7. Gruppentheorie und die Sätze von Sylow

In den letzten beiden Kapiteln haben wir mit Hilfe der Galoistheorie die Frage nach Zwischenkörpern einer gegebenen Körpererweiterung auf die Frage nach Untergruppen einer gegebenen Gruppe zurückgeführt. Wir wollen nun also Gruppen untersuchen und uns dabei insbesondere fragen, ob und wie man in einer (endlichen) Gruppe Untergruppen einer gegebenen Ordnung finden kann. Im Gegensatz zur direkten Suche nach Zwischenkörpern wird sich dies in der Tat als deutlich einfacher herausstellen.

Man kann diese Fragestellung in gewissem Sinne als eine „Umkehrung des Satzes von Lagrange" bezeichnen: ist G eine endliche Gruppe und $U \leq G$ eine Untergruppe, so besagt dieser Satz ja bekanntlich, dass $|U|$ stets ein Teiler von $|G|$ ist [G, Satz 5.10]. Wir wollen uns jetzt die umgekehrte Frage stellen: ist n ein Teiler von $|G|$, gibt es dann immer eine Untergruppe $U \leq G$ mit $|U| = n$? Wie wir in Aufgabe 7.36 noch sehen werden, ist die Antwort auf diese Frage im Allgemeinen nein. Wir werden in diesem Kapitel aber einige hinreichende Kriterien angeben, die die Existenz einer solchen Untergruppe sicher stellen, und die für die Behandlung unserer Probleme aus Kapitel 0 genügen werden.

Am einfachsten wäre diese Frage natürlich zu beantworten, wenn man eine Klassifikation aller Gruppen hätte, also eine vollständige (und halbwegs überschaubare) Liste aller Gruppen modulo Isomorphie. In diesem Fall müsste man ja einfach nur alle Gruppen der gegebenen Ordnung in dieser Liste durchgehen und explizit nachprüfen, ob in diesen Fällen eine Untergruppe der gewünschten Ordnung existiert oder nicht.

Für *abelsche* Gruppen führt diese Strategie in der Tat zum Erfolg: hier können wir eine Klassifikation aller endlichen Gruppen konkret angeben und dadurch dann einfach sehen, dass für jede dieser Gruppen G zu einem gegebenen Teiler n von $|G|$ auch immer eine Untergruppe der Ordnung n existiert. Da es nicht mehr Aufwand ist, werden wir diese Klassifikation nicht nur für *endliche* abelsche Gruppen durchführen, sondern sogar für alle, die von endlich vielen Elementen erzeugt werden können.

Definition 7.1 (Endlich erzeugte Gruppen)**.** Eine Gruppe G heißt **endlich erzeugt**, wenn es endlich viele Elemente $a_1, \dots, a_k$ gibt mit $G = \langle a_1, \dots, a_k \rangle$.

Beispiel 7.2.

(a) Natürlich ist jede endliche Gruppe endlich erzeugt (nämlich z. B. von allen ihren Elementen).

(b) Für alle $k \in \mathbb{N}_{>0}$ ist die Gruppe $\mathbb{Z}^k$ endlich erzeugt, nämlich z. B. von den k Einheitsvektoren $(1,0,\dots,0), \dots, (0,\dots,0,1)$.

(c) Die Gruppe $\mathbb{R}$ ist nicht endlich erzeugt: sind $a_1, \dots, a_k \in \mathbb{R}$, so ist

$$\langle a_1, \dots, a_k \rangle = \{n_1 a_1 + \dots + n_k a_k : n_1, \dots, n_k \in \mathbb{Z}\} \quad \subset \mathbb{R}.$$

Diese Menge ist aber stets abzählbar und kann somit nicht gleich der überabzählbaren Menge $\mathbb{R}$ sein.

Die Hauptarbeit der angekündigten Klassifikation endlich erzeugter abelscher Gruppen steckt in dem folgenden Lemma. Dazu erinnern wir uns zunächst daran, dass eine Gruppe *zyklisch* heißt, wenn sie von *einem* Element erzeugt werden kann [G, Definition 6.20], und dass diese zyklischen Gruppen genau $\mathbb{Z}$ und $\mathbb{Z}_n$ für $n \in \mathbb{N}_{>0}$ sind [G, Satz 6.21 (a)]. Wir wollen nun sehen, dass eine abelsche Gruppe, die von endlich vielen Elementen erzeugt werden kann, einfach ein Produkt von solchen zyklischen Gruppen ist.

Lemma 7.3. *Jede endlich erzeugte abelsche Gruppe ist ein (endliches) Produkt zyklischer Gruppen.*

Beweis. Es sei G eine abelsche Gruppe, die von k Elementen erzeugt werden kann. Wie bei abelschen Gruppen üblich schreiben wir die Gruppenverknüpfung in G als „+“. Wir zeigen die Aussage des Lemmas nun mit Induktion über k. Der Induktionsanfang für $k = 1$ ist dabei klar, denn dann ist G ja bereits selbst zyklisch.

Für den Induktionsschritt sei nun also $k > 1$. Wir wählen $a_1, \dots, a_k \in G$ und $n_1, \dots, n_k \in \mathbb{Z}$ mit den folgenden drei Eigenschaften:

(a) $G = \langle a_1, \dots, a_k \rangle$;

(b) $n_1 a_1 + \cdots + n_k a_k = 0 \in G$;

(c) $|n_1| \neq 0$ ist minimal.

Ausführlich bedeutet Bedingung (c) also, dass es keine andere Wahl $a'_1, \dots, a'_k \in G$ und $n'_1, \dots, n'_k \in \mathbb{Z}$ gibt, für die ebenfalls (a) und (b) gilt, aber $0 \neq |n'_1| < |n_1|$ ist. Da G nach Voraussetzung von k Elementen erzeugt werden kann, ist eine solche Wahl mit $|n_1| \neq 0$ nur dann unmöglich, wenn es zwischen beliebigen Erzeugern $a_1, \dots, a_k$ überhaupt keine nicht-trivialen Relationen der Form (b) gibt. Dann ist für fest gewählte Erzeuger $a_1, \dots, a_k$ von G aber

$$\mathbb{Z}^k \to G,\ (n_1, \dots, n_k) \mapsto n_1 a_1 + \cdots + n_k a_k$$

ein Gruppenisomorphismus, d. h. $G \cong \mathbb{Z}^k$ ist ein k-faches Produkt der zyklischen Gruppe $\mathbb{Z}$ und wir sind fertig.

Wir können also annehmen, dass wir eine Wahl von $a_1, \dots, a_k$ und $n_1, \dots, n_k$ mit den obigen drei Eigenschaften getroffen haben. Durch evtl. Multiplikation der $n_1, \dots, n_k$ mit -1 können wir weiterhin ohne Einschränkung $n_1 > 0$ annehmen.

Wir behaupten nun, dass n_1 ein Teiler von $n_2, \dots, n_k$ ist. Aus Symmetriegründen reicht es natürlich, dies für n_2 zu zeigen. Nach Division mit Rest können wir $n_2 = q n_1 + r$ mit $q \in \mathbb{Z}$ und $0 \leq r < n_1$ schreiben und erhalten aus (b)

$$n_1 a_1 + (q n_1 + r) a_2 + n_3 a_3 + \cdots + n_k a_k = 0,$$

also

$$r a_2 + n_1 (a_1 + q a_2) + n_3 a_3 + \cdots + n_k a_k = 0.$$

Nun ist aber $\langle a_2, a_1 + q a_2, a_3, \dots, a_k \rangle = \langle a_1, \dots, a_k \rangle = G$, und damit sind $a_2, a_1 + q a_2, a_3, \dots, a_k$ Erzeuger von G, die mit den Koeffizienten $r, n_1, n_3, \dots, n_k$ die Bedingungen (a) und (b) erfüllen. Wegen $0 \leq r < n_1$ muss nach der Minimalitätsforderung (c) also $r = 0$ gelten, d. h. $n_1 \mid n_2$.

