

Invariantentheorie

Vorlesung 5

Invariantenringe zu Untergruppen

PROPOSITION 5.1. *Es sei $R \times G \rightarrow R$ eine Operation einer Gruppe G auf einem kommutativen Ring durch Ringautomorphismen. Sei $H \subseteq G$ eine Untergruppe. Dann gelten folgende Aussagen.*

- (1) $R^G \subseteq R^H$.
 (2) Sind H_1 und H_2 Untergruppen in G mit $G = H_1 \cdot H_2$, so ist

$$R^{H_1} \cap R^{H_2} = R^G.$$

- (3) Ist H ein Normalteiler in G , so operiert die Restklassengruppe G/H auf R^H durch

$$f[\sigma] := f\sigma.$$

Dabei ist

$$R^G = (R^H)^{G/H}.$$

Beweis. (1) ist klar. (2). Die Voraussetzung bedeutet, dass man $\sigma = \prod_{i=1}^n \sigma_i$ mit gewissen $\sigma_i \in H_1$ oder $\sigma_i \in H_2$ schreiben kann.

Die Inklusion \supseteq ist nach (1) klar. Die Inklusion \subseteq ist wegen

$$f\sigma = f \prod_{i=1}^n \sigma_i = f\sigma_1 \prod_{i=2}^n \sigma_i = f \prod_{i=2}^n \sigma_i = f$$

klar. (3). Die Operation ist zunächst wohldefiniert, d.h. unabhängig vom Repräsentanten. Seien dazu $\sigma, \sigma' \in G$ gegeben mit $\sigma'\sigma^{-1} \in H$. Dann ist

$$f\sigma' = f\sigma'\sigma^{-1}\sigma = f\sigma.$$

Wegen der Normalteilereigenschaft gibt es für $\sigma \in G$ und $\tau \in H$ ein $\tau' \in H$ mit $\sigma\tau = \tau'\sigma$. Für $f \in R^H$ ist

$$(f\sigma)\tau = f\tau'\sigma = f\sigma$$

und somit gehört $f\sigma$ ebenfalls zu R^H . Wir haben also eine Abbildung

$$R^H \times G \longrightarrow R^H.$$

Diese Abbildung ist in der Tat eine Gruppenoperation. Das neutrale Element wirkt identisch und die Assoziativität ergibt sich aus

$$f([\sigma][\tau]) = f[\sigma\tau] = f(\sigma\tau) = (f\sigma)\tau = (f[\sigma])\tau = (f[\sigma])[\tau].$$

Es liegt also eine Operation von G auf R^H vor, und da die Elemente $\sigma \in H$ identisch wirken, induziert dies eine Operation von G/H auf R^H . Bei den Abbildungen $f \mapsto f\sigma$ handelt es sich um Ringautomorphismen, da es sich um Einschränkungen von Ringautomorphismen auf R handelt, wobei sich die Surjektivität aus der Existenz von σ^{-1} ergibt.

Wir kommen zur Gleichheit

$$R^G = (R^H)^{G/H}.$$

Zum Beweis der Inklusion \subseteq sei $f \in R^G$. Dann ist insbesondere $f \in R^H$. Wegen $f[\sigma] = f\sigma = f$ ist f auch G/H -invariant. Zum Beweis der Inklusion \supseteq sei $f \in (R^H)^{G/H} \subseteq R^H$. Doch dann ist für $\sigma \in G$ wiederum $f\sigma = f[\sigma] = f$. \square

LEMMA 5.2. *Es sei*

$$R \times G \longrightarrow R$$

eine Operation einer Gruppe G auf einem kommutativen Ring R durch Ringautomorphismen. Es seien $H, H' \subseteq G$ konjugierte Untergruppen. Dann sind die Invariantenringe R^H und $R^{H'}$ in natürlicher Weise isomorph.

