Prof. Dr. H. Brenner **Osnabrück WS 2012/2013**

Invariantentheorie

Vorlesung 2

Gruppenoperationen

In den beiden Beispielen der ersten Vorlesung operiert eine Gruppe auf einer Menge: Die Kongruenzabbildungen bilden eine Gruppe, und eine Kongruenz überführt ein Dreieck in ein weiteres (kongruentes) Dreieck. Eine Permutation $\sigma \in S_n$ überführt ein n-Tupel in ein weiteres Tupel und ein Polynom (in n Variablen) in ein Polynom über. Diese Situation wird durch den Begriff der Gruppenoperation erfasst, welcher grundlegend für die Invariantentheorie ist.

Es sei G eine zumeist multiplikativ geschriebene Gruppe mit neutralem Element e.

Definition 2.1. Es sei G eine Gruppe und M eine Menge. Eine Abbildung

$$G \times M \longrightarrow M,\ (g,x) \longmapsto gx,$$

heißt *Gruppenoperation* (von G auf M), wenn die beiden folgenden Eigenschaften gelten.

(1) $ex = x$ für alle $x \in M$.
(2) $(gh)x = g(hx)$ für alle $g,h \in G$ und für alle $x \in M$.

Man spricht auch von einer *Aktion* oder einer *Wirkung* der Gruppe G auf M. Im Zusammenhang von Gruppenoperationen schreibt man die Gruppe zumeist multiplikativ, und ebenso schreibt man die Operation multiplikativ.

Definition 2.2. Es sei G eine Gruppe und M eine Menge. Eine Gruppenoperation von G auf M heißt *treu*, wenn aus $gx = x$ für alle $x \in M$ folgt, dass $g = e$ ist.

Lemma 2.3. *Es sei G eine Gruppe und M eine Menge. Es sei* $\operatorname{Perm}(M)$ *die Gruppe der Permutationen auf M. Dann gelten folgende Aussagen.*

(1) *Wenn G auf M operiert, so ist die Abbildung*

$$G \longrightarrow \operatorname{Perm}(M),\ g \longmapsto (x \mapsto gx),$$

ein Gruppenhomomorphismus.

(2) *Wenn umgekehrt ein Gruppenhomomorphismus*

$$\varphi\colon\ G \longrightarrow \operatorname{Perm}(M),$$

vorliegt, so wird durch

$$G \times M \longrightarrow M,\ (g,x) \longmapsto (\varphi(g))(x),$$

eine Gruppenoperation von G auf M definiert.

Beweis. Siehe Aufgabe 2.1. □

Unter dieser Korrespondenz ist die Operation genau dann treu, wenn φ injektiv ist.

Beispiel 2.4. Nach Lemma 2.3 (2) und nach Lemma 4.4 (Körper- und Galoistheorie (Osnabrück 2011)) ist eine Gruppenoperation von $(\mathbb{Z}, 0, +)$ auf einer Menge M dasselbe wie eine bijektive Abbildung

$$F\colon M \longrightarrow M,$$

wobei die 1 wie F wirkt. Bei gegebenem F ist also die Gruppenwirkung für $x \in M$ durch

$$n \cdot x = F^n(x)$$

definiert, wobei F^n bei $n \geq 0$ die n-fache Hintereinanderschaltung von F und bei $n < 0$ die $-n$-fache Hintereinanderschaltung der Umkehrabbildung F^{-1} bedeutet.

Definition 2.5. Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Man nennt zwei Elemente $x, y \in M$ *G-äquivalent* (oder äquivalent unter G), wenn es ein $g \in G$ mit $y = gx$ gibt.

Diese Relation ist in der Tat eine Äquivalenzrelation, wie man sich direkt überlegen kann. Die Äquivalenzklassen bekommen einen eigenen Namen.

Definition 2.6. Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Die Äquivalenzklassen auf M zur G-Äquivalenz nennt man die *Bahnen der Operation*.

Definition 2.7. Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Zu $x \in M$ heißt

$$G_x = \{g \in G |\, gx = x\}$$

die *Isotropiegruppe* zu x.

Dabei handelt es sich um eine Untergruppe von G. Andere Bezeichnungen hierfür sind *Standgruppe* oder *Stabilisator*.

Definition 2.8. Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Ein Punkt $x \in M$ heißt *Fixpunkt der Operation*, wenn $gx = x$ ist für alle $g \in G$.

