Seminar
Facetten der geometrischen Gruppentheorie
Oleg Bogopolski

Vortrag 1, 09.06.2020
Freie Gruppen, Semidirekte Produkte von Gruppen, Kranzprodukte, Lamplighter-Gruppe

Asri Ferati

1 Freie Gruppen

Freie Gruppen [1, Section 3 von Chapter 2] kommen vor allem in der kombinatorischen Gruppentheorie zum Einsatz. Interessant ist eine Analogie zu Vektorräumen, die folgende Definition sehr gut wiedergibt:

Definition 1.1 (Freie Gruppe, Variante 1)**.** Sei F eine Gruppe mit neutralem Element e. Sei ferner $X \subset F$ sodass $X \cap X^{-1} = \emptyset$ mit $X^{-1} := \{x^{-1} \mid x \in X\}$. Dann heißt F *freie Gruppe mit Basis* X, falls jedes $f \in F \setminus \{e\}$ eine eindeutige Darstellung

$$f = x_1 x_2 \dots x_n \tag{1}$$

mit $x_i \in X^{\pm} := X \cup X^{-1}$ und $x_i x_{i+1} \neq e$ besitzt.

Zur Frage der Existenz von freien Gruppen liefert bereits folgendes, einfaches Beispiel eine Antwort: $(\mathbb{Z}, +)$ ist eine freie Gruppe mit Basis $\{1\}$.
In der Tat lässt sich sogar zeigen, dass man freie Gruppen konkret konstruieren kann:

Satz 1.2. *Für eine beliebige Menge X existiert eine freie Gruppe mit Basis X.*

Zum Beweis ist noch etwas Vorarbeit nötig, wir benötigen ein paar Definitionen:

Definition 1.3. Sei X eine beliebige Menge. Wie eben sei $X^{-1} := \{x^{-1} \mid x \in X\}$, wobei diesmal x^{-1} ein zu x gehörendes abstraktes Element symbolisieren soll mit $(x^{-1})^{-1} := x$ und $X \cap X^{-1} = \emptyset$. Des Weiteren bezeichnen wir die Menge $X^{\pm} := X \cup X^{-1}$ als *Alphabet* und die entsprechenden Elemente als *Buchstaben*. Dann liegt nahe Folgen von Buchstaben

$$x_1 x_2 \dots x_n$$

Wörter zu nennen, also $x_i \in X^{\pm}$ und $n \geq 0$. Definiere zudem für $f = x_1 x_2 \dots x_n$ die *Wortlänge* von f als $|f| := n$. Im Falle $n = 0$ sprechen wir vom *leeren Wort* und schreiben dafür $\emptyset$. Abschließend sei noch ein *Teilwort* von f als Teilfolge von hintereinander stehenden Buchstaben erklärt.

Wir sind nun in der Lage die im Satz 1.2 zu konstruierende Gruppe aufzubauen. Hierfür sei zunächst W die Menge aller Wörter die aus dem Alphabet $X^{\pm}$ erzeugt werden können. Dann können wir leicht ein Produkt auf W erklären, indem wir für $f, g \in W$ das Wort fg als Aneinanderreihung von g an f verstehen. Die Menge W ist dann zusammen mit dieser Operation zwar leider noch keine Gruppe (inverse Elemente fehlen), aber wir können trotzdem mithilfe von Äquivalenzklassen unser Ziel erreichen:

Definition 1.4. Auf W definieren wir eine Äquivalenzrelation durch

$$u \sim v :\Leftrightarrow \exists f_1, \dots, f_k \in W \colon u = f_1, v = f_k,$$

wobei jedes f_{i+1} aus f_i durch Hinzufügen oder Löschen von Teilwörtern der Form xx^{-1} mit $x \in X^{\pm}$ gewonnen werden kann. Die entsprechenden Wörter $f_1, \dots, f_k$ nennen wir eine die Wörter u und v *verbindende Folge*. Ferner bezeichne im Folgenden

$$[F] := \{[f] \mid f \in W\}$$

die Menge aller entsprechenden Äquivalenzklassen.

