LinA 2
Algebraische Strukturen
Anton Deitmar
Sommer 25

Inhaltsverzeichnis

1 Gruppen **1**
1.1 Permutationen . . . 1
1.2 Ordnung . . . 2
1.3 Nebenklassen . . . 5
1.4 Homomorphismen und Operationen . . . 7
1.5 Zyklische Gruppen . . . 12
1.6 Normalteiler . . . 13

1 Gruppen

1.1 Permutationen

Für eine beliebige Menge M bezeichnen wir mit $\mathrm{Per}(M)$ die Gruppe der **Permutationen** von M, d.h., die Menge aller bijektiven Abbildungen $\sigma : M \to M$ mit der Hintereinanderausführung als Gruppenmultiplikation. Für eine natürliche Zahl n sei dann $\mathrm{Per}(n)$ die Gruppe $\mathrm{Per}(\{1,\dots,n\})$. Wir nennen $\mathrm{Per}(n)$ auch die Gruppe der Permutationen in n Buchstaben.

Die Elemente der Permutationsgruppe $\mathrm{Per}(n)$ schreibt man zB in der Form $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, wobei wir das Bild jeweils unter das Element schreiben, also in diesem Beispiel $\tau(1) = 2$, $\tau(2) = 3$ und $\tau(3) = 1$. Eine andere Schreibweise für dasselbe Element ist die **Zykelschreibweise**:

$$\tau = (1,2,3)$$

was soviel bedeutet wie 1 geht auf 2 geht auf 3 geht auf 1. Das Element, das 1 und 2 vertauscht, schreibt sich dann als $(1,2)$. Nicht jedes Element von $\mathrm{Per}(n)$ ist als ein einziger Zykel schreibbar, so ist zum Beispiel in $\mathrm{Per}(4)$ das Element $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ in der Zykelschreibweise gleich

$$(1,2)(3,4).$$

Definition 1.1.1. Ein **Zykel** in $\mathrm{Per}(n)$ ist ein Tupel $(j_1, j_2, \dots, j_r)$, $r \geq 2$ von verschiedenen natürlichen Zahlen $1 \leq j_1, j_2, \dots, j_r \leq n$. Ein Zykel repräsentiert eine Permutation, die j_ν auf $j_{\nu+1}$ und j_r auf j_1 wirft und alle anderen Zahlen festhält. Der Zykel $(j_1,\dots,j_r)$ repräsentiert dieselbe Permutation wie der Zykel $(j_2, j_3, \dots, j_r, j_1)$, deshalb kann man den Zykel stets durch einen ersetzen, für den j_1 die kleinste der Zahlen $j_1,\dots,j_k$ ist. Ein Zykel in dieser Form heisst **kanonisch**.

Zwei Zykel $(j_1,\dots,j_k)$ und $(i_1,\dots,i_s)$ heissen **disjunkt**, falls sie keine gemeinsamen Zahlen haben, also falls

$$\{j_1,\dots,j_k\} \cap \{i_1,\dots,i_s\} = \varnothing.$$

Beispiel 1.1.2. Wir schreiben die Permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 7 & 5 & 2 & 4 & 3 \end{pmatrix}$ als Produkt kanonischer Zykel:

$$(2,6,4,5)(3,7).$$

Satz 1.1.3.

(a) *Zwei kanonische Zykel stellen genau dann dieselbe Permutation dar, wenn sie gleich sind.*

(b) *Zwei disjunkte Zykel, aufgefasst als Elemente von* $\mathrm{Per}(n)$*, kommutieren miteinander.*

(c) *Jede Permutation* $\neq \mathrm{Id}$ *in* $\mathrm{Per}(n)$ *lässt sich als Produkt paarweise disjunkter kanonischer Zykel schreiben, diese sind eindeutig bestimmt bis auf die Reihenfolge.*

Beweis. (a) Seien $(j_1, j_2, \ldots, j_r)$ und $(i_1, i_2, \ldots, i_s)$ zwei kanonische Zykel, die dieselbe Permutation γ darstellen. Dann ist j_1 das kleinste Element von $\{1, \ldots, n\}$, das von γ überhaupt vertauscht wird und dasselbe gilt von i_1, also folgt $j_1 = i_1$. Ferner ist $j_2 = \gamma(j_1) = \gamma(i_1) = i_2$ und so weiter.

(b) Sei $\gamma = (j_1, \ldots, j_k)$ ein Zykel in $\mathrm{Per}(n)$ und sei $\tau \in \mathrm{Per}(n)$. Es gilt dann

$$\tau\gamma\tau^{-1} = (\tau(j_1), \ldots, \tau(j_k)).$$

Ist $\tau = (i_1, \ldots, i_s)$ auch ein Zykel, dann sind die $i_1, \ldots, i_s$ genau die Zahlen, die von τ überhaupt verändert werden. Ist also τ zu γ disjunkt, so folgt $\tau\gamma\tau^{-1} = \gamma$.

