

Invariantentheorie

Vorlesung 3

Lineare Operationen

Eine Operation einer Gruppe G auf einer (geometrischen) Menge M ist das gleiche wie ein Gruppenhomomorphismus der Gruppe in die Permutationsgruppe des geometrischen Objektes. Häufig betrachtet man nur solche Operationen, deren zugehörige Permutationen *Automorphismen* sind, also die relevanten geometrischen Eigenschaften des Objektes respektieren. Bei einer Operation auf einer Mannigfaltigkeit wird man beispielsweise fordern, dass die Automorphismen Diffeomorphismen sind. Wenn das geometrische Objekt ein Vektorraum ist, so interessiert man sich insbesondere für die linearen Automorphismen.

DEFINITION 3.1. Es sei K ein Körper und V ein K -Vektorraum. Es sei G eine Gruppe. Eine Operation

$$\mu: G \times V \longrightarrow V$$

heißt *linear*, wenn für jedes $\sigma \in G$ die Abbildung

$$V \longrightarrow V, v \longmapsto \mu(\sigma, v),$$

K -linear ist.

Bei einer linearen Operation sind die Abbildungen $\varphi_\sigma = \mu(\sigma, -)$ sogar K -Automorphismen. Eine lineare Operation ist das gleiche wie ein Gruppenhomomorphismus

$$G \longrightarrow \text{GL}(V).$$

BEISPIEL 3.2. Es sei V ein K -Vektorraum über einem Körper K . Die allgemeine lineare Gruppe $\text{GL}(V)$ operiert in natürlicher Weise linear auf V . Die Elemente $\varphi \in \text{GL}(V)$ sind ja definiert als K -Automorphismen von V in sich und somit ist die Abbildung

$$\text{GL}(V) \times V \longrightarrow V, (\varphi, v) \longmapsto \varphi(v),$$

wohldefiniert. Da die Verknüpfung auf $\text{GL}(V)$ einfach die Hintereinanderschaltung von Abbildungen ist, ergibt sich sofort

$$\varphi(\psi(v)) = (\varphi \circ \psi)(v),$$

so dass es sich um eine Gruppenoperation handelt. Diese Operation besitzt nur zwei Bahnen, nämlich den Nullpunkt 0 und $V \setminus \{0\}$, da es zu zwei von 0 verschiedenen Vektoren v_1 und v_2 stets einen Automorphismus gibt, der v_1 in v_2 überführt.

BEISPIEL 3.3. Es sei V ein K -Vektorraum über einem Körper K . Die natürliche lineare Operation der allgemeinen linearen Gruppe $\text{GL}(V)$ auf V , also die Abbildung

$$\text{GL}(V) \times V \longrightarrow V, (\varphi, v) \longmapsto \varphi(v),$$

induziert für jede Untergruppe $G \subseteq \text{GL}(V)$ eine lineare Operation

$$G \times V \longrightarrow V, (\varphi, v) \longmapsto \varphi(v).$$

Diese einfache Konstruktion beinhaltet eine Vielzahl von interessanten Operationen. Wichtige Untergruppen der $\text{GL}(V)$ sind die spezielle lineare Gruppe $\text{SL}(V)$ (dazu muss V endlichdimensional sein) und alle endlichen Gruppen (wenn die Dimension von V hinreichend groß ist). Wenn der Vektorraum weitere Strukturen trägt, beispielsweise eine Bilinearform (beispielsweise ein Skalarprodukt bei $K = \mathbb{R}$ oder $K = \mathbb{C}$), so lassen sich weitere wichtige Untergruppen definieren, wie die orthogonale Gruppe $\text{O}(V)$ und die eigentliche Isometriegruppe $\text{SO}(V)$.

BEISPIEL 3.4. Die symmetrische Gruppe S_n ist die Gruppe der Permutationen auf der Menge $I = \{1, \dots, n\}$, also

$$S_n = \{\sigma : I \rightarrow I \mid \sigma \text{ Bijektion}\}$$

mit der Hintereinanderschaltung als Verknüpfung. Das neutrale Element ist die Identität. Eine Permutation wird typischerweise als Wertetabelle geschrieben,

$$\begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}.$$

S_n ist eine Gruppe mit $n!$ Elementen.

