Algebra leicht*er* gemacht

Lösungsvorschläge zu Aufgaben des Ersten Staatsexamens für das Lehramt an Gymnasien

von
Martina Kraupner

Oldenbourg Verlag München

Die Collage auf dem Cover zeigt Porträts des französischen Mathematikers Évariste Galois, erstellt von Kevin Danz, Philip Junk, Benedikt Meßmer, Cornelia Oczycz, Franziska Schmitt und Tobias Schulz.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Rosenheimer Straße 145, D-81671 München
Telefon: (089) 45051-0
www.oldenbourg-verlag.de

Lektorat: Kathrin Mönch
Herstellung: Constanze Müller
Einbandgestaltung: hauser lacour
Gesamtherstellung: Grafik + Druck, München

Dieses Papier ist alterungsbeständig nach DIN/ISO 9706.

ISBN 978-3-486-70544-7

Vorwort

Dieses Buch richtet sich in erster Linie an alle Studenten des gymnasialen Lehramts im Fach Mathematik in Bayern. Auch Nichtbayern und Nichtlehrämtler, die den Stoff der Grundvorlesungen der Algebra vertiefen wollen, sind eingeladen, sich mit den ausführlichen Lösungen zu 175 Aufgaben aus dem Bayerischen Staatsexamen zur Algebra (und Zahlentheorie) zu beschäftigen.

Erfahrungsgemäß fällt es Studenten am Anfang ihrer Vorbereitungsphase auf das Staatsexamen sehr schwer, Prüfungsaufgaben eigenständig zu lösen. Die Algebra-Vorlesungen liegen häufig bereits einige Semester zurück, Zulassungsarbeit und erziehungswissenschaftliches Staatsexamen haben die Beschäftigung mit Algebra in den Hintergrund rücken lassen. Einige wenige arbeiten sich spielend wieder in die Inhalte der Vorlesung ein und sind schnell in der Lage, Aufgaben zu lösen. Den meisten aber erscheint der Berg, den es zu besteigen gilt, schier unbezwingbar. Für die Einen wie die Anderen ist dieses Übungsbuch gedacht.

Die Lösungsvorschläge für die Prüfungstermine Herbst 2003 bis Herbst 2009 wurden während der vergangenen Semester im Zuge der Staatsexamens-Tutorien an der Universität Passau erstellt. Sie sollten nicht als Musterlösungen verstanden werden, denn an einigen Stellen ist die Beantwortung viel ausführlicher, als es im Staatsexamen verlangt wird. Vielmehr wurde versucht, die Lösungen so aufzubereiten, dass sie auch für Studenten, die am Anfang ihrer Lernphase stehen, verständlich sind. Ich hoffe, das ist gelungen, und wünsche allen, die mit diesem Buch lernen, besonders viel Erfolg im Examen.

Mein herzlichster Dank geht an Markus Kriegl, Philipp Jovanovic und Bettina Kreuzer für die hervorragende und wertvolle Korrekturarbeit an diesem Buch. Ich danke meinem wunderbaren Bürokollegen Thomas Stadler, der mir in vielen Dingen eine unschätzbare Hilfe war. Vielen Dank an Prof. Dr. Martin Kreuzer für die Betreuung in den letzten drei Jahren und die rettenden Ideen bei Aufgaben, an denen ich mir fast die Zähne ausgebissen hätte. Ebenso danke ich Herrn Peter-Paul Rast und dem Leistungskurs Kunst des Gymnasiums Neubiberg für die wunderschönen Porträts des Evariste Galois, Stefan Schuster und allen Mitarbeitern des Lehrstuhls für Symbolic Computation der Universität Passau und den vielen engagierten Studenten der Tutorien der letzten Semester.

Martina Kraupner

Inhaltsverzeichnis

Themenverzeichnis

Gruppen

Sylow-Gruppen

Gruppenoperationen

Permutationsgruppen und Diedergruppen

Direkte und semidirekte Produkte

Sonstiges

Ringe

Euklidische Ringe

Faktorielle Ringe

Chinesischer Restsatz

Irreduzibilität von Polynomen

Sonstiges

Körper

Endliche Körper

Galoistheorie

Zahlentheorie

Konstruktionen mit Zirkel und Lineal

Lineare Algebra

Teil I.