Da n_1 ein Teiler von $n_2, \dots, n_k$ ist, können wir nun das Element

$$a'_1 := a_1 + \frac{n_2}{n_1} a_2 + \cdots + \frac{n_k}{n_1} a_k \quad \in G$$

betrachten. Natürlich ist dann auch $\langle a'_1, a_2, \dots, a_k \rangle = \langle a_1, \dots, a_k \rangle = G$. Der Morphismus

$$F : \langle a'_1 \rangle \times \langle a_2, \dots, a_k \rangle \to G, \quad (u, v) \mapsto u + v$$

ist also surjektiv. Er ist aber auch injektiv: es sei $F(u,v) = 0$ mit $u = m_1 a'_1$ und $v = m_2 a_2 + \cdots + m_k a_k$. Nach Konstruktion von a'_1 sowie (b) ist $n_1 a'_1 = 0$, aufgrund der Minimalitätsbedingung (c) jedoch $n a'_1 \neq 0$ für $0 < n < n_1$. Also ist $\langle a'_1 \rangle \cong \mathbb{Z}_{n_1}$, und wir können in der Darstellung für u ohne Einschränkung $0 \leq m_1 < n_1$ annehmen. Dann besagt $F(u,v) = u + v = 0$ aber

$$m_1 a'_1 + m_2 a_2 + \cdots + m_k a_k = 0,$$

was wiederum wegen der Minimalitätsbedingung (c) aufgrund von $0 \leq m_1 < n_1$ nur für $m_1 = 0$ möglich ist. Damit ist $u = 0$, mit $F(u,v) = u + v = 0$ also auch $v = 0$, d. h. F ist auch injektiv.

Aufgrund des Isomorphismus F ist G also isomorph zum Produkt der zyklischen Gruppe $\langle a'_1 \rangle$ mit $\langle a_2, \dots, a_k \rangle$. Da dieser zweite Faktor von $k-1$ Elementen erzeugt werden kann, ist er nach Induktionsvoraussetzung ein endliches Produkt zyklischer Gruppen. Damit ist auch G wie behauptet ein endliches Produkt zyklischer Gruppen. □

11

Mit diesem Lemma können wir nun wie angekündigt alle endlich erzeugten abelschen Gruppen klassifizieren.

Folgerung 7.4 (Hauptsatz über endlich erzeugte abelsche Gruppen). *Es sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es eindeutig bestimmte $r,m \in \mathbb{N}$ und bis auf die Reihenfolge eindeutige (aber nicht notwendig verschiedene) Primzahlpotenzen $p_1^{k_1}, \dots, p_m^{k_m}$, so dass*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}.$$

Beweis. Für die Existenz einer solchen Darstellung genügt es nach Lemma 7.3, eine zyklische Gruppe zu betrachten, also $G = \mathbb{Z}$ oder $G = \mathbb{Z}_n$ für ein $n \in \mathbb{N}_{>0}$. Für $G = \mathbb{Z}$ ist natürlich nichts zu zeigen; für $\mathbb{Z}_n$ dagegen gilt nach dem chinesischen Restsatz [G, Satz 11.22]

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}},$$

wenn $p_1^{k_1} \cdot \dots \cdot p_m^{k_m}$ die Primfaktorzerlegung von n ist.

Die Eindeutigkeit der Darstellung ergibt sich aus Teil (b) der folgenden Aufgabe. □

Aufgabe 7.5 (Eindeutigkeit im Hauptsatz über endlich erzeugte abelsche Gruppen)**.**

(a) Es sei $G = \mathbb{Z}^r \times \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}}$ für gewisse $r,n,k_1,\dots,k_n \in \mathbb{N}$ und (nicht notwendig verschiedene) Primzahlen $p_1,\dots,p_n$. Zeige, dass für alle $k \in \mathbb{N}$ und jede Primzahl p

$$\log_p |G/p^k G| = kr + \sum_{i:\, p_i = p} \min\{k, k_i\}$$

gilt, wobei wie üblich $p^k G = \{p^k x : x \in G\}$ und $\log_p$ der Logarithmus zur Basis p ist.

(b) Wir betrachten nun eine beliebige Gruppe G, die isomorph zu einer Gruppe der Form $\mathbb{Z}^r \times \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}}$ wie in (a) ist. Zeige, dass dann r, n und alle Primzahlpotenzen $p_1^{k_1}, \dots, p_n^{k_n}$ (bis auf die Reihenfolge) durch G eindeutig bestimmt sind.

Bemerkung 7.6. Mit Folgerung 7.4 können wir insbesondere leicht alle endlichen abelschen Gruppen einer gegebenen Ordnung n angeben, indem wir n auf alle möglichen Arten als Produkt von (nicht notwendig verschiedenen) Primzahlpotenzen schreiben. So erhalten wir zum Beispiel:

(a) Es gibt genau zwei abelsche Gruppen der Ordnung 12, nämlich

$$\mathbb{Z}_4 \times \mathbb{Z}_3 \quad \text{und} \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$$

(dass diese beiden Gruppen nicht isomorph sind, sieht man hier auch direkt ohne Aufgabe 7.5 (b), da die erste ein Element der Ordnung 4 besitzt, die zweite jedoch nicht). Die erste dieser beiden Gruppen ist nach dem chinesischen Restsatz isomorph zu $\mathbb{Z}_{12}$.

(b) Ist n ein Produkt von paarweise verschiedenen Primzahlen, so gibt es nur eine abelsche Gruppe der Ordnung n (nämlich $\mathbb{Z}_n$).

Mit Hilfe der Klassifikation aus Folgerung 7.4 können wir nun für abelsche Gruppen leicht die in der Einleitung zu diesem Kapitel genannte Frage nach der Existenz von Untergruppen einer gegebenen Ordnung beantworten.

Folgerung 7.7 (Untergruppen in abelschen Gruppen)**.** *Es sei G eine endliche abelsche Gruppe und $n \in \mathbb{N}_{>0}$ ein Teiler von $|G|$. Dann gibt es eine Untergruppe $U \leq G$ mit $|U| = n$.*

Beweis. Nach Folgerung 7.4 dürfen wir mit den dortigen Bezeichnungen $G = \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}$ mit $|G| = p_1^{k_1} \cdot \dots \cdot p_m^{k_m}$ annehmen. Da n ein Teiler dieser Zahl ist, können wir n natürlich (nicht notwendig eindeutig) in der Form $n = p_1^{a_1} \cdot \dots \cdot p_m^{a_m}$ mit $a_i \leq k_i$ für alle i schreiben. Nun ist aber für alle i

$$U_i := \langle p_i^{k_i - a_i} \rangle = \{r \cdot p_i^{k_i - a_i} : 0 \leq r < {p_i}^{a_i}\}$$

eine Untergruppe von $\mathbb{Z}_{p_i^{k_i}}$ der Ordnung $p_i^{a_i}$. Also ist $U_1 \times \cdots \times U_m \leq G$ wie gewünscht eine Untergruppe der Ordnung n. □

Übertragen wir dieses Ergebnis nun mit Hilfe der Galoistheorie auf Körpererweiterungen, können wir damit also im Fall einer galoisschen Körpererweiterung mit abelscher Galoisgruppe die Existenz von Zwischenkörpern mit gegebenem Grad zeigen. Dies ermöglicht es uns z. B. schon, die Frage nach der Konstruierbarkeit des regelmäßigen n-Ecks mit Zirkel und Lineal nun endgültig zu lösen, indem wir zeigen, dass die in Folgerung 3.33 gefundene notwendige Bedingung für die Konstruierbarkeit auch hinreichend ist.

Folgerung 7.8 (Konstruierbarkeit des n-Ecks)**.** *Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn n von der Form*

$$n = 2^m \cdot p_1 \cdot \cdots \cdot p_r$$

für ein $m \geq 0$ und verschiedene Fermatsche Primzahlen $p_1, \ldots, p_r$ ist (also für Primzahlen der Form $p_i = 2^{2^{a_i}} + 1$ mit $a_i \in \mathbb{N}$).

Beweis. Aus Folgerung 3.33 wissen wir bereits, dass das n-Eck höchstens dann konstruierbar sein kann, wenn n von der angegebenen Form ist.