(c) Wir geben ein Verfahren zum Finden der Zykel zu einem gegebenen $\gamma \in \mathrm{Per}(n)$. Sei j_1 die kleinste Zahl in $\{1, \ldots, n\}$, die von γ überhaupt verändert wird. Sei dann $j_2 = \gamma(j_1)$ und so weiter. Die Folge $j_1, j_2, \ldots$ kann nicht unendlich sein, also gibt es ein kleinstes $k \in \mathbb{N}$ und zu diesem ein kleinstes $s \in \mathbb{N}$ so dass $j_{k+s} = j_k$ gilt. Das heisst also $\gamma(j_{k+s-1}) = j_k$. Ist $k > 1$, so gilt aber auch $\gamma(j_{k-1}) = j_k$, woraus aber $j_{k+s-1} = j_{k-1}$ folgt, was der Minimalität von k widerspricht. Es ist also $k = 1$ und damit ist $\alpha = (j_1, \ldots, j_s)$ ein Zykel, der die Zahlen $(j_1, \ldots, j_s)$ genauso abbildet wie γ, so dass $\alpha^{-1}\gamma$ sie alle festhält. Dieser ist dann gleich e oder nicht, in welchem Fall wir das Verfahren wiederholen und einen zweiten Zykel β finden, der disjunkt zu α ist und so weiter. Das Verfahren bricht wegen Endlichkeit des Problems ab. □

Beispiel 1.1.4. Wir können die Elemente von $\mathrm{Per}(3)$ als Zykel hinschreiben: $e, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)$.

1.2 Ordnung

Definition 1.2.1. Ist G eine endliche Gruppe, so nennt man die Anzahl $|G|$ der Elemente die **Ordnung** der Gruppe G,

$$\mathrm{ord}(G) = |G|.$$

Wir schreiben auch 1 für das neutrale Element e einer Gruppe.

Ist $a \in G$, so bezeichnet $\langle a \rangle$ die von a **erzeugte Gruppe**, also die kleinste Untergruppe von G, die a enthält. Diese beschreibt man einmal als

$$\langle a \rangle = \bigcap_{\substack{H \text{ Untergruppe} \\ H \ni a}} H,$$

wobei man sich klarmachen muss, dass dies wieder eine Untergruppe ist. Andererseits kann man $\langle a \rangle$ konstruktiv beschreiben:

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}.$$

Ist $\langle a \rangle$ eine endliche Gruppe, so nennt man die Ordnung von $\langle a \rangle$ auch die **Ordnung** des Elements a und man schreibt

$$\operatorname{ord}(a) = \operatorname{ord}(\langle a \rangle) = |\langle a \rangle|.$$

Ist $\langle a \rangle$ nicht endlich, so setzt man $\operatorname{ord}(a) = \infty$.

Beispiel 1.2.2. Ist $z \in \operatorname{Per}(n)$ ein Zykel $z = (j_1, \ldots, j_k)$, dann gilt

$$\operatorname{ord}(z) = k.$$

Wir nennen k dann wahlweise die Ordnung oder die **Länge** des Zykels z.

Lemma 1.2.3. *Sei a ein Element der Gruppe G. Die von a erzeugte Gruppe $\langle a \rangle$ ist genau dann endlich, wenn es ein $n \in \mathbb{N}$ gibt mit $a^n = 1$. Es gilt*

$$\operatorname{ord}(a) = \min\{n \in \mathbb{N} : a^n = 1\}.$$

Ist k die Ordnung von a so gilt für jedes $n \in \mathbb{N}$

$$a^n = 1 \quad \Leftrightarrow \quad k \mid n.$$

Beweis. Sei $\langle a \rangle$ endlich. Da die Elemente $1, a, a^2, \ldots$ nicht alle verschieden sein können, gibt es ein $m, n \in \mathbb{N}$ so dann $a^m = a^{m+n}$, also $1 = a^n$ gilt. Die Umkehrung ist klar, da $\langle a \rangle$ genau aus den Potenzen von a besteht. Ist schliesslich $k \in \mathbb{N}$ die kleinste natürliche Zahl mit $a^k = 1$, dann besteht $\langle a \rangle$ genau aus den Elementen $1, a, a^2, \ldots, a^{k-1}$.

Zum Schluss sei $k = \operatorname{ord}(a)$ und $a^n = 1$. Dann folgt $n \geq k$, wir können also $n = rk + s$ schreiben mit $0 \leq s < k$. Es ist dann

$$1 = a^n = a^{rk+s} = (a^k)^r a^s = a^s,$$

so dass $s = 0$, also $k \mid n$ folgt. Die Umkehrung ist klar. □

Lemma 1.2.4. *Ist G eine abelsche Gruppe und $a, b \in G$ von endlichen Ordnungen m, n. Sind m und n teilerfremd, dann hat ab die Ordnung mn.*

Beweis. Ist $1 = (ab)^k = a^k b^k$, also $a^k = b^{-k}$. Die Ordnung von a^k ist ein Teiler von m, die Ordnung von b^{-k} ist ein Teiler von n, daher müssen beide Ordnungen gleich 1 sein, also $a^k = 1 = b^k$. Damit ist k ein Vielfaches von m und von n, die Ordnung von ab ist also mn. □

Definition 1.2.5. Sind G, H zwei Gruppen, so wird das Produkt $G \times H$ durch die Vorschrift

$$(g,h)(g',h') = (gg',hh')$$

eine Gruppe. Das neutrale Element ist $(1,1)$. Das Inverse zu (g,h) ist (g^{-1},h^{-1}). Für die Ordnungen gilt

$$\operatorname{ord}(G \times H) = \operatorname{ord}(G) \operatorname{ord}(H).$$

Beispiele 1.2.6.