Grundlagen

In diesem ersten Teil sind alle Definitionen und Sätze formuliert, deren Kenntnis in den vergangenen Jahren zur Lösung der Examensaufgaben notwendig und hilfreich war. Dabei wurden die Sätze häufig nicht in ihrer allgemeinsten Fassung, sondern so aufgeschrieben, wie sie in den in Teil II vorgestellten Lösungsvorschlägen verwendet werden.

Diese Grundlagen sollten zum größten Teil aus den Vorlesungen bekannt sein. Sie sind ohne weitere Erklärungen und anschauliche Beispiele aufgeführt. Sollte das Verständnis einer Auffrischung bedürfen, wird hier auf die Literaturvorschläge (Seite 293) verwiesen.

Sicherlich gibt es in der Algebra noch viele andere schöne Sätze und interessante Themen. Es kann auch nicht ausgeschlossen werden, dass diese in den kommenden Prüfungsterminen eine Rolle spielen. Die Sammlung erhebt insofern keinerlei Anspruch auf Vollständigkeit. Trotzdem kann wohl davon ausgegangen werden, dass ein Großteil der üblicherweise im Examen abgefragten Grundlagen von dieser Zusammenstellung abgedeckt wird.

Der erste Teil gliedert sich in sechs Kapitel zu sechs Themenblöcken, die sich inhaltlich gut voneinander abgrenzen lassen. Es empfiehlt sich, die Lernphase gemäß dieser Themenblöcke zu organisieren. Die zugehörigen Aufgaben sind im Themenverzeichnis (Seite xiii) aufgeführt.

1. Gruppen

Definition 1.1 Eine nichtleere Menge G zusammen mit einer Abbildung $\circ : G \times G \to G$ heißt eine **Gruppe**, falls gilt:

i) Für alle $g, h, l \in G$ ist $g \circ (h \circ l) = (g \circ h) \circ l$.

ii) Es existiert ein $e \in G$, so dass $e \circ g = g = g \circ e$ für alle $g \in G$ gilt.

iii) Zu jedem $g \in G$ existiert ein $h \in G$ mit $g \circ h = e$.

Ist nur i) erfüllt, so heißt G eine **Halbgruppe**.

Gilt zusätzlich

iv) $g \circ h = h \circ g$ für alle $g, h \in G$,

so heißt $(G, \circ)$ eine **kommutative** oder **abelsche** Gruppe.

Definition 1.2 Ist $(G, \circ)$ eine Gruppe, so heißt das Element $e \in G$, für das $e \circ g = g = g \circ e$ für alle $g \in G$ gilt, **neutrales Element** von G. Für $g \in G$ heißt das Element $h \in G$, für das $g \circ h = e$ gilt, das **zu** g **inverse Element** oder **Inverses von** g und wird mit g^{-1} bezeichnet.

Definition 1.3 Eine nichtleere Teilmenge U einer Gruppe G heißt **Untergruppe** von G, falls $g \circ h^{-1} \in U$ für alle $g, h \in U$ gilt.

Definition 1.4 Eine Untergruppe U einer Gruppe G heißt **maximale Untergruppe** von G, falls für alle Untergruppen $V \subseteq G$, die $U \subseteq V$ erfüllen, $U = V$ oder $V = G$ gilt.

Definition 1.5 Die Anzahl der Elemente einer Gruppe G heißt **Ordnung** von G und wird mit $|G|$ bezeichnet. Ist $|G| < \infty$, so heißt G **endlich**.

Definition 1.6 Seien $(G, \cdot)$ und $(H, \circ)$ Gruppen. Ein **Gruppenhomomorphismus** ist eine Abbildung $\varphi : G \to H$, die $\varphi(x \cdot y) = \varphi(x) \circ \varphi(y)$ für alle $x, y \in G$ erfüllt.

