Bahnen, Stabilisatoren und Fundamentallemma (für endliche Gruppen)

Wenn wir eine Gruppenoperation $\diamond : G \times M \to M$ einer Gruppe $(G, *)$ auf einer Menge M gegeben haben, können wir versuchen, die Elemente der Menge M besser zu beschreiben. Wir zerlegen die Menge M in sogenannte „Bahnen“ von G.

Definition 1. Sei eine Gruppenoperation $\diamond : G \times M \to M$ einer Gruppe $(G, *)$ auf einer Menge M gegeben und $m \in M$ fest.

Dann nennen wir $G \diamond m := \{g \diamond m \mid g \in G\} \subseteq M$ die *Bahn von m unter G*. (Das sind also alle Elemente in M, die wir aus dem vorgegebenen m mit Hilfe der Gruppe G „erzeugen“ können.)

Weiterhin definieren wir $G_m := \{g \in G \mid g \diamond m = m\} \subseteq G$, den *Stabilisator von m (bzgl. $\diamond : G \times M \to M$)*. (Das sind also alle Elemente aus G, die ein gegebenes $m \in M$ festlassen.)

Lemma 1. *Der Stabilisator G_m ist eine Untergruppe von G.*

Beweis. Gruppenaxiome durchrechnen (siehe Vorlesung). $\square$

Definition 2. Ist M eine endliche Menge, so bezeichnen wir mit $|M|$ die Anzahl der Elemente von M. (Ist G eine Gruppe, so nennen wir die Anzahl $|G|$ auch *Ordnung von G*.)

Satz 1 (Fundamentallemma)**.** *Sei G eine endliche Gruppe und $\diamond : G \times M \to M$ eine Gruppenoperation von G auf einer Menge M und $m \in M$. Dann gilt:*

$$|G| = |G \diamond m| \cdot |G_m|.$$

Mit anderen Worten: Die Gruppenordnung lässt sich berechnen als „Bahnenlänge“ (= Anzahl der Elemente in der Bahn) mal der Stabilisatorordnung.

Bevor wir das Fundamentallemma beweisen, zunächst noch ein paar Eigenschaften von Stabilisatoren und Bahnen:

Satz 2. *Sei $\diamond : G \times M \to M$ eine Gruppenoperation einer Gruppe $(G, *)$ auf einer Menge M.*

- *Ist $g \in G$ und $m \in M$, so gilt:*

$$G_{g \diamond m} = \{g * h * g^{-1} \mid h \in G_m\}.$$

- *Sind $m, m' \in M$, so gilt entweder $G \diamond m = G \diamond m'$ oder $G \diamond m \cap G \diamond m' = \emptyset$.*

Beweis. Mengengleichheit zeigen (siehe Vorlesung). $\square$

Nun zum Beweis des Fundamentallemmas:

Beweis von Satz 1 (Fundamentallemma). Wir betrachten die Abbildung $F : G \to G \diamond m$, $g \mapsto g \diamond m$. Natürlich ist F nach Definition surjektiv. (Ist $x \in G \diamond m$, also $x = \tilde{g} \diamond m$, so wird x von $\tilde{g} \in G$ getroffen, denn $F(\tilde{g}) = \tilde{g} \diamond m$ (nach Definition).)

Wir schauen uns die Urbilder $F^{-1}(x) := \{g \in G \mid F(x) = g \diamond m = x\}$ für $x \in G \diamond m$ an. Insbesondere ist nach Definition das Urbild $F^{-1}(m) := \{g \in G \mid F(m) = g \diamond m = m\} = G_m$, der Stabilisator von $m \in M$, und hat also $|G_m|$ Elemente.[1]

Es gilt:

$$G = \dot{\bigcup}_{m' \in G \diamond m} F^{-1}(m'),$$

denn $F : G \to G \diamond m$ ist surjektiv, also sind alle Urbilder nicht leer und zusammen genommen gleich G. (Weiterhin sind die Urbilder bei jeder Abbildung disjunkt, denn ein Element kann ja nicht auf zwei verschiedene Elemente abgebildet werden.)

Damit folgt:

$$|G| = \sum_{m' \in G \diamond m} |F^{-1}(m')|.$$

Wir zeigen, dass die Anzahl der Elemente in dem Urbild $F^{-1}(m')$ unabhängig von dem gewählten $m' \in G \diamond m$ ist, dass also auch $|F^{-1}(m')| = |G_m|$ ist. (Dann folgt sofort: $|G| = |G \diamond m| \cdot |G_m|$.)

Sei nun $m' = g \diamond m \in G \diamond m$ fest vorgegeben. Dann ist $f : G_m \to F^{-1}(m')$, $h \mapsto g * h$ eine *Bijektion*. (Damit ist dann die Anzahl der Elemente *jedes* Urbilds $F^{-1}(m')$ gleich $|G_m|$.)

Als erstes müssen wir zeigen, dass $g * h$ überhaupt in $F^{-1}(m')$ liegt, damit wir eine *Abbildung* bekommen.[2]

Sei also $h \in G_m$. Dann gilt:

$$F(g * h) = (g * h) \diamond m = g \diamond (h \diamond m) = g \diamond m = m',$$

also $g * h \in F^{-1}(m')$.

Die Abbildung f ist *injektiv*, denn seien $h, h' \in G$ mit $f(h) = g * h = g * h' = f(h')$, so gilt schon $h = (g^{-1} * g) \diamond h = g^{-1} \diamond (g \diamond h) = g^{-1} \diamond (g \diamond h') = (g^{-1} * g) \diamond h' = h'$.

Außerdem ist f *surjektiv*. Sei $g' \in F^{-1}(m')$. Dann gilt: $g' \diamond m = m' = g \diamond m$, also $(g^{-1} * g') \diamond m = g^{-1} \diamond (g' \diamond m) = g^{-1} \diamond (g \diamond m) = (g^{-1} * g) \diamond m = e \diamond m = m$. Damit ist $h := g^{-1} \diamond g' \in G_m$, und wir haben $g' = g * h$, also ein $h \in G_m$ mit $f(h) = g * h = g'$.

Es gilt also insbesondere:

$$|F^{-1}(m')| = |G_m| \text{ für } \textit{alle } m' \in G \diamond m.$$

Also gilt:

$$|G| = \sum_{m' \in G \diamond m} |F^{-1}(m')| = |G \diamond m| \cdot |G_m|.$$

□

[1] **Achtung!** Im Allgemeinen ist $F^{-1}(x)$ *nicht* der Stabilisator von x, denn hierfür müsste die Bedingung ja $g \diamond x = x$ und nicht $g \diamond m = x$ lauten. Wir werden jedoch zeigen, dass die Anzahl der Elemente in $F^{-1}(x)$ unabhängig von $x \in G \diamond m$ ist.

[2] Die rechte Seite $F^{-1}(m')$ ist nach Konstruktion von F nicht leer, da F surjektiv ist.