Es sei nun also n von dieser Form. Die Körpererweiterung $\mathbb{Q}\big(e^{\frac{2\pi i}{n}}\big)/\mathbb{Q}$ ist nach Beispiel 5.3 (c) und 5.7 galoissch mit Galoisgruppe $G = \mathbb{Z}_n^*$. Ihre Ordnung ist nach Satz 3.29 gleich $|\mathbb{Z}_n^*| = \varphi(n)$ und damit nach Lemma 3.31 für das betrachtete n eine Zweierpotenz 2^r für ein $r \in \mathbb{N}$. Da $G = \mathbb{Z}_n^*$ natürlich abelsch ist, können wir mit Folgerung 7.7 also rekursiv eine Untergruppenkette

$$G = U_0 \geq U_1 \geq \cdots \geq U_r = \{e\}$$

mit $|U_k| = 2^{r-k}$ für $k = 0, \ldots, r$ finden. Nach der Galois-Korrespondenz aus Folgerung 6.9 erhalten wir nun mit $Z_k := \mathbb{Q}\big(e^{\frac{2\pi i}{n}}\big)^{U_k}$ eine entsprechende Kette von Zwischenkörpern

$$\mathbb{Q} = Z_0 \leq Z_1 \leq \cdots \leq Z_r = \mathbb{Q}\big(e^{\frac{2\pi i}{n}}\big)$$

mit $[\mathbb{Q}\big(e^{\frac{2\pi i}{n}}\big) : Z_k] = 2^{r-k}$, nach der Gradformel aus Satz 2.17 also $[Z_k : Z_{k-1}] = 2$ für alle $k = 1, \ldots, r$. Damit ist Z_k/Z_{k-1} gemäß Aufgabe 2.21 (b) für alle i eine einfache 2-Radikalerweiterung. Also ist $\mathbb{Q}\big(e^{\frac{2\pi i}{n}}\big)$ nach Definition 1.18 (b) eine 2-Radikalerweiterung von $\mathbb{Q}$. Da sie natürlich das Element $e^{\frac{2\pi i}{n}}$ enthält, ist das n-Eck damit wie in Beispiel 1.23 (C) erläutert mit Zirkel und Lineal konstruierbar. □

Wir wollen nun sehen, in wie weit wir auch im nicht-abelschen Fall Aussagen zur Klassifikation von Gruppen und zur Existenz von Untergruppen gegebener Ordnung machen können. Natürlich ist dies hier viel schwieriger, und die Ergebnisse werden auch deutlich schwächer ausfallen als im abelschen Fall. Zur Vorbereitung müssen wir zunächst etwas ausholen und das Konzept der Gruppenoperation auf einer Menge einführen.

Definition 7.9 (Gruppenoperationen)**.** Es seien $(G, \cdot)$ eine Gruppe und M eine Menge. Eine **Gruppenoperation** von G auf M ist eine Abbildung

$$* \colon G \times M \to M, \quad (a, x) \mapsto a * x,$$

so dass

(a) $e * x = x$ für alle $x \in M$ (wobei $e \in G$ wie üblich das neutrale Element bezeichnet);

(b) $a * (b * x) = (a \cdot b) * x$ für alle $a, b \in G$ und $x \in M$.

Bemerkung 7.10. Genau wie bei Gruppenverknüpfungen kann man eine Gruppenoperation natürlich auch mit einem anderen Symbol als „$*$“ bezeichnen. Oft verwendet man für eine Gruppenoperation sogar das gleiche Symbol „$\cdot$“ wie für die Gruppenverknüpfung, weil dadurch, ob zwei Elemente von G miteinander verknüpft werden oder eines von G mit einem von M, ja in der Regel bereits eindeutig erkennbar ist, ob die Gruppenverknüpfung oder die Gruppenoperation gemeint ist. Da man eine Gruppenoperation außerdem auch so auffassen kann, dass ein Gruppenelement a eine Funktion ist, die einem Element $x \in M$ ein Element $a * x \in M$ zuordnet (daher kommt natürlich auch die Sprechweise, dass G auf M operiert), sieht man in der Literatur auch oft die Schreibweise $a(x)$ für $a * x$. Wir werden in diesem Skript jedoch ausschließlich die Schreibweise $a * x$ verwenden, da diese wohl am wenigsten zu Verwirrungen führen kann.

Beispiel 7.11 (Permutationen als Gruppenoperation)**.** Es seien $G \leq S_n$ eine Untergruppe der symmetrischen Gruppe und $M = \{1,\dots,n\}$. Dann operiert G auf M einfach dadurch, dass man eine Permutation aus G auf eine Zahl in M anwendet, d. h. indem wir

$$\sigma * i := \sigma(i) \quad \in M$$

für $\sigma \in G$ und $i \in M$ setzen. Die Eigenschaften (a) und (b) aus Definition 7.9 sind dabei natürlich offensichtlich, denn es ist ja $\mathrm{id}(i) = i$ und $\sigma(\tau(i)) = (\sigma \circ \tau)(i)$ für alle $i \in M$ und $\sigma, \tau \in G \leq S_n$.

In der Tat ist dies ein sehr „typisches“ Beispiel für eine Gruppenoperation – denn die folgende Bemerkung zeigt, dass die Elemente von G im Fall einer Operation auf einer Menge M immer als Permutationen auf M operieren.

Bemerkung 7.12 (Gruppenoperationen als Morphismen in die symmetrische Gruppe)**.** Es sei G eine Gruppe, die auf einer Menge M operiert. Für ein festes $a \in G$ ist dann die Abbildung

$$\sigma_a : M \to M,\ x \mapsto a * x$$

bijektiv mit Umkehrabbildung $\sigma_{a^{-1}}$, denn nach Definition 7.9 gilt für alle $x \in M$

$$\sigma_{a^{-1}}(\sigma_a(x)) = a^{-1} * (a * x) = (a^{-1} \cdot a) * x = e * x = x$$

und analog auch $\sigma_a(\sigma_{a^{-1}}(x)) = x$. Wir erhalten so also eine Abbildung

$$G \to S(M),\ a \mapsto \sigma_a$$

der Gruppe G in die symmetrische Gruppe $S(M)$ aller bijektiven Abbildungen von M in sich [G, Konstruktion 2.1]. Diese Abbildung ist sogar ein Gruppenhomomorphismus, denn nach Definition 7.9 gilt für alle $x \in M$ und $a, b \in G$

$$\sigma_a(\sigma_b(x)) = a * (b * x) = (a \cdot b) * x = \sigma_{a \cdot b}(x)$$

und damit $\sigma_a \circ \sigma_b = \sigma_{a \cdot b}$. Eine Operation einer Gruppe G auf einer Menge M bestimmt also einen Morphismus von G in die symmetrische Gruppe $S(M)$. Im Fall von Beispiel 7.11, wo eine Untergruppe $G \leq S_n$ der symmetrischen Gruppe durch Permutation auf $M = \{1,\dots,n\}$ operiert, ist dieser Morphismus offensichtlich gerade die Einbettung $G \to S_n = S(M)$.

In der Tat bestimmt auch umgekehrt ein Morphismus von G in die symmetrische Gruppe $S(M)$ eine Gruppenoperation von G auf M, wie die folgende einfache Aufgabe zeigt.

Aufgabe 7.13. Es seien G eine Gruppe und M eine Menge. Zeige, dass eine Gruppenoperation von G auf M „dasselbe“ ist wie ein Morphismus von G in die symmetrische Gruppe $S(M)$, d. h. dass die Konstruktion aus Bemerkung 7.12 eine bijektive Abbildung

$$\{\text{Gruppenoperationen von } G \text{ auf } M\} \quad \overset{1:1}{\longleftrightarrow} \quad \{\text{Morphismen } G \to S(M)\}$$

liefert.

Wir werden später in Konstruktion 7.18 und im Beweis der Sätze 7.29 und 7.30 noch weitere für uns relevante Gruppenoperationen kennen lernen. Zunächst einmal wollen wir jedoch ein paar Begriffe einführen, mit denen man Gruppenoperationen untersuchen kann.

Definition 7.14 (Bahnen, Fixgruppen und Fixpunkte)**.** Es sei G eine Gruppe, die auf einer Menge M operiert. Für ein festes $x \in M$ heißt dann

(a) $G * x := \{a * x :\ a \in G\} \subset M$ die **Bahn** von x;

(b) $G_x := \{a \in G :\ a * x = x\} \leq G$ die **Fixgruppe** oder der **Stabilisator** von x (man prüft sofort nach, dass dies in der Tat eine Untergruppe von G ist);

(c) x ein **Fixpunkt** der Operation, falls $a * x = x$ für alle $a \in G$. Offensichtlich ist dies äquivalent zu $G * x = \{x\}$ und zu $G_x = G$.