Die Permutationsgruppe S_n operiert als Gruppe von linearen Automorphismen auf K^n wie folgt: Der i -te Basisvektor e_i wird auf $e_{\sigma(i)}$ geschickt, also $e_i \mapsto e_{\sigma(i)}$. Dies definiert nach Satz 12.3 (Mathematik (Osnabrück 2009-2011)) einen linearen Automorphismus

$$\sigma : K^n \longrightarrow K^n,$$

den wir ebenfalls mit σ bezeichnen. In Matrixschreibweise wird diese lineare Abbildung durch diejenige Matrix beschrieben, bei der in der i -ten Spalte in der $\sigma(i)$ -ten Zeile eine 1 steht, und sonst überall 0. Eine solche Matrix nennt man eine Permutationsmatrix. Wenn E_{ij} diejenige Matrix bezeichnet, die genau an der Stelle ij (i -te Zeile, j -te Spalte) eine 1 und sonst überall eine 0 als Eintrag besitzt, so ist die zu σ gehörende Permutationsmatrix gleich

$$E_\sigma = \sum_{i=1}^n E_{\sigma(i)i}.$$

Diese Matrix ist in gewissem Sinn der Graph der Permutation.

Die Menge der Permutationsmatrizen bilden eine endliche Untergruppe der allgemeinen linearen Gruppe $\text{GL}_n(K)$, und die Zuordnung $\sigma \mapsto E_\sigma$ ist ein

Gruppenisomorphismus zwischen der Permutationsgruppe S_n und dieser endlichen Untergruppe. Nach Beispiel 3.3 operiert die Permutationsgruppe S_n linear auf dem K^n .

DEFINITION 3.5. Es sei K ein Körper und G eine Gruppe, die auf einem K -Vektorraum V linear operiere. Ein Untervektorraum $U \subseteq V$ heißt G -invariant, wenn für alle $\sigma \in G$ und alle $v \in U$ auch $\sigma v \in U$ ist.

Dies kann man auch so ausdrücken, dass jede zu $\sigma \in G$ gehörende Abbildung φ_σ den Unterraum U in sich selbst abbildet. D.h. U ist φ_σ -invariant für jedes $\sigma \in G$. Bei endlichdimensionalem V ist dann sogar stets

$$\varphi_\sigma(U) = U.$$

Die Operation lässt sich in natürlicher Weise auf einen jeden invarianten Unterraum einschränken. Man nennt diese Räume daher auch einfach G -Räume.

DEFINITION 3.6. Es sei K ein Körper und G eine Gruppe, die auf einem K -Vektorraum V linear operiere. Der Untervektorraum

$$\{v \in V \mid \sigma v = v \text{ für alle } \sigma \in G\}$$

heißt der *Fixraum* der Gruppenoperation.

Der Fixraum ist einfach die Menge aller Fixpunkte der Operation. Er ist ein G -invarianter Untervektorraum.

Darstellungstheorie

Eine lineare Operation einer Gruppe auf einem Vektorraum nennt man auch eine Darstellung der Gruppe. In der Darstellungstheorie steht die Frage im Mittelpunkt, auf wie viele (wesentlich verschiedene) Arten eine bestimmte Gruppe auf einem Vektorraum operieren kann. Mit dieser Kenntnis kann man sowohl die Gruppe selbst als auch ihre Operationen besser verstehen.

DEFINITION 3.7. Es sei G eine Gruppe, K ein Körper und V ein (endlichdimensionaler) K -Vektorraum. Einen Gruppenhomomorphismus

$$\rho: G \longrightarrow \text{GL}(V)$$

nennt man eine (endlichdimensionale) *Darstellung* (über K).

Man spricht auch von einer *linearen Darstellung*. Bei $V = K^r$ spricht man auch von einer *Matrix-Darstellung*. Das Bild der Darstellung ist eine Untergruppe der allgemeinen linearen Gruppe. Die Dimension des Vektorraumes V nennt man auch die *Dimension der Darstellung*.

Eine Darstellung von G in $\text{GL}(V)$ ist das gleiche wie eine Operation von G auf V . Die *Darstellungstheorie* einer gegebenen Gruppe beschäftigt sich mit der Menge aller möglichen Darstellungen zu dieser Gruppe.