- Wir bezeichnen mit $\mathbb{Z}/m\mathbb{Z}$ oder auch $\mathbb{Z}/m$ die **zyklische Gruppe** mit m Elementen, $m \in \mathbb{N}$, also die Gruppe $\{0, 1, 2, \ldots, m-1\}$ mit Verknüpfung: $a \boxplus b =$ Rest von $a + b$ modulo m.
- Sei $n \in \mathbb{N}$ die **Diedergruppe** D_{2n} der Ordnung $2n$ ist eine Gruppe erzeugt von zwei Elementen σ, τ mit den Relationen

$$\sigma^n = 1 = \tau^2 \quad \text{und} \quad \tau\sigma\tau^{-1} = \sigma^{-1}.$$

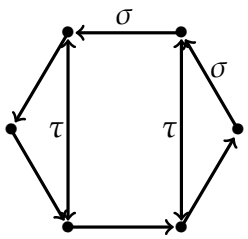
Insbesondere soll σ die Ordnung n haben und τ die Ordnung 2.

Das bedeutet, D_{2n} besteht genau aus den Elementen

$$1, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \tau\sigma, \ldots, \tau\sigma^{n-1}$$

und die Produkte dieser Elemente rechnet man mit den Relationen aus.

Man kann sie als Untergruppe von $\mathrm{Per}(n)$ wie folgt darstellen. Stellen wir uns die Elemente von $\{1, 2, \ldots, n\}$ auf einem Kreis in gleichen Abständen angeordnet vor. Dann ist σ die Rotation um den Winkel $2\pi/n$ und τ ist irgendeine Spiegelung an einer Geraden, die die Menge $\{1, \ldots, n\}$ in sich abbildet.



Es gilt $D_2 \cong \mathbb{Z}/2$, sowie $D_4 \cong (\mathbb{Z}/2) \times (\mathbb{Z}/2)$ und schliesslich

$$D_6 \cong \mathrm{Per}(3).$$

Proposition 1.2.7. *Ist $g \in \mathrm{Per}(n)$ eine Permutation, die wir gemäß Satz 1.1.3 als Produkt disjunkter Zykel schreiben:*

$$g = z_1 \cdots z_k$$

und sei $l_j = l(z_j)$ die jeweilige Länge des j-ten Zykels. Dann gilt

$$\mathrm{ord}(g) = \mathrm{kgV}(l_1, \ldots, l_k).$$

Beweis. Die z_j vertauschen miteinander. Da jedes z_j eine andere Teilmenge von $\{1, \ldots, n\}$ permutiert, folgt für $\nu \in \mathbb{N}$

$$g^\nu = 1 \quad \Leftrightarrow \quad z_j^\nu = 1 \text{ für jedes } j = 1, \ldots, k.$$

Dies ist genau dann der Fall, wenn ν ein Vielfaches von $\mathrm{ord}(z_j) = l_j$ ist für jedes j, daher ist die Ordnung $\mathrm{ord}(g) = \min\{\nu \in \mathbb{N} : g^\nu = 1\}$ das kleinste gemeinsame Vielfache der Einzelordnungen. □

1.3 Nebenklassen

Definition 1.3.1. Sei G eine Gruppe und sei $H \subset G$ eine Untergruppe. Ist $a \in G$, so ist die **Linksnebenklasse** von a nach H gleich der Menge

$$aH = \{ah : h \in H\}.$$

Da H eine Gruppe ist, gilt für $h \in H$ schon

$$hH = H.$$

Beispiele 1.3.2.

- Ist V ein Vektorraum und $U \subset V$ ein Unterraum, dann sind die Nebenklassen nach U genau die affinen Räume $v + U$, die U als linearen Teil haben.
- Sei $G = D_{2n}$ die Diedergruppe und sei $H = \langle \tau \rangle$ die von τ erzeugte Untergruppe, dann ist $H = \{1, \tau\}$ und die H-Linksnebenklassen sind

$$\underbrace{\{1, \tau\}}_{=H}, \underbrace{\{\sigma, \sigma\tau\}}_{=\sigma H}, \ldots, \underbrace{\{\sigma^{n-1}, \sigma^{n-1}\tau\}}_{=\sigma^{n-1}H}.$$