Beispiel 7.15. Es sei $\sigma \in S_4$ der 3-Zykel $\sigma = (1\ 2\ 3)$. Wie in Beispiel 7.11 operiere die Gruppe $G = \langle \sigma \rangle = \{\mathrm{id}, \sigma, \sigma^2\} \leq S_4$ auf der Menge $M = \{1,2,3,4\}$ durch Permutation. Die Elemente in G vertauschen also die Zahlen $1,2,3 \in M$ zyklisch und lassen das Element $4 \in M$ fest. In der Sprechweise von Definition 7.14 bedeutet dies:

(a) Die Bahn des Elements $1 \in M$ ist $G*1 = \{\mathrm{id}(1), \sigma(1), \sigma^2(1)\} = \{1,2,3\}$. Da von den Elementen von G nur die Identität das Element 1 fest lässt, ist die zugehörige Fixgruppe $G_1 = \{\mathrm{id}\}$. Natürlich ist 1 kein Fixpunkt der Gruppenoperation. Dieselben Aussagen gelten analog für die Elemente 2 und 3 von M.

(b) Die Bahn des Elements $4 \in M$ ist $G*4 = \{\mathrm{id}(4), \sigma(4), \sigma^2(4)\} = \{4\}$. Hier ist also die zugehörige Fixgruppe $G_4 = G$, und 4 ist ein Fixpunkt der Gruppenoperation.

Bemerkung 7.16 (Bahnen als Äquivalenzklassen)**.** Die Gruppe G operiere wieder auf der Menge M. Wir definieren eine Relation $\sim$ auf M durch

$$y \sim x \quad :\Leftrightarrow \quad \text{es gibt ein } a \in G \text{ mit } y = a*x.$$

Man prüft sofort nach, dass dies eine Äquivalenzrelation ist [G, Definition 5.1]. Außerdem ist die Äquivalenzklasse eines Elements $x \in M$, also die Menge der Elemente $y \in M$ mit $y \sim x$, nach Konstruktion natürlich genau die Bahn $G*x$. Insbesondere ist M also stets die disjunkte Vereinigung aller Bahnen der Gruppenoperation [G, Satz 5.3 (b)].

Die wichtigste Eigenschaft einer Gruppenoperation ist die sogenannte Bahnengleichung, die wir jetzt beweisen wollen.

Satz 7.17 (**Bahnengleichung**)**.** *Eine endliche Gruppe G operiere auf einer endlichen Menge M. Dann gilt:*

(a) *Für alle $x \in M$ ist $|G| = |G_x| \cdot |G*x|$.*

(b) *Ist $\{x_1, \ldots, x_n\} \subset M$ ein Repräsentantensystem der Bahnen, d. h. sind $G*x_1, \ldots, G*x_n$ genau die verschiedenen Bahnen der Gruppenoperation, so gilt*

$$|M| = \sum_{i=1}^{n} |G*x_i| = \sum_{i=1}^{n} \frac{|G|}{|G_{x_i}|}.$$

Beweis.

(a) Wie üblich bezeichne G/G_x die Menge der Linksnebenklassen von G_x in G [G, Definition 5.6]. Beachte, dass dies keine Gruppe ist, da die Fixgruppe G_x in der Regel kein Normalteiler in G ist. Das brauchen wir aber auch nicht, denn wir behaupten lediglich, dass die Abbildung

$$G/G_x \to G*x, \quad \overline{a} \mapsto a*x$$

wohldefiniert und bijektiv ist. In der Tat gilt für alle $a, b \in G$

$$\begin{aligned} \overline{a} = \overline{b} \in G/G_x &\Leftrightarrow a^{-1}b \in G_x && \text{(Definition von } G/G_x) \\ &\Leftrightarrow (a^{-1}b)*x = x && \text{(Definition der Fixgruppe } G_x) \\ &\Leftrightarrow b*x = a*x. \end{aligned}$$

Lesen wir diese Äquivalenz in der Richtung „$\Rightarrow$“, so ergibt sich, dass die oben genannte Abbildung wohldefiniert ist. Lesen wir die Äquivalenz in der Richtung „$\Leftarrow$“, so bedeutet dies genau die Injektivität. Außerdem ist die Abbildung natürlich surjektiv, denn nach Definition der Bahn ist ja jedes Element von $G*x$ von der Form $a*x$ für ein $a \in G$.

Also ist die obige Abbildung bijektiv, d. h. es ist insbesondere $|G/G_x| = |G*x|$. Mit dem Satz von Lagrange [G, Satz 5.10] ergibt sich also die Behauptung $|G| = |G_x| \cdot |G/G_x| = |G_x| \cdot |G*x|$.

(b) Dies folgt nun sofort aus Bemerkung 7.16 und Teil (a) des Satzes. □

Wir werden nun eine für uns im Folgenden besonders wichtige Gruppenoperation kennen lernen, nämlich die Gruppenkonjugation. Eine Besonderheit dieser Operation ist, dass eine Gruppe G hierbei auf sich selbst operiert, d. h. in der Notation von Definition 7.9 die Menge M gleich der Gruppe G ist. Demzufolge liegen auch die Bahnen und Fixgruppen dieser Operation beide in G, während sonst ja die Bahnen in M und die Fixgruppen in G liegen. Da die Gruppenkonjugation besonders wichtig ist, haben die Begriffe aus Definition 7.14 für diesen Fall alle einen besonderen Namen.

Konstruktion 7.18 (Gruppenkonjugation)**.** Es sei G eine Gruppe.

(a) Die Vorschrift
$$b * a := bab^{-1} \quad \text{für } a, b \in G$$
definiert eine Gruppenoperation von G auf sich selbst, denn für alle $a, b, c \in G$ ist
$$e * a = eae^{-1} = a \quad \text{und} \quad c * (b * a) = cbab^{-1}c^{-1} = (cb)a(cb)^{-1} = (cb) * a.$$
Sie wird als **Konjugation** bezeichnet. Die Bahnen dieser Operation nennt man die **Konjugationsklassen** von G. Zwei Elemente $a_1, a_2 \in G$ heißen **konjugiert** zueinander, wenn sie in derselben Konjugationsklasse liegen, also wenn es ein $b \in G$ gibt mit $a_2 = ba_1b^{-1}$.

(b) Für ein $a \in G$ heißt die Fixgruppe von a bezüglich der Konjugation
$$G_a = \{b \in G : \ bab^{-1} = a\} = \{b \in G : \ ba = ab\} \quad \leq G$$
(also die Menge der Gruppenelemente, die mit dem gegebenen a kommutieren) der **Zentralisator** von a in G. Er wird mit $C_G(a)$ bezeichnet, bzw. (wenn die zugrunde liegende Gruppe aus dem Zusammenhang klar ist) einfach mit $C(a)$.

(c) Die Menge der Fixpunkte der Konjugation
$$Z(G) := \{a \in G : \ bab^{-1} = a \text{ für alle } b \in G\} = \{a \in G : \ ba = ab \text{ für alle } b \in G\}$$
(also die Menge der Gruppenelemente, die mit allen anderen Elementen kommutieren) heißt das **Zentrum** von G. Offensichtlich ist G genau dann abelsch, wenn $Z(G) = G$ ist. Man prüft leicht nach, dass $Z(G)$ eine Untergruppe von G ist [G, Aufgabe 3.6 (e)]. In der Tat ist sogar jede Untergruppe U des Zentrums ein Normalteiler von G, denn für alle $u \in U$ und $a \in G$ gilt ja $aua^{-1} = u \in U$.

