Die Sylowsätze

Alexander Hölzle

28.08.2006
21.01.2012

Inhaltsverzeichnis

I. Motivation und Einleitung

In diesem Dokument setzen wir voraus, dass der Leser grundlegendes über Gruppen und Faktorgruppe weiß und so bedeutende Sätze wie den Satz von Cayley oder den Satz von Lagrange beherrscht.

Zur genauen Beschreibung einer endlichen Gruppe gehören insbesondere Aussagen über ihre Untergruppen, vor allem wird man nach Existenz und Eigenschaften von Untergruppen vorgegebener Ordnung fragen. Existiert eine Untergruppe H einer Gruppe G, so ist nach dem Satz von Lagrange die Ordnung von H ein Teiler der Gruppenordnung G. Sei G eine Gruppe von Ordnung n und sei $T := \{t \in \mathbb{N} : \ t|n\}$ die Menge der positiven Teiler von n, dann existiert im Allgemeinen nicht für jedes $t \in T$ eine Untergruppe H von G.

Schränkt man jedoch die Voraussetzungen ein, so kann man in der Tat die Existenz gewisser Untergruppen mit entsprechender Ordnung nachweisen. Dies ist die Hauptaussage des ersten Sylowsatzes. Der zweite Sylowsatz gibt darüber Auskunft welche Struktur diese speziellen Untergruppen einnehmen (sie liegen alle auf einer Bahn bzw. sind Teilmenge von p-Sylow-Gruppen). Schließlich gibt der letzte und damit dritte Sylow-Satz Auskunft über die Anzahl von p-Sylow-Gruppen.

Um diese für die Gruppentheorie sehr bedeutenden Sylowsätze beweisen zu können, benötigt man Wissen zu so genannten Gruppenoperationen. Das ist quasi eine „Standpunktwechsel“ des Satzes von Cayley. Am Ende des bereitgestellten Dokuments werden wir uns noch zwei typische Anwendungsbeispiele der Sylowsätze näher betrachten.

II. Gruppenoperationen

1. Der Satz von Cayley und Homomorphismen

Der Satz von Cayley besagt, dass jede Gruppe G (der Ordnung n) isomorph zu einer Gruppe von Permutationen (vom Grad n) ist. Wir werden im Folgenden durch Angabe eines Gruppenisomorphismus $G \to S(G)$ die Grundidee eines Beweises für diesen Satz aufzeigen.

II.1.1 Definition: Seien $(G, \cdot)$ eine Gruppe, $S(G)$ die Gruppe der bijektiven Selbstabbildungen von G mit der Komposition $\circ$ als Gruppenoperation und $a \in G$. Dann nennen wir die Abbildung

$$L_a : G \to G \qquad \text{definiert durch} \qquad g \mapsto a \cdot g$$

Linksmultiplikation oder **Linkstranslation** auf G mit a.

Vermöge der Linksmultiplikation L_a sei

$$L : G \to S(G), \quad \text{definiert durch} \quad a \mapsto L_a$$

ein injektiver Gruppenhomomorphismus von G in die symmetrische Gruppe $S(G)$. Durch Einschränkung des Wertebereichs auf $\mathrm{Bild}(L)$ erhalten wir dadurch einen Isomorphismus $G \to \mathrm{Bild}(L) \subseteq S(G)$. Es ist daher legitim G mit $\mathrm{Bild}(L)$ zu identifizieren, so dass G zu einer Untergruppe von $S(G)$ Anlass gibt. Der Homomorphismus L heißt oft auch die **Cayleysche Darstellung** von G. Diese Bezeichnung deutet bereits an, dass der Satz von Cayley als Ausgangspunkt für die Darstellungstheorie angesehen werden kann. Vergleichen Sie bitte auch mit Beispiel II.2.2 b).

Wechseln wir nun den Standpunkt und betrachten Homomorphismen $\phi : G \to S(X)$ von einer Gruppe G in die symmetrische Gruppe $S(X)$, wobei X eine beliebige nicht leere Menge sei. Wir notieren abkürzend $g \bullet x := \phi_g(x)$, wobei wir g festhalten und die Variable x stellvertretend für die Elemente von X steht. Eine Beispielklasse derartiger Homomorphismen haben wir eben mit Hilfe der Linksmultiplikation konstruiert, doch in diesem Fall war $X = G$ eine Gruppe.

Sei $(G, \cdot)$ eine Gruppe und e dessen neutrales Element, $X \neq \varnothing$ eine Menge und $\phi : G \to S(X)$ ein Homomorphismus. Aufgrund der Definition des Homomorphismus sind sowohl

$$\phi_e(x) = \mathrm{id}(x) = x \qquad \text{als auch} \qquad \phi_{g \cdot h}(x) = (\phi_g \circ \phi_h)(x) \tag{ExHom}$$

für alle $x \in X$ gültige Gleichungen. Dabei sei $\circ$ im Kontext der symmetrischen Gruppe stets die Komposition.

2. Definition und Beispiele

Um uns von der bestimmten Wahl des Homomorphismus ϕ aus dem letzten Abschnitt unabhängig zu machen, führen wir folgende Definition ein.

II.2.1 Definition: Seien $(G,\cdot)$ eine Gruppe, X eine nicht leere Menge und $e \in G$ das neutrale Element von G. Wir sagen G **operiert auf** X, wenn es eine Abbildung $\psi : (G \times X) \to X$ gibt mit den Eigenschaften

(Op1) $\psi(e,x) = x \qquad \forall x \in X$ und das neutrale Element $e \in G$;

(Op2) $\psi(g,\psi(h,x)) = \psi(g \cdot h, x) \qquad \forall x \in X$ sowie $\forall g,h \in G$.

Sodann heißt ψ auch **Gruppenoperation** oder schlicht **Operation** von G auf X.

Wie bereits im letzten Abschnitt erwähnt, werden wir vor allem weiter unten die abkürzende Schreibweise $g \bullet x := \psi(g,x)$ verwenden.

Gruppenoperationen hängen offenbar mit der im letzten Teilabschnitt aufgeworfenen Existenzfrage nach Homomorphismen $G \to S(X)$ eng zusammen. Das ist kein Zufall. Jeder Homomorphismus von $G \to S(X)$ liefert wegen den Gleichungen (ExHom) eine Operation von G auf X.

Weitere Beispiele werden die Definition veranschaulichen:

II.2.2 Beispiel:

a) *Jede* Gruppe G operiert auf *jeder* Menge X durch die Operation

$$G \times X \to X \quad \text{definiert durch} \quad (g,x) \mapsto g \bullet x := x$$

mit $g \in G, x \in X$. Diese Operation heißt **triviale Operation** von G auf X. Beachtet man, dass das Bild stets gleich x ist so ist der Nachweis von (Op1) und (Op2) einfach.

b) Eine Gruppe $(G,\cdot)$ mit $G = X$ operiert auf sich selbst durch *Linksmultiplikation*

$$L_g : G \times X \to X \quad \text{definiert durch}$$
$$(g,x) \mapsto (g \cdot x)$$

$\forall x \in X = G$ und $\forall g \in G$. Die definierenden Eigenschaften (Op1) und (Op2) folgen unmittelbar aus den Gruppeneigenschaften von G. Insbesondere ist L_g bijektiv, denn aus $L_g(x) = L_g(y)$ mit $x,y \in X$ folgt $g \cdot x = g \cdot y$ also $x = y$ und somit die Injektivität. Um die Surjektivität zu beweisen, müssen wir zeigen, dass jedes $x \in X$ durch die Funktion L_g „getroffen“ werden kann. Dies folgt durch die Umformung

$$x = (g \cdot g^{-1}) \cdot x = g \cdot (g^{-1} \cdot x) = L_g(g^{-1} \cdot x)$$

und den Eigenschaften einer Gruppe, denn es muss $g^{-1} \cdot x \in X = G$ gelten. Es ist also $L_g \in S(G)$ eine bijektive Selbstabbildung.

Allerdings ist die bijektive Funktion L_g für $g \neq e$ *kein Gruppen-Homomorphismus*, denn $L_g(e) = g \cdot e = g \neq \mathrm{id}$. Betrachtet man jedoch die Abbildung $L : G \to S(G)$ mit $g \mapsto L_g$, so erklärt diese einen Homomorphismus von Gruppen. Für $g, h \in G$ und beliebiges $x \in X$ gilt

$$L_{g\cdot h}(x) = (g \cdot h) \cdot x = g \cdot (h \cdot x) = L_g(L_h(x)) = (L_h \circ L_g)(x),$$

also ist $L_{g\cdot h} = L_h \circ L_g$ und daher ist L ein Homomorphismus.

c) Seien $X \neq \varnothing$ eine Menge, σ ein Element der symmetrischen Gruppe $S(X)$ und

$$S(X) \times X \to X \quad \text{definiert durch} \quad (\sigma, x) \mapsto \sigma \bullet x := \sigma(x).$$

Offenbar ist $\mathrm{id} \bullet x = \mathrm{id}(x) = x$ für alle $x \in X$, womit (Op1) bewiesen ist. Ferner gelten $\forall \sigma, \tau \in S(X)$ die Gleichungen

$$\begin{aligned} (\sigma \circ \tau) \bullet x &= (\tau \bullet (\sigma \bullet x)), \quad \text{d.h.} \\ (\sigma \circ \tau)(x) &= \tau(\sigma(x)), \end{aligned}$$

was (Op2) belegt.