Definition 1.7 Ein Gruppenhomomorphismus $\varphi : G \to H$ heißt

i) **Endomorphismus**, falls $H = G$ gilt.

ii) **Isomorphismus**, falls φ bijektiv ist.

iii) **Automorphismus**, falls $H = G$ gilt und φ bijektiv ist.

Definition 1.8 Die identische Abbildung $\mathrm{id} : G \to G$ mit $\mathrm{id}(x) = x$ wird auch **trivialer Automorphismus** genannt.

Definition 1.9 Zwei Gruppen G und H heißen **isomorph**, falls es einen Isomorphismus $\varphi : G \to H$ gibt. Wir schreiben dann $G \cong H$.

Definition 1.10 Ist $\varphi : G \to H$ ein Gruppenhomomorphismus und e das neutrale Element von H, so heißt $\{g \in G \mid \varphi(g) = e\}$ der **Kern** von φ und wird mit $\ker(\varphi)$ oder auch $\mathrm{Kern}(\varphi)$ bezeichnet.
Die Menge $\{h \in H \mid \varphi(x) = h \text{ für ein } x \in G\}$ heißt das **Bild** von φ und wird mit $\mathrm{Bild}(\varphi)$ oder auch $\mathrm{im}(\varphi)$ bezeichnet.
Ist X eine Teilmenge von H, so heißt die Menge $\{g \in G \mid \varphi(g) \in X\}$ das **Urbild von** X unter φ und wird mit $\varphi^{-1}(X)$ bezeichnet.

Satz 1.11 Ein Gruppenhomomorphismus $\varphi : G \to H$ ist genau dann injektiv, wenn der Kern von φ nur aus dem neutralen Element von G besteht.

Satz 1.12 Sei G eine endliche Gruppe und $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann ist $\mathrm{im}(\varphi)$ eine Untergruppe von H, $\ker(\varphi)$ eine Untergruppe von G und es gilt $|G| = |\mathrm{im}(\varphi)| \cdot |\ker(\varphi)|$.

Satz 1.13 Sei $\varphi : G \to H$ ein Gruppenhomomorphismus, sei e_G das neutrale Element von G und e_H das neutrale Element von H. Dann ist $\varphi(e_G) = e_H$ und das zu einem Element $g \in G$ inverse Element g^{-1} wird durch φ auf das Inverse des Bildes von g abgebildet.

Definition 1.14 Sei G eine Gruppe und X eine nichtleere Teilmenge von G. Die Menge

$$\langle X \rangle := \{x_1 \cdot \ldots \cdot x_l \mid l \in \mathbb{N}, x_i \in X \vee x_i^{-1} \in X, 1 \leq i \leq l\}$$

ist eine Untergruppe von G und heißt **die von X erzeugte Untergruppe**. Ist U eine Untergruppe von G und X eine Teilmenge von G mit $U = \langle X \rangle$, so heißt X ein **Erzeugendensystem von** U.

Definition 1.15 Sei G eine Gruppe. Die Untergruppe $\langle \{ghg^{-1}h^{-1} \mid g, h \in G\} \rangle$ heißt **Kommutatorgruppe von** G.

Satz 1.16 Sei G eine Gruppe und X ein Erzeugendensystem von G.

a) Gilt $ab = ba$ für alle $a, b \in X$, so ist G abelsch.

b) Stimmen zwei Gruppenhomomorphismen $\varphi, \psi : G \to H$ auf X überein, so gilt $\varphi = \psi$.

1.1. Zyklische Gruppen

Definition 1.17 Sei G eine Gruppe und g ein Element in G. Die Ordnung der von $\{g\}$ erzeugten Untergruppe heißt **Ordnung von** g. Man schreibt dafür $\mathrm{ord}(g)$. Die von $\{g\}$ erzeugte Untergruppe wird mit $\langle g \rangle$ bezeichnet. Falls es ein $g \in G$ gibt mit $G = \langle g \rangle$, heißt G **zyklisch**.