Ein Element $x \in M$ ist genau dann ein Fixpunkt der Operation, wenn die Bahn durch diesen Punkt einelementig ist, und dies ist genau dann der Fall, wenn die zugehörige Standgruppe ganz G ist.

Beispiel 2.9. Es sei G eine Gruppe und M eine Menge. Dann gibt es stets die sogenannte *triviale Operation* von G auf M, die durch $gx = x$ für alle $g \in G$ und alle $x \in M$ gegeben ist. In diesem Fall ist jeder Punkt ein Fixpunkt und alle Bahnen sind einelementig.

Definition 2.10. Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Die Operation heißt *transitiv*, wenn es zu je zwei Elementen $x, y \in M$ ein $g \in G$ mit $gx = y$ gibt.

Eine Operation ist genau dann transitiv, wenn es nur eine Bahn gibt.

Beispiel 2.11. Sei G eine Gruppe. Die Verknüpfung

$$G \times G \longrightarrow G,\ (g, h) \longmapsto gh,$$

kann man als eine Gruppenoperation der Gruppe G auf sich selbst ansehen. Diese Operation ist treu und transitiv, es gibt also nur eine Bahn. Für zwei Elemente g_1 und g_2 ist ja $g_1 = (g_1 g_2^{-1}) g_2$.

Beispiel 2.12. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Dann liefert die Verknüpfung

$$H \times G \longrightarrow G,\ (h, g) \longmapsto hg,$$

eine Gruppenoperation von H auf G. Die Bahnen dieser Operation stimmen mit den Rechtsnebenklassen zu dieser Untergruppe überein. Wenn G endlich ist, so sind die Bahnen (nach dem Beweis zu Satz 4.16 (Körper- und Galoistheorie (Osnabrück 2011))) alle gleichmächtig, was bei einer beliebigen Gruppenoperation keineswegs der Fall sein muss.

Beispiel 2.13. Sei $n \in \mathbb{N}$, $M = \{1, \ldots, n\}$ und S_n die Gruppe der Permutationen auf M. Dann liegt eine natürliche Operation

$$S_n \times M \longrightarrow M,\ (\sigma, i) \longmapsto \sigma(i),$$

vor. Der zugehörige Gruppenhomomorphismus ist die Identität. Die Operation ist treu, da jede Permutation $\neq \mathrm{id}_M$ mindestens ein Element aus M bewegt. Zu jedem $i \in M$ ist die Isotropiegruppe G_i isomorph zur Permutationsgruppe $S_{n-1} \cong \mathrm{Perm}\,(M \setminus \{i\})$. Für je zwei Elemente $i, j \in M$ gibt es eine Permutation (z.B. eine Transposition), die i in j überführt. Bei dieser Gruppenoperation gibt es also nur eine Bahn.

Beispiel 2.14. Es sei R ein kommutativer Ring und $G = R^\times$ seine Einheitengruppe. Die Einschränkung der Ringmultiplikation

$$R^\times \times R \longrightarrow R,\ (r, s) \longmapsto rs,$$

liefert eine Gruppenoperation der Einheitengruppe auf dem Ring. Diese Operation ist treu, das Nullelement ist ein Fixpunkt der Operation. Zwei Elemente $a, b \in R$, die bezüglich dieser Operation äquivalent sind, heißen assoziiert. Dieser Begriff spielt bei der eindeutigen Primfaktorzerlegung in einem faktoriellen Bereich eine wichtige Rolle.

Satz 2.15. *Es sei G eine endliche Gruppe, die auf einer endlichen Menge M operiere. Es sei F die Menge der Fixpunkte der Operation und es seien*

$G_1, \ldots, G_n$ die verschiedenen Bahnen mit mindestens zwei Elementen. Dann ist

$$\#(M) \,=\, \#(F) + \sum_{i=1}^{n} \#(G_i).$$

Beweis. Die Menge M ist zerlegt in die Bahnen der Operation, und diese sind entweder einelementig und entsprechen den Fixpunkten, oder mehrelementig, und werden dann rechts mitgezählt. □

Beispiel 2.16. Sei G eine Gruppe. Die Konjugation kann man als eine Operation von G auf sich selbst auffassen, indem man

$$g \cdot x = gxg^{-1}$$

setzt. Dabei haben wir die Gruppenverknüpfung symbolfrei und die Operation zur Unterscheidung mit $\cdot$ geschrieben. Dass eine Operation vorliegt kann man direkt nachprüfen oder aus Lemma 5.2 (Körper- und Galoistheorie (Osnabrück 2011)) folgern. Die Äquivalenzklassen unter dieser Operation, also die Bahnen der Konjugation, heißen *Konjugationsklassen*. Die Elemente im Zentrum der Gruppe sind genau die Fixpunkte.