Beweis. Die beiden Untergruppen seien vermöge $\tau \in G$ zueinander konjugiert, d.h. die Abbildung

$$H \longrightarrow H', \sigma \longmapsto \tau^{-1}\sigma\tau,$$

sei ein Gruppenisomorphismus. Wir betrachten den zu τ gehörenden Ringautomorphismus

$$R \longrightarrow R, f \longmapsto f\tau,$$

und seine Einschränkung auf $R^G \subseteq R$. Für $f \in R^H$ und $\sigma' \in H'$ mit $\sigma' = \tau^{-1}\sigma\tau$ ist

$$(f\tau)\sigma' = (f\tau)(\tau^{-1}\sigma\tau) = f\sigma\tau = f\tau,$$

also liegt das Bild in $R^{H'}$. Da man die Rollen von H und H' vertauschen kann, liegt ein Isomorphismus vor. \square

Polynomiale Dreiecksinvarianten

BEISPIEL 5.3. Wir betrachten die Menge der Dreiecke, aufgefasst mit der Operation der Kongruenzabbildungen, siehe Beispiel 1.1. Die Vektoren $v \in \mathbb{R}^2$ fasst man als Verschiebungen T_v und damit als Kongruenzabbildungen auf. Mit einer beliebigen Kongruenz φ besteht die Beziehung $\varphi \circ T_v = T_{\varphi(v)} \circ \varphi$. Daher bilden die Verschiebungen einen Normalteiler in der Kongruenzgruppe G (der uneigentlichen affinen Isometriegruppe). Nach Proposition 5.1 kann man den Invariantenring $\mathbb{R}[X_1, Y_1, X_2, Y_2, X_3, Y_3]^G$ sukzessive berechnen. Unter der Untergruppe V der Verschiebungen ist der Invariantenring offenbar gleich

$$\mathbb{R}[X_1, Y_1, X_2, Y_2, X_3, Y_3]^V = \mathbb{R}[X_1 - X_3, Y_1 - Y_3, X_2 - X_3, Y_2 - Y_3].$$

Dieser Übergang entspricht geometrisch der Verschiebung des dritten Eckpunktes in den Nullpunkt. Die Operation der Restklassengruppe, die ja die uneigentliche Drehgruppe ist, auf diesem Polynomring in vier Variablen (die wir jetzt U_1, V_1, U_2, V_2 nennen) rührt von der natürlichen (und linearen) Operation der Drehgruppe auf dem \mathbb{R}^2 her. Die Determinante induziert einen surjektiven Gruppenhomomorphismus

$$\mathrm{O}_2(\mathbb{R}) \longrightarrow \{1, -1\},$$

deren Kern die eigentliche Drehgruppe $\mathrm{SO}_2(\mathbb{R})$ ist (das Urbild von -1 bilden die *Drehspiegelungen*). Daher gibt es eine natürliche Operation der $\mathbb{Z}/(2)$ auf

$$\mathbb{R}[U_1, V_1, U_2, V_2]^{\mathrm{SO}_2(\mathbb{R})},$$

und man sollte zuerst diesen Invariantenring ausrechnen. Aufgrund der geometrischen Interpretation (die drei Quadrate der Längen des Dreiecks, das Skalarprodukt der Seiten am Nullpunkt, der orientierte Flächeninhalt (bis auf Skalierung)) müssen

$$U_1^2 + V_1^2, U_2^2 + V_2^2, (U_1 - U_2)^2 + (V_1 - V_2)^2, U_1U_2 + V_1V_2, U_1V_2 - U_2V_1$$

invariante Polynome sein, was man auch direkt durch Rechnungen bestätigen kann. Das Skalarprodukt ist dabei unmittelbar mit den ersten drei Längenquadraten polynomial ausdrückbar. Da die drei Längen zwar die unorientierte Kongruenzklasse des Dreiecks bestimmen, es zu einem (nicht entarteten) Längentripel aber zwei entgegengesetzt orientierte Dreiecke gibt, muss es ein weiteres $\mathrm{SO}_2(\mathbb{R})$ -invariantes Polynom geben, das aber nicht $\mathrm{O}_2(\mathbb{R})$ -invariant ist, sondern Orientierungswechsel respektiert. Die Orientierung ist am fünften Polynom, der Determinante, ablesbar. Die drei Längenquadrate und die Determinante bestimmen die orientierte Kongruenzklasse des Dreiecks eindeutig, somit repräsentieren diese vier Funktionen die Quotientenabbildung. Das Quadrat der Determinante kann man als Polynom in den Längenquadraten ausdrücken (beispielsweise ausgehend von der *Heronischen Flächenformel*).