d) Sei $G := (\mathbb{Z}^2, +)$ die additive Gruppe und $X := \mathbb{R}^2$ die reelle Zahlenebene. Die Abbildung

$$G \times X \to X \quad \text{definert durch} \quad (m, n) \bullet (x, y) := (x + m, y + n)$$

erklärt eine Gruppenoperation auf der reellen Zahlenebene. Offenbar gelten

$$(0, 0) \bullet (x, y) = (x, y)$$

sowie

$$\begin{aligned} (m, n) \bullet [(m', n') \bullet (x, y)] &= (m, n) \bullet [(x + m', y + n')] \\ &= (x + m' + m, y + n' + n) \\ &= (m + m', n + n') \bullet (x, y) \end{aligned}$$

aufgrund der Gruppeneigenschaften von G, d.h. (Op1) als auch (Op2) sind erfüllt.

e) Sei $(n\mathbb{Z}, +)$ die Gruppe der ganzzahligen Vielfachen einer natürlichen Zahl $n \in \mathbb{N}$. $n\mathbb{Z}$ ist eine Untergruppe der additven Gruppe $(\mathbb{Z}, +)$, wobei $+$ die gewöhnliche Addition zweier ganzer Zahlen ist. In diesem Beispiel setzen wir $X := \mathbb{Z}$ und behaupten, dass die Gruppe $n\mathbb{Z}$ auf der Menge X vermöge

$$(n\mathbb{Z} \times \mathbb{Z}) \to \mathbb{Z} \quad \text{definiert durch} \quad (nq, r) \;\mapsto\; nq \bullet r := (nq + r)$$

operiert. Offenbar ist $(nq \bullet 0) = nq + 0 = nq$, weshalb (Op1) erfüllt ist. Die zweite Eigenschaft (Op2) ergibt sich ebenso einfach durch

$$\begin{aligned} nq' \bullet (nq \bullet r) &= nq' \bullet (nq + r) \\ &= nq' + nq + r = n(q' + q) + r \\ &= (nq' + nq) \bullet r. \end{aligned}$$

3. Bahn, Orbit, Stabilisatoren, Isotropie-Gruppe und die Bahnengleichung

Fasst man die bisher gewonnen Erkenntnisse zusammen, so gelangen wir zu folgendem

II.3.1 Satz: Es sei $(G, \cdot)$ eine Gruppe und $X \neq \varnothing$ eine Menge. Dann operiert G genau dann auf X, wenn ein Gruppen-Homomorphismus $\phi : G \to S(X)$ existiert.

Ein Gruppe G operiert also genau dann auf einer nicht leeren Menge X, wenn ein Gruppen-Homomorphismus in die symmetrische Gruppe $S(X)$ existiert. Die folgende Beweisführung ist recht konstruktiv, deshalb werden Sie vielleicht die ein oder andere Idee aus den Beispielen wiederfinden.

Beweis. „⇒“: Nach Voraussetzungen operiert G auf X, d.h. es muss eine Abbildung ψ existieren, welche die Definition einer Gruppen-Operation erfüllt. Betrachten wir nun die Abbildung $\phi : G \to S(X)$ definiert durch $g \mapsto \phi(g) := \psi(g, x)$, so gilt

$$\phi(g \cdot h) = \psi(g \cdot h, x) = \psi(g, \psi(h, x)) = \phi(h) \circ \phi(g).$$

Es bleibt noch zu zeigen, dass ϕ das neutrale Element aus G auf das neutrale Element aus $S(X)$ abbildet. Dazu sei e das neutrale Element von G.

$$\phi(e) = \psi(e, x) = x.$$

Hm, entspricht x dem geforderten neutralen Element von $S(X)$? Ja, man sollte sich daran entsinnen, dass der Bildraum von ϕ eine Menge von Abbildungen $X \to X$ ist, d.h. $\mathrm{id}(x) = x$ entspricht tatsächlich dem neutralen Element.

„⇐“: Nach Voraussetzungen existiert ein Homomorphismus $\phi : G \to S(X)$, d.h. es gilt $\phi(g \cdot h) = \phi(g) \circ \phi(h)$. Auch hier ist zu beachten, dass $\phi(g)$ eine Abbildung mit Definitionsbereich X ist. Daher setzen wir $(\phi(g))(x) =: \psi(g, x)$. Sodann gilt für beliebige $x \in X$ und $g, h \in G$

$$\phi(g \cdot h)(x) = \psi(g \cdot h, x) = (\phi(g) \circ \phi(h))(x) = \psi(g, \psi(h, x)),$$

womit (Op2) bereits gezeigt ist. Da ϕ homomorph ist, gilt $\phi(e) = \mathrm{id}$, d.h. es gilt $\phi(e)(x) = x$. Insgesamt folgt die Behauptung. □

Bemerkung: Eine Operation von G auf X ist also *im Wesentlichen das Gleiche wie ein Homomorphismus* $G \to S(X)$.

Operiert eine Gruppe G auf einer Menge X, so ergibt sich daraus eine *Äquivalenzrelation* - eine disjunkte Zerteilung der Menge X in „Bahnen“.

II.3.2 Satz: Es operiere die Gruppe G auf der nicht leeren Menge X mit der Gruppenoperation ψ. Dann ist

$$R(G) := \{ (x, y) \in (X \times X) \mid \exists g \in G \text{ mit } \psi(g, x) = y \}$$

eine Äquivalenzrelation.

Beweis. Im Folgenden sei $\psi(g,x)$ abgekürzt durch $g \bullet x$. Wegen $e \bullet x = x$ nach (Op1) ist $(x,x) \in R(G)$, d.h. die Relation ist reflexiv. Sei nun $(x,y) \in R(G)$, d.h. $\exists g \in G$, so dass $y = g \bullet x$, dann ist auch $(y,x) \in R(G)$, da $g^{-1} \in G$, also $g^{-1}y = g^{-1}g \bullet x = e \bullet x = x$. Also ist die Relation symmetrisch. Sind weiter $(x,y) \in R(G)$ und $(y,z) \in R(G)$, d.h. $\exists g,h \in G$ mit $y = g \bullet x$ und $z = h \bullet y$. Dann ist $(hg) \bullet x = h \bullet (g \bullet x) = h \bullet y = z$ also ist auch $(x,z) \in R(G)$ und damit ist die Relation transitiv. Es handelt sich also um eine Äquivalenzrelation. □

Wie uns bekannt ist, zerlegt eine Äquivalenzrelation die zu Grunde gelegte Menge X in disjunkte Äquivalenzklassen. Die einzelnen Äquivalenzklassen $[x_i]$ (x_i seien entsprechende Repräsentaten) mit $x_i \in X$ von $R(G)$ heißen *Orbits* oder *Bahnen* von G in X.

II.3.3 Definition (Bahn): Für festes $x \in X$ definieren wir

$$Gx \;:=\; \{g \bullet x \mid g \in G\} \;\subseteq\; X.$$

Gx heißt **Bahn** oder **Orbit** von x unter der Operation $\bullet$ von G auf X. Die Mächtigkeit einer Bahn $|Gx|$ bezeichnen wir als **Länge** einer Bahn.

Es wird sich im Laufe dieses Dokuments herauskristalisieren, dass man die Bahnen als verallgemeinerte Linksnebenklassen interpretieren kann.

Bemerkung: Es sei $[x]$ die Äquivalenzklasse von $x \in X$ bezüglich der Relation

$$R(G) := \{\ (x,y) \in (X \times X) \mid \exists g \in G \text{ mit } \psi(g,x) = y\ \},$$

dann gilt definitionsgemäß

$$[x] \;=\; \{\ y \in X \mid \exists g \in G, \text{ so dass } y = g \bullet x\} \;=\; \{g \bullet x \mid g \in G\ \} \;=\; Gx.$$

Da $R(G)$ eine Äquivalenzrelation auf X definiert und $[x]$ die Äquivalenzklassen sind, gilt offenbar

$$X = \bigcup_{x \in X} Gx.$$

Vielen wird die folgende Charakterisierung der Gleichheit von Orbits bzw. Bahnen sehr bekannt vorkommen – zu Recht, schließlich ist dies z.B. bei Faktorräumen oder etwas allgemeiner bei R-Faktor-Moduln ganz ähnlich.

II.3.4 Lemma: Es sei G eine Gruppe, welche auf X operiert und $[x]$ bzw. $[y]$ die Äquivalenzklasse von $x,y \in X$ bezüglich der Relation $R(G)$. Dann gilt:

$$[x] = [y] \;\Leftrightarrow\; Gx = Gy \;\Leftrightarrow\; \exists g \in G \text{ mit } g \bullet x = y.$$

Beweis. Die erste Äquivalenz haben wir in der letzten Bemerkung aufgezeigt. Es bleit also noch $Gx = Gy \Leftrightarrow \exists g \in G$ mit $g \bullet x = y$ zu beweisen:

„$\Rightarrow$“: Aus $Gx = Gy$ folgt mit Hilfe der Definition $\{g \bullet x \mid g \in G\} = \{g \bullet y \mid g \in G\}$. Beachtet man, dass $e \in G$, so erhält man $\exists g \in G : e \bullet x = x = g \bullet y$ und damit folgt die Behauptung.