Satz 1.18 Sei G eine Gruppe mit neutralem Element e und sei $g \in G$. Gibt es ein $a \in \mathbb{N} \setminus \{0\}$ mit $g^a = e$, so ist $\mathrm{ord}(g)$ ein Teiler von a.

Satz 1.19 Ist p eine Primzahl und G eine Gruppe der Ordnung p, so ist G zyklisch.

Satz 1.20 Untergruppen zyklischer Gruppen sind zyklisch.

Satz 1.21 Ist $G = \langle z \rangle$ eine zyklische Gruppe der Ordnung $n \in \mathbb{N}$, so ist

$$\begin{array}{rcl} \varphi : \mathbb{Z}/n\mathbb{Z} & \to & G \\ a + (n) & \mapsto & z^a \end{array}$$

ein Isomorphismus von Gruppen. Bis auf Isomorphie gibt es also genau eine zyklische Gruppe der Ordnung $n \in \mathbb{N}$.

Satz 1.22 Zyklische Gruppen sind abelsch.

Definition 1.23 Sei $n \in \mathbb{N}$. Die Anzahl der zu n teilerfremden Zahlen $m \in \mathbb{N}$ mit $1 \leq m \leq n$ wird mit $\varphi(n)$ bezeichnet. Die Funktion $\varphi : \mathbb{N} \to \mathbb{N}$, $n \mapsto \varphi(n)$ heißt **Eulersche Phi-Funktion**.

Satz 1.24 Sei φ die Eulersche Phi-Funktion.

a) Für eine Primzahl p und eine natürliche Zahl $k > 0$ gilt

$$\varphi(p^k) = p^k - p^{k-1}.$$

b) Für die Primfaktorzerlegung einer natürlichen Zahl $n = p_1^{k_1} \cdots p_l^{k_l}$ gilt

$$\varphi(n) = \varphi(p_1^{k_1}) \cdots \varphi(p_l^{k_l}).$$

c) Es gilt die Summenformel

$$n = \sum_{d|n, d \geq 1} \varphi(d).$$

Satz 1.25 Sei G eine zyklische Gruppe der Ordnung $n \in \mathbb{N}$ und φ die Eulersche Phi-Funktion. Dann hat G genau $\varphi(n)$ erzeugende Elemente, also $\varphi(n)$ Elemente der Ordnung n.

Satz 1.26 Sei G eine endliche Gruppe. Ist G abelsch, so gibt es zu jedem Teiler der Gruppenordnung eine Untergruppe dieser Ordnung. Ist G zyklisch, so gibt es zu jedem Teiler der Gruppenordnung genau eine Untergruppe dieser Ordnung.

Definition 1.27 Sei G eine Gruppe. Die Menge aller Automorphismen auf G mit der Hintereinanderausführung als Verknüpfung ist eine Gruppe und heißt **Automorphismengruppe** von G. Sie wird mit $\mathrm{Aut}(G)$ bezeichnet.

Satz 1.28 Die Automorphismengruppe der zyklischen Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ ist isomorph zur Einheitengruppe des Rings $\mathbb{Z}/n\mathbb{Z}$ (vgl. 2.11).

Satz 1.29 Seien $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$. Dann gilt

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/(m \cdot n)\mathbb{Z}.$$

Satz 1.30 (**Hauptsatz über endliche abelsche Gruppen)**
Sei G eine endliche abelsche Gruppe. Dann gibt es zyklische Untergruppen $Z_1, \ldots, Z_r$ von G mit $G \cong Z_1 \times \ldots \times Z_r$. Die Ordnungen der Z_i sind Primzahlpotenzen. Die Anzahl der zyklischen Untergruppen einer gegebenen Ordnung ist dabei eindeutig bestimmt.

1.2. Normalteiler und Faktorgruppen

Definition 1.31 Sei G eine Gruppe und U eine Untergruppe von G. Die Menge $gU := \{gu \mid u \in U\}$ heißt **Linksnebenklasse von g bezüglich** U. Die Menge $Ug := \{ug \mid u \in U\}$ heißt **Rechtsnebenklasse von g bezüglich** U. Die Anzahl der Linksnebenklassen ist gleich der Anzahl der Rechtsnebenklassen bezüglich U und heißt **Index von U in G**. Der Index wird mit $[G : U]$ bezeichnet.