Beispiel 7.19 (Konjugationsklassen in S_n)**.** Im Fall der symmetrischen Gruppe S_n haben die Konjugationsklassen eine besonders einfache Interpretation. Es sei dazu $\sigma \in S_n$ eine Permutation, deren Zykelzerlegung aus disjunkten Zykeln der Längen $k_1, \dots, k_m$ mit $k_1 + \dots + k_m = n$ besteht [G, Konstruktion 2.10], also
$$\sigma = (a_{1,1} \cdots a_{1,k_1}) \ \cdots \ (a_{m,1} \cdots a_{m,k_m})$$
für $a_{i,j}$ mit $\{a_{i,j} : 1 \leq i \leq m, 1 \leq j \leq k_i\} = \{1, \dots, n\}$. Ist nun $\tau \in S_n$ beliebig und setzen wir $b_{i,j} := \tau(a_{i,j})$, so ergibt einfaches Nachrechnen, dass
$$\tau\sigma\tau^{-1} = (b_{1,1} \cdots b_{1,k_1}) \ \cdots \ (b_{m,1} \cdots b_{m,k_m}). \qquad (*)$$
Die zu σ konjugierten Permutationen haben in ihrer Zykelzerlegung also Zykel der gleichen Längen wie σ. Haben wir umgekehrt eine Permutation wie auf der rechten Seite von $(*)$, die aus Zykeln der gleichen Länge wie σ besteht, so können wir durch $\tau(a_{i,j}) := b_{i,j}$ ein Element $\tau \in S_n$ definieren, für das die Gleichung $(*)$ gilt. Die Konjugationsklasse von σ besteht also genau aus allen Permutationen, deren Zykelzerlegung aus disjunkten Zykeln der Längen $k_1, \dots, k_m$ besteht. So ist z. B. die Konjugationsklasse von $(1\ 2)$ in S_n genau die Menge aller Transpositionen (hier ist $k_1 = 2$ und $k_2 = \dots = k_m = 1$ für $m = n - 1$).

12

Bemerkung 7.20 (Klassengleichung)**.** Es sei G eine Gruppe. Wenden wir die Bahnengleichung aus Satz 7.17 auf die Konjugationsoperation aus Konstruktion 7.18 an, so erhalten wir offensichtlich
$$|G| = \sum_{i=1}^{n} \frac{|G|}{|C(a_i)|},$$
wobei $a_1, \dots, a_n$ ein Repräsentantensystem der Konjugationsklassen ist. Typischerweise formuliert man diese Gleichung etwas um, indem man aus dieser Summe alle Terme herauszieht, die den Wert 1 haben. Dies sind genau die i mit $C(a_i) = G$, also für die a_i mit allen Gruppenelementen kommutiert und damit $a_i \in Z(G)$ gilt. Umgekehrt kommt natürlich auch jedes Element des Zentrums unter

den a_i vor, da jedes solche Element seine eigene Konjugationsklasse bildet. Wir erhalten damit die sogenannte **Klassengleichung**

$$|G| = |Z(G)| + \sum_{i=1}^{m} \underbrace{\frac{|G|}{|C(a_i)|}}_{>1}$$

für G, wobei wir die obigen Repräsentanten der Konjugationsklassen jetzt so nummeriert haben, dass $a_1, \ldots, a_m$ genau die Klassen mit mehr als einem Element repräsentieren und $a_{m+1}, \ldots, a_n$ im Zentrum von G liegen.

Als erste Anwendung unseres Studiums von Gruppenoperationen können wir nun ein kleines Resultat zur Klassifikation beliebiger (d. h. nicht notwendig abelscher) Gruppen zeigen. Wir wissen ja bereits, dass es zu einer Primzahl p bis auf Isomorphie nur eine Gruppe mit p Elementen gibt, nämlich $\mathbb{Z}_p$. Ein ähnliches Ergebnis können wir nun für Gruppen zeigen, deren Ordnung ein Primzahlquadrat ist.

Aufgabe 7.21 (Klassifikation der Gruppen der Ordnung p^2)**.** Es sei G eine Gruppe mit $|G| = p^2$ für eine Primzahl p.

(a) Zeige mit Hilfe der Klassengleichung, dass $|Z(G)| = p^2$.

(b) Zeige, dass $G \cong \mathbb{Z}_{p^2}$ oder $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Als weitere Anwendung der Klassengleichung wollen wir nun wieder zum Problem der Existenz von Untergruppen einer gegebenen Ordnung zurück kommen. Wie wir in Aufgabe 7.36 noch sehen werden, ist es – im Gegensatz zum abelschen Fall in Folgerung 7.7 – für eine beliebige endliche Gruppe G und einen Teiler n von $|G|$ im Allgemeinen nicht mehr richtig, dass G dann eine Untergruppe der Ordnung n besitzt. Allerdings können wir die Existenz einer solchen Untergruppe zumindest noch dann zeigen, wenn n eine Primzahlpotenz ist.

Satz 7.22 (1. Satz von Sylow). *Es sei G eine endliche Gruppe. Ferner seien p eine Primzahl und $k \in \mathbb{N}_{>0}$, so dass p^k ein Teiler von $|G|$ ist. Dann gibt es eine Untergruppe $U \leq G$ mit $|U| = p^k$.*

Beweis. Wir zeigen die Aussage mit Induktion über $|G|$; für $|G| = 1$ ist natürlich nichts zu zeigen. Für den Induktionsschritt unterscheiden wir zwei Fälle:

(a) $p \mid |Z(G)|$: Da das Zentrum $Z(G)$ eine abelsche Gruppe ist, gibt es nach Folgerung 7.7 eine Untergruppe $N \leq Z(G) \leq G$ mit $|N| = p$. Im Fall $k = 1$ können wir dann also natürlich $U = N$ wählen und sind fertig.

Andernfalls können wir die Faktorgruppe G/N betrachten, da N nach Konstruktion 7.18 (c) als Untergruppe des Zentrums sogar ein Normalteiler in G ist. Wegen $p^k \mid |G|$ gilt dann $p^{k-1} \mid \frac{1}{p} \cdot |G| = |G/N|$. Nach Induktionsvoraussetzung gibt es also eine Untergruppe $V \leq G/N$ mit $|V| = p^{k-1}$. Ist dann $\pi : G \to G/N$, $a \mapsto \overline{a}$ die Restklassenabbildung, so ist $U := \pi^{-1}(V)$ eine Untergruppe von G mit $U/N = V$, also wie gewünscht $|U| = |N| \cdot |V| = p \cdot p^{k-1} = p^k$.

(b) $p \nmid |Z(G)|$: Wegen $p \mid |G|$ und $p \nmid |Z(G)|$ muss es nach der Klassengleichung

$$|G| = |Z(G)| + \sum_{i=1}^{m} \underbrace{\frac{|G|}{|C(a_i)|}}_{>1}$$

aus Bemerkung 7.20 (mit den dortigen Notationen) ein $i = 1, \ldots, m$ geben mit $p \nmid \frac{|G|}{|C(a_i)|}$. Da dieser Quotient also keinen Primfaktor p mehr enthält, folgt mit $p^k \mid |G|$ auch $p^k \mid |C(a_i)|$. Wegen $\frac{|G|}{|C(a_i)|} > 1$, also $|C(a_i)| < |G|$, finden wir nun nach Induktionsvoraussetzung eine Untergruppe $U \leq C(a_i) \leq G$ mit $|U| = p^k$. □

Mit Hilfe der Galois-Korrespondenz erhalten wir aus diesem Satz nun natürlich sofort eine analoge Aussage über die Existenz von Zwischenkörpern.

Folgerung 7.23 (Existenz von Zwischenkörpern)**.** *Es sei L/K eine galoissche Körpererweiterung von Charakteristik 0. Ferner seien p prim und $k \in \mathbb{N}_{>0}$ mit $p^k \mid [L:K]$. Dann gibt es einen Zwischenkörper Z von L/K mit $[L:Z] = p^k$.*

Beweis. Weil L/K galoissch ist, ist $|\mathrm{Gal}(L/K)| = [L:K]$, d. h. nach Voraussetzung ist p^k ein Teiler von $|\mathrm{Gal}(L/K)|$. Der 1. Satz von Sylow liefert also die Existenz einer Untergruppe $U \leq \mathrm{Gal}(L/K)$ mit $|U| = p^k$. Nach dem Hauptsatz der Galoistheorie aus Folgerung 6.9 gibt es nun einen zugehörigen Zwischenkörper $Z = L^U$ von L/K mit $[L:Z] = |U| = p^k$. □

Dieses Resultat ermöglicht es uns nun, wie in Problem 0.1 der Einleitung angekündigt einen algebraischen Beweis des Fundamentalsatzes der Algebra zu geben. Allerdings ist dieser Beweis nicht wirklich vollständig algebraisch, sondern verwendet auch ein Hilfsresultat aus der Analysis – was aber auch so sein muss, da die besonderen Eigenschaften von $\mathbb{R}$ gegenüber $\mathbb{Q}$ (z. B. die Vollständigkeit) und damit auch die von $\mathbb{C} = \mathbb{R}(i)$ gegenüber $\mathbb{Q}(i)$ (wo ja z. B. das Polynom $t^2 - 2$ nicht in Linearfaktoren zerfällt) nun einmal analytischer und nicht algebraischer Natur sind. Im folgenden Lemma stellen wir bereit, was wir aus der Analysis benötigen.