Wir werden zeigen, dass $[F]$ die freie Gruppe aus Satz 1.2 ist. Dazu brauchen wir noch folgenden Begriff: Ein Wort $g \in W$ heißt *reduziert*, falls es in g keine Teilwörter der Form xx^{-1} mit $x \in X^{\pm}$ gibt. In Bezug zu den Äquivalenzklassen gilt damit:

Lemma 1.5. *Jedes $[f]$ enthält genau ein reduziertes Wort.*

Beweis. Nach Definition der Äquivalenzrelation ist klar, dass $[f]$ ein reduziertes Wort enthalten muss. Wir müssen lediglich die Eindeutigkeit zeigen: Angenommen es gäbe zwei reduzierte Wörter $u, v \in [f]$ mit $u \neq v$. Wir wissen dann, dass $u \sim v$ und wählen eine verbindende Folge $u = f_1, \ldots, v = f_k$ so, dass $\sum_{i=1}^{k} |f_i|$ minimal ist. Da $u \neq v$ reduziert sind, muss zwangsläufig $|u| = |f_1| < |f_2|$ und $|f_{k-1}| > |f_k| = |v|$ gelten. Per Induktion ist dann klar, dass es ein $i \in \{2, \ldots, k-1\}$ gibt mit $|f_{i-1}| < |f_i|$ und $|f_i| > |f_{i+1}|$. Anschaulich betrachtet: Man erhält f_i aus f_{i-1} indem man in f_{i-1} ein neues Teilwort xx^{-1} einfügt und analog f_{i+1} aus f_i indem man ein Teilwort yy^{-1} entfernt. Wir betrachten nun 2 Fälle:

1. Fall: xx^{-1} und yy^{-1} sind in f_i disjunkt.
   Dann kann man das Wort yy^{-1} aus f_{i-1} streichen und falls f_i' das so entstehende Wort bezeichnet, so erhält man f_{i+1} durch Einfügen von xx^{-1} in f_i'. Mit f_i' anstelle von f_i gibt es also eine neue die Wörter u und v verbindende Folge mit $|f_i'| < |f_i|$, ein Widerspruch zur Minimalitätsvoraussetzung.

2. Fall: xx^{-1} und yy^{-1} haben in f_i eine gemeinsame Schnittmenge.
   Dieses Szenario ist nur möglich bei $y = x^{-1}$. Dann enthält f_i das Teilwort $x^{-1}xx^{-1}$ oder $xx^{-1}x$. Aus Symmetriegründen folgt hier $f_{i-1} = f_{i+1}$ und somit sind f_i sowie f_{i+1} „überflüssig" und können aus der verbindenden Folge gestrichen werden, erneut ein Widerspruch zur Minimalitätsvoraussetzung.

□

Jetzt können wir Satz 1.2 beweisen:

Beweis von Satz 1.2. Wir zeigen zunächst, dass $[F]$ mit der Operation $[f][g] := [fg]$ eine Gruppe ist. Offenbar gilt für $f, g, h \in W$, dass

$$([f][g])[h] = [fg][h] = [fgh] = [f][gh] = [f]([g][h])$$

sowie

$$[f][\emptyset] = [\emptyset][f] = [f].$$

Somit ist Assoziativität und Existenz eines neutralen Elements klar. Für beliebiges $f \in W$ gibt es ferner $x_i \in X^{\pm}$, so dass $f = x_1 \ldots x_n$ und somit

$$[f] = [x_1 \ldots x_n] = [x_1] \ldots [x_n]. \tag{2}$$

Also ist das Inverse zu $[f]$ gegeben durch $[x_n^{-1} \ldots x_1^{-1}]$. Damit ist $[F]$ tatsächlich eine Gruppe. Zeige nun noch, dass $[F]$ eine freie Gruppe ist: Offenbar sind X und die Menge

$$[X] := \{[x] \mid x \in X\}$$

isomorph mit $[X] \subset [F]$. Die notwendige eindeutige Darstellung (1) folgt aus Lemma 1.5 und (2). □

Wir haben bisher mit einer relativ expliziten Definition einer freien Gruppe gearbeitet. Für weitere Resultate ist folgender Ansatz hilfreich:

Definition 1.6 (Freie Gruppe, Variante 2)**.** Sei F eine Gruppe und $X \subset F$. Dann heißt *F freie Gruppe mit Basis X*, falls für jede Gruppe G und jede Abbildung $\varphi\colon X \to G$ eine eindeutige Fortsetzung $\varphi^*\colon F \to G$ existiert, die ein Gruppenhomomorphismus ist.