„$\Leftarrow$“: Aus $\exists g \in G$ mit $g \bullet x = y$ folgt, dass $(x, y) \in R(G)$ gilt. D.h. auch, dass $y \in Gx \Rightarrow Gy \subset Gx$. Da $R(G)$ eine Äquivalenzrelation ist, folgt auch $(y, x) \in R(G)$ – analog zu eben folgt also $Gx \subset Gy$. Daraus ergibt sich schließlich die gewünschte Identität $Gx = Gy$. □

Operiert also eine Gruppe G auf der Menge X, so sind zwei Bahnen Gx und Gy entweder gleich oder disjunkt. Ist die Menge X endlich, so existieren folglich auch nur endlich viele Bahnen. Wählen wir in jeder dieser Bahnen ein $x_i \in X$, dann sind $Gx_1, \ldots, Gx_i, \ldots, Gx_k$ die verschiedenen Bahnen, welche vereinigt gerade X ergeben.

II.3.5 Beispiel:

a) Der komplexe Einheitskreis $S := \{\ z \in \mathbb{C}\ \ |z| = 1\ \}$ ist zusammen mit der komplexen Multiplikation $\cdot$ eine Gruppe. Dabei beachte man, dass die Multiplikation komplexer Zahlen als Drehstreckung (formaler Beweis mit Hilfe von Polarkoordinaten und den Eulerschen Identitäten) aufgefasst werden kann.

   Sodann operiert S durch die komplexe Mulitplikation auf $\mathbb{C}$. Das Einselement 1 aus $\mathbb{C}$ liegt in S und $\forall z \in \mathbb{C}$ gilt demnach $1 \cdot z = z$. Da die Gruppenoperation und die Verknüpfung der Gruppe S dieselbe ist, folgt damit auch unmittelbar $\forall s_1, s_2 \in S, z \in \mathbb{C} : (s_1 s_2) \cdot z = s_1 \cdot (s_2 \cdot z)$. Es handelt sich also tatsächlich um eine Gruppenoperation.

   Die Bahnen der Gruppenoperationen entsprechen allen Kreisen um den Nullpunkt! Die Gruppenoperation ist eine Multiplikation mit zwei Faktoren, wobei ein Element aus dem Einheitskreis ist und somit Betrag 1 besitzt. Die komplexe Multiplikation kann als Drehstreckung (Addition der Wikel) interpretiert werden, weshalb klar ist, dass eine Bahn dieser Gruppenoperation alle Zahlen mit demselben Betrag $Sz = \{\ z' \in \mathbb{C} \mid z' = |z|\ \}$ umfasst. Das ist vielleicht der *Grund*, warum man diese Menge Orbits bzw. Bahnen genannt hat. Die Menge $\mathbb{C}$ setzt sich also aus der Vereinigung aller Kreise um den Nullpunkt zusammen, darin ist auch der Kreis um den Nullpunkt mit Radius 0 (dem Nullpunkt selbst) enthalten.

b) Die triviale Operation auf G hat $Gx = \{x\}$, die Linksmultiplikation $Gx = G$ als Bahn.

c) Die Bahnen der Gruppenoperation aus Beispiel II.2.2 d) entsprichen den Einheitsgittern durch den Punkt (x, y) auf der reellen Zahlenebene.

d) Die Bahnen der Operation aus Beispiel II.2.2 e) entsprechen den Restklassengruppen

$$\mathbb{Z}/n\mathbb{Z} \ = \ \{\ qn + r \mid r \in \mathbb{Z}\ \} \ \subseteq \mathbb{Z}.$$

An diesem Beispiel ist die bereits angesprochene Analogie zwischen Gruppenoperationen und der Bildung von Nebenklassen sehr schön zu erkennen.

Nun kommen wir zu einer für diesen Abschnitt sehr bedeutenden Definition - diese werden wir später noch öfter benötigen.

II.3.6 Definition (Stabilisator): Es sei G eine Gruppe, die auf einer nicht leeren Menge X operiert. Wir nennen

$$G_x := \{ g \in G \mid g \bullet x = x \} \subseteq G \tag{II.1}$$

Stabilisator von $x \in X$ in G.

Ein Stabilisator von $x \in X$ wird oftmals auch **Isotropie-** oder **Fix-Gruppe** von $x \in X$ genannt - nicht ohne Grund, denn G_x ist in der Tat eine (Unter-)Gruppe (von G) für jedes $x \in X$. Das Wesentliche an einem Stabilisator ist, dass die Elemente dieser Menge invariant gegenüber der Gruppenoperation bei festgehaltenem $x \in X$ sind.

II.3.7 Satz: Es operiere die Gruppe G auf der nicht leeren Menge X, dann ist der Stabilisator G_x für jedes $x \in X$ eine Untergruppe von G und es gilt

$$|Gx| = [G : G_x]. \tag{II.2}$$

Dabei sei $[G : G_x]$ der Index von G_x in G, also die Anzahl der verschiedenen Linksnebenklassen der Faktorgruppe G/G_x.

Beweis. Es gilt $e \in G_x \neq \varnothing$, da das neutrale Element die Gleichung $e \bullet x = x$ per Definition erfüllt. Sei $h \in G_x$, dann liegt auch das Inverse h^{-1} in G_x. Wir müssen nachweisen, dass h^{-1} die Gleichung $h^{-1} \bullet x = x$ erfüllt. Dazu betrachten wir

$$\begin{aligned} h^{-1} \bullet x &= h^{-1} \bullet (\overbrace{h \bullet x}^{=x}) \\ &= (h^{-1}h) \bullet x \\ &= e \bullet x \\ &= x \end{aligned}$$

woraus schließlich $h^{-1} \in G_x$ folgt. Bei den Umformungen beachte man die Definition einer Gruppenoperation und dass $h \in G_x$. Ist außerdem noch $g \in G_x$ so haben wir $(gh) \bullet x = g \bullet (h \bullet x) = g \bullet x = x$, also $gh \in G_x$. Mit dem Untergruppenkriterium folgt der erste Teil der Behauptung.

Es sei G/G_x die Menge der Linksnebenklassen (da G_x im Allgemeinen kein Normalteiler ist, ist G/G_x keine (Faktor-)Gruppe). Es ist hinreichend, eine bijektive Abbildung

$$\gamma : G/G_x \to Gx$$

anzugeben. Diese Abbildung wird durch

$$\gamma(gG_x) := g \bullet x \qquad \text{für } g \in G$$

definiert. Die Abbildung ist *wohldefiniert*. Gilt für die Nebenklassen $gG_x = g'G_x$, also $g' = gh$ mit $h \in G_x$, so gelten die folgenden Gleichungen

$$\gamma(g'G_x) = g' \bullet x = (gh) \bullet x \overset{(Op2)}{=} g \bullet (\underbrace{h \bullet x}_{=x}) = g \bullet x = \gamma(gG_x).$$

Die Abbildung γ ist offensichtlich surjektiv und sie ist auch injektiv. Angenommen $\gamma(gG_x) = \gamma(g'G_x)$, d.h. $g \bullet x = g' \bullet x$, dann ist $(g^{-1}g') \bullet x = x$ und somit $g^{-1}g' \in G_x$. Die Elemente g und g' erzeugen demnach dieselben Nebenklassen, es ist also $gG_x = g'G_x$. □

Die Gleichung (II.2) besagt, dass die Länge einer Bahn und die Anzahl der aus dem Stabilisator gebildeten Nebenklasse identisch sind. Wie wir im eben gemachten Beweis gesehen haben, dient eine Gruppenoperation dazu eine bijektive Abbildung zwischen beiden Mengen zu konstruieren.

II.3.8 Folgerung: Es operiere eine endliche Gruppe G auf einer Menge $X \neq \varnothing$. Dann ist für jedes $x \in X$ die Anzahl der Elemente in der Bahn Gx ein Teiler der Gruppenordnung $|G|$.

Beweis. Folgt aus der Gleichung (II.2) und dem Satz von Lagrange. □

II.3.9 Satz: Es operiere die Gruppe G auf der nicht leeren Menge X. Für die Anzahl $|X|$ der Elemente von X gilt

$$|X| = \sum_{x \in I} |G : G_x| = \sum_{x \in I} |Gx| \tag{II.3}$$

Beweis. Aus Satz II.3.2 folgt $X = \bigcup_{x \in I} Gx$, wobei I ein Vertretersystem für die Aufteilung von X in verschiedene und damit disjunkte Äquivalenzklassen ist. Beachten wir noch Satz II.3.7 und Gleichung (II.2), so folgt die Behauptung insgesamt. □

Wir bezeichnen künftig ein *Vertretersystem* bzw. *Repräsentantensystem* für Bahnen stets mit der Menge I. Sollte die Menge endlich sein, so notieren wir dessen Repräsentanten, d.h. die Elemente von I, durch $x_1, \ldots, x_k$.

In Prosa gefasst lautet die Gleichung (II.3) wie folgt: Die Bahn Gx enthält so viele Elemente, wie Linksnebenklassen des Stabilisators G_x in G existieren.

Dass Stabilisatoren Untergruppen sind ist von großer Bedeutung für die sylowschen Sätze, da die so genannten p-Sylow-Gruppen, wie wir noch sehen werden, gerade Stabilisatoren spezieller Ordnung sind.

Im folgenden Beispiel werden die Verbindungen der entwickelten Theorie zu gewöhnlichen Untergruppen und Linksnebenklassen aufgezeigt.