Lemma 7.24.

(a) *Es gibt keinen Erweiterungskörper L von $\mathbb{R}$ mit $[L:\mathbb{R}] = q$ für ein ungerades $q > 1$.*

(b) *Es gibt keinen Erweiterungskörper L von $\mathbb{C}$ mit $[L:\mathbb{C}] = 2$.*

Beweis.

(a) Angenommen, es gäbe einen Körper $L \geq \mathbb{R}$ mit $[L:\mathbb{R}] = q > 1$ ungerade. Nach dem Satz 4.28 vom primitiven Element ist $L = \mathbb{R}(a)$ für ein $a \in L$. Das Minimalpolynom f von a über $\mathbb{R}$ ist dann natürlich nach Lemma 2.6 und Satz 2.14 (a) irreduzibel und hat Grad q. Nun wissen wir aber aus dem Zwischenwertsatz der Analysis, dass ein solches reelles Polynom ungeraden Grades immer eine Nullstelle in $\mathbb{R}$ besitzt, da $f(x)$ für $x \to \infty$ und $x \to -\infty$ unterschiedliche Vorzeichen hat. Also spaltet f über $\mathbb{R}$ einen Linearfaktor ab und kann damit nicht über $\mathbb{R}$ irreduzibel sein, was ein Widerspruch ist.

(b) Wir nehmen nun an, dass $L \geq \mathbb{C}$ mit $[L:\mathbb{C}] = 2$. Wie in Teil (a) ist dann $L = \mathbb{C}(a)$ für ein $a \in L$; das Minimalpolynom f von a über $\mathbb{C}$ ist wieder irreduzibel und hat diesmal Grad 2. Nach der bekannten Lösungsformel für quadratische Gleichungen (und weil in $\mathbb{C}$ jede Zahl eine Quadratwurzel besitzt) hat f dann aber eine Nullstelle in $\mathbb{C}$, zerfällt also über $\mathbb{C}$ in Linearfaktoren und kann damit nicht irreduzibel sein, was wieder ein Widerspruch ist. □

Satz 7.25 (**Fundamentalsatz der Algebra**)**.** *Jedes komplexe Polynom zerfällt über $\mathbb{C}$ in Linearfaktoren. (Insbesondere hat also jedes nicht-konstante komplexe Polynom eine Nullstelle in $\mathbb{C}$.)*

Beweis. Es sei $f \in \mathbb{C}[t]$. Es genügt zu zeigen, dass das reelle Polynom $g := f \cdot \overline{f} \in \mathbb{R}[t]$ über $\mathbb{C}$ in Linearfaktoren zerfällt, da dies wegen der eindeutigen Primfaktorzerlegung in $\mathbb{C}[t]$ [G, Satz 11.9] dann natürlich auch für f gelten muss.

Wir betrachten nun den Zerfällungskörper L von g über $\mathbb{C}$. Da wir diesen auch als Zerfällungskörper von $(t^2+1)g$ über $\mathbb{R}$ schreiben können, sind die Körpererweiterungen $L/\mathbb{C}$ und $L/\mathbb{R}$ nach Satz 5.8 galoissch. Wir wollen zeigen, dass $L = \mathbb{C}$ ist, also dass g bereits über $\mathbb{C}$ in Linearfaktoren zerfällt.

Dazu schreiben wir den Grad der Körpererweiterung $L/\mathbb{R}$ als $[L:\mathbb{R}] = q \cdot 2^k$ für ein ungerades q – jede natürliche Zahl lässt sich ja so schreiben. Da $L/\mathbb{R}$ galoissch ist, gibt es nun nach Folgerung 7.23 einen Zwischenkörper $\mathbb{R} \leq Z \leq L$ mit $[L:Z] = 2^k$, nach der Gradformel aus Satz 2.17 also $[Z:\mathbb{R}] = q$. Dies ist nach Lemma 7.24 (a) aber nur möglich für $q = 1$.

Wir haben also $[L:\mathbb{R}] = 2^k$ und damit $[L:\mathbb{C}] = 2^{k-1}$. Wäre nun $k \geq 2$, so gäbe es wiederum nach Folgerung 7.23 einen Zwischenkörper $\mathbb{C} \leq Z' \leq L$ mit $[L:Z'] = 2^{k-2}$, also $[Z':\mathbb{C}] = 2$. Dies ist nach Lemma 7.24 (b) aber unmöglich. Also ist $k = 1$, d. h. $[L:\mathbb{C}] = 1$ und damit $L = \mathbb{C}$. □

Bemerkung 7.26 (Algebraische Erweiterungen von $\mathbb{C}$)**.** Eine äquivalente Formulierung des Fundamentalsatzes der Algebra ist, dass es keine (echte) algebraische Körpererweiterung von $\mathbb{C}$ gibt: ist $L/\mathbb{C}$ eine algebraische Körpererweiterung und $a \in L$ beliebig, so ist das Minimalpolynom von a

über $\mathbb{C}$ irreduzibel und damit nach dem Fundamentalsatz linear; also ist $[a:\mathbb{C}]=1$ und damit bereits $a\in\mathbb{C}$. Auf ähnliche Art zeigt man, dass die einzige echte algebraische Körpererweiterung von $\mathbb{R}$ der Körper der komplexen Zahlen ist.

Beachte aber, dass es natürlich (viele) *transzendente* Körpererweiterungen von $\mathbb{C}$ gibt, z. B. den Körper der rationalen komplexen Funktionen aus Beispiel 1.2 (c).

Im 1. Satz von Sylow (siehe Satz 7.22) haben wir gesehen, dass zu einer endlichen Gruppe G und einer Primzahlpotenz p^k mit $p^k\mid|G|$ stets eine Untergruppe U von G mit $|U|=p^k$ existiert. Für viele Anwendungen wäre es nun nützlich, noch weitere Angaben über diese Untergruppen machen zu können, z. B. über deren Anzahl. Wenn wir z. B. wüssten, dass es genau eine Untergruppe der Ordnung p^k gibt, so wüssten wir damit nach [G, Aufgabe 6.9 (b)] auch schon, dass diese ein Normalteiler sein muss.

Für derartige Fragen gibt es noch zwei weitere Sätze von Sylow, die wir jetzt zum Abschluss dieses Kapitels behandeln wollen. Sie werden im wesentlichen mit dem gleichen Argument bewiesen; die Aufteilung in zwei Sätze hat hier lediglich historische Gründe. Besonders starke Aussagen machen sie über die Untergruppen $U\leq G$ mit $|U|=p^k$, für die p^k die maximale Potenz von p ist, die $|G|$ teilt. Derartigen Untergruppen gibt man daher einen besonderen Namen.

Definition 7.27 (p-Gruppen und p-Sylowgruppen)**.** Es sei G eine Gruppe.

(a) Ist $|G|=p^k$ für eine Primzahl p und ein $k\in\mathbb{N}_{>0}$, so heißt G eine **p-Gruppe**.

(b) Es sei $|G|=q\,p^k$ für eine Primzahl p, ein $k\in\mathbb{N}_{>0}$ und ein q mit $p\nmid q$, d. h. der Primfaktor p tritt in $|G|$ genau mit der Vielfachheit k auf. Dann heißt eine Untergruppe $U\leq G$ mit $|U|=p^k$ (also eine p-Untergruppe von G mit maximal möglicher Ordnung) eine **p-Sylowgruppe** bzw. **p-Sylowuntergruppe** von G. Die Menge aller p-Sylowgruppen von G wird mit $\mathrm{Syl}_p(G)$ bezeichnet.

Bemerkung 7.28. Nach dem 1. Satz von Sylow (siehe Satz 7.22) ist offensichtlich $\mathrm{Syl}_p(G)\neq\emptyset$ für jeden Primteiler p der Ordnung einer endlichen Gruppe G.