Lemma 1.3.3. *Sei G eine Gruppe und H eine Untergruppe. Zwei Linksnebenklassen sind*

entweder gleich oder disjunkt, daher kann man G disjunkt in seine Nebenklassen zerlegen, es gibt also eine Familie $(x_i)_{i\in I}$ in G so dass

$$G = \bigsqcup_{i\in I} x_i H.$$

Beweis. Sei $xH \cap yH \neq \varnothing$. Wir zeigen $xH \subset yH$. Aus Symmetrie folgt dann die andere Richtung. Sei also $z \in xH \cap yH$, dann existieren $h_1, h_2 \in H$ so dass $z = xh_1 = yh_2$. Es folgt $x = yh_2h_1^{-1} \in yH$ und ist $u \in xH$, also $u = xh_3$, so folgt $u = xh_3 = y\underbrace{h_2h_1^{-1}h_3}_{\in H} \in yH$. □

Proposition 1.3.4. *Sei G eine endliche Gruppe. Ist H eine Untergruppe, dann ist die Ordnung $|H|$ ein Teiler der Ordnung $|G|$ von G. Genauer gilt*

$$|G| = |H||G/H|,$$

wobei G/H die Menge aller Nebenklassen aH ist.

Insbesondere gilt für jedes Element x

$$\operatorname{ord}(x) \mid \operatorname{ord}(G),$$

d.h., die Ordnung von x teilt die Gruppenordnung. Insbesondere folgt

$$x^{\operatorname{ord}(G)} = 1.$$

Beweis. Wir haben $G = \bigsqcup_{i\in I} x_i H$, und da G endlich ist, muss I endlich sein, wir finden also $x_1, \dots, x_n \in G$ so dass $G = \bigsqcup_{j=1}^{n} x_j H$. Also folgt

$$\operatorname{ord}(G) = \sum_{j=1}^{n} |x_j H|.$$

Die Untergruppe H bildet selbst eine Nebenklasse, wir können also $x_1 = e$ annehmen. Die Abbildung $h \mapsto x_j H$ ist eine Bijektion von H nach $x_j H$, also haben alle Nebenklassen gleich viele Elemente, nämlich $\operatorname{ord}(H)$ viele, es ist also

$$\operatorname{ord}(G) = \sum_{j=1}^{n} \operatorname{ord}(H) = n \operatorname{ord}(H).$$

Ist $a \in G$ ein beliebiges Element und ist $H = \langle a \rangle$ die von a erzeugte Untergruppe, dann ist $\operatorname{ord}(a) = \operatorname{ord}(H)$ ein Teiler von $\operatorname{ord}(G)$. □

1.4 Homomorphismen und Operationen

Definition 1.4.1. Eine Abbildung $\phi : G \to H$ zwischen zwei Gruppen heisst **Gruppenhomomorphismus**, falls

$$\phi(ab) = \phi(a)\phi(b)$$

für alle $a, b \in G$ gilt.

Lemma 1.4.2. *Ist $\phi : G \to H$ ein Gruppenhomomorphismus, dann gilt $\phi(1) = 1$ und $\phi(a^{-1}) = \phi(a)^{-1}$.*

Beweis. Übungsaufgabe Blatt 1. □

Beispiele 1.4.3.

- Ist G eine Gruppe und ist $a \in G$, dann ist die Abbildung

  $$\phi : x \mapsto axa^{-1}$$

  Ein Homomorphismus von G nach G.

  Beweis. Für $x, y \in G$ gilt $\phi(xy) = axya^{-1} = axa^{-1}aya^{-1} = \phi(x)\phi(y)$. □

- Sind V, W Vektorräume über einem Körper K, so ist jede lineare Abbildung $T : V \to W$ ein Gruppenhomomorphismus $(V, +) \to (W, +)$.

- Sei G die Gruppe $\mathrm{GL}_n(K)$ aller invertierbarer $n \times n$ Matrizen über dem Körper K. Dann ist die Abbildung $\psi : G \to G$,

  $$\psi(A) = A^{-t} = (A^t)^{-1} = (A^{-1})^t$$

  ein Gruppenhomomorphismus.

- Ist $G = \mathrm{Per}(n)$ die Gruppe der Permutationen in $\{1, \ldots, n\}$, dann ist die Vorzeichen- oder **Signumabbildung**

  $$\mathrm{sign} : \mathrm{Per}(n) \to \{\pm 1\}$$

  ein Gruppenhomomorphismus, wie in der Linearen Algebra gezeigt wird.

Definition 1.4.4. Sei G eine Gruppe und M eine Menge. Eine **Operation** von G auf M ist eine Abbildung

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

mit den Eigenschaften

- $1.m = m$ (das neutrale Element operiert neutral)
- $(ab).m = a.(b.m)$ (Operation und Multiplikation sind kompatibel)

Beispiele 1.4.5.

- Sei G eine Gruppe. Dann definiert die Vorschrift

$$g.m = gm$$

eine Operation der Gruppe auf sich selbst, die **Linkstranslationsoperation**.

