

2.6 Ergänzungen und Beispiele: Semidirekte Produkte

Wir befassen uns mit der “Zerlegung” von Gruppen in kleinere Gruppen, bzw. der Konstruktion einer Gruppe aus kleineren Gruppen. Das folgende bekannte Resultat wird hierfür die einfachsten Beispiele liefern.

Beispiel 2.6.1 Es sei G eine Gruppe der Ordnung $|G| = 6$. Dann gilt $G \cong Z_6$ (zyklische Gruppe) oder $G \cong S_3$ (symmetrische Gruppe).

BEWEISSKIZZE: Man benutzt Ordnungen von Elementen und den Satz von Lagrange. Falls es ein Element der Ordnung 6 gibt, ist G zyklisch, der Fall muss nicht weiter betrachtet werden.

Es gibt in G ein Element x der Ordnung 3 und ein Element y der Ordnung 2. Dieses erhält man entweder als (vergleichsweise trivialen) Spezialfall der Sylowsätze, oder direkt aus dem sog. Lemma von Cauchy, oder ganz “zu Fuß”, indem man die gegenteilige Annahme (alle Elemente haben die Ordnung 2 oder 3, aber nur eine Ordnung kommt vor) zum Widerspruch führt. Es folgt weiter

$$G = \{e, x, x^2, y, xy, x^2y\},$$

denn die angegebenen Elemente sind alle verschieden voneinander (siehe auch Lemma 2.6.2).

Man betrachtet nun das Konjugierte $x' := yxy^{-1} = yxy$. Dieses ist wieder von der Ordnung 3, muss also gleich x oder x^2 sein. (Wenn es weitere Elemente der Ordnung 3 gäbe, dann gäbe es zwei verschiedene Untergruppen der Ordnung 3, und G hätte insgesamt mindestens 9 Elemente.) Aus der Information $yx = x'y = xy$ bzw. $= x^2y$ kann man nun die gesamte Verknüpfungstafel hinschreiben: im ersten Fall ist G zyklisch, erzeugt etwa von xy , im zweiten Fall ist G isomorph zur Diedergruppe D_3 der Ordnung 6 (näheres unten unter 2.6.9), die wiederum isomorph zu S_3 ist.

Wir halten einen ständig benutzten elementaren Schluss explizit als Hilfssatz fest:

Lemma 2.6.2 Es sei G eine Gruppe und $A \leq G, B \leq G$ zwei endliche Untergruppen mit $A \cap B = \{e\}$, sei $|A| =: \ell$ und $|B| =: m$. Dann besteht $AB := \{ab \mid a \in A, b \in B\}$ aus ℓm Elementen.

BEWEISSKIZZE: Die Abbildung $A \times B \rightarrow AB, (a, b) \mapsto ab$ ist bijektiv. \square

Die Voraussetzung $A \cap B = \{e\}$ ist insbesondere erfüllt, wenn ℓ und m teilerfremd sind.

Wir erinnern daran, dass das kartesische Produkt $A \times B$ zweier Gruppen mit der komponentenweisen Verknüpfung wieder eine Gruppe ist. Es wird auch als *direktes Produkt* (genauer: *externes direktes Produkt*) von A und B bezeichnet.

Definition und Bemerkung 2.6.3 (Direktes Produkt) Eine Gruppe G heißt (internes) *direktes Produkt* von zwei Untergruppen $A, B \leq G$, wenn folgendes gilt:

1. $G = AB$
2. $A \cap B = \{e\}$
3. A und B sind “elementweise vertauschbar”, d.h. für alle $a \in A, b \in B$ gilt $ab = ba$.

Unter diesen Voraussetzungen gilt: $G \cong A \times B$.

BEWEIS: Unter der (zusätzlichen) Voraussetzung von 3. ist die Abbildung aus 2.6.2 ein Homomorphismus, also ein Isomorphismus. \square

Die Bemerkung besagt also, dass das interne direkte Produkt zweier Untergruppen A und B isomorph zum externen direkten Produkt ist, das man aus den Gruppen A und B konstruieren kann. Dieser Sachverhalt hat auch eine offensichtliche Umkehrung, nämlich die folgende: Es sei eine Gruppe G definiert als $G = A \times B$, wobei A, B zwei völlig beliebige Gruppen sind. Betrachte:

- $\tilde{A} = A \times \{e_B\} \subseteq G$
- $\tilde{B} = \{e_A\} \times B \subseteq G$

Dann gelten die drei Bedingungen aus 2.6.3, d.h. G ist das direkte Produkt der Untergruppen \tilde{A} und \tilde{B} .

Man sieht sofort, dass in einem direkten Produkt $G = AB$ die beiden Untergruppen A und B normal sind. Das folgende Lemma besagt, dass unter Voraussetzung von 1. und 2. die Normalität schon ausreichend ist für das Vorliegen eines direkten Produktes.