II.3.10 Beispiel: Wie wir bereits in Beispiel II.2.2 b) festgestellt haben opieriert eine Gruppe G auf $G =: X$ sich selbst durch Linksmultiplikation. Sei H eine Untergruppe von

G, dann sind die Bahnen $Hx = \{\ hx \mid h \in H\ \}$ von $x \in G = X$ gerade die Linksnebenklassen von H in G. Der Stabilisator $H_x = \{h \in H \mid \quad hx = x\}$ von $x \in G = X$ entspricht dem neutralen Element $\{e\}$ aus H (und damit aus G), denn $hx = x$ gilt nur für $h = e$ in einer Gruppe.

Für ein Vertretersystem $I = \{x_1, \ldots, x_k\}$ der Linksnebenklassen von H, also $|I| = k = [G : H]$, folgt aus der Bahnengleichung (II.3)

$$|G| = \sum_{i=1}^{k} Hx = \sum_{i=1}^{k} [H : \{e\}] = \sum_{i=1}^{k} |H| = [G : H]|H|$$

der Satz von Lagrange. Die Bahnengleichung kann offenbar als **Verallgemeinerung des Satzes von Lagrange** interpretiert werden. Beachten Sie bei den Gleichungen, dass $\{e\}$ eine Untergruppe von H ist.

4. Der Fixpunktsatz

II.4.1 Definition (Fixpunktmenge): Eine Gruppe G operiere auf $X \neq \varnothing$. Dann heißt

$$\mathrm{Fix}_G(X) := \{\ x \in X \mid g \bullet x = x \quad \forall g \in G\ \} \subseteq X \tag{II.4}$$

Fixpunktmenge von X unter G. Die Elemente von $\mathrm{Fix}_G(X)$ nennen wir **Fixpunkten** von X unter G.

Die Menge $\mathrm{Fix}_G(X)$ besteht also aus den Elementen von X, die unter der Gruppenoperation $\bullet$ von G festgelassen werden. Im Gegensatz dazu besteht G_x aus Gruppenelementen $g \in G$, so dass $g \bullet x = x$ für ein festes $x \in X$ gilt.

II.4.2 Lemma: Es operiere die Gruppe G auf der nicht leeren Menge X. Ist dann $x \in \mathrm{Fix}_G(X)$ ein Fixpunkt, so gilt:

$$x \in \mathrm{Fix}_G(X) \ \Leftrightarrow\ G_x = G \ \Leftrightarrow\ Gx = \{x\} \ \Leftrightarrow\ |Gx| = 1 \ \Leftrightarrow\ [G : G_x] = 1 \tag{II.5}$$

Beweis. Sei $x \in \mathrm{Fix}_G(X)$, dann ist $g \bullet x = x$ für alle $g \in G$. Das ist genau dann der Fall, wenn $G_x = G$ gilt. Gemäß Definition besteht damit die Bahn $Gx = \{\ g \bullet x \mid g \in G\ \}$ nur aus dem Element x, d.h. $|Gx| = 1$. Da eine Bahn unter Gruppenoperation entsteht und eine Gruppe stets ein neutrales Element $e \in G$ besitzt, muss $e \bullet x = x$ in Gx enthalten sein. Aufgrund der Definition einer Faktorgruppe ist auch die Äquivalenz $[G : G_x] = 1$ genau dann wenn $G_x = G$ klar. □

Ein Elemente $x \in \mathrm{Fix}_G(X)$ ist in jedem Vertretersystem I zu finden, da gemäß Lemma II.4.2 die Äquivalenzklasse $Gx = \{x\}$ gilt. Da also die Bahn einelementig ist, bleibt einem gar keine andere Wahl als den Fixpunkt stellvertretend für die Äquivalenzklasse und somit als Element für das Vertretersystem I zu wählen. Wenn wir die Bahnengleichung

zunächst über die Fixpunkte x (mit $[G : G_x] = 1$) summieren und dann über die restlichen Summanden (mit $[G : G_x] > 1$), so erhalten wir Bahnengleichung in der Form

$$|X| = |\mathrm{Fix}_G(X)| + \sum_{\substack{x_i \in I \\ [G:G_{x_i}]>1}} [G : G_{x_i}], \tag{II.6}$$

wobei I ein entsprechendes Vertretersystem der Äquivalenzklassen von X mit $[G : G_x] > 1$ sein soll.

Beweis. Beachten wir, dass $\sum_{\substack{x \in I \\ [G:G_{x_i}]=1}} [G : G_{x_i}] = \sum_{\substack{x \in I \\ [G:G_{x_i}]=1}} 1 = |\mathrm{Fix}_G(X)|$ gilt, folgt durch die Anwendung der Bahnengleichung die Behauptung. □

Die Formel (II.6) erlaubt Aussagen über die Anzahl der Fixpunkte - später werden wir einen Satz über die Anzahl der Elemente einer speziellen Fixpunktmenge (genannt Zentrum) mit Hilfe dieser Formel beweisen.

II.4.3 Satz: (Fixpunktsatz)
Es sei G eine Gruppe der Ordnung p^r und p sei eine Primzahl. Operiert G auf einer endlichen Menge X, dann gilt

$$|X| = |\mathrm{Fix}_G(X)| \mod p$$

Insbesondere gibt es wenigstens einen Fixpunkt, wenn $|X|$ und p teilerfremd sind.

Bemerkung: Beachten Sie für den nachfolgenden Beweis, dass für ganze Zahlen a, b, c aus $c|a$ und $c|b$ folgt, dass $c|(a + b)$. Da $c|a$ und $c|b$ existieren ganze Zahlen $q_1, q_2 \in \mathbb{Z}$, so dass gilt: $a = q_1 c$ bzw. $b = q_2 c \Rightarrow c|(q_1 c + q_2 c)$.

Beweis. Nach Gleichung (II.6) ist $|X| - |\mathrm{Fix}_G(X)| = \sum_{[G:G_x]>1} [G : G_x]$. Auf der rechten Seite der Gleichug ist jeder einzelne Summand nach dem Satz von Lagrange ein Teiler von $|G| = p^r$. Aufgrund der Nebenbedingung $[G : G_x] > 1$ im Index der Summe, muss der Teiler von der Form $p^l, l \geq 1$ sein. Somit ist auch die Summe durch p teilbar, d.h. $p|(\sum_{[G:G_x]>1} [G : G_x])$ also auch $p|(|X| - |\mathrm{Fix}_G(X)|)$. Es ist demnach $|X| - |\mathrm{Fix}_G(X)|$ ein Vielfaches von p. Somit existiert eine ganze Zahl $q \in \mathbb{Z}$, so dass

$$\begin{aligned} pq &= |X| - |\mathrm{Fix}_G(X)| \\ \Rightarrow 0 &= |X| - |\mathrm{Fix}_G(X)| \mod p \\ \Rightarrow |X| &= |\mathrm{Fix}_G(X)| \mod p. \end{aligned}$$

Sind $|X|$ und p teilerfremd, dann ist p natürlich kein Teiler von X und es muss $\mathrm{Fix}_G(X)$ von Null verschieden sein. □

5. Die Konjugation

In diesem Abschnitt führen wir eine spezielle und sehr bedeutende Gruppenoperation ein - die Konjugation.

II.5.1 Definition: Sei $(G, \cdot)$ eine Gruppe, welche durch

$$\forall g, x \in G: \qquad g \bullet x := g \cdot x \cdot g^{-1}$$

auf sich selbst operiert. Die Operation $\bullet$ nennen wir **Konjugation** oder **Operation durch innere Automorphismen**. Zwei Elemente $x, y \in G$ heißen **konjugiert**, wenn es ein $g \in G$ gibt mit $y = gxg^{-1}$.

Bemerkung: Der gemäß Satz II.3.1 zur Konjugation assoziierte Homomorphismus $i : G \to \mathrm{Aut}(G)$ mit $\mathrm{Aut}(G) \subset S(G)$ ist definiert durch $g \mapsto i_g$. Dabei ist $i_g : G \times X \to X$ erklärt durch

$$x \mapsto i_g(x) := g \bullet x = g \cdot x \cdot g^{-1}.$$

Die Bahnen $Gh = \{\ g \bullet x = gxg^{-1} \mid g \in G\ \}$ der Konjugation heißen **Klassen Konjugierter**. Die Stabilisatoren für festes $x \in G$ ist - gemäß Definition - von der Form

$$G_x \ = \ \{\ g \in G \mid gxg^{-1} \ = \ x\ \} \ \subset \ G.$$

Formen wir die Gleichung $gxg^{-1} = x$ durch Multiplikation mit g von rechts um, so erhalten wir $gx = xg$. Daher besteht ein Stabilisator unter Konjugation gerade aus allen Gruppenelementen $g \in G$ die mit $x \in X$ vertauschbar sind.

II.5.2 Definition: Sei G eine Gruppe, die durch Konjugation $g \bullet x := gxg^{-1}$ auf sich selbst operiert.

1. Den Stabilisator

   $$Z_G(x) := G_x \ = \ \{\ g \in G \mid gxg^{-1} \ = \ x\ \}$$

   für ein $x \in G$ unter Konjugation bezeichnen wir als **Zentralisator** von $x \in G$.

2. Sei U eine Teilmenge von G, dann bezeichnen wir

   $$gUg^{-1} := \ \{\ gug^{-1} \mid u \in U\ \}$$

   als den **Normalisator** von U.