Beweis. Es gilt $1.m = 1m = m$ und $(ab).m = (ab)m = a(bm) = a.(b.m)$. □

- Sei G eine Gruppe, dann operiert G durch

$$g.m = mg^{-1}$$

auf sich selbst, dies ist die **Rechtstranslationsoperation**.

Beweis. Es gilt $1.m = m1^{-1} = m1 = m$ und
$(ab).m = m(ab)^{-1} = (mb^{-1})a^{-1} = a.(b.m)$. □

- Sei G eine Gruppe, dann operiert G auf sich selbst durch die Vorschrift

$$g.m = gmg^{-1}$$

dies ist die **Konjugationsoperation**.

Beweis. Es gilt $1.m = 1m1^{-1} = m$ und $(ab).m = abm(ab)^{-1} = abmb^{-1}a^{-1} = a.(b.m)$. □

- (Abgeleitete Operationen.) Operiert die Gruppe G auf der Menge M und ist S eine weitere Menge, dann operiert G auf der Menge $A = \mathrm{Abb}(M, S)$ aller Abbildungen von M nach S durch

$$g.\phi(m) = \phi(g^{-1}.m).$$

Beweis. Es ist $e.\phi(m) = \phi(e^{-1}.m) = \phi(m)$ und
$(ab).\phi(m) = \phi((ab)^{-1}.m) = \phi(b^{-1}.a^{-1}.m) = b.\phi(a^{-1}.m) = a.(b.\phi)(m)$. □

Lemma 1.4.6. *Sei $M \neq \varnothing$ eine Menge. Operiert die Gruppe G auf der Menge M, dann ist die Abbildung $\phi : G \to \mathrm{Per}(M)$, $g \mapsto (m \mapsto gm)$ ein Gruppenhomomorphismus. Ist umgekehrt $\phi : G \to \mathrm{Per}(M)$ ein Gruppenhomomorphismus, dann definiert*

$$gm = \phi(g)(m)$$

eine Operation. Diese Zuordnungen (Operation)↦(Gruppenhomomorphismus) und umgekehrt sind invers zueinander. Also ist eine Operation dasselbe wie ein Gruppenhomorphismus nach $\mathrm{Per}(M)$.

Beweis. Die Gruppe G operiere auf M. Für $g \in G$ sei $\phi(g) : M \to M$, $m \mapsto gm$. Zunächst müssen wir zeigen, dass $\phi(g)$ bijektiv ist, wir also wirklich in $\mathrm{Per}(M)$ landen. Wir behaupten, dass $\phi(g^{-1})$ eine Umkehrabbildung zu $\phi(g)$ ist. Dies folgt aus

$$\phi(g)(\phi(g^{-1})(m)) = \phi(g)(g^{-1}m) = gg^{-1}m = 1m = m$$

und

$$\phi(g^{-1})(\phi(g)(m)) = \phi(g^{-1})(gm) = g^{-1}gm = 1m = m.$$

Wir haben also in der Tat eine Abbildung $\phi : G \to \mathrm{Per}(M)$. Wir rechnen nun nach, dass dies ein Gruppenhomomorphismus ist. Für $g, h \in G$ gilt

$$\phi(gh)(m) = (gh)m = g(hm) = \phi(g)(hm) = \phi(g)(\phi(h)(m)) = \phi(g)\phi(h)(m).$$

Also ist ϕ ein Gruppenhomorphismus. Die Umgekehrte Richtung ist leicht nachzurechnen und die Tatsache, dass diese Zuordnungen invers zueinander sind, auch. □

Die Gruppe G operiere auf der Menge M. Für gegebenes $m \in M$ nennen wir die Menge

$$[m] = Gm = \{gm : g \in G\}$$

die **Bahn** oder das **Orbit** von m. Ferner ist

$$G_m = \{g \in G : gm = m\}$$

der **Stabilisator** von m.

Satz 1.4.7. *Die Gruppe G operiere auf der Menge M.*

(a) *Der Stabilisator eines Punktes $m \in M$ ist eine Untergruppe von G. Er wird auch die* **Standgruppe** *von m genannt.*

(b) *Sei $H = G_m$ der Stabilisator von m. Die Abbildung $gH \mapsto gm$ ist eine Bijektion von G/H zum Orbit von m.*

(c) *Die Orbiten zweier Punkte sind entweder gleich oder disjunkt, man kann deshalb M disjunkt in seine Orbiten zerlegen. Man schreibt $G\backslash M$ für die Menge aller Orbiten.*

(d) *(Bahnengleichung) Sind G und M endliche Mengen und seien $[m_1], \dots, [m_k]$ die Bahnen, so gilt*

$$|M| = \sum_{j=1}^{k} \frac{|G|}{|G_{m_j}|}.$$

Man kann Teil (c) auch so ausdrücken, dass man sagt: die Operation von G definiert eine Äquivalenzrelation auf M, wobei m und m' äquivalent heissen, falls sie in demselben Orbit liegen. Der Quotient nach dieser Äquivalenzrelation wird dann mit $G\backslash M$ bezeichnet.