Beispiel 2.17. Es sei M eine Menge und

$$F \colon\, M \longrightarrow M$$

eine bijektive Abbildung mit der zugehörigen Gruppenoperation von $\mathbb{Z}$ auf M. Die Operation ist genau dann trivial, wenn F die Identität ist. Die Fixpunkte der Operation sind genau die Fixpunkte von F. Die Isotropiegruppe zu $x \in M$ ist $\mathbb{Z}k$ ($k \geq 1$), falls x ein Fixpunkt der k-ten Hintereinanderschaltung F^k und k minimal mit dieser Eigenschaft ist; andernfalls ist sie gleich 0. Die durch $x \in M$ definierte Bahn besteht aus

$$\{F^n(x) |\, n \in \mathbb{Z}\} \ .$$

Dabei können natürlich einzelne Bahnen endlich sein, auch wenn die Operation treu ist.

Definition 2.18. Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Dann nennt man die Menge der Bahnen den *Bahnenraum* der Operation. Er wird mit

$$M \backslash G$$

bezeichnet. Die Abbildung

$$M \longrightarrow M\backslash G,\ x \longmapsto [x],$$

wobei $[x]$ die Bahn durch x bezeichnet, heißt *Quotientenabbildung.*

Der Bahnenraum ist also einfach die Quotientenmenge der Äquivalenzrelation, die durch die Gruppenoperation festgelegt wird, und die angegebene Quotientenabbildung ist die zugehörige kanonische Projektion.

Beispiel 2.19. Wir betrachten die n-dimensionale Sphäre

$$S = \left\{x \in \mathbb{R}^{n+1} \mid \ ||x|| = 1\right\}$$

und die antipodale Abbildung

$$\alpha\colon S \longrightarrow S,\, x \longmapsto -x,$$

die also jeden Punkt auf seinen gegenüberliegenden Punkt abbildet. Wegen

$$\alpha \circ \alpha = \mathrm{Id}_S$$

gibt dies Anlass zu einer Operation von $G = \{1, -1\} \cong \mathbb{Z}/(2)$ auf der Sphäre S, bei der 1 durch die Identität und -1 durch α operiert. Diese Operation ist treu und jede Bahn ist zweielementig von der Form $\{x, -x\}$. Insbesondere besitzt die Operation keinen Fixpunkt. Der Bahnenraum (versehen mit einer geeigneten Topologie) heißt n-dimensionaler *reell-projektiver Raum*.

Definition 2.20. Sei G eine Gruppe und seien M und N zwei Mengen, auf denen jeweils G operiert. Dann heißt eine Abbildung

$$\varphi\colon M \longrightarrow N$$

G-invariant (oder *G-verträglich*) wenn für alle $g \in G$ und alle $x \in M$ die Gleichheit

$$\varphi(gx) = g\varphi(x)$$

gilt.

Dieser Begriff wird insbesondere auch dann verwendet, wenn die Gruppe G auf der zweiten Menge N trivial operiert.

Lemma 2.21. *Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Es sei $M\backslash G$ der Bahnenraum zu dieser Operation. Dann gelten folgende Aussagen.*

(1) *Die Quotientenabbildung*

$$q\colon M \longrightarrow M\backslash G,\, x \longmapsto [x],$$

ist G-invariant (wobei G auf dem Bahnenraum trivial operiert).

(2) *Wenn N eine weitere Menge ist und*

$$\varphi\colon M \longrightarrow N$$

eine G-invariante Abbildung (wobei die Operation von G auf N trivial sei), so gibt es genau eine Abbildung

$$\tilde{\varphi}\colon M\backslash G \longrightarrow N$$

mit $\varphi = \tilde{\varphi} \circ q$.

Beweis. (1) Für $x \in M$ und $g \in G$ sind x und gx in der gleichen Äquivalenzklasse, also ist

$$q(gx) = [gx] = [x] = g[x].$$

(2) folgt aus Lemma 6.17 (Einführung in die Algebra (Osnabrück 2009)) (5).