3. Die Menge der Fixpunkte

   $$Z(G) := \mathrm{Fix}_G(G) \ = \ \{x \in G \mid gxg^{-1} = x \quad \forall g \in G\ \}$$

   unter der Konjugation nennen wir **Zentrum** einer Gruppe.

Der Normalisator besteht aus denjenigen $g \in G$, für die gilt, dass U unter Konjugation mit g invariant ist. Die Bahnengleichung heißt für die spezielle Gruppenoperation Konjugation auch Klassengleichung.

II.5.3 Satz: (Klassengleichung)
Sei G eine endliche Gruppe und sei $I = \{x_1, \ldots, x_i, \ldots, x_k\}$ ein Vertretersystem der Konjugationsklassen in $G \setminus Z(G)$, also $[G : G_{x_i}] > 1$. Dann gilt

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : G_{x_i}]. \tag{II.7}$$

Beweis. Folgt unmittelbar aus Gleichung II.6 und der Identität $Z(G) = \mathrm{Fix}(G)$. □

II.5.4 Folgerung: Ist G eine Gruppe der Ordnung p^r und p ist eine Primzahl, dann hat G ein nicht trivales Zentrum $Z(G) \neq \{e\}$, d.h. $|Z(G)| > 1$.

Beweis. Da das Zentrum $Z(G)$ eine Untergruppe von G ist, hat $Z(G)$ nach dem Satz von Lagrange die Ordnung p^k mit $k \in \mathbb{N} \cup \{0\}$ und $0 \leq k \leq r$. Nach Gleichung II.7 ist

$$|Z(G)| \;=\; |G| - \sum_{x \in I} [G : G_x],$$

wobei I ein Vertretersystem sei. Aus $p|\mathrm{ord}(G)$ und $p|(\sum_{x\in I} [G : G_x])$ folgt, dass $|Z(G)|$ ebanfalls durch p teilbar ist. Das bedeutet aber $k \geq 1$ bzw. $|Z(G)| > 1$. □

Den Beweis der letzten Folgerung kann man mittels eines Widerspruchbeweises sehr schön führen.

Beweis. Dazu nimmt man an, dass $Z(G)$ ein triviales Zentrum -unter gegebenen Voraussetzungen- hat, d.h. $Z(G) = 1$. Da $|G| = p^r$ gilt, folgt damit

$$\sum_{x \in I} [G : G_x] = p^r - 1.$$

Da jedoch $p| \sum_{x\in I} [G : G_x]$ kann $|Z(G)| = 1$ nicht gelten. Widerspruch! □

Beachten Sie, dass wir zum Beweis der letzten Folgerung auch den Fixpunktsatz anwenden hätten können - daher ähnelnt sich auch die Beweisführung beider Sätze.

III. Die Sätze von Sylow

Die klassischen Sätze von Ludwig SYLOW (norwegischer Mathematiker, 1832-1918), welche wir in diesem Abschnitt studieren werden, geben Auskunft über die Existenz und Anzahl bestimmter Untergruppen einer endlichen Gruppen. Kehren wir noch einmal zum Satz von Lagrange zurück - dieser besagt, dass eine Untergruppe H von G, falls Sie denn überhaupt existiert, Teiler der Gruppenordnung $|G|$ sein muss. Allerdings existiert im Allgemeinen nicht zu jedem Teiler einer Gruppenordnung eine entsprechende Untergruppen. So besitzen z.B. die alternierenden Gruppen A_n für $n \geq 5$ keinen nicht-trivialen Normalteiler und haben damit auch keine Untergruppe der Ordnung $\frac{1}{2}|A_n|$ mit $|A_n|$ gerade.

Für zyklische Gruppen haben wir eine genaue Übersicht über sämtliche Untergruppen, für allgemeine endliche Gruppen ist man noch weit von diesem Ziel entfernt. Die Sylowsätze garantieren zumindest die Existenz von Untergruppen zu bestimmten Ordnungen. Insofern könnte man die Sylowsätze auch als *teilweise „Umkehrung" des Satzes von Lagrange* interpretieren.

1. Erster Sylowsatz

Für den Beweis des ersten Sylowsatzes benötigen wir die folgenden zahlentheoretische Überlegungen.

III.1.1 Lemma: Sei $n \in \mathbb{N}$, p eine Primzahl und $n = p^r m$ mit $\mathrm{ggT}(p, m) = 1$, d.h. p^r ist die höchste p-Potenz die n teilt (man sagt auch: „die in n aufgeht"). Dann gilt für jedes natürliche $1 \leq s \leq r$:

$$p^{r-s+1} \nmid \binom{n}{p^s} \tag{III.1}$$

Beweis. Gemäß Definition des Binomialkoeffizienten ist $\binom{n}{p^s} = \frac{n(n-1)\ldots(n-p^s+1)}{1\cdot 2\ldots p^s}$. Setzen wir nun $n = mp^r$ ein, so erhalten wir

$$\begin{aligned}\frac{n(n-1)\dots(n-p^s+1)}{1\cdot 2\dots\cdot p^s} &= \frac{mp^r(mp^r-1)\dots(mp^r-p^s+1)}{1\cdot 2\dots\cdot p^s}\\ &= mp^{r-s}\prod_{i=1}^{p^s-1}\frac{mp^r-i}{i}\\ &= mp^{r-s}\left(\frac{mp^r-1}{1}\right)\left(\frac{mp^r-2}{2}\right)\dots\left(\frac{mp^r-(p^s-1)}{(p^s-1)}\right)\\ &= mp^{r-s}\binom{n-1}{p^s-1}\end{aligned}$$

Da $mp^{r-s} < p^{r-s+1}$ kann $p^{r-s+1} \nmid mp^{r-s}$ und aufgrund der obigen Identitäten, müssen wir noch $p^{r-s+1} \nmid \binom{n-1}{p^s-1}$ zeigen. Wir schreiben dazu

$$\binom{n-1}{p^s-1} = \prod_{i=1}^{p^s-1}\frac{mp^r-i}{i} =: \prod_{i=1}^{p^s-1}\frac{a_i}{b_i},$$

wobei $a_i, b_i \in \mathbb{N}$ teilerfremd sind.

Wir werden in jedem Faktor aus $\prod_{i=1}^{p^s-1}\frac{mp^r-i}{i}$, welches eine ganze Zahl ist, die möglichen p-Potenzen kürzen und im Anschluss daran prüfen, ob das gekürzte Produkt noch durch p teilbar ist.

Wir nehmen nun an, dass p ein Teiler dieses Produkts sei, so muss p erst recht ein Teiler des Produts der Zähler sein. Da p eine Primzahl ist, teilt p wenigstens einen Faktor, sagen wir $p|(mp^{r_k}-k)$. Da wir wegen $i \le p^s-1 \le p^s \le p^r \Rightarrow s \le r$ in den Faktoren $\frac{mp^r-i}{i}$ nur kleinere p-Potenz kürzen können, müssen die verbleibenden Exponenten r_j sämtlich größer 0 sein - insbesondere muss $r_k > 0$ sein. Damit folgt aus $p|(mp^{r_k}-k)$, dass $p|k$. Das widerspricht jedoch $\mathrm{ggT}(k,p) = 1$, denn p ist eine Primzahl. Also ist p kein Teiler des obigen Produkts und p^{r-s} ist die höchste p-Potenz, die in $\binom{n}{p^s}$ aufgeht. □

III.1.2 Satz: (Erster Sylowsatz)
Ist G eine endliche Gruppe der Ordnung $n = mp^r$, wobei p eine Primzahl ist, die m nicht teilt, d.h. $\mathrm{ggT}(p,m) = 1$.
Dann gibt es zu jedem s mit $1 \le s \le r$ eine Untergruppe von G der Ordnung p^s.

Beweis. Es sei $X := \{A \subseteq G : |A| = p^s, 1 \le s \le r\}$ die Menge aller Teilmengen von G, die genau p^s Elemente enthalten. Wir wissen aus der Kombinatorik, dass X dann $|X| = \binom{n}{p^s}$ gilt.

G operiert auf X durch $g \bullet A = gA := \{ga | a \in A\}, g \in G, A \in X$. Sodann gilt $|gA| = |A|$, da die Operation $\bullet : G \times X \to X$ mit $(g,A) \mapsto gA$ eine bijektive Abbildung erklärt.