LEMMA 5.4. *Die Drehgruppe*

$$\mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \mid \alpha \in [0, 2\pi) \right\}$$

operiere linear und simultan auf dem $\mathbb{R}^4 = \mathbb{R}^2 \times \mathbb{R}^2$. Dann ist der Invariantenring der zugehörigen Operation auf dem Polynomring $\mathbb{R}[U_1, V_1, U_2, V_2]$ gleich

$$\mathbb{R}[U_1, V_1, U_2, V_2]^{\mathrm{SO}_2(\mathbb{R})} = \mathbb{R}[U_1^2 + V_1^2, U_2^2 + V_2^2, U_1U_2 + V_1V_2, U_1V_2 - U_2V_1].$$

Dabei sind die ersten drei Erzeuger algebraisch unabhängig, und das Quadrat von $U_1V_2 - U_2V_1$ lässt sich durch die ersten drei Erzeuger ausdrücken.

Beweis. Die Invarianz der angegebenen Polynome sowie ihre inhaltliche Bedeutung wurden schon in Beispiel 5.3 bemerkt. Wir betrachten die Erweiterung

$$\mathbb{R}[U_1, V_1, U_2, V_2] \subset \mathbb{C}[U_1, V_1, U_2, V_2].$$

Die angegebene Operation der $\text{SO}_2(\mathbb{R})$ auf dem reellen Polynomring lässt sich direkt auf den komplexen Polynomring fortsetzen, da das Gruppenelement

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

durch $U_i \mapsto \cos \alpha U_i - \sin \alpha V_i$ etc. wirkt, und diese Ringhomomorphismen reell oder komplex aufgefasst werden können.¹ Ein Polynom $F \in \mathbb{R}[U_1, V_1, U_2, V_2]$ ist genau dann invariant, wenn es aufgefasst in $\mathbb{C}[U_1, V_1, U_2, V_2]$ invariant ist. Wir führen neue komplexe Variablen ein, nämlich

$$W_1 = U_1 + iV_1, Z_1 = U_1 - iV_1, W_2 = U_2 + iV_2, Z_2 = U_2 - iV_2.$$

Es bestehen die Beziehung

$$W_1 Z_1 = (U_1 + iV_1)(U_1 - iV_1) = U_1^2 + V_1^2,$$

$$W_2 Z_2 = (U_2 + iV_2)(U_2 - iV_2) = U_2^2 + V_2^2,$$

$$W_1 Z_2 = (U_1 + iV_1)(U_2 - iV_2) = U_1 U_2 + V_1 V_2 - i(U_1 V_2 - U_2 V_1)$$

und

$$W_2 Z_1 = (U_2 + iV_2)(U_1 - iV_1) = U_1 U_2 + V_1 V_2 + i(U_1 V_2 - U_2 V_1).$$

Die beiden letzten Gleichungen zeigen, dass sich umgekehrt auch $U_1 U_2 + V_1 V_2$ und $U_1 V_2 - U_2 V_1$ durch $W_1 Z_2$ und $W_2 Z_1$ ausdrücken lassen. Die beiden Systeme erzeugen also die gleiche \mathbb{C} -Unteralgebra von

$$\mathbb{C}[U_1, V_1, U_2, V_2] \cong \mathbb{C}[W_1, Z_1, W_2, Z_2].$$

Wir schreiben die Elemente der operierenden Gruppe als

$$\sigma = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} = \cos \alpha + i \sin \alpha,$$

wobei wir die Drehgruppe mit den komplexen Zahlen vom Betrag 1 (zusammen mit der komplexen Multiplikation) identifizieren. Die Operation wird dann zu (\bullet bezeichne die aus dem Reellen fortgesetzte Operation und \cdot die komplexe Multiplikation)

$$\begin{aligned} W_1 \bullet \sigma &= (U_1 + iV_1) \bullet \sigma \\ &= (\cos \alpha) U_1 - (\sin \alpha) V_1 + i((\sin \alpha) U_1 + (\cos \alpha) V_1) \\ &= (U_1 + iV_1) (\cos \alpha + i \sin \alpha) \\ &= W_1 \cdot \sigma \end{aligned}$$