Lemma 2.6.4 (Produktzerlegung) Es sei G eine Gruppe und A, B Untergruppe mit den folgenden Eigenschaften:

1. $G = AB$
2. $A \cap B = \{e\}$
3. A, B sind beide Normalteiler

Dann ist G das direkte Produkt von A und B .

BEWEIS: Für $a \in A, b \in B$ liegt der Kommutator $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1}$ wegen der vorausgesetzten Normalität sowohl in A als auch in B , ist also gleich e . \square

Aus 2.6.2, 2.6.4 und 2.6.3 ergibt sich nun folgendes einfache Kriterium:

Korollar 2.6.5 Sei G endliche Gruppe, ihre Ordnung zerlegt als $|G| = \ell m$, wobei $\text{ggT}(\ell, m) = 1$. Es seien A, B Normalteiler in G mit $|A| = \ell$, $|B| = m$. Dann gilt $G \cong A \times B$.

Im allgemeinen werden Normalteiler mit den gewünschten Ordnungen nicht existieren und deshalb das Lemma nicht anwendbar sein. Eine Ausnahme von dieser Regel haben wir im vergleichsweise trivialen Fall der abelschen Gruppen. Hier ist erstens Normalität keine Bedingung, und zweitens existieren zu jeder teilerfremden Zerlegung der Gruppenordnung entsprechende Untergruppen. Als kleinen Exkurs halten wir das Ergebnis im folgenden Satz fest.

Satz 2.6.6 Es sei G eine endliche abelsche Gruppe, $|G| = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$, wobei die p_i paarweise verschiedene Primzahlen sind und $k_i \in \mathbb{N}$. Setze

$$G_i = \{x \in G \mid x^{p_i^{k_i}} = e\}.$$

Dann sind die G_i , $i = 1, \dots, r$ Untergruppen von G mit $|G_i| = p_i^{k_i}$, und es gilt

$$G \cong G_1 \times G_2 \times \dots \times G_r.$$

Es muss betont werden, dass der Beweis dieses Satzes nicht auf dem vorigen Resultat 2.6.5 beruht. Wenn man nämlich zeigt, dass die dortigen Untergruppen G_i die richtige Ordnung haben, kann man gleich die komplette Aussage über die direkte Summe beweisen. Es handelt sich hier übrigens um eine einfache Verallgemeinerung des chinesischen Restsatzes, der entsprechendes für zyklische Gruppen (bzw. die Ringe $\mathbb{Z}/m\mathbb{Z}$) behauptet.

Wir kehren zum Fall allgemeiner Gruppen zurück. Der folgende Satz ist eine Standardanwendung der Sylowsätze, kombiniert mit obigem Korollar 2.6.5.

Satz 2.6.7 Es sei G ein Gruppe der Ordnung pq , wobei p und q Primzahlen sind mit $p < q$. Weiter sei $q \not\equiv 1 \pmod{p}$ vorausgesetzt. Dann gilt $G \cong Z_p \times Z_q \cong Z_{pq}$, wobei Z_m die zyklische Gruppe der Ordnung m bezeichnet.

Unter den genannten Voraussetzungen ist also die Gruppe G durch ihre Ordnung bis auf Isomorphie eindeutig bestimmt. Sie ist direktes Produkt von zyklischen Gruppen von Primzahlordnung, und auch selbst zyklisch, insbesondere abelsch.

Die Voraussetzung $q \not\equiv 1 \pmod{p}$ in diesem Satz ist essentiell. Sie liefert, dass die p -Sylowgruppe normal ist. Wenn $q \equiv 1 \pmod{p}$ ist, kann man tatsächlich eine Gruppe konstruieren, die q p -Sylowgruppen enthält; diese Gruppe ist insbesondere nicht abelsch. Wir kommen unten darauf zurück.

Für $p = 2$ ist der Satz nie anwendbar, weil dann für jede weitere Primzahl q gilt $q \equiv 1 \pmod{2}$. Die angekündigte nicht-abelsche Gruppe der Ordnung $2q$ ist dann die Diedergruppe.

Als kleinen Exkurs wollen wir jetzt die Diedergruppen etwas ausführlicher behandeln. Hierzu zunächst eine ganz allgemeine Definition:

Bemerkung und Definition 2.6.8 (Erzeugnis, Erzeugendensystem)

Es sei G eine Gruppe, $X \subseteq G$ eine Teilmenge. Setze

$$\langle X \rangle := \{x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n} \mid n \in \mathbb{N}, x_i \in X, \varepsilon_i \in \{\pm 1\}, i = 1, \dots, n\}.$$

- a) $\langle X \rangle$ ist eine Untergruppe von G
- b) $\langle X \rangle$ ist die kleinste Untergruppe von G , die X enthält. Mit anderen Worten, wenn $H \subseteq G$ eine Untergruppe mit $X \subseteq H$ ist, so ist auch $\langle X \rangle \subseteq H$.