Beweis. (a) Sei $H = G_m$, dann gilt offensichtlich $e \in H$. Sind $a, b \in H$, dann ist

$$(ab)m = a(bm) = am = m,$$

also liegt auch ab wieder in H. Ferner folgt aus $am = m$ durch Anwenden von a^{-1} schon $m = a^{-1}m$, so dass auch $a^{-1} \in H$ folgt. Also ist H eine Untergruppe.

(b) Sei $\psi : G/H \to Gm$ diese Abbildung. Zunächst ist festzustellen, dass sie überhaupt wohldefiniert ist, ist also $gH = g'H$, dann ist $g' = gh$ für ein $h \in H$ und damit ist $g'm = g(hm) = gm$, somit ist ψ wohldefiniert.
Injektivität. Sei $\psi(aH) = \psi(bH)$, dann ist $am = bm$ also $a^{-1}bm = m$, was soviel heisst wie $a^{-1}b \in H$ und somit $bH = aH$.
Surjektivität. Sei $z \in Gm$, also $z = gm$ für ein $g \in G$, dann folgt $z = \phi(gH)$.

(c) Sei $Gm \cap Gm' \neq \varnothing$, dann ist zu zeigen, dass $Gm = Gm'$ gilt. Sei $z \in Gm \cap Gm'$ dann existieren also $g, g' \in G$ so dass $gm = z = g'm'$. Es folgt $m' = (g')^{-1}gm$ so dass $m' \in Gm$ und damit $hm' \in Gm$ für jedes $h \in G$, was soviel heisst wie $Gm' \subset Gm$. Aus Symmetrie folgt die umgekehrte Inklusion.

(d) Wir haben die disjunkte Zerlegung $M = \bigsqcup_{j=1}^{k} [m_j]$. Daher ist $|M| = \sum_{j=1}^{k} \big|[m_j]\big|$. Nach Teil (b) ist fuer jedes $m \in M$ mit Stabilisator $H = G_m$,

$$\big|[m]\big| = \big|G/H\big|.$$

Es bleibt also zu zeigen $\big|G/H\big| = |G|/|H|$ oder $|G| = |H|\,\big|G/H\big|$. Seien $h_1H, \dots, h_lH$ die Nebenklassen, dann zerlegen sie G disjunkt, also

$$|G| = \sum_{j=1}^{j} \underbrace{|h_jH|}_{|H|} = l|H|.$$

Hierbei beachte, dass die Abbildung $h \mapsto m_jh$ eine Bijektion $H \to m_jH$ ist. Nach

Definition ist $l = |G/H|$, also folgt die Behauptung. □

Dieser Teil wurde noch nicht in der Vorlesung behandelt. Sei G eine Gruppe. Das **Zentrum** $Z = Z(G)$ von G ist die Menge aller $x \in G$, die mit allen Elementen vertauschen, also

$$Z(G) = \left\{x \in G : xy = yx \ \forall_{y \in G}\right\}.$$

Beispiele 1.4.8.

- Ist G abelsch, so gilt $Z(G) = G$ und umgekehrt.
- Ist $G = \mathrm{GL}_n(K)$ für einen Körper K, dann besteht das Zentrum aus die Matrizen der Form λI, wobei $\lambda \in K^\times$. Dies ist eine Übungsaufgabe der Linearen Algebra. (Man löse zuerst den Fall $n = 2$, dann sieht man auch den allgemeinen Beweis.)
- Ist $n \geq 3$, dann ist das Zentrum von $G = \mathrm{Per}(n)$ die triviale Gruppe.

  Beweis. Sei σ im Zentrum von $\mathrm{Per}(n)$ und $n \geq 3$. Sei $1 \leq i \leq n$ und sei $1 \leq j \leq n$ von i und von $\sigma(i)$ verschieden. Dann vertauscht σ mit der Transposition $\tau = \tau_{i,j}$, die man als Zykel in der Form (i, j) schreibt. Es gilt also $\sigma(j) = \sigma(\tau(i)) = \tau(\sigma(i))$. Waere nun $\sigma(i)$ von i und j verschieden, dann waere $\sigma(j) = \tau(\sigma(i)) = \sigma(i)$, was der Injektivitaet von σ widerspricht! Damit muss $\sigma(i)$ gleich i oder j sein, der Fall j ist aber in der Annahme ausgeschlossen. Es folgt $\sigma(i) = i$ und also $\sigma = \mathrm{Id}$. □

Wir lassen nun die endliche Gruppe G durch Konjugation auf sich selbst operieren und wenden die Bahnengleichung an. Die Orbiten unter der Konjugation heissen auch **Konjugationsklassen**. Die Konjugationsklasse des Elementes $x \in G$ ist also die Menge

$$[x] = \left\{yxy^{-1} : y \in G\right\}.$$

Satz 1.4.9 (Klassengleichung)**.** *Sei G eine endliche Gruppe mit Zentrum Z und sei $x_1, \ldots, x_n$ ein Vertretersystem der Konjugationsklassen von $G \setminus Z$. Dann gilt*

$$\mathrm{ord}(G) = \mathrm{ord}(Z) + \sum_{j=1}^{n} \frac{|G|}{|G_{x_j}|},$$

wobei G_{x_j} der **Zentralisator** *von x_j ist:*

$$G_{x_j} = \left\{y \in G : yx_j = x_j y\right\}.$$

Beweis. Dies ist die Bahnengleichung auf die Konjugationsoperation angewendet. □

1.5 Zyklische Gruppen

Eine Gruppe G heisst **zyklisch**, wenn G von einem Element erzeugt ist.