In der Tat sorgt diese Definition nicht für Verwirrung. Man kann zeigen, dass sie zu Definition 1.1 äquivalent ist. Als Anwendung ergibt sich ein interessantes Analogon zu Basen von Vektorräumen:

Satz 1.7. *Basen einer freien Gruppe F besitzen die gleiche Mächtigkeit.*

Beweis. Sei X eine Basis von F. Betrachte den Restklassenkörper $\mathbb{Z}_2 = \{0, 1\}$ und setze

$$H := \{f\colon X \to \mathbb{Z}_2 \mid |f^{-1}(\{1\})| < \infty\}.$$

Dann ist H zusammen mit der punktweisen Addition $(f + g)(x) := f(x) + g(x)$ für $f, g \in H$ und $x \in X$ eine Gruppe. Wir definieren des Weiteren die Funktion $\delta_x\colon X \to \mathbb{Z}_2$ mit

$$\delta_x(y) = \begin{cases} 1, & \text{falls } y = x \\ 0, & \text{sonst.} \end{cases}$$

Für jedes $x \in X$ ist somit $\delta_x \in H$ und nach Definition 1.6 existiert für die Abbildung $X \to H$, $x \mapsto \delta_x$ eine homomorphe Fortsetzung $\varphi : F \to H$. Zusätzlich ist φ surjektiv, da für jedes $f \in H \setminus \{0\}$ (beachte $f(e) = 0$) nach Voraussetzung $f^{-1}(\{1\}) = \{x_1, \ldots, x_n\}$ für $x_i \in X$ und somit

$$\varphi(x_1 \cdots x_n) = \sum_{i=1}^{n} \delta_{x_i} = \sum_{x \in f^{-1}(\{1\})} \delta_x = f. \tag{3}$$

Nach dem Homomorphiesatz ist daher H isomorph zu $F/\ker\varphi$. Wir wollen nun $\ker\varphi$ bestimmen. Per Definition von φ folgt aus einer ähnlichen Darstellung wie in (3), dass jedes $z \in \ker\varphi$ eine gerade „Wortlänge“ besitzen muss und eine gerade Anzahl an „Buchstaben“ x bzw. x^{-1}. Konkret gilt wegen

$$\varphi(w^2) = 2\varphi(w) = 0$$

für $w \in F$ die Beziehung $\langle w^2 \mid w \in F\rangle \subset \ker\varphi$. In der Tat gilt auch die andere Richtung, die wir nun per Induktion beweisen wollen:

Beweis. Sei $z \in \ker\varphi$. Nach der Vorüberlegung haben wir $|z| = 2n$ für ein $n \in \mathbb{N}$.
Induktionsanfang $n \to 1$: $z = x^2$ bzw. $z = x^{-2}$, also $z \in \langle w^2 \mid w \in F\rangle$.
Induktionsschritt $n \to n + 1$: Betrachte zunächst die Fälle $z = xuxv$ bzw. $z = x^{-1}uxv$ für $u, v \in F$ mit $|uv| = 2n$ und $x \in X$. Dann gilt

$$0 = \varphi(xuxv) = \varphi(xuxuu^{-1}v) = \varphi((xu)^2u^{-1}v) = \varphi((xu)^2) + \varphi(u^{-1}v) = \varphi(u^{-1}v),$$

also $u^{-1}v \in \ker\varphi$ und damit nach Induktionsvoraussetzung $u^{-1}v \in \langle w^2 \mid w \in F\rangle$ bzw. $z = (xu)^2u^{-1}v \in \langle w^2 \mid w \in F\rangle$. Analog im Falle $z = x^{-1}uxv$ wegen $x^{-1}uxv = x^{-2}(xu)^2u^{-1}v$. Die anderen Konstellationen lassen sich ähnlich behandeln bzw. auf die oberen Fälle reduzieren. □