Eine Darstellung

$$\rho: G \longrightarrow \mathrm{GL}(V)$$

einer Gruppe in einen K -Vektorraum V heißt *treu*, wenn ρ injektiv ist.

Man interessiert sich hauptsächlich für die treuen Darstellungen. Wenn eine Darstellung der Gruppe G nicht treu ist, so besitzt sie einen nichttrivialen Kern $H \subseteq G$, und es ergibt sich nach Satz 5.12 (Körper- und Galoistheorie (Osnabrück 2011)) eine treue Darstellung der Restklassengruppe G/H .

Man unterscheide sorgfältig zwischen abstrakten intrinsischen Eigenschaften einer Gruppe und Eigenschaften, die mit ihrer Einbettung in die allgemeine lineare Gruppe zusammenhängen. Die Eigenschaften einer linearen Operation hängen von beiden ab.

DEFINITION 3.8. Es sei G eine endliche Gruppe und K ein Körper. Unter der *regulären Darstellung* von G versteht man den Gruppenhomomorphismus¹

$$G \longrightarrow \mathrm{GL}(K^G), \sigma \longmapsto (e_\tau \mapsto e_{\sigma\tau}).$$

Diese Darstellung ist die Verknüpfung des injektiven Gruppenhomomorphismus

$$G \longrightarrow \mathrm{Perm}(G), \sigma \longmapsto (\tau \mapsto \sigma\tau),$$

der auch im Satz von Cayley auftaucht, mit dem ebenfalls injektiven Gruppenhomomorphismus, der einer Permutation π auf einer Menge I (die im vorliegenden Fall G ist) ihre lineare, durch $e_i \mapsto e_{\pi(i)}$ festgelegte Realisierung zuordnet. Insbesondere ist die reguläre Darstellung treu, und somit gibt es für jede endliche Gruppe überhaupt eine treue Darstellung. Es lässt sich also jede endliche Gruppe als Untergruppe der Gruppe der invertierbaren Matrizen realisieren, und zwar über jedem Körper.

Charaktere

DEFINITION 3.9. Es sei G ein Monoid und K ein Körper. Dann heißt ein Monoidhomomorphismus

$$\chi: G \longrightarrow (K^\times, 1, \cdot)$$

ein *Charakter* von G in K .

Die Menge der Charaktere von G nach K bezeichnen wir mit $\mathrm{Char}(G, K)$. Mit dem *trivialen Charakter* (also der konstanten Abbildung nach 1) und der Verknüpfung

$$(\chi_1 \cdot \chi_2)(g) := \chi_1(g) \cdot \chi_2(g)$$

¹Hierbei wird durch die Zuordnung $\tau \mapsto \sigma\tau$ eine Permutation auf G definiert; diese gibt die zugehörige lineare Abbildung auf der Standardbasis des K^G vor. Unter K^G verstehen wir die Menge der Abbildungen von G nach K , der isomorph zu $K^{\#(G)}$ ist.

ist $\text{Char}(G, K)$ selbst ein Monoid, und zwar ein Untermonoid des Abbildungsmonoid von G nach K^\times . Da es zu jedem Charakter den inversen Charakter χ^{-1} gibt, der durch

$$\chi^{-1}(g) = (\chi(g))^{-1}$$

definiert ist, bildet $\text{Char}(G, K)$ sogar eine kommutative Gruppe (siehe unten). Ein Charakter einer Gruppe ist nichts anderes als eine eindimensionale Darstellung.

DEFINITION 3.10. Es sei G eine Gruppe und K ein Körper. Dann nennt man die Menge der Charaktere

$$G^\vee := \text{Char}(G, K) = \{\chi : G \rightarrow K^\times \mid \chi \text{ Charakter}\}$$

die *Charaktergruppe* von G (in K).

LEMMA 3.11. Sei G eine Gruppe, K ein Körper und $G^\vee = \text{Char}(G, K)$ die Charaktergruppe zu G . Dann gelten folgende Aussagen.

- (1) G^\vee ist eine kommutative Gruppe.
- (2) Bei einer direkten Gruppenzerlegung $G = G_1 \times G_2$ ist $(G_1 \times G_2)^\vee = G_1^\vee \times G_2^\vee$.

Beweis. Siehe Aufgabe 3.9. □

LEMMA 3.12. Es sei G eine endliche kommutative Gruppe mit dem Exponenten m , und es sei K ein Körper, der eine primitive m -te Einheitswurzel besitzt. Dann sind G und G^\vee isomorphe Gruppen.

