Definition 1. Sei G eine Menge und $\cdot : G \times G \to G, (g_1, g_2) \mapsto g_1 \cdot g_2 = g_1 g_2$ eine Abbildung (genannt Verknüpfung). Dann heißt $(G, \cdot)$ eine **Gruppe**, wenn gilt:

1. $(g_1 g_2)g_3 = g_1(g_2 g_3) \quad \forall g_1, g_2, g_3 \in G$
2. Es existiert $1 \in G$ mit $1g = g1 = g \quad \forall g \in G$
3. Zu jedem $g \in G$ existiert $g^{-1} \in G$ mit $gg^{-1} = g^{-1}g = 1$

Definition 2. Eine Gruppe G heißt **endlich**, falls die zugrundeliegende Menge G endlich ist.
$|G| :=$ **Ordnung** von $G :=$ Anzahl der Elemente
Falls G nicht endlich ist, schreibt man $|G| := \infty$

Definition 3. G Gruppe, $U \subseteq G$. U heißt **Untergruppe** von G, falls gilt:

1. $U \neq \emptyset$
2. $g, h \in U \Rightarrow gh^{-1} \in U$

Wir schreiben: $U \leq G$

Bemerkung 1. Eine Untergruppe ist wieder eine Gruppe bzgl. der Einschränkung der Verknüpfung.

Definition 4. G Gruppe, M Menge. Eine Abbildung $G \times M \to M : (g, m) \mapsto gm$ mit

1. neutrales Element: $1m = m \quad \forall m \in M$
2. „Assoziativität“: $(g_1 g_2)m = g_1(g_2 m) \quad \forall m \in M, g_1, g_2 \in G$

heißt (Links-)**