Beispiele 1.5.1.
- Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch von unendlicher Ordnung.
- Für jedes $n \in \mathbb{N}$ gibt es eine zyklische Gruppe der Ordnung n, nämlich $\mathbb{Z}/n$.

Proposition 1.5.2. *Ist G zyklisch, dann ist G isomorph zu $\mathbb{Z}$ oder zu $\mathbb{Z}/n$, wobei $n = \mathrm{ord}(G)$.*

Mit anderen Worten, alle unendlichen zyklischen Gruppen sind isomorph und eine endliche zyklische Gruppe ist durch ihre Ordnung festgelegt.

Beweis. Sei G zyklisch und sei τ ein Erzeuger.

1. Fall. τ hat endliche Ordnung $n \in \mathbb{N}$. Dann ist die Abbildung $\mathbb{Z}/n \to G$, $k \mapsto \tau^k$ ein Gruppenisomorphismus.
2. Fall. τ hat keine endliche Ordnung. Dann ist die Abbildung $\mathbb{Z} \to G$, $k \mapsto \tau^k$ ein Isomorphismus. □

Fangen wir an mit Gruppen der Ordnung 1. Diese sind alle isomorph zu $\{1\}$, damit ist dieser erste Schritt abgeschlossen. Bevor wir uns mit den Ordnungen 2 und 3 herumschlagen, beweisen wir lieber einen Satz.

Satz 1.5.3. *Sei p eine Primzahl. Jede Gruppe der Ordnung p ist zyklisch, also isomorph zu der Gruppe $\mathbb{Z}/p$.*

Beweis. Sei G eine Gruppe der Ordnung p. Sei $e \neq \tau \in G$. Dann muss $\mathrm{ord}(\tau)$ ein Teiler von p sein. Da $\tau \neq e$, ist die Ordnung $\neq 1$, also ist $\mathrm{ord}(\tau) = p$, damit hat die zyklische Untergruppe $\langle\tau\rangle$, die von τ erzeugt wird, die Ordnung p, ist also gleich G. □

Satz 1.5.4. *Es gibt bis auf Isomorphie zwei Gruppen der Ordnung 4, die zyklische $\mathbb{Z}/4$ und die* **Kleinsche Vierergruppe** $(\mathbb{Z}/2) \times (\mathbb{Z}/2)$.

Beweis. Sei G eine Gruppe der Ordnung 4, die nicht zyklisch ist. Das bedeutet, dass jedes Element $\neq e$ die Ordnung 2 haben muss. Sei also a ein nichttriviales Element. Die Untergruppe $H = \langle a\rangle$ hat Index 2, ist also normal. sei $b \in G$, so folgt $bHb^{-1} = H$, da H nur aus zwei Elementen, e und a besteht, folgt $bab^{-1} = a$, also ist G abelsch. Seien nun a, b zwei verschiedene Elemente von $G \setminus \{e\}$. Dann liefert die Abbildung $(\mathbb{Z}/2) \times (\mathbb{Z}/2) \to G$, $(i, j) \mapsto a^i b^j$ einen injektiven Gruppenhomomorphismus. Das Bild hat Ordnung 4, ist also G und G damit isomorph zur Vierergruppe. □

Satz 1.5.5. *Jede Untergruppe einer zyklischen Gruppe ist zyklisch.*

Proof. Sei $G = \langle\tau\rangle$ eine zyklische Gruppe und sei $\{1\} \neq H \subset G$ eine Untergruppe. Sei N die kleinste natuerliche Zahl mit $\gamma = \tau^N \in H$. Wir zeigen, dass H von γ erzeugt ist. Sei hierzu $h = \tau^n \in H$, dann ist $h\gamma^k = \tau^{n+kN} \in H$. Es gibt ein $k \in \mathbb{Z}$ mit $0 \leq n + kN < N$. Aus der Minimalitaet von N folgt $n + kN = 0$ und daher $h = \gamma^{-k}$. □

1.6 Normalteiler

Definition 1.6.1. Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Der **Kern** von ϕ ist die Menge

$$\ker(\phi) = \{g \in G : \phi(g) = 1\}.$$

Lemma 1.6.2. *Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Dann ist der Kern N eine Untergruppe von G mit der Eigenschaft, dass*

$$gNg^{-1} = N$$

für alle $g \in G$ gilt.