Satz 7.29 (2. Satz von Sylow). *Es seien G eine Gruppe und p ein Primteiler von $|G|$. Dann gilt:*

(a) *Jede p-Untergruppe von G ist in einer p-Sylowuntergruppe von G enthalten.*

(b) *Alle p-Sylowgruppen von G sind zueinander konjugiert, d. h. für alle $S_1,S_2\in\mathrm{Syl}_p(G)$ gibt es ein $a\in G$ mit $S_2=aS_1a^{-1}$.*

Satz 7.30 (3. Satz von Sylow). *Es seien wieder G eine endliche Gruppe und p ein Primteiler von $|G|$. Wir schreiben die Ordnung von G als $|G|=q\,p^k$ für ein $k\in\mathbb{N}_{>0}$ und ein q mit $p\nmid q$. Dann gilt für die Anzahl $s_p:=|\mathrm{Syl}_p(G)|$ der p-Sylowgruppen in G:*

(a) $s_p=1 \mod p$;

(b) $s_p\mid q$.

Beweis von Satz 7.29 und 7.30. Es sei $|G|=q\,p^k$ für eine Primzahl p, ein $k\in\mathbb{N}_{>0}$ und ein q mit $p\nmid q$. Der Beweis beider Sätze besteht im wesentlichen aus einer zweimaligen geschickten Anwendung der Bahnengleichung für geeignete Gruppenoperationen.

Als Erstes lassen wir die Gruppe G durch Konjugation auf der Menge $\mathrm{Syl}_p(G)$ aller p-Sylowgruppen in G operieren, d. h. als $a*U:=aUa^{-1}$ für $a\in G$ und $U\in\mathrm{Syl}_p(G)$ (beachte, dass aUa^{-1} nach [G, Aufgabe 3.7 (a) und Lemma 5.9] in der Tat eine Untergruppe derselben Ordnung wie U, also ebenfalls eine p-Sylowgruppe ist). Für eine im Folgenden fest gewählte p-Sylowgruppe $S\in\mathrm{Syl}_p(G)$ sei nun $\Omega=\{aSa^{-1}:\ a\in G\}\subset\mathrm{Syl}_p(G)$ die Bahn von S unter dieser Konjugationsoperation. Natürlich ist die Aussage von Satz 7.29 (b) letztlich, dass bereits $\Omega=\mathrm{Syl}_p(G)$ ist, aber das wissen wir momentan noch nicht. Allerdings wissen wir nach der Bahnengleichung aus Satz 7.17 (a), dass

$$|G|=|G_S|\cdot|\Omega| \tag{1}$$

gilt, wobei $G_S = \{a \in G : aSa^{-1} = S\} = \{a \in G : aS = Sa\}$ die Fixgruppe von S ist. Nun ist aber $aS = Sa = S$ für alle $a \in S$, und damit $S \leq G_S$. Nach dem Satz von Lagrange [G, Satz 5.10] ist $|S| = p^k$ also ein Teiler von $|G_S|$. Alle Primfaktoren p von $|G|$ stecken in der Gleichung (1) damit bereits in $|G_S|$, und wir sehen, dass

$$p \nmid |\Omega|. \tag{2}$$

Wir kommen nun zur zweiten bereits angekündigten Gruppenoperation. Hierfür sei H eine beliebige p-Untergruppe von G, die wir wieder durch Konjugation auf p-Sylowgruppen operieren lassen – allerdings diesmal nur auf der Menge Ω aller p-Sylowgruppen, die man aus dem fest gewählten S durch Konjugation mit beliebigen Gruppenelementen erreichen kann. Die Bahnengleichung aus Satz 7.17 (b) lautet für diese Operation

$$|\Omega| = \sum_{i=1}^{n} \frac{|H|}{|H_{S_i}|}, \tag{3}$$

wobei $S_1, \dots, S_n \in \Omega$ ein Repräsentantensystem der Bahnen und $H_{S_i} = \{a \in H : aS_ia^{-1} = S_i\}$ ist. Da H eine p-Gruppe ist, ist jeder Summand auf der rechten Seite dieser Gleichung eine Potenz von p, also entweder gleich $p^0 = 1$ oder durch p teilbar. Da $|\Omega|$ nach (2) aber nicht durch p teilbar ist, muss demnach mindestens einmal ein Summand 1 vorkommen, d. h. wir sehen:

$$\text{für jede } p\text{-Gruppe } H \text{ in } G \text{ gibt es ein } S_i \in \Omega \text{ mit } H_{S_i} = H. \tag{4}$$

Für ein solches S_i ist also $aS_ia^{-1} = S_i$ für alle $a \in H$. Nach [G, Aufgabe 6.11] folgt hieraus, dass HS_i eine Untergruppe von G ist. Ihre Ordnung ist nach der Produktformel [G, Aufgabe 5.5 (c)] gleich $\frac{|H| \cdot |S_i|}{|H \cap S_i|}$, also insbesondere eine Potenz von p, da H und S_i beides p-Gruppen sind. Damit ist HS_i eine p-Untergruppe von G, die die maximale p-Untergruppe S_i enthält. Es muss demnach $HS_i = S_i$ und damit insbesondere $H \leq HS_i = S_i$ gelten. Also haben wir:

$$\text{für jedes } H \text{ und } S_i \text{ wie in (4) ist } H \leq S_i. \tag{5}$$

Wir können nun alle unsere Ergebnisse zusammensetzen, um den 2. und 3. Satz von Sylow zu beweisen: ist H eine beliebige p-Untergruppe von G, so liegt H nach (4) und (5) in einer p-Sylowgruppe $S_i \in \Omega$, was Satz 7.29 (a) zeigt. Im Spezialfall, wenn H selbst eine p-Sylowgruppe ist und damit genauso viele Elemente wie S_i hat, ist dann natürlich sogar $H = S_i$. Insbesondere ist dann also schon $H \in \Omega$, also $H = aSa^{-1}$ für ein $a \in G$, was Satz 7.29 (b) und außerdem $\Omega = \mathrm{Syl}_p(G)$ beweist. Wir haben demnach $s_p = |\mathrm{Syl}_p(G)| = |\Omega|$. Darüber hinaus gilt für eine p-Sylowgruppe H dann natürlich nur für ein S_i, dass $H \leq S_i$ (nämlich für $S_i = H$). Nach (5) gilt also auch nur für dieses eine S_i, dass $H_{S_i} = H$ und der zugehörige Summand in (3) damit gleich 1 ist. Also hat in (3) genau ein Summand den Wert 1, während alle anderen durch p teilbar sind, d. h. es gilt $s_p = |\Omega| = 1 \mod p$ und damit Satz 7.30 (a). Nach (1) ist schließlich $s_p = |\Omega| \mid |G| = q\,p^k$; da s_p wegen $s_p = 1 \mod p$ keinen Primfaktor p enthalten kann also $s_p \mid q$, d. h. Satz 7.30 (b). □

Beispiel 7.31. Wir betrachten die 3-Sylowgruppen in der symmetrischen Gruppe S_4. Wegen $|S_4| = 24 = 2^3 \cdot 3$ haben diese jeweils 3 Elemente. Sie sind also zyklisch [G, Satz 6.21 (b)] und werden damit von jeweils einem Element der Ordnung 3, also einem 3-Zykel erzeugt. Die verschiedenen 3-Sylowgruppen von S_4 sind damit

$$U_1 = \langle (1\ 2\ 3) \rangle = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}, \qquad U_2 = \langle (1\ 2\ 4) \rangle = \{\mathrm{id}, (1\ 2\ 4), (1\ 4\ 2)\},$$
$$U_3 = \langle (1\ 3\ 4) \rangle = \{\mathrm{id}, (1\ 3\ 4), (1\ 4\ 3)\}, \qquad U_4 = \langle (2\ 3\ 4) \rangle = \{\mathrm{id}, (2\ 3\ 4), (2\ 4\ 3)\}.$$

Wir hatten in Beispiel 7.19 bereits gesehen, dass alle 3-Zykel und damit auch alle $U_1, \dots, U_4$ zueinander konjugiert sind – was Satz 7.29 (b) in diesem Fall bestätigt. Gemäß Satz 7.30 erfüllt die Anzahl $s_3 = 4$ der 3-Sylowgruppen auch $s_3 = 1 \mod 3$ und $s_3 \mid 2^3 = 8$.

13

Wie bereits angekündigt können wir nun in den Fällen, in denen wir aus dem 3. Satz von Sylow wissen, dass es genau eine Untergruppe einer gegebenen Ordnung gibt, darauf schließen, dass diese dann auch ein Normalteiler sein muss. Dies ist z. B. für die folgenden Gruppenordnungen der Fall.