Definition 1.32 Sei Y eine endliche Menge, seien $X_1, \ldots, X_n$ Teilmengen von Y. Man sagt, $X_1, \ldots, X_n$ bilden eine **Partition** von Y, falls die Teilmengen paarweise disjunkt sind und $Y = X_1 \cup \ldots \cup X_n$ gilt.

Satz 1.33 Sei G eine endliche Gruppe und U eine Untergruppe von G. Dann bilden die Rechtsnebenklassen (bzw. die Linksnebenklassen) von U eine Partition von G.

Satz 1.34 (**Lagrange)**
Ist U Untergruppe einer endlichen Gruppe G, dann gilt $|G| = [G : U] \cdot |U|$.

Definition 1.35 Sei G eine Gruppe und U eine Teilmenge von G. Die Menge U heißt **Normalteiler** von G, wenn U eine Untergruppe von G ist und eine der folgenden äquivalenten Bedingungen erfüllt ist:

i) Für alle $g \in G$ gilt $gUg^{-1} \subseteq U$.

ii) Für alle $g \in G$ gilt $gUg^{-1} = U$.

iii) Für alle $g, h \in G$ gilt $(gU)(hU) = ghU$.

iv) Für alle $g \in G$ gilt $gU = Ug$.

Satz 1.36 Jede Gruppe G hat mindestens zwei Normalteiler, nämlich $\{e\}$ und G. Diese beiden Normalteiler werden als triviale Normalteiler bezeichnet.

Satz 1.37 Ist G eine abelsche Gruppe, so ist jede Untergruppe von G Normalteiler von G.

Satz 1.38 Ist N Normalteiler einer Gruppe G, so bilden die Nebenklassen von N mit der Verknüpfung

$$(gN)(hN) = ghN$$

eine Gruppe. Sie heißt **Faktorgruppe von G modulo N** und wird mit G/N bezeichnet.

Satz 1.39 Sei G eine endliche Gruppe und N ein Normalteiler von G. Dann gilt $|G| = |N| \cdot |G/N|$.

Definition 1.40 Sei G eine Gruppe und N ein Normalteiler von G. Dann ist die Abbildung $\varepsilon : G \to G/N$ definiert durch $g \mapsto gN$ ein surjektiver Homomorphismus. Er heißt der **kanonische Epimorphismus** von G auf G/N.

Definition 1.41 Eine Gruppe G, die keine Normalteiler außer $\{e\}$ und G hat, heißt **einfach**.

Satz 1.42 Sei G eine Gruppe und $(N_i)_{i \in I}$ eine Familie von Normalteilern von G. Dann ist $\bigcap_{i \in I} N_i$ ein Normalteiler von G.

Satz 1.43 Sei G eine Gruppe und U eine endliche Untergruppe von G. Ist U die einzige Untergruppe der Ordnung $|U|$ von G, dann ist U ein Normalteiler von G.

Satz 1.44 Sei G eine endliche Gruppe und U eine Untergruppe von G. Ist U vom Index 2 in G, dann ist U ein Normalteiler von G.
Allgemeiner gilt: Ist p der kleinste Primteiler von $|G|$ und U eine Untergruppe vom Index p in G, dann ist U ein Normalteiler von G.

Satz 1.45 Sei G eine endliche Gruppe und U eine echte Untergruppe von G. Ist $|G|$ kein Teiler von $[G : U]!$, so besitzt G einen nichttrivialen Normalteiler, ist also nicht einfach.

Definition 1.46 Sei G eine Gruppe und X eine nichtleere Teilmenge von G. Die Menge $N_G(X) := \{g \in G \mid gXg^{-1} = X\} = \{g \in G \mid gX = Xg\}$ heißt **Normalisator** von X in G.