Da wir also mit G auf X operieren, können wir X in seine disjunkten Bahnen zerlegen, d.h. $X = \bigcup_{A\in X} GA$ und Satz II.3.9 liefert

$$\binom{n}{p^s} = |X| = \sum_{A\in I}|GA| = \sum_{A\in I}[G : G_A], \tag{III.2}$$

wobei I ein Vertretersystem für die Bahnen sein soll. Da $p^{r-s+1} \nmid \binom{n}{p^s}$ nach Lemma III.1.1, gibt es wenigsten einen Summanden auf der rechten Seite von Gleichung III.2, der nicht durch p^{r-s+1} teilbar ist. D.h. es gibt $A' \in X$ mit $p^{r-s+1} \nmid [G : G_{A'}]$, es ist also p^{r-s} die höchste p-Potenz, die als Teiler von $[G : G_{A'}]$ in Frage kommt. Nach Satz II.3.7 ist $G_{A'}$ eine Untergruppe von G, daher folgt mit Hilfe des Satz von Lagrange die Gleichung

$$p^r m = |G| = [G : G_{A'}]|G_{A'}|.$$

D.h. p kommt als Faktor genau r-mal im Produkt $[G : G_{A'}]|G_{A'}|$ vor, jedoch nach dem Vorgehrgehenden höchstens $r - s$ mal in $[G : G_{A'}]$. Folglich ist der Faktor p in der Untergruppenordnung $|G_{A'}|$ mindesten s mal enthalten; insbesondere gilt $|G_{A'}| \geq p^s$. Ist nun $a' \in A'$, so folgt aus der Definition des Stabilisators $G_{A'}A' = A'$ bzw. $G_{A'}a' \subseteq A'$. Das ergibt für die Anzahl der Elemente des Stabilisators $G_{A'} : |G_{A'}| = |G_{A'}a'| \leq |A'| = p^s$. Insgesamt folgt also $|G_{A'}| = p^s$. Der Stabilisator $G_{A'}$ von A' ist demnach die gesuchte Untergruppe von G der Ordnung p^s. □

Eine wichtige Folgerung aus dem ersten Sylow-Satz ist

III.1.3 Folgerung: (Satz von Cauchy)
Ist G eine endliche Gruppe und die Primzahl p ein Teiler der Ordnung von G, d.h. $p|\mathrm{ord}(G)$, dann enthält G ein Element der Ordnung p.

Beweis. Nach dem ersten Sylowsatz exisitert eine Untergruppe P von G mit Ordnung p. Jede Gruppe mit Primzahlordnung ist zyklisch, d.h. auch P ist zyklisch. Damit muss es also ein Element $a \in P$ geben mit $\langle a \rangle = P$. Somit ist a das gesuchte Element. □

Der erste Sylowsatz proklamiert also, dass eine Gruppe G der Ordnung mp^r stets Untergruppen P_s der Ordnungen p^s mit $(1 \leq s \leq r)$ besitzt. Damit sind die Untergruppenordnungen Teiler der Gruppenordnungen. Es ist klar, dass solche Gruppen ausgezeichent sind. Im nächsten Beispiel b) werden wir die Beweisidee des ersten Sylowsatzes am Einzelfall durchspielen.

III.1.4 Beispiel: a) Es sei G eine Gruppe der Ordnung $12 = 2^2 \cdot 3$, d.h. $|G| = 12$. Nach dem ersten Sylowsatz existiert mindestens jeweils eine Untergruppe der Ordnungen $2, 2^2 = 4$ und 3. Wie wir später noch sehen werden sind die Gruppen der Ordnungen 4 und 3 so genannte p-Sylow-Gruppen.

b) Betrachten wir alle 2-elementigen Mengen der Restklassengruppe $\mathbb{Z}/4\mathbb{Z}$, dann erhalten wir die $\binom{4}{2} = \frac{4 \cdot 3}{2} = 6$-elementige Mengefamilie

$$X := \{\ \{0,1\},\ \{0,2\},\ \{0,3\},\ \{1,2\},\ \{1,3\},\ \{2,3\}\ \}$$

Die Gruppe $\mathbb{Z}/4\mathbb{Z}$ operiert auf der Menge X vermöge

$$(\mathbb{Z}/4\mathbb{Z}) \times X \to X \quad \text{definiert durch} \quad (g, A) \mapsto g \bullet A := gA := \{\ g + a \mid a \in A\ \}.$$

Die Zerlegung von X in Äquivalenzklassen bzw. Bahnen ist gegeben durch

$$X = \underbrace{\{\ \{0,1\}, \{0,3\}, \{1,2\}, \{2,3\}\ \}}_{=:X_1} \cup \underbrace{\{\ \{0,2\}, \{1,3\}\ \}}_{=:X_2},$$

wobei die Bahnen wie folgt erzeugt werden:

$$X_1 = (\mathbb{Z}/4\mathbb{Z})\{0,1\} = (\mathbb{Z}/4\mathbb{Z})\{0,3\} = (\mathbb{Z}/4\mathbb{Z})\{1,2\} = (\mathbb{Z}/4\mathbb{Z})\{2,3\} \quad \text{und}$$
$$X_2 = (\mathbb{Z}/4\mathbb{Z})\{0,2\} = (\mathbb{Z}/4\mathbb{Z})\{1,3\}.$$

Das zugehörige Repräsentantensystem I enthält demnach exakt zwei Mengen, z.B. $\{0,1\}$ und $\{0,2\}$. Für alle $A \in X_1$ ist der Stabilisator trivial, d.h. es ist $(\mathbb{Z}/4\mathbb{Z})_A = \{0\}$. Für $A \in X_2$ entspricht der Stabilisator $(\mathbb{Z}/4\mathbb{Z})_A$ der Menge $\{0,2\}$. Gemäß Satz II.3.9 ist

$$6 = \binom{4}{2^1} = |X| = \sum_{A \in I} |(\mathbb{Z}/4\mathbb{Z})A| = \sum_{A \in I} [(\mathbb{Z}/4\mathbb{Z}) : (\mathbb{Z}/4\mathbb{Z})_A].$$

Da $4 \nmid 6$ gibt es wenigstens ein $A' \in X$ mit $4 \nmid [(\mathbb{Z}/4\mathbb{Z}) : (\mathbb{Z}/4\mathbb{Z})_{A'}]$. Wie Sie wohl schon vermuten kann A' aus der Bahn X_2 beliebig gewählt werden. Als Stabilisator ist $(\mathbb{Z}/4\mathbb{Z})_{A'}$ eine Gruppe und mit dem Satz von Lagrange folgt

$$2^2 = 4 = |\mathbb{Z}/4\mathbb{Z}| = [(\mathbb{Z}/4\mathbb{Z}) : (\mathbb{Z}/4\mathbb{Z})_{A'}] \cdot |(\mathbb{Z}/4\mathbb{Z})_{A'}|,$$

d.h. 2 kommt als Faktor genau zwei Mal im Produkt vor, jedoch genau einmal in $6 = 2 \cdot 3$. Folglich ist 2 als Faktor in $|(\mathbb{Z}/4\mathbb{Z})_{A'}|$ enthalten. Offenbar ist dies in diesem Fall gerade die Gruppenordnung von $\{0,2\}$.

2. p-Gruppen und p-Sylow-Gruppen

III.2.1 Definition: Es sei p eine Primzahl und G eine Gruppe. G heißt eine **p-Gruppe**, wenn jedes Element von G eine p-Potenz als Ordnung hat; d.h., wenn es zu jedem $g \in G$ ein $k \in \mathbb{N}_0$ gibt mit $g^{p^k} = e$.

Eine dazu äquivalente Charakterisierung von p-Gruppen haben wir in folgende Bemerkung gefasst.

Bemerkung: Sei p eine Primzahl. Eine endliche Gruppe G heißt p-Gruppe, falls die Ordnung von G eine Potenz von p ist, also $|G| = p^k$ für ein $k \in \mathbb{N}_0$ gilt.

Beweis. Weil nach dem Satz von Lagrange die Ordnung einer Untergruppe die Gruppenordnung teilt, ist *jede* Untergruppe einer p-Gruppe ebenfalls eine p-Gruppe (nämlich mit Ordnung $p^l, l \leq k$). Jede Untergruppe ist selbst auch zyklisch und die Ordnung eines *jeden* Elements einer p-Gruppe ist eine Potenz von p. Weil für einen Normalteiler N von G die Formel

$$|G| = |N| \cdot |G/N|, \qquad \text{also} \qquad |G/N| = \frac{|G|}{|N|}$$

gilt, ist auch jede Faktorgruppe G/N einer p-Gruppe selbst eine p-Gruppe. □

Unter den zu jedem Primteiler p der Gruppenordnung mp^r von G gefundenen p-Untergruppen wollen wir die mit mit maximaler Ordnung etwas näher betrachten. Die Definition fassen wir dabei so, dass sie auch für beliebige, nicht nur für endliche, Gruppen gelten.

III.2.2 Definition: Es sei G eine Gruppe und $P \leq G$ eine Untergruppe. P heißt p-**Sylow-Gruppe** von G, wenn gilt

(S_1) P ist eine p-Untegruppe von G.

(S_2) Ist H eine p-Untergruppe von G mit $P \subseteq H$, dann ist $P = H$.

Die p-Sylowgruppen sind also in der durch (S_2) präzisierten Bedeutung maximal unter den p-Untergruppen. Insbesondere ist jede p-Gruppe G gleich ihrer *einzigen* p-Sylow-Gruppe P, in diesem Fall ist die Gruppenordnung ja $|G| = mp^r = p^r$, also $m = 1$. Aufgrund der Maximalitätseigenschaft der p-Sylowgruppe P von G muss damit $G = P$ gelten.

III.2.3 Satz: Ist G eine endliche Gruppe der Ordnung $n = mp^r$, mit einer Primzahl p, die m nicht teilt, dann ist jede Untergruppe P der Ordnung p^r eine p-Sylow-Gruppe von G.