$\langle X \rangle$ heißt die von X erzeugte Untergruppe oder kurz das *Erzeugnis* von X . Die Menge X heißt auch *Erzeugendensystem* der Gruppe $\langle X \rangle$. Eine Gruppe heißt *endlich erzeugt*, wenn sie ein endliches Erzeugendensystem besitzt.

Hier noch ein paar ergänzende Bemerkungen zu diesen Definitionen:

1. Für $X = \{x_1, \dots, x_k\}$ endlich schreibe kurz $\langle x_1, \dots, x_k \rangle$ statt $\langle \{x_1, \dots, x_k\} \rangle$.
2. Man kann in der Definition von $\langle X \rangle$ die ε_i auch durch \mathbb{Z} laufen lassen und erhält dieselbe Menge (durch Zusammenfassen gleicher Faktoren zu Potenzen).
3. Insbesondere ist $\langle x \rangle$ (für festes $x \in G$) wie früher definiert die von x erzeugte zyklische Untergruppe.

Im folgenden Beispiel betrachten wir die Diedergruppe als Symmetriegruppe des Quadrates, dessen Ecken zyklisch von 1 bis 4 nummeriert sind, also gleichzeitig als Untergruppe der symmetrischen Gruppe S_4 .

Beispiel Die Diedergruppe der Ordnung 8 ist von zwei Elementen erzeugt: es gilt $Di_4 = \langle \rho, \sigma \rangle$ mit $\rho = (1, 2, 3, 4)$ und $\sigma = (1, 3)$. Man überlegt sich genauer $Di_4 = \{\rho^i \sigma^j \mid i = 0, 1, 2, 3, j = 0, 1\}$.

Satz 2.6.9 (Kennzeichnung der Diedergruppen) *Es sei $n \in \mathbb{N}$. Dann gibt es bis auf Isomorphie genau eine Gruppe G mit den folgenden Eigenschaften: $G = \langle x, y \rangle$ für zwei Elemente $x, y \in G$ für die gilt*

$$(D1) \quad x \neq y, \text{ ord}(x) = n, \text{ ord}(y) = 2$$

$$(D2) \quad yxy^{-1} = x^{-1}$$

Diese Gruppe hat die Ordnung $|G| = 2n$; sie heißt die Diedergruppe der Ordnung $2n$, Bezeichnung Di_n oder D_n .

BEWEISSKIZZE: (Existenz) Wir betrachten in der symmetrischen Gruppe die Elemente $\rho = (1, 2, 3, \dots, n)$ und $\sigma = (1, n)(2, n-1) \cdots (n/2, n/2+1)$ für gerades n , ähnlich für ungerades n . Die Untergruppe $Di_n := \langle \rho, \sigma \rangle \subseteq S_n$ hat offenbar beide Eigenschaften. Das gleiche gilt übrigens für die von der Drehung um $2\pi/n$ und einer beliebigen Spiegelung erzeugte Untergruppe der orthogonalen Gruppe $O(\mathbb{R}^2)$; vergleiche die frühere Behandlung der Symmetrien des Quadrates.

(Eindeutigkeit) Wenn x, y Elemente in irgendeiner Gruppe G sind, die (D1) und (D2) erfüllen, dann rechnet man nach, dass $\langle x \rangle \cup \langle x \rangle y$ eine Untergruppe ist, also gleich ganz G , wenn $\langle x, y \rangle = G$, und dass jede weitere solche Gruppe $G' = \langle x', y' \rangle$ durch $x^i y^j \mapsto x'^i y'^j$, $i = 0, \dots, n-1, j = 0, 1$ zu G isomorph ist. \square
Der Satz gilt übrigens auch für $n = \infty$.

Wir schwächen nun die Voraussetzungen eines direkten Produktes ab und betrachten Produkte von zwei Untergruppen, von denen nur eine als Normalteiler vorausgesetzt ist. Hierzu zunächst ein kleines Lemma:

Lemma 2.6.10 Es sei G eine Gruppe und $T, H \leq G$ zwei Untergruppen derart, dass T von H normalisiert wird: $hth^{-1} \in T$ für alle $h \in H, t \in T$. Dann ist TH eine Untergruppe von G .

BEWEISSKIZZE:

$$(M) \quad tht'h' = t(ht'h^{-1})(hh')$$

$$(I) \quad (th)^{-1} = h^{-1}t^{-1} = (h^{-1}t^{-1}h)h^{-1}$$

Die Voraussetzung kann auch so ausgedrückt werden: H ist im Normalisator $N_G(T)$ enthalten. Das ist natürlich erfüllt, wenn T ein Normalteiler in G ist. Wegen $ht = (tht^{-1})t$ gilt unter den Voraussetzungen des Lemmas $TH = HT$, d.h. auf die Reihenfolge der Faktoren in einem semidirekten Produkt kommt es nicht an. (Auf die Reihenfolge der Gruppen nicht, auf die der Elemente schon.)