□

Beispiel 2.22. Es sei X eine Menge und $n \in \mathbb{N}_+$. Wir setzen

$$M = X \times \cdots \times X$$

mit n Faktoren. Die Permutationsgruppe S_n operiert auf M durch

$$\sigma(x_1, \ldots, x_n) = \left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right),$$

d.h. σ vertauscht die Indizes. Die Fixpunkte dieser Operation sind genau die Diagonalelemente, also die Elemente der Form $(y, \ldots, y)$. Wenn r die Anzahl der verschiedenen Elemente in $x = (x_1, \ldots, x_n)$ bezeichnet und a_i, $1 \leq i \leq r$, die Anzahl angibt, wie oft die einzelnen Werte auftreten, so ist die Isotropiegruppe zu x gleich $S_{a_1} \times \cdots \times S_{a_r}$ (das sind diejenigen Permutationen, die einen jeden Index auf einen Index mit gleichem Eintrag abbilden) und besitzt genau $a_1! \cdots a_r!$ Elemente. Die zugehörige Bahn besitzt entsprechend $\frac{n!}{a_1! \cdots a_r!}$ Elemente.

Bei $X = \mathbb{R}$ sind die polynomialen Funktionen

$$x_1 + \ldots + x_n, \sum_{i<j} x_i x_j, \ldots, x_1 \cdots x_n$$

(also die elementarsymetrischen Polynome) S_n-invariante Abbildungen nach $\mathbb{R}$.

Beispiel 2.23. Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Es sei L eine weitere Menge und Abb (L, M) die Menge der Abbildungen von L nach M. Dann wird durch

$$G \times \operatorname{Abb}(L, M) \longrightarrow \operatorname{Abb}(L, M), \, (g, \varphi) \longmapsto g\varphi,$$

wobei $g\varphi$ durch

$$(g\varphi)(x) = g(\varphi(x))$$

definiert sei, eine Operation von G auf Abb (L, M) gegeben. Für das neutrale Element $e \in G$ gilt ja

$$(e\varphi)(x) = e(\varphi(x)) = \varphi(x)$$

für jedes $x \in M$, also $e\varphi = \varphi$, und für beliebige $g, h \in G$, $\varphi \in \operatorname{Abb}(L, M)$ und $x \in M$ gilt

$$((gh)\varphi)(x) = (gh)(\varphi(x)) = g(h(\varphi(x))) = g((h\varphi)(x)) = (g(h\varphi))(x),$$

also $(gh)\varphi = g(h\varphi)$.

Zu einer Gruppe G nennt man die Menge G mit der durch

$$g \cdot_{\mathrm{op}} h := hg$$

definierten Verknüpfung die *oppositionelle Gruppe* zu G. Sie wird mit G^{op} bezeichnet.

Beispiel 2.24. Es liege eine Gruppenoperation einer Gruppe G auf einer Menge M vor. Es sei N eine weitere Menge und Abb (M,N) die Menge der Abbildungen von M nach N. Dann wird durch

$$G^{\rm op} \times \operatorname{Abb}(M,N) \longrightarrow \operatorname{Abb}(M,N)\,,\, (g,\varphi) \longmapsto g\varphi,$$

wobei $g\varphi$ durch

$$(g\varphi)(x) = (\varphi(gx))$$

definiert sei, eine Operation der oppositionellen Gruppe $G^{\rm op}$ auf Abb (M,N) gegeben. Für das neutrale Element $e \in G$ gilt ja

$$(e\varphi)(x) \,=\, \varphi(ex) \,=\, \varphi(x)$$

für jedes $x \in M$, also $e\varphi \,=\, \varphi$, und für beliebige $g,h \in G$, $\varphi \in$ Abb (M,N) und $x \in M$ gilt

$$\begin{aligned} ((g \cdot_{\rm op} h)\varphi)(x) &= ((hg)\varphi)(x) \\ &= \varphi((hg)(x)) \\ &= \varphi(h(gx)) \\ &= (h\varphi)(gx) \,=\, (g(h\varphi))(x), \end{aligned}$$

also $(g \cdot_{\rm op} h)\varphi \,=\, g(h\varphi)$. Statt mit der oppositionellen Gruppe zu arbeiten kann man diese Konstruktion auch als eine Operation von rechts auffassen.

Die Fixelemente von Abb (M,N) unter dieser Operation sind gerade die G-invarianten Abbildungen von M nach N. Diese Konstruktion wird insbesondere bei $N = \mathbb{R}$ o.Ä. angewendet, wenn es also um auf M definierte Funktionen geht.