Satz 1.47 Sei G eine Gruppe. Für eine Teilmenge X von G ist $N_G(X)$ eine Untergruppe von G. Für eine Untergrupppe U ist $N_G(U)$ die größte Untergruppe von G, von der U Normalteiler ist. Für einen Normalteiler N von G ist $N_G(N) = G$.

Definition 1.48 Sei G eine Gruppe. Für eine nichtleere Teilmenge X und eine Untergruppe H von G heißt $Z_H(X) := \{g \in H \mid gx = xg \text{ für alle } x \in X\}$ **Zentralisator** von X in H und $Z(G) := \{g \in G \mid gh = hg \text{ für alle } h \in G\}$ heißt **Zentrum** von G. Das Zentrum heißt **trivial**, wenn $Z(G) = \{e\}$ gilt.

Satz 1.49 Sei G ein Gruppe. Für eine Teilmenge X und eine Untergruppe H von G ist der Zentralisator $Z_H(X)$ eine Untergruppe von G. Das Zentrum von G ist ein Normalteiler von G.

Satz 1.50 Sei $\varphi : G \to H$ ein Gruppenhomomorphismus.

a) Ist U eine Untergruppe von G, so ist $\varphi(U)$ eine Untergruppe von H. Ist $U = \langle X \rangle$, so ist $\varphi(U) = \langle \varphi(X) \rangle$.

b) Ist V eine Untergruppe von H, so ist $\varphi^{-1}(V)$ eine Untergruppe von G.

c) Ist φ surjektiv und N ein Normalteiler von G, so ist $\varphi(N)$ ein Normalteiler von H.

d) Ist N ein Normalteiler von H, so ist $\varphi^{-1}(N)$ ein Normalteiler von G.

e) Der Kern von φ ist ein Normalteiler von G.

Satz 1.51 (**Universelle Eigenschaft der Faktorgruppe**)
Sei $\varphi : G \to H$ ein Gruppenhomomorphismus und sei N ein Normalteiler von G mit $N \subseteq \ker(\varphi)$. Dann gibt es genau einen Homomorphismus $\overline{\varphi} : G/N \to H$ mit $\overline{\varphi} \circ \varepsilon = \varphi$, wobei $\varepsilon : G \to G/N$ den kanonischen Epimorphismus von G auf G/N bezeichne.

Satz 1.52 (**Homomorphiesatz**)
Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann ist

$$\begin{aligned} \overline{\varphi} : G/\ker(\varphi) &\to H \\ g\ker(\varphi) &\mapsto \varphi(g) \end{aligned}$$

injektiv. Insbesondere ist $G/\ker(\varphi) \cong \mathrm{im}(\varphi)$.

Satz 1.53 (**Erster Isomorphiesatz**)
Sei G eine Gruppe, H eine Untergruppe und N ein Normalteiler von G. Dann ist HN eine Untergruppe von G mit Normalteiler N und $H \cap N$ ist ein Normalteiler von H. Weiter ist $H/(H \cap N) \cong HN/N$.

Satz 1.54 (**Zweiter Isomorphiesatz**)
Sei G eine Gruppe und seien N, H Normalteiler von G mit $N \subseteq H$. Dann ist N ein Normalteiler von H, H/N ein Normalteiler von G/N und es gilt $(G/N)/(H/N) \cong G/H$.

Satz 1.55 (**Dritter Isomorphiesatz**)
Sei $\varphi : G \to H$ ein Gruppenhomomorphismus, M ein Normalteiler von H und $N := \varphi^{-1}(M)$. Dann gibt es einen injektiven Homomorphismus $\Phi : G/N \to H/M$. Falls φ surjektiv ist, ist Φ ein Isomorphismus.

Satz 1.56 (**Korrespondenzsatz**)
Sei G eine Gruppe und N ein Normalteiler von G. Die Untergruppen (bzw. Normalteiler) von G/N entsprechen bijektiv den Untergruppen (bzw. Normalteilern) von G, die N enthalten. Der zugehörige Isomorphismus ist der kanonische Epimorphismus $\varepsilon : G \to G/N$.