Beweis. Nach Lemma 3.11 (2) und Korollar Anhang 4.2 (Körper- und Galoistheorie (Osnabrück 2011)) kann man annehmen, dass $G = \mathbb{Z}/(n)$ eine endliche zyklische Gruppe ist, und dass K eine n -te primitive Einheitswurzel besitzt. Jeder Gruppenhomomorphismus

$$\varphi: G \longrightarrow K^\times$$

ist durch $\zeta = \varphi(1)$ eindeutig festgelegt, und wegen

$$\zeta^n = (\varphi(1))^n = \varphi(n) = \varphi(0) = 1$$

ist ζ eine n -te Einheitswurzel. Umgekehrt kann man zu jeder n -ten Einheitswurzel ζ durch die Zuordnung $1 \mapsto \zeta$ nach Lemma 4.4 (Körper- und Galoistheorie (Osnabrück 2011)) und Satz 5.10 (Körper- und Galoistheorie (Osnabrück 2011)) einen Gruppenhomomorphismus von $\mathbb{Z}/(n)$ nach K^\times definieren. Die Menge der n -ten Einheitswurzeln ist, da eine primitive Einheitswurzel vorhanden ist, eine zyklische Gruppe der Ordnung n . Also gibt es n solche Homomorphismen. Wenn ζ eine primitive Einheitswurzel ist, dann besitzt der durch $1 \mapsto \zeta$ festgelegte Homomorphismus die Ordnung n und ist damit ein Erzeuger der Charaktergruppe, also $(\mathbb{Z}/(n))^\vee \cong \mathbb{Z}/(n)$. □

Darstellungen der zyklischen Gruppe

Eine endliche zyklische Gruppe $\mathbb{Z}/(r)$ lässt sich auf unterschiedliche Weise als Untergruppe der allgemeinen linearen Gruppe $\mathrm{GL}(V)$ bzw. $\mathrm{GL}_n(K)$ auffassen, wie die folgenden Beispiele zeigen.

BEISPIEL 3.13. Es sei K ein Körper, der eine r -te primitive Einheitswurzel ζ besitzt. Dann ist die Untergruppe

$$\mu_r(K) := \{\zeta^i \mid i = 0, 1, \dots, r-1\} \subseteq K^\times$$

eine zyklische Gruppe der Ordnung r . Somit ist die Zuordnung

$$\mathbb{Z}/(r) \longrightarrow K^\times, i \longmapsto \zeta^i,$$

eine (treue) eindimensionale Darstellung (also ein Charakter) einer zyklischen Gruppe.

BEISPIEL 3.14. Es sei K ein Körper und $G = \mathbb{Z}/(r)$. Der Erzeuger 1 operiert auf $\mathbb{Z}/(r)$ durch Addition mit 1, die zugehörige Permutation ist also durch $k \mapsto k+1$ (und $r \mapsto 1$) gegeben. Die zugehörige Permutationsmatrix ist

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}.$$

Somit ist die Zuordnung

$$\mathbb{Z}/(r) \longrightarrow \mathrm{GL}_r(K), i \longmapsto \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}^i,$$

die reguläre Darstellung der zyklischen Gruppe.

BEISPIEL 3.15. Es sei K ein Körper und $\zeta_1, \dots, \zeta_n \in K$ seien Einheitswurzeln. Dann ist

$$\left\{ \begin{pmatrix} \zeta_1^i & 0 & \dots & \dots & 0 \\ 0 & \zeta_2^i & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & \zeta_{n-1}^i & 0 \\ 0 & \dots & \dots & 0 & \zeta_n^i \end{pmatrix} \mid i = 0, 1, \dots \right\},$$

eine zyklische Untergruppe der allgemeinen linearen Gruppe $GL_n(K)$. Ihre Ordnung ist das kleinste gemeinsame Vielfache (nennen wir es r) der Ordnungen der ζ_j . Die Zuordnung

$$\mathbb{Z}/(r) \longrightarrow GL_n(K), i \longmapsto \begin{pmatrix} \zeta_1^i & 0 & \cdots & \cdots & 0 \\ 0 & \zeta_2^i & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \zeta_{n-1}^i & 0 \\ 0 & \cdots & \cdots & 0 & \zeta_n^i \end{pmatrix},$$

ist eine n -dimensionale Darstellung einer zyklischen Gruppe.