In der folgenden Definition wird noch die bekannte Bedingung hinzugefügt, dass die beiden Untergruppen trivialen Schnitt haben.

Definition 2.6.11 Eine Gruppe G heißt (*internes*) *semidirektes Produkt* von zwei Untergruppen T und H , falls gilt

$$(1) \quad G = TH$$

$$(2) \quad T \cap H = \{e\}$$

$$(3) \quad T \trianglelefteq G$$

Beispiele 2.6.12 (1) Die Würfelgruppe \mathbb{O} (aufgefasst als Untergruppe der orthogonalen 3×3 -Matrizen) ist das semidirekte Produkt der Untergruppe T der Diagonalmatrizen in \mathbb{O} mit der Gruppe H der Permutationsmatrizen (vergl. Übungen).

- (2) Die affine Gruppe $\text{AGL}(V)$ eines Vektorraumes V ist das semidirekte Produkt der Translationsgruppe $T(V)$ mit der Gruppe der Vektorraumautomorphismen $\text{GL}(V)$ (siehe Lineare Algebra II).

Wenn $G = TH$ ein semidirektes Produkt wie in 2.6.10 ist, dann operiert H auf T durch (von G auf T eingeschränkte) innere Automorphismen (die Abbildung $H \times T \rightarrow T$, $(h, t) \mapsto hth^{-1}$ ist eine Gruppenoperation). Nach den im Beweis von 2.6.10 angegebenen Formeln ist die Verknüpfung in G bekannt, wenn die beiden Verknüpfungen in T und H bekannt sind und ferner die genannte Operation. Mit anderen Worten, die Struktur eines semidirekten Produktes ergibt sich aus der Struktur der beiden beteiligten einzelnen Gruppen zusammen mit einer Operation der einen Gruppe auf der anderen. Wenn wir noch beachten, dass nach 2.3.9 eine Operation einer Gruppe H auf einer Menge T (hier: ebenfalls einer Gruppe) im wesentlichen dasselbe ist wie ein Homomorphismus von H in die Permutationsgruppe $\text{Per}(T)$ (hier $\text{Aut}(T)$), so kommt man auf den folgenden Satz.

Satz und Definition 2.6.13 a) *Es seien T und H Gruppen und $\alpha : H \rightarrow \text{Aut}(T)$ eine Operation von H auf T durch Gruppenautomorphismen von T . Dann ist das Produkt $T \times H$ mit der Verknüpfung*

$$(x, g)(y, h) := (x\alpha(g)(y), gh), \quad x, y \in T, \quad g, h \in H$$

eine Gruppe. Dieses wird mit $T \rtimes H$, genauer $T \rtimes_{\alpha} H$ bezeichnet und heißt (externes) semidirektes Produkt (mittels α) von T und H .

- b) *Wenn $G = TH$ semidirektes Produkt zweier Untergruppen mit normalem T ist und $\alpha : H \rightarrow \text{Aut}(T)$ durch $\alpha(h)(t) = hth^{-1}$ definiert wird, dann ist die Abbildung $T \rtimes_{\alpha} H \rightarrow G$, $(t, h) \mapsto th$ ein Gruppenisomorphismus.*

Der Teil b) gibt nur wieder, was wir uns als Hinführung zur Definition des externen semidirekten Produktes überlegt hatten. Das wesentliche an Teil a) dieses Satzes ist, dass er genau angibt, wie man aus zwei gegebenen Gruppen und einer Zusatzinformation, eben dem Homomorphismus α , eine neue Gruppe konstruiert. Die Konstruktion ist so eingerichtet, dass bis auf Isomorphie diese Gruppen genau die vorher schon betrachteten internen semidirekten Produkte von Untergruppen sind. Wir halten das zur Abrundung noch explizit als Zusatz zum letzten Satz fest:

Zusatz 2.6.14 Die Teilmengen $\tilde{T} = T \times \{e\}$ und $\tilde{H} = \{e\} \times H$ sind Untergruppen von $T \rtimes H$, dabei ist $\tilde{T} \trianglelefteq (T \rtimes H)$ normal, $H \cong \tilde{H}$, $T \cong \tilde{T}$. Die Gruppe $T \rtimes H$ ist das (interne) semidirekte Produkt dieser Untergruppen: $T \rtimes H = \tilde{T}\tilde{H}$. Die Operation von \tilde{H} auf \tilde{T} durch Konjugation entspricht der gegebenen Operation α von H auf T .