Definition 1.6.3. Eine Untergruppe $N \subset G$ mit der Eigenschaft aus dem Lemma heisst **Normalteiler** von G.

Beweis des Lemmas. Es reicht zu zeigen, dass $gNg^{-1} \subset N$ ist, denn dies gilt dann ja für jedes g, also auch für g^{-1}, also $g^{-1}Ng \subset N$. Daraus folgt durch Rechtsmultiplikation mit g, dass $Ng \subset gN$ und hieraus $N \subset gNg^{-1}$.

Sei also $n \in N$, d.h., $\phi(n) = 1$. Dann gilt für beliebiges $g \in G$:

$$\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g)^{-1} = \phi(g)1\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = 1,$$

also ist $gng^{-1} \in N$ wie verlangt. □

Beispiele 1.6.4.

- Ist G abelsch, dann ist jede Untergruppe ein Normalteiler.
- Sei $G = \mathrm{Per}(3)$ und H die Untergruppe erzeugt von $(1,2)$. Dann ist H kein Normalteiler, denn mit dem Element $\gamma = (1,3)$ gilt

$$\gamma(1,2)\gamma^{-1} = (2,3).$$

- Ist G irgendeine Gruppe, dann ist das Zentrum Z von G stets ein Normalteiler.

Beweis. Sei $z \in Z$ und $g \in G$. Dann ist

$$gzg^{-1} = zgg^{-1} = z \in Z,$$

also folgt $gZg^{-1} = Z$. □

- Ist G eine Gruppe und H eine Untergruppe vom Index 2, dann ist H ein Normalteiler.

  Beweis. Es gibt genau zwei Linksnebenklassen $G = H \sqcup sH$, also ist $sH = G \setminus H$ und ebenso fuer Rechtsnebenklassen: $G = H \sqcup Hs$, also $sH = G \setminus H = Hs$, oder $sHs^{-1} = H$. Dies gilt fuer jedes $s \notin H$ und fuer $s \in H$ gilt es sowieso. □

Satz 1.6.5. *Ist $N \subset G$ ein Normalteiler, so lässt sich auf der Menge der Nebenklassen G/N genau eine Gruppenstruktur installieren, so dass die Projektion $G \to G/N$ ein Gruppenhomomorphismus ist.*

Ist umgekehrt $H \subset G$ eine Untergruppe mit einer Gruppenstruktur auf dem Nebenklassenraum G/H so dass die Projektion $G \to G/H$ ein Homomorphismus ist, dann ist H ein Normalteiler.

Insbesondere folgt, dass die Normalteiler genau die Kerne von Homomorphismen sind.

Beweis. Die zweite Aussage folgt sofort aus Lemma 1.6.2, beweisen wir also die erste. Sei N ein Normalteiler in G. Wir wollen eine Gruppenstruktur auf dem Nebenklassenraum G/N definieren durch

$$(aN)(bN) = abN.$$

Wir zeigen die Wohldefiniertheit: Sei $aN = a'N$ und $bN = b'N$, so ist zu zeigen, dass $abN = a'b'N$ gilt. Es gibt $n_1, n_2 \in N$ mit $a' = an_1$ und $b' = bn_2$. Da N ein Normalteiler ist, gilt

$$a'b' = an_1bn_2 = ab\underbrace{(b^{-1}n_1b)}_{\in N}n_2 \in abN,$$

also folgt $a'b'N \subset abN$ und aus Symmetriegründen folgt auch die umgekehrte Inklusion. Die so definierte Multiplikation definiert eine Gruppenstruktur auf G/N so dass die Projektion $G \to G/N$ ein Homomorphismus ist. Da dieser surjektiv ist, ist die Gruppenstruktur eindeutig bestimmt. □

Beispiel 1.6.6. Sei $G = \mathbb{Z}$ und $N = m\mathbb{Z}$ für ein gegebenes $m \in \mathbb{N}$. Da G abelsch ist, ist die Untergruppe N normal. Der Quotient $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m$ ist eine endliche Gruppe der Ordnung m, die von einem Element, der 1, erzeugt wird.

Proposition 1.6.7. *Sei G eine Gruppe mit Zentrum Z. Ist G/Z zyklisch, dann ist G abelsch.*

Beweis. Sei $a \in G$, so dass G/Z von der Restklasse $[a]$ erzeugt wird. Sind dann $b, c \in G$ mit Restklassen $[b] = [a]^m$ und $[c] = [a]^n$, dann ist $b = a^m z$ und $c = a^n w$ mit $z, w \in Z$. Es folgt

$$bc = a^m z a^n w = a^n w a^m z = cb. \qquad \square$$

Korollar 1.6.8. *Sei G eine Gruppe und Z ihr Zentrum. Dann kann die Ordnung von G/Z keine Primzahl sein.*

Beweis. Ist $\mathrm{ord}(G/Z)$ eine Primzahl, dann ist G/Z nach Satz 1.5.3 zyklisch, dann ist G aber abelsch nach Proposition 1.6.7, somit also $G = Z$ und damit $G/Z = \{e\}$. $\square$