Folgerung 7.32 (Existenz von Normalteilern)**.** *Es sei G eine Gruppe mit $|G| = q\,p^k$ für ein $k \in \mathbb{N}_{>0}$ und zwei verschiedene Primzahlen p,q mit $q \neq 1 \mod p$. Dann besitzt G genau eine p-Sylowuntergruppe (der Ordnung p^k), und diese ist ein Normalteiler in G.*

Beweis. Nach Satz 7.30 (b) ist die Anzahl s_p der p-Sylowgruppen von G ein Teiler von q und kann damit nur 1 oder q sein. Gleichzeitig gilt nach Satz 7.30 (a) aber auch $s_p = 1 \mod p$; wegen $q \neq 1 \mod p$ ist $s_p = q$ also unmöglich. Damit gibt es genau eine p-Sylowuntergruppe $U \leq G$. Nach [G, Aufgabe 6.9 (b)] ist diese dann auch ein Normalteiler (denn für alle $a \in G$ ist aUa^{-1} wieder eine p-Sylowuntergruppe von G und muss damit gleich U sein). □

Mit Hilfe dieser Existenzaussage für Normalteiler können wir nun für eine weitere Klasse von Gruppenordnungen eine Klassifikation angeben.

Folgerung 7.33 (Klassifikation der Gruppen der Ordnung pq mit $p \neq 1 \mod q$ und $q \neq 1 \mod p$)**.** *Es sei G eine Gruppe mit $|G| = pq$ für zwei verschiedene Primzahlen p,q mit $p \neq 1 \mod q$ und $q \neq 1 \mod p$. Dann ist $G \cong \mathbb{Z}_{pq}$.*

Beweis. Nach Folgerung 7.32 gibt es Normalteiler $U_p, U_q \trianglelefteq G$ mit $|U_p| = p$ und $|U_q| = q$. Beachte, dass $U_p \cap U_q = \{e\}$ gilt, da $|U_p \cap U_q|$ nach dem Satz von Lagrange [G, Satz 5.10] ein Teiler von p und q sein muss.

Wir behaupten nun, dass die Abbildung

$$f : U_p \times U_q \to G, \quad (a,b) \mapsto ab$$

ein Isomorphismus ist.

- f ist ein Morphismus: für alle $a,a' \in U_p$ und $b,b' \in U_q$ ist
$$f((a,b)\cdot(a',b')) = f(aa',bb') = aa'bb' \qquad \text{und} \qquad f(a,b)\cdot f(a',b') = aba'b'.$$
Wir müssen zeigen, dass diese beiden Elemente gleich sind, also dass $a'b = ba'$, d. h. $a'ba'^{-1}b^{-1} = e$ gilt. Da $b \in U_q$ und U_q ein Normalteiler in G ist, ist $a'ba'^{-1} \in U_q$ und damit auch $a'ba'^{-1}b^{-1} \in U_q$. Umgekehrt ist genauso $ba'^{-1}b^{-1} \in U_p$ und damit auch $a'ba'^{-1}b^{-1} \in U_p$. Also ist $a'ba'^{-1}b^{-1} \in U_p \cap U_q = \{e\}$, d. h. f ist ein Morphismus.
- f ist injektiv: ist $(a,b) \in U_p \times U_q$ mit $f(ab) = ab = e$, so ist $a = b^{-1} \in U_p \cap U_q = \{e\}$, also $(a,b) = (e,e)$. Damit ist $\operatorname{Ker} f = \{(e,e)\}$, d. h. f ist injektiv.
- f ist surjektiv: dies folgt nun aus der Injektivität, da $|U_p \times U_q| = |G| = pq$.

Damit ist $G \cong U_p \times U_q$. Da U_p und U_q als Gruppen von Primzahlordnung isomorph zu $\mathbb{Z}_p$ bzw. $\mathbb{Z}_q$ sind [G, Satz 6.21 (b)], ist G also isomorph zu $\mathbb{Z}_p \times \mathbb{Z}_q$ und damit nach dem chinesischen Restsatz [G, Satz 11.22] auch zu $\mathbb{Z}_{pq}$. □

Beispiel 7.34. Nach Folgerung 7.33 ist jede Gruppe der Ordnung $15 = 3 \cdot 5$ isomorph zu $\mathbb{Z}_{15}$, denn $3 \neq 1 \mod 5$ und $5 \neq 1 \mod 3$. Für Gruppen der Ordnung $6 = 2 \cdot 3$ hingegen macht Folgerung 7.33 keine Aussage, da $3 = 1 \mod 2$ – und in der Tat gibt es hier neben $\mathbb{Z}_6$ ja auch noch die nicht-abelsche Gruppe S_3.

Aufgabe 7.35 (Klassifikation der Gruppen der Ordnung $2p$)**.** Es sei G eine Gruppe mit $|G| = 2p$ für eine ungerade Primzahl p. Man zeige:

(a) Hat G kein Element der Ordnung $2p$, so gibt es Elemente $a,b \in G$ mit $\operatorname{ord} a = p$, $\operatorname{ord} b = 2$ und $ba = a^{-1}b$.

(b) G ist entweder isomorph zu $\mathbb{Z}_{2p}$ oder zur Diedergruppe D_{2p} aus [G, Aufgabe 3.17].

Aufgabe 7.36. Zeige, dass A_4 keine Untergruppe der Ordnung 6 besitzt. (Wegen $|A_4| = 12$ ist dies also ein Beispiel dafür, dass zu einer endlichen Gruppe G und einem $n \mid |G|$ nicht notwendig eine Untergruppe $U \leq G$ mit $|U| = n$ existieren muss).

Bemerkung 7.37 (Klassifikation endlicher Gruppen)**.** Wir wollen jetzt noch einmal die Ergebnisse zur Klassifikation endlicher Gruppen zusammenfassen, die wir mit unseren bisherigen Methoden erzielen konnten. Ist G eine endliche Gruppe der Ordnung n, so wissen wir:

- Ist $n = p$ eine Primzahl, so ist $G \cong \mathbb{Z}_p$ [G, Satz 6.21 (b)].
- Ist $n = p^2$ ein Primzahlquadrat, so ist $G \cong \mathbb{Z}_{p^2}$ oder $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ (Aufgabe 7.21).
- Ist $n = 2p$ für eine ungerade Primzahl p, so ist G isomorph zu $\mathbb{Z}_{2p}$ oder zur Diedergruppe D_{2p} (Aufgabe 7.35).
- Ist $n = pq$ für zwei verschiedene Primzahlen p und q mit $p \not\equiv 1 \mod q$ und $q \not\equiv 1 \mod p$, so ist $G \cong \mathbb{Z}_{pq}$ (Folgerung 7.33).

Für andere Gruppenordnungen ist die grobe Faustregel, dass mit zunehmender Anzahl von (nicht notwendig verschiedenen) Primfaktoren in n sowohl die Anzahl der Gruppen der Ordnung n als auch der Aufwand für den Klassifikationsbeweis schnell ansteigt. In der Tat ist eine Klassifikation endlicher Gruppen für beliebige Gruppenordnungen derzeit nicht bekannt – und aufgrund der Struktur der bisher bekannten Ergebnisse auch kaum zu erwarten. Für „kleine“ Gruppenordnungen (bis etwa 1000) kann man allerdings noch mit einer Mischung aus Computeralgebra und theoretischen Methoden eine vollständige Liste aller Gruppen erzeugen. Die folgende Tabelle zeigt beispielhaft für alle $n < 100$ die Anzahlen der Gruppen der Ordnung n [BE]. Es ist sicher erstaunlich, dass eine so einfache und grundlegende mathematische Struktur wie die einer Gruppe zu solch einer unüberschaubaren Klassifikation führt!

n	0	1	2	3	4	5	6	7	8	9
0		1	1	1	2	1	2	1	5	2
10	2	1	5	1	2	1	14	1	5	1
20	5	2	2	1	15	2	2	5	4	1
30	4	1	51	1	2	1	14	1	2	2
40	14	1	6	1	4	2	2	1	52	2
50	5	1	5	1	15	2	13	2	2	1
60	13	1	2	4	267	1	4	1	5	1
70	4	1	50	1	2	3	4	1	6	1
80	52	15	2	1	15	1	2	1	12	1
90	10	1	4	2	2	1	231	1	5	2