Beweis. Offensichtlich ist P eine p-Untergruppe, denn ihre Ordnung p^r ist eine p-Potenz, welche sogar $|G| = mp^r$ teilt. Wir müssen also lediglich noch (S_2) zeigen. Dazu sei $H \leq G$ eine p-Untergruppe mit $P \subseteq H \subseteq G$ - da alle Untergruppen einer p-Gruppe selbst wieder p-Gruppen sind, folgt $|H| = p^l$. Mit dem Satz von Lagrange folgt daher $l \leq r$, also $|H| \leq |P|$. Nach Voraussetzungen ist $P \subseteq H$, also $|P| \leq |H| \Rightarrow P = H$. □

Dieser Satz bzw. dessen Beweis bringt die bereits genannte und die ebenfalls sehr beliebte (nun folgende) alternative bzw. äquivalente Definition einer p-Sylow-Gruppe zusammen:

III.2.4 Definition: Es sei G eine endliche Gruppe, p eine Primzahl und $|G| = p^r m$ mit m teilerfremd zu p. Eine Untergruppe P von G heißt **p-Sylow-Gruppe** von G, falls $|P| = p^r$ gilt. Die Ordnung von P ist also die höchste p-Potenz, die $|G|$ teilt.

III.2.5 Folgerung: Hat die Gruppe G die Ordnung mp^r, p eine Primzahl und $\mathrm{ggT}(m, p) = 1$, dann enhält G wenigstens eine p-Sylow-Gruppe der Ordnung p^r.

Beweis. Der erste Sylowsatz besagt, dass G eine Untergruppe der Ordnung p^r enthält, diese ist gemäß Satz III.2.3 eine p-Sylow-Gruppe von G. □

III.2.6 Beispiel: Es sei die Gruppe $\mathbb{Z}_{4900}$ gegeben. Es ist $4900 = 2^2 \cdot 5^2 \cdot 7^2$. Nach dem ersten Sylowsatz existieren also Untergruppen der Ordnungen $2, 4, 5, 25, 7$ und 49. Insbesondere existiert mindestens eine 2-Sylow-Gruppe P_2, eine 5-Sylow-Gruppe P_5 und eine 7-Sylow-Gruppe P_7. Die Sylowgruppen sind gerade diejenigen mit maximaler p-Potenz, d.h. P_2 besteht aus 2^2 Elementen, P_5 bestehend aus 5^2 Elementen und P_7 besteht aus 7^2 Elementen.

Wir untersuchen nun das Verhalten von p-Sylow-Gruppen unter Konjugation.

III.2.7 Lemma: Es sei P eine p-Sylow-Gruppe von G. Dann sind alle zu P konjugierten Untergruppen gPg^{-1}, $g \in G$, auch p-Sylow-Gruppen von G.

Beweis. Zum Beweis verwenden wir die im Abschnitt über Konjugation definierte Abbildung i_g. Diese stellt einen bijektiven Homomorphismus (genauer Automorphismus) dar. Das Bild einer Gruppe unter einem Homomorphismus ist selbst eine Untergruppe des Bildraumes; da die Abbildung zudem bijektiv ist hat das Bild dieselbe Mächtigkeit wie P. Insgesamt folgt, dass gPg^{-1} eine p-Sylow-Gruppe ist. □

III.2.8 Satz: Es sei P eine p-Sylow-Gruppe von G. Ist P die einzige p-Sylow-Gruppe von G, so ist P ein Normalteiler.

Beweis. Ist P die einzige p-Sylow-Gruppe, so ist $gPg^{-1} = P \Leftrightarrow gP = Pg$ für alle $g \in G$ gemäß Lemma III.2.7. Demnach ist P ein Normalteiler von G. □

Die Aussage des letzten Satzes wird oft in Anwendungen der Sylow-Sätze verwendet. Kann man nachweisen, dass nur eine Sylowgruppe existiert, so muss diese ein Normalteiler sein.

III.2.9 Folgerung: Sei G eine abelsche Gruppe, dann gibt es genau eine p-Sylowgruppe.

Beweis. Da in abelschen Gruppen jede Untergruppe ein Normalteiler ist, impliziert der letzte Satz gerade die Behauptung. □

3. Zweiter Sylowsatz

Der nun folgende zweite Satz von Sylow gibt Auskunft über die Lage der p-Untergruppen bzw. der p-Sylowgruppen.

III.3.1 Satz: (Zweiter Sylowsatz)
Es sei G eine endliche Gruppe der Ordnung mp^r, p eine Primzahl und P eine p-Sylowgruppe von G. Dann gilt:

(i) Ist H eine Untergruppe von G, die eine p-Gruppe ist, so ist H in einer zu P konjugierten p-Sylow-Gruppe enthalten.

(ii) Alle p-Sylow-Gruppen von G sind konjugiert, insbesondere also isomorph.

Beweis. Wir nehmen zuerst an, dass P eine p-Sylow-Gruppe der Ordnung p^r ist. Es sei $X := \{gP | g \in G\}$ die Menge aller Linksnebenklassen von P in G. Ferner sei U eine beliebige p-Untergruppe von G. Wir lassen U auf X durch $(u, gP) \mapsto (ug)P$ operieren, d.h. die p-Untergruppe opiert auf der Menge aller Linksnebenklassen von P. Verifizieren Sie dies bitte!

Es zerfällt X in disjunkte Bahnen, $X = \bigcup UgP$. Wegen $|X| = [G : P] = \frac{|G|}{|P|} = \frac{mp^r}{p^r} = m$ ist p kein Teiler von X, da nach Voraussetzungen $\mathrm{ggT}(p, m) = 1$. Daher muss es in $|X| = \sum |UgP|$ wenigstens einen Summanden geben, der nicht durch p teilbar ist. Wir erinnern uns, hier werden die Kardinalitäten der einzelnen Bahnen $UgP \subset X$ aufaddiert.

Es sei also UaP eine Bahn mit $p \nmid |UaP|$.

Mit der Formel II.2 folgt die Gleichung $|UaP| = [U : U_{aP}]$. Wenden wir nun die Folgerung II.3.8 auf die Untergruppe U an, so folgt, dass jede U-Bahn (Wortspiel!) ein Teiler der Gruppenordnung U und demnach selbst eine p-Potenz ist. Also muss $|UaP| = 1 \Leftrightarrow aP \in \mathrm{Fix}_U X$ gelten. Da aP ein Fixpunkt ist, muss für alle $u \in U : uaP = aP$ bzw. $(a^{-1}ua)P = P$ oder $(aua^{-1}) \in P$ für alle $u \in U$. Somit haben wir (i) des Satzes für p-Sylow-Gruppen der Ordnung p^r bewiesen.

Wenden wir den bewiesenen Teil an und setzen dabei $U := P'$, d.h. U ist nun selbst eine beliebige p-Sylow, so zeigt sich, dass $bP'b^{-1} \subseteq P$ für ein $b \in G$ (und $|P| = p^r$). Da auch alle konjugierten p-Sylow-Gruppen selbst p-Sylow-Gruppen sind (vgl. Bemerkung 6) und mit (S_2) folgt $bP'b^{-1} = P$, womit gezeigt ist, dass alle p-Sylow-Gruppen die Ordnung p^r haben und die zuerst gemachte Einschränkung $|P| = p^r$ in Wirklichkeit keine ist. □

III.3.2 Lemma:

(i) Es sei G eine Gruppe und p eine Primzahl. Ist G abelsch, so gibt es nur eine p-Sylow-Gruppe von G.

(ii) Ist N ein Normalteiler von G, der eine p-Gruppe ist, so ist N in allen p-Sylow-Gruppen von G enthalten.

(iii) Ist K ein Normalteiler von G und P eine p-Sylow-Gruppe von K, so gilt $G = KN_G(P)$. Diese Erkenntnis ist auch unter dem Namen Frattini-Argument bekannt.

Beweis. (i) Ist P eine p-Sylowgruppe einer abelschen Gruppe G, so gilt $\forall g \in G, p \in P : gp = pg \Rightarrow gP = Pg \Rightarrow gPg^{-1} = P$. Weil alle p-Sylow-Gruppen einer Gruppe G konjugiert zueinander sind, also von der Form gPg^{-1} für ein $g \in G$ sind, ist P dann die einziege p-Sylow-Gruppe.

(ii) Nach dem zweiten Sylowsatz ist H zunächst in einer p-Sylow-Gruppe P enthalten, also $H \subset P$. Für beliebiges $g \in G$ ergibt sich

$$H = gHg^{-1} \subset gPg^{-1},$$

denn N ist nach Voraussetzungen ein Normalteiler. Da jede p-Sylow-Gruppe von G von der Form gPg^{-1} ist, ist damit die Behauptung gezeigt.

(iii) Beachten Sie, dass $N_G(P)$ den Stabilisator der Konjugation auf der Menge aller Untergruppen bezeichnet und P eine einzelne (die p-Sylow-Gruppe von K) ist. Weil K ein Normalteiler ist, ist gPg^{-1} für ein beliebiges $g \in G$ eine Untergruppe von K, also wieder eine p-Sylow-Gruppe von K. Weil alle p-Sylowgruppen von K konjugiert in K sind, gibt es ein $k \in K$ mit

$$gPg^{-1} = kPk^{-1}, \text{ also } (k^{-1}g)P(k^{-1}g)^{-1} = P.$$

Daher ist $k^{-1}g \in N_G(P)$, also $g = k(k^{-1}g) \in KN_G(P)$. Damit haben wir $G = KN_G(P)$.

□

4. Dritter Sylowsatz

Über die Anzahl der p-Sylow-Gruppen, gibt schließlich der letzt der Sylowsätze Auskunft.