(ebenso für W_2) und

$$\begin{aligned} Z_1 \bullet \sigma &= (U_1 - iV_1) \bullet \sigma \\ &= (\cos \alpha) U_1 - (\sin \alpha) V_1 - i((\sin \alpha) U_1 + (\cos \alpha) V_1) \end{aligned}$$

¹Die operierende Gruppe wird also nicht komplexifiziert.

$$\begin{aligned}
&= (U_1 - iV_1)(\cos \alpha - i \sin \alpha) \\
&= Z_1 \cdot \sigma^{-1}
\end{aligned}$$

(ebenso für Z_2). Wir betrachten auf $\mathbb{C}[W_1, Z_1, W_2, Z_2]$ die \mathbb{Z} -Graduierung², bei der W_1, W_2 den Grad 1 und Z_1, Z_2 den Grad -1 bekommen. Die Operation der Gruppe ist homogen bezüglich dieser Graduierung. Daher ist der Invariantenring ein graduierter Unterring. Auf der d -ten Stufe des Ringes ist die Operation für $t \in S^1 \subset \mathbb{C}^\times$ durch $H \mapsto t^d H$ gegeben. Für $d = 0$ ist dies die Identität, so dass die 0-te Stufe invariant ist. Für $d \neq 0$ gibt es $t \in S^1$ mit $t^d \neq 1$, so dass es außer 0 keine weiteren invarianten Polynome gibt. Der Invariantenring ist also die 0-te Stufe. Diese besteht aus Linearkombinationen von Monomen der 0-ten Stufe, und ein Monom vom nullten Grad muss ein Produkt der Elemente $W_i Z_j$ sein. Der Invariantenring ist also

$$\begin{aligned}
\mathbb{C}[W_1, Z_1, W_2, Z_2]^{\text{SO}_2(\mathbb{R})} &= \mathbb{C}[W_1 Z_1, W_1 Z_2, W_2 Z_1, W_2 Z_2] \\
&= \mathbb{C}[U_1^2 + V_1^2, U_2^2 + V_2^2, U_1 U_2 + V_1 V_2, U_1 V_2 - U_2 V_1].
\end{aligned}$$

Wir kehren zur reellen Situation zurück. Es sei $F \in \mathbb{R}[U_1, V_1, U_2, V_2]$ ein invariantes Polynom. Dann gibt es ein komplexes Polynom P in vier Variablen mit

$$F = P(U_1^2 + V_1^2, U_2^2 + V_2^2, U_1 U_2 + V_1 V_2, U_1 V_2 - U_2 V_1).$$

Mit Hilfe der komplexen Konjugation sieht man, dass es auch ein reelles Polynom mit dieser Eigenschaft geben muss. Daher gilt für den reellen Invariantenring

$$\mathbb{R}[U_1, V_1, U_2, V_2]^{\text{SO}_2(\mathbb{R})} = \mathbb{R}[U_1^2 + V_1^2, U_2^2 + V_2^2, U_1 U_2 + V_1 V_2, U_1 V_2 - U_2 V_1].$$

Für den Zusatz siehe Aufgabe 5.4. \square

Der folgende Satz ist die polynomial-invariantentheoretische Version der Aussage, dass die Kongruenzklasse eines Dreiecks durch die drei Seitenlängen (SSS) bzw. einen Winkel und zwei anliegende Seitenlängen (SWS) festgelegt ist. Aufgrund dieses elementar-geometrischen Satzes weiß man, dass man jede Invariante der Kongruenzklasse eines Dreiecks „irgendwie“ als eine Funktion der drei Längen ausdrücken kann. Daraus folgt aber keineswegs automatisch, dass man eine polynomiale Invariante auch polynomial ausdrücken kann.

SATZ 5.5. *Die orthogonale Gruppe $O_2(\mathbb{R})$ (der Drehungen und der Drehspiegelungen) operiere linear und simultan auf dem*

$$\mathbb{R}^4 = \mathbb{R}^2 \times \mathbb{R}^2.$$

Dann ist der Invariantenring der zugehörigen Operation auf dem Polynomring $\mathbb{R}[U_1, V_1, U_2, V_2]$ gleich

$$\mathbb{R}[U_1, V_1, U_2, V_2]^{O_2(\mathbb{R})} = \mathbb{R}[U_1^2 + V_1^2, U_2^2 + V_2^2, U_1 U_2 + V_1 V_2].$$

²Wir werden Graduierungen mit einer beliebigen graduierenden Gruppe und die zugehörige Operation der Charaktergruppe in der siebten Vorlesung besprechen.