BEISPIEL 3.16. Es sei K ein Körper, der eine r -te primitive Einheitswurzel ζ besitzt. Dann ist die Untergruppe

$$\left\{ \begin{pmatrix} \zeta^i & 0 \\ 0 & \zeta^{-i} \end{pmatrix} \mid i = 0, 1, \dots, r-1 \right\},$$

der speziellen linearen Gruppe $SL_2(K)$ eine zyklische Gruppe der Ordnung r ist. Die Zuordnung

$$\mathbb{Z}/(r) \longrightarrow SL_2(K), i \longmapsto \begin{pmatrix} \zeta^i & 0 \\ 0 & \zeta^{-i} \end{pmatrix},$$

ist eine zweidimensionale Darstellung einer zyklischen Gruppe.

BEISPIEL 3.17. Eine jede invertierbare Matrix $M \in GL_n(K)$ endlicher Ordnung über einem Körper K erzeugt eine endliche zyklische Untergruppe der allgemeinen linearen Gruppe. Ihre Determinante muss eine Einheitswurzel sein, deren Ordnung die Ordnung der Matrix teilt. Auch die Eigenwerte einer solchen Matrix müssen Einheitswurzeln sein. Wie das reelle Beispiel $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ zeigt, muss eine Matrix endlicher Ordnung weder diagonalisierbar noch trigonalisierbar sein. Über einem endlichen Körper besitzt jede invertierbare Matrix eine endliche Ordnung.

BEISPIEL 3.18. Es sei K ein Körper der positiven Charakteristik $p > 0$. Dann bilden die Matrizen

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{Z}/(p) \right\}$$

eine zyklische Untergruppe der $SL_2(K)$ mit p Elementen.

SATZ 3.19. *Es sei K ein algebraisch abgeschlossener Körper der Charakteristik 0. Dann ist jede invertierbare Matrix $M \in GL_n(K)$, die endliche Ordnung besitzt, diagonalisierbar.*

Beweis. Die Matrix ist trigonalisierbar und besitzt eine jordanische Normalform. Wir zeigen, dass die einzelnen Jordanblöcke

$$\begin{pmatrix} \lambda & 1 & 0 & \cdots & \cdots & 0 \\ 0 & \lambda & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \lambda & 1 & 0 \\ 0 & \cdots & \cdots & 0 & \lambda & 1 \\ 0 & \cdots & \cdots & \cdots & 0 & \lambda \end{pmatrix}$$

trivial sind. Wegen der endlichen Ordnung muss λ eine Einheitswurzel sein. Durch Multiplikation mit $\lambda^{-1}E_n$ können wir davon ausgehen, dass eine Matrix der Form

$$\begin{pmatrix} 1 & a & 0 & \cdots & \cdots & 0 \\ 0 & 1 & a & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & a & 0 \\ 0 & \cdots & \cdots & 0 & 1 & a \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

(mit $a \neq 0$) vorliegt. Wenn dies keine 1×1 -Matrix ist, so gibt es zwei Vektoren u, v , wobei u ein Eigenvektor ist und v auf $v + au$ abgebildet wird. Die k -te Iteration der Matrix schiebt dann v auf $v + kau$ und wegen Charakteristik 0 ist dies nicht v , im Widerspruch zur endlichen Ordnung. \square

KOROLLAR 3.20. *Es sei K ein algebraisch abgeschlossener Körper der Charakteristik 0. Dann ist jede Darstellung einer endlichen zyklischen Gruppe $\mathbb{Z}/(r)$ in $\mathrm{GL}_n(K)$ in einer geeigneten Basis von der Form*

$$\mathbb{Z}/(r) \longrightarrow \mathrm{GL}_n(K), i \longmapsto \begin{pmatrix} \zeta_1^i & 0 & \cdots & \cdots & 0 \\ 0 & \zeta_2^i & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \zeta_{n-1}^i & 0 \\ 0 & \cdots & \cdots & 0 & \zeta_n^i \end{pmatrix},$$

mit gewissen Einheitswurzeln ζ_j .

Beweis. Dies folgt unmittelbar aus Satz 3.19. \square