Definition 1.57 Eine endliche Gruppe G heißt **auflösbar**, wenn es Untergruppen $U_0, \ldots, U_l$ von G gibt, für die gilt:

i) $G = U_0 \supset U_1 \supset \ldots \supset U_l = \{e\}$,

ii) U_{i+1} ist ein Normalteiler von U_i für $i = 0, \ldots, l-1$ und

iii) U_i/U_{i+1} ist abelsch für alle $i = 0, \ldots, l-1$.

Satz 1.58 Abelsche Gruppen sind auflösbar.

Satz 1.59 Ist eine Gruppe G auflösbar, so ist jede Untergruppe und jede Faktorgruppe von G auflösbar.

Satz 1.60 Sei N ein Normalteiler einer Gruppe G. Die Gruppe G ist genau dann auflösbar, wenn N und G/N auflösbar sind.

1.3. Gruppenoperationen

Definition 1.61 Sei G eine Gruppe und M eine Menge. Man sagt, G **operiert auf** M **mittels** γ, falls es eine Abbildung $\gamma : G \times M \to M$ gibt, für die gilt:

i) $\gamma(e_G, m) = m$ für alle $m \in M$;

ii) $\gamma(g, \gamma(h, m)) = \gamma(gh, m)$ für alle $g, h \in G$ und $m \in M$.

Eine solche Abbildung heißt **(Gruppen-)Operation** von G auf M.

Satz 1.62 Die Gruppenoperationen $G \times M \to M$ entsprechen bijektiv den Gruppenhomomorphismen $G \to S_M$. Genauer gilt:

a) Ist $\gamma : G \times M \to M$ eine Gruppenoperation, so ist

$$\begin{aligned} \varphi : G &\to S_M \\ g &\mapsto \gamma_g \end{aligned}$$

mit $\gamma_g : M \to M, m \mapsto \gamma(g, m)$ ein Gruppenhomomorphismus.

b) Ist $\varphi : G \to S_M$ ein Gruppenhomomorphismus, so definiert

$$\begin{aligned} \gamma : G \times M &\to M \\ (g, m) &\mapsto \varphi(g)(m) \end{aligned}$$

eine Gruppenoperation von G auf M.

Definition 1.63 Man spricht von einer trivialen Operation $G \times M \to M$, wenn $(g, m) \mapsto m$ für alle $(g, m) \in G \times M$ gilt, also wenn der zur Operation gehörige Gruppenhomomorphismus $G \to S_M$ konstant ist.

Satz 1.64 (**Satz von Cayley**)
Jede endliche Gruppe der Ordnung n ist isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.

Definition 1.65 Sei G eine Gruppe, M eine Menge und $\gamma : G \times M \to M$ eine Gruppenoperation.

a) Für $m \in M$ heißt $B_m = \{\gamma(g, m) \mid g \in G\}$ die **Bahn von** m unter γ.

b) Die Operation γ heißt **transitive Operation**, falls es nur eine Bahn gibt, d.h. falls $B_m = M$ für alle $m \in M$ gilt.

c) Für $m \in M$ ist die Menge $G_m = \{g \in G \mid \gamma(g, m) = m\}$ eine Untergruppe von G. Sie heißt **Fixgruppe** oder **Stabilisator von** m.

Satz 1.66
Sei G eine endliche Gruppe und $\gamma : G \times M \to M$ eine Gruppenoperation. Für alle $m \in M$ gilt $|G| = |B_m| \cdot |G_m|$.

Satz 1.67 (**Bahnengleichung**)
Eine Gruppe G operiere auf einer Menge M durch γ. Seien $B_{m_1}, \ldots, B_{m_l}$ die verschiedenen Bahnen unter γ. Dann bilden die Bahnen $B_{m_1}, \ldots, B_{m_l}$ eine Partition von M und es gilt $|M| = \sum_{j=1}^{l} |B_{m_j}|$.

Satz 1.68 Eine Gruppe G operiert genau dann transitiv auf einer Menge M durch γ, wenn es für alle $m_1, m_2 \in M$ ein $g \in G$ gibt mit $\gamma(g, m_1) = m_2$.