Die drei Erzeuger sind dabei algebraisch unabhängig. Jede polynomiale Invariante eines (nummerierten) Dreieckes lässt sich polynomial in den drei Seitenquadraten ausdrücken.

Beweis. Wie in Beispiel 5.3 erwähnt, gibt es eine kurze exakte Sequenz

$$1 \longrightarrow \mathrm{SO}_2(\mathbb{R}) \longrightarrow \mathrm{O}_2(\mathbb{R}) \longrightarrow \{1, -1\} \longrightarrow 1.$$

Wir können daher aufgrund von Proposition 5.1 den Invariantenring

$$\mathbb{R}[U_1, V_1, U_2, V_2]^{\mathrm{O}_2(\mathbb{R})}$$

aus dem Invariantenring zu

$$\mathbb{R}[U_1, V_1, U_2, V_2]^{\mathrm{SO}_2(\mathbb{R})}$$

ausrechnen, der in Lemma 5.4 zu

$$B = \mathbb{R}[U_1^2 + V_1^2, U_2^2 + V_2^2, U_1U_2 + V_1V_2, U_1V_2 - U_2V_1]$$

bestimmt wurde. Das nichttriviale Element der Restklassengruppe $\{1, -1\}$ wirkt auf B durch einen beliebigen Repräsentanten, beispielsweise durch die Spiegelung $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Der zugehörige Ringautomorphismus lässt U_1, U_2 unverändert und schickt V_1, V_2 auf ihr Negatives. Unter dieser Abbildung sind die drei vorderen Erzeuger invariant und der hintere Erzeuger wird auf sein Negatives abgebildet. Da das Quadrat des vierten Erzeugers zu $A = \mathbb{R}[U_1^2 + V_1^2, U_2^2 + V_2^2, U_1U_2 + V_1V_2]$ gehört, liegt eine Operation auf einem Ring der Form $A[X]/(X^2 - a)$ durch $X \leftrightarrow -X$ vor. In einem solchen Fall ist A der Invariantenring. \square

Quotientenkörper von Invariantenringen

PROPOSITION 5.6. *Es sei G eine Gruppe, die auf einem Integritätsbereich R als Gruppe von Ringautomorphismen operiere. Dann gelten folgende Eigenschaften.*

- (1) *Der Invariantenring R^G ist ein Integritätsbereich.*
- (2) *Die Operation induziert eine Operation von G auf dem Quotientenkörper $Q(R)$ als Gruppe von Körperautomorphismen.*
- (3) *Es ist $Q(R^G) \subseteq (Q(R))^G$.*
- (4) *Es ist*

$$R \cap (Q(R))^G = R^G.$$

Beweis. (1) ist wegen $R^G \subseteq R$ klar. (2). Es sei $K = Q(R)$ der Quotientenkörper von R . Zu jedem $\sigma \in G$ setzt sich der Ringautomorphismus $f \mapsto f\sigma$ aufgrund der universellen Eigenschaft der Nenneraufnahme zu einem Körperautomorphismus $\frac{f}{g} \mapsto \frac{f\sigma}{g}$ fort. (3). Ein Element aus dem Quotientenkörper $Q(R^G)$ hat die Form $\frac{f}{g}$ mit invarianten Elementen $f, g \in R^G$. Es ist also insbesondere invariant unter der induzierten Operation auf K .

