verschwindet also dieses Monom, d.h.  $G$  hat einen kleineren Grad in der gradlexikographischen Ordnung. Da  $G$  ebenfalls symmetrisch ist, liefert die Induktionsvoraussetzung die Behauptung. Zur Eindeutigkeit. Wir zeigen, dass die elementarsymmetrischen Polynome algebraisch unabhängig sind. Sei also

$$H(E_1, \dots, E_n) = 0,$$

wobei  $H \neq 0$  ein Polynom in den  $n$  Variablen  $Y_1, \dots, Y_n$  sei. Wir schreiben  $H$  als Summe von Monomen der Form

$$Y_1^{a_1 - a_2} Y_2^{a_2 - a_3} \dots Y_n^{a_n}$$

mit  $a_1 \geq \dots \geq a_n$ . Es sei  $(a_1, \dots, a_n)$  dasjenige Tupel mit  $a_i \geq a_{i+1}$ , das in der gradlexikographischen Ordnung maximal ist unter allen Tupeln, für die  $Y_1^{a_1 - a_2} Y_2^{a_2 - a_3} \dots Y_n^{a_n}$  in  $H$  vorkommt (es werden also die  $a$  verglichen, nicht die Differenzen). Dann besitzt  $H(E_1, \dots, E_n)$  als Polynom in  $X$  das Leitmonom  $X_1^{a_1} \dots X_n^{a_n}$  und wäre nicht 0.  $\square$

Insbesondere ist der Ring der symmetrischen Polynome selbst isomorph zu einem Polynomring in  $n$  Variablen.