Wir wissen also $H \cong F/\langle w^2 \mid w \in F\rangle$. Ferner haben wir H so konstruiert, dass $|H| = 2^{|X|}$, falls $|X|$ endlich ist (da hier $\mathcal{P}(X) \cong \{f : X \to \mathbb{Z}_2\}$) und sonst $|H| = |X| = \infty$, d.h. die Anzahl an Elementen in X hängt nur von F ab. $\square$

2 Semidirekte Produkte von Gruppen

Wir werden nun weitere Gruppen gemäß [2, Section 2.3.1 von Part I] konstruieren. Dabei stellt sich heraus, dass direkte Produkte bei folgendem Begriff wichtig sind:

Definition 2.1 (Gruppenerweiterung)**.** Eine Sequenz

$$G_0 \xrightarrow{f_1} G_1 \xrightarrow{f_2} G_2 \xrightarrow{f_3} \dots \xrightarrow{f_n} G_n$$

von Gruppen G_i sowie Homomorphismen $f_i \colon G_i \to G_{i+1}$ heißt *exakt*, falls stets $\operatorname{im}(f_{i-1}) = \ker(f_i)$ gilt.
Für Gruppen Q und N bezeichnen wir exakte Sequenzen der Form

$$e \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow e,$$

als *Erweiterung von N durch Q*. Insbesondere ist hier i injektiv und π surjektiv mit $\operatorname{im}(i) = \ker(\pi)$.

Mit $G = N \times Q$ als direktem Produkt, der Einbettung $i \colon N \to G, n \mapsto (n, e)$ und der Projektion $\pi \colon G \to Q, (n, q) \mapsto q$ ist offenbar immer eine Erweiterung von N durch Q gegeben. Dass im Umkehrschluss nicht bei jeder Erweiterung die Gruppe G auch ein direktes Produkt ist, sieht man durch eine Verallgemeinerung ein:

Definition 2.2 (Äußeres semidirektes Produkt)**.** Seien Q und N Gruppen sowie $\varphi \colon Q \to \operatorname{Aut}(N)$ ein Gruppenhomomorphismus (z.B eine Gruppenoperation von Q auf N). Dann ist $N \times Q$ mit der Operation

$$(n_1, q_1) * (n_2, q_2) := (n_1\varphi(q_1)(n_2), q_1q_2)$$

eine Gruppe. Wir schreiben zur Unterscheidung dafür $N \rtimes_\varphi Q$, das *(äußere) semidirekte Produkt von N mit Q bezüglich φ*.

Falls $\varphi(q) \equiv id_N$ für alle $q \in Q$ der triviale Homomorphismus ist, so ist das semidirekte Produkt offenbar gleich dem direkten Produkt. Des Weiteren ist analog zu oben für jedes semidirekte Produkt eine Erweiterung gegeben. Hier gilt sogar im Prinzip die Umkehrung, wenn man eine zusätzliche Bedingung stellt:

Definition 2.3. Wir nennen eine Gruppenerweiterung $e \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow e$ *zerlegbar*, falls ein injektiver Homomorphismus $s \colon Q \to G$ mit $\pi \circ s = id_Q$ existiert.

Beispiel 2.4. Die Erweiterung

$$e \longrightarrow N \xrightarrow{i} N \rtimes_\varphi Q \xrightarrow{\pi} Q \longrightarrow e$$

ist zerlegbar für beliebiges φ. Dazu setzt man einfach $s \colon Q \to N \rtimes_\varphi Q, q \mapsto (e, q)$.

In der Tat gilt auch: Bei jeder zerlegbaren Erweiterung $e \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} Q \longrightarrow e$ mit zugehöriger Funktion s ist G isomorph zu einem (äußeren) semidirekten Produkt.