Daher gilt $Q(R^G) \subseteq (Q(R))^G$. (4). Die Inklusion $R^G \subseteq R \cap Q(R)^G$ ist direkt klar. Die andere Inklusion ergibt sich, da die Operation von G auf $Q(R)$ eingeschränkt auf R die ursprüngliche Operation ist. Wenn also $f \in R$ ist und aufgefasst in $Q(R)$ invariant ist, so ist es überhaupt invariant. \square

BEMERKUNG 5.7. Mit Proposition 5.6 hängt die Invariantentheorie von Integritätsbereichen eng mit der Galoistheorie des Quotientenkörpers zusammen. In der Situation des Satzes ist bei endlichem G die Körpererweiterung $K^G \subseteq K$ eine Galoiserweiterung, wie aus dem Satz von Artin folgt. K^G ist ja gerade der Fixring unter den Körperautomorphismen zu G . Die Untergruppen $H \subseteq G$ liefern Zwischenkörper $K^G \subseteq M = K^H \subseteq K$ und $M \cap R = R^H$ ist der zugehörige Zwischenring (man darf aber nicht erwarten, dass es eine bijektive Korrespondenz zwischen Zwischenringen und Untergruppen gibt). Häufig besitzen Aussagen der Invariantentheorie stärkere Analoga aus der Galoistheorie. Zu Proposition 5.1 (3) vergleiche man etwa die Rückrichtung von Satz 16.4 (Körper- und Galoistheorie (Osnabrück 2011)) (1).

Es gibt aber auch erhebliche Unterschiede zwischen Invariantentheorie und Galoistheorie. Beispielsweise geht man in der klassischen Galoistheorie eher von einem Grundkörper K aus und untersucht Körpererweiterungen $K \subseteq L$ zusammen mit der K -Automorphismengruppe, während man in der klassischen Invariantentheorie eher mit dem Erweiterungsring anfängt und versucht, die Fixringe zu einer gewissen Operation zu bestimmen. Auch in der Invariantentheorie wird häufig ein Grundkörper k vorausgesetzt, doch tritt dieser kaum als Invariantenring auf, sondern übernimmt die Rolle, dass alle beteiligten Ringe k -Algebren über diesem Körper und alle Ringhomomorphismen k -Algebrahomomorphismen sind. Beispielsweise ist die Bestimmung von Invariantenringen zum Polynomring $k[X_1, \dots, X_n]$ zu (linearen) Gruppenoperationen schon ein riesiges Teilgebiet der Invariantentheorie.

Bei einer endlichen Gruppe gilt in Proposition 5.6 (3) sogar Gleichheit, wie die folgende Aussage zeigt.

LEMMA 5.8. *Es sei G eine endliche Gruppe, die auf einem Integritätsbereich als Gruppe von Ringautomorphismen operiere. Dann ist*

$$Q(R^G) = (Q(R))^G.$$

Beweis. Die Inklusion $Q(R^G) \subseteq (Q(R))^G$ gilt nach Proposition 5.6 (3) für jede Gruppe. Zum Beweis der Umkehrung seien $f, g \in R$, $g \neq 0$, mit $\frac{f}{g} \in (Q(R))^G$ gegeben. Wir betrachten

$$h = \prod_{\sigma \in G, \sigma \neq e_G} g\sigma.$$

Dann gelten in $Q(R)$ die Identitäten

$$\frac{f}{g} = \frac{hf}{hg}$$

$$\begin{aligned}
&= \frac{hf}{\left(\prod_{\sigma \in G, \sigma \neq e_G} g\sigma\right)g} \\
&= \frac{hf}{\prod_{\sigma \in G} g\sigma}.
\end{aligned}$$

Nach Voraussetzung ist der Bruch und in dieser Darstellung offenbar auch der Nenner invariant. Also muss auch der Zähler invariant sein und somit ist $\frac{f}{g} \in Q(R^G)$. \square

BEISPIEL 5.9. Es sei K ein unendlicher Körper. Wir betrachten auf $R = K[X, Y]$ die Operation von K^\times durch skalare Multiplikation. Zu $\lambda \in K^\times$ gehört also der durch $X \mapsto \lambda X, Y \mapsto \lambda Y$ gegebene K -Algebrahomomorphismus. Der Invariantenring dazu ist K , also ein Körper. Der Quotientenkörper von $K[X, Y]$ ist der Funktionenkörper $K(X, Y)$ in zwei Variablen. Sein Invariantenring unter der Operation ist $K\left(\frac{X}{Y}\right)$, also der Funktionenkörper in einer Variablen. In dieser Situation gilt also

$$Q(R^G) \neq (Q(R))^G.$$