III.4.1 Satz: (Dritter Sylowscher Satz)
Es sei G eine endliche Gruppe, p eine Primzahl und Teiler der Gruppenordnung $|G|$, sowie s_p die Anzahl der p-Sylow-Gruppen von G. Dann gilt:

(i) s_p ist ein Teiler der Gruppenordnung $|G|$, d.h. $s_p | ord(G)$,

(ii) $s_p - 1$ ist ein Vielfaches von p, d.h. $s_p \equiv 1[modp]$, insbesondere $s_p \neq 0$.

Bemerkung: Die Voraussetzung, dass p die Gruppenordnung teilt wird in vielen Versionen des dritten Sylowsatzes mit aufgenommen. Jedoch ist diese Voraussetzung nicht notwendig: Im Fall, dass $p \nmid ord(G)$ (also insb. auch für $p > |G|$) erfüllt die triviale p-Sylow-Gruppe $\{1\}$ den Satz. Sodann ist $r = 0$ die höchste p-Potenz, die in der Gruppenordnung aufgeht. Natürlich muss hierzu die triviale p-Sylow-Gruppe $\{1\}$ in der Definition mit berücksichtigt sein.

Beweis. Wir haben in Lemma III.3.2 gesehen, dass alle p-Sylow-Gruppen von G konjugiert sind. G operiert also transitiv auf der Menge

$$X := \{\ P \leq G\ :\ P\ \text{ ist eine } p\text{-Sylow-Gruppe von G }\}$$

aller p-Sylow-Gruppen von G durch Konjungtion, d.h. $\psi(g, P) := g \cdot P := gPg^{-1}$. Die Bahn $G \cdot P = \{g \cdot P | g \in G\}$ jeder p-Sylow-Gruppe P ist also gleich X nach dem zweiten Sylowsatz. Daher ist

$$s_P = |X| = |G \cdot P| = [G : G_P]$$

ein Teiler von $|G|$. Dazu wende man den Satz von Lagrange auf die Untergruppe G_P von G an und beachte letzte Gleichung.

Zum Beweis der zweiten Behauptung lassen wir eine p-Sylow-Gruppe P auf X durch Konjugation operieren durch $P \cdot x := PxP^{-1}$. Beachten Sie, dass nun nicht mehr G, sondern eine einzelne p-Sylow-Gruppe auf X operiert. Weil P eine p-Gruppe ist, gilt mit dem Fixpunktsatz

$$s_P = |X| = |\mathrm{Fix}_P(X)| + mp \text{ für ein } m \in \mathbb{N}_0.$$

Wir behaupten nun

$$\mathrm{Fix}_P(X) = \{P\}, \text{ also } |\mathrm{Fix}_P(X)| = 1.$$

Daraus folgt dann, dass $s_p - 1 = mp$ ein Vielfaches von p ist.

Wegen $pPp^{-1} = P$ für alle $p \in P$ ist offenbar $P \in \mathrm{Fix}_P(X)$, da P eine Gruppe ist. Es sei nun $P' \in \mathrm{Fix}_P(X)$, also P' eine p-Sylow-Gruppe mit

$$pP'p^{-1} = P' \text{ für alle } p \in P.$$

Jetzt haben wir die Situation des ersten Isomorphiesatzes. Es ist also $P \cap P'$ Normalteiler von P und P' ist ein Normalteiler von PP'. Damit gibt es einen Isomorphismus nach dem ersten Isomorphiesatz, so dass

$$PP'/P' \cong P/(P \cap P').$$

Da P bzw. P' jeweils p-Sylow-Gruppen sind und damit selbstverständlich p-Gruppen, ist auch die Faktorgruppe $P/(P \cap P')$ und damit PP'/P' eine p-Gruppe. Also ist auch PP' eine p-Gruppe. Offensichtlich gilt $PP' \supset P'$. Da PP' ein p-Gruppe und P' eine p-Sylow-Gruppe ist (und damit ein Element enthält, welches Ordnung mit maximale p-Potenz hat) kann nur $PP' = P'$ gelten. Damit folgt $P \subset P'$ und somit die Identität $P = P'$.

Damit ist $\mathrm{Fix}_P(X) = \{P\}$ gezeigt und damit die Behauptung. □

IV. Anwendungen der Sylowsätze

Abschließend werden wir noch einige typische (aber auch ebenso einfache) Anwendungen der Sylowsätze betrachten. Wir beginnen diesen Abschnitt mit einem Hilfssatz, den wir im darauffolgenden Beispiel benötigen werden.

1. Anwendungen

IV.1.1 Lemma: Sind P und Q Normalteiler einer Gruppe G mit $P \cap Q = \{e\}$, so sind P, Q elementweise vertauschbar, also $ab = ba$ für alle $a \in P, b \in Q$.

Beweis. Für $a \in P, b \in Q$ ist $aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in Q$, weil Q ein Normalteiler ist. Analog folgt dann $a(ba^{-1}b^{-1}) \in P$, weil P ein Normalteiler ist. Also ist $aba^{-1}b^{-1} \in P \cap Q = \{e\}$. □

IV.1.2 Beispiel: *Jede Gruppe der Ordnung 15 ist zyklisch.*

Es ist $15 = 3 \cdot 5$, damit folgt mit dem ersten Sylowsatz, dass mindestens eine Gruppe der Ordnung 5^1 und mindestens eine Gruppe der Ordnung 3^1 existiert. Diese sind dann jeweils 3- bzw. 5-Sylow-Gruppen.

Es sei s_3 die Anzahl der 3-Sylow-Gruppen und s_5 die Anzahl der 5-Sylow-Gruppen von G. Nach dem dritten Sylow-Satz ist dann $s_3 \in \{1, 3, 5, 15\}$, da s_3 ein Teiler der Gruppenordnung $|G| = 15$ ist. Ferner gilt $s_3 \in \{1, 4, 7, 10, 13, 16, \ldots\}$, da $s_3 = 1 + 3k, k \in \mathbb{N}_0$. Bildet man die Schnittmenge beider Mengen, so ergibt sich dadurch die mögliche Anzahl an 3-Sylow-Gruppen s_3. Wir sehen also, dass nur $s_3 = 1$ gelten kann. Analog ermitteln wir die Anzahl s_5 der 5-Sylow-Gruppen, dabei ergeben sich die Mengen $\{1, 3, 5, 15\}$ bzw. $\{1, 6, 11, 16, \ldots\}$ also $s_5 = 1$. Es sei im Folgenden G die einzige 5-Sylow-Gruppe und Q die einzige 3-Sylow-Gruppe.

Nun wenden wir Satz III.2.8 an und erkennen, dass die P und Q beide Normalteiler von G sind. Das ermöglicht uns Lemma IV.1.1 anzuwenden, d.h. P und Q sind elementeweise vertauschbar. Als Gruppen von Primzahlordnung sind P und Q zyklisch. Es gibt also ein $a \in P$ der Ordnung 3 und ein $b \in Q$ der Ordnung 5. Wegen $ab = ba$ hat ab die Ordnung 15, da $\mathrm{ggT}(3, 5) = 1$. Also wird G von ab erzeugt und G ist zyklisch.

Mit Hilfe der p-Sylow-Sätze kann man auch weitreichende theoretische Erkenntnisse gewinnen, z.B. kann man zeigen, dass eine endliche abelsche Gruppe das direkte Produkt seiner p-Sylow-Gruppen ist.

Wir beschränken uns hier jedoch auf einfache Anwendungen, wie auch das folgende

IV.1.3 Beispiel: Wir untersuchen nun Gruppen G der Ordnung $12 = 3 \cdot 2^2$.

Wieder wenden wir den dritten Sylowsatz an, sei dazu s_3 die Anzahl der 3-Sylow-Gruppen und s_5 die Anzahl der 5-Sylow-Gruppen.

Es ist $s_3 \in \{1, 2, 3, 4, 6\}$, da s_3 ein Teiler der Gruppenordnung ist. Weiter ist $s_3 \in \{1, 4, 7, 10, 13, \ldots\}$, da $s_3 = 1 + 3k, k \in \mathbb{N}_0$. Die Schnittmenge bildet die potentiellen Kandidaten für die Anzahl der 3-Sylowgruppen, also $s_3 \in \{1, 4\}$. Analog erhalten wir $s_2 \in \{1, 3\}$.

Der Fall, dass $s_3 = 4$ und $s_2 = 2$ kann ausgeschlossen werden: Da der Durchschnitt einer jeden p-Sylow-Gruppe kann nur $\{e\}$ sein, es bleiben also noch 11 Elemente für die Sylow-Gruppen über. Vier verschiedene 3-Sylow-Gruppen haben zusammen $2 \cdot 4$ Elemente ungleich e. Zusammen mit e sind dies dann allein 9 Elemente, die von den vier 3-Sylow-Gruppen in Anspruch genommen werden. Damit bleiben lediglich noch 3 Elemente für die 2-Sylow-Gruppen, d.h. es kann keine zwei 2-Sylow-Gruppen geben.

Literaturverzeichnis

[1] Algebra, Teil 1, K. Meyberg, 1980, Hanser Verlag.

[2] Algebra, Teil 2, K. Meyberg, 1980, Hanser Verlag.

[3] Algebra – Erster Teil, L. Rédei, 1959, Akademische Verlagsgesellschaft Geest & PortigK.-G.

[4] Repetitorium der Algebra, Michael Holz, 2005, 2. Auflage, Binomi Verlag.

[5] Algebra I, Winfried Scharlau, 2004, FernUniversität in Hagen.

[6] Einführung in die Mengenlehre, Oliver Deister, 2004, Springer Verlag.