Beweis. Wir zeigen zunächst, dass die beiden Mengen $N \times Q$ und G via

$$\Psi\colon N \times Q \to G, (n,q) \mapsto i(n) \cdot s(q)$$

isomorph sind. Dafür beweisen wir, dass die Inverse durch

$$\Psi^{-1}\colon G \to N \times Q, g \mapsto (i^{-1}(g \cdot (s \circ \pi(g))^{-1}), \pi(g))$$

gegeben ist. Beachte dabei, dass das Element $i^{-1}(g \cdot (s \circ \pi(g))^{-1})$ wegen $\ker(\pi) = \mathrm{im}(i)$ und $\pi(g \cdot (s \circ \pi(g))^{-1}) = \pi(g)(\pi \circ s \circ \pi(g))^{-1} = e$ tatsächlich existiert. Somit gilt für beliebige $g \in G$ bzw. $(n,q) \in N \times Q$:

$$\begin{aligned}\Psi(\Psi^{-1}(g)) = \Psi(i^{-1}(g \cdot (s \circ \pi(g))^{-1}), \pi(g)) &= i(i^{-1}(g \cdot (s \circ \pi(g))^{-1})) \cdot (s \circ \pi(g)) \\ &= g \cdot (s \circ \pi(g))^{-1} \cdot (s \circ \pi(g)) = g\end{aligned}$$

bzw.

$$\begin{aligned}\Psi^{-1}(\Psi(n,q)) &= \Psi^{-1}(i(n) \cdot s(q)) \\ &= (i^{-1}(i(n) \cdot s(q) \cdot (s \circ \pi(i(n) \cdot s(q)))^{-1}), \pi(i(n) \cdot s(q))) \\ &= (i^{-1}(i(n) \cdot s(q) \cdot (s \circ \pi \circ i(n) \cdot s \circ \pi \circ s(q))^{-1}), \pi \circ i(n) \cdot \pi \circ s(q)) \\ \pi \circ i \equiv e, \pi \circ s = id_Q \mid &= (i^{-1}(i(n) \cdot s(q) \cdot (s(q))^{-1}), q) = (n,q).\end{aligned}$$

Wir müssen also nur noch zeigen, dass es ein passendes φ gibt, so dass $\Psi\colon N \rtimes_\varphi Q \to G$ ein Gruppenhomomorphismus ist. Setze dazu nun $\varphi\colon Q \to \mathrm{Aut}(N)$ mit

$$\varphi(q)(n) = i^{-1}(s(q) \cdot i(n) \cdot s(q)^{-1}).$$

Analog zu oben hat man wieder $\pi(s(q) \cdot i(n) \cdot s(q)^{-1}) = \pi \circ s(q) \cdot \pi \circ i(n) \cdot (\pi \circ s(q))^{-1} = q \cdot e \cdot q^{-1} = e$. Daher folgt mit der Voraussetzung $\mathrm{im}(i) = \ker(\pi)$ die Wohldefiniertheit von φ. Dass ebenso $\varphi(q)$ für jedes q ein Automorphismus von N ist, vergewissert man sich dadurch, dass die Inverse $\varphi(q)^{-1}$ genau durch $\varphi(q^{-1})$ gegeben ist. Somit haben wir für $(n_1,q_1),(n_2,q_2) \in N \rtimes_\varphi Q$:

$$\begin{aligned}\Psi((n_1,q_1) * (n_2,q_2)) &= \Psi(n_1 \cdot \varphi(q_1)(n_2), q_1 \cdot q_2) \\ &= i(n_1 \cdot i^{-1}(s(q_1) \cdot i(n_2) \cdot s(q_1)^{-1})) \cdot s(q_1 \cdot q_2) \\ &= i(n_1) \cdot s(q_1) \cdot i(n_2) \cdot s(q_1)^{-1} \cdot s(q_1) \cdot s(q_2) \\ &= i(n_1) \cdot s(q_1) \cdot i(n_2) \cdot s(q_2) = \Psi(n_1,q_1) \cdot \Psi(n_2,q_2)\end{aligned}$$

□

Wir können nun dieses Resultat benutzen, um bekannte Gruppen als semidirekte Produkte zu identifizieren:

Beispiel 2.5. Es gibt passende i, π und s, so dass

$$e \longrightarrow \mathbb{Z}_3 \xrightarrow{i} S_3 \xrightarrow{\pi} \mathbb{Z}_2 \longrightarrow e$$

eine zerlegbare Gruppenerweiterung ist. Insbesondere existiert also ein entsprechendes φ mit $S_3 \cong \mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_2$.

Beweis. Offenbar ist $\mathbb{Z}_3$ isomorph zur Untergruppe $\langle(123)\rangle = \{id, (123), (132)\}$ von S_3 durch z.B.

$$0 \mapsto id, 1 \mapsto (123), 2 \mapsto (132).$$

Somit ist i genau durch diese Einbettung gegeben. Für π muss nach Voraussetzung $\operatorname{im}(i) = \ker(\pi)$ gelten, dass $id, (123), (132) \mapsto 0$. Daher haben wir also

$$\pi\colon id, (123), (132) \mapsto 0; (12), (13), (23) \mapsto 1.$$

Schließlich wählt man s als den Isomorphismus zwischen $\mathbb{Z}_2$ und $\langle(12)\rangle = \{id, (12)\}$ wodurch somit $\pi \circ s = id_{\mathbb{Z}_2}$ □

Offenbar ist klar, dass es noch ein Konzept von semidirekten Produkten gibt:

Definition 2.6 (Inneres semidirektes Produkt)**.** Es seien N und Q Untergruppen von G. Dann heißt G *(inneres) semidirektes Produkt von N und Q*, falls

(a) N ist Normalteiler von G, d.h. $gNg^{-1} = N$ für alle $g \in G$.

(b) $N \cap Q = \{e\}$.

(c) $G = NQ$.

Man schreibt dann $N \rtimes Q = G$.

Beim äußeren semidirekten Produkt wird aus zwei beliebigen Gruppen eine „neue“ Gruppe anhand einer passenden Abbildung konstruiert. Wogegen ein inneres semidirektes Produkt dadurch identifiziert ist, dass geeignete Untergruppen bestimmte Eigenschaften besitzen. Interessant zu erwähnen ist nun, dass bei inneren Produkten eine zerlegbare Gruppenerweiterung immer vorliegt:

$$e \longrightarrow N \xrightarrow{i} N \rtimes Q \xrightarrow{\pi} Q \longrightarrow e,$$

wobei i die Einbettung von N nach Q ist und $\pi(g) = \pi(nq) := q$ für die nach Voraussetzungen in Definition 2.6 eindeutigen $n \in N$ und $q \in Q$ zu jedem $g \in G$ gewählt wird.

Zum Abschluss wollen wir nun noch zwei wichtige Beispiele von (äußeren) semidirekten Produkten geben. Wir beginnen mit der Lamplighter-Gruppe.

Beispiel 2.7 (Lamplighter-Gruppe)**.** Es sei G eine beliebige Gruppe. Dann ist die *Lamplighter-Gruppe über G* das semidirekte Produkt $(\prod_\mathbb{Z} G) \rtimes_\varphi \mathbb{Z}$, wobei

$$\varphi\colon \mathbb{Z} \to \operatorname{Aut}\Big(\prod_\mathbb{Z} G\Big), z \mapsto \big((g_n)_{n\in\mathbb{Z}} \mapsto (g_{n+z})_{n\in\mathbb{Z}}\big). \tag{4}$$

Oder allgemeiner:

Beispiel 2.8 (Kranzprodukt)**.** Das *Kranzprodukt* von zwei Gruppen G und H ist das semidirekte Produkt $(\prod_H G) \rtimes_\varphi H$, wobei φ analog zu (4) eine entsprechende „Verschiebung“ ist:

$$\varphi\colon H \to \mathrm{Aut}\Big(\prod_H G\Big), h \mapsto \big((g_k)_{k\in H} \mapsto (g_{kh})_{k\in H}\big).$$

Man schreibt dann auch $G \wr H$ für das Kranzprodukt.

Literatur

[1] Oleg Bogopolski. *Introduction to group theory*. European Mathematical Society Publishing House, 2008.

[2] Clara Löh. *Geometric group theory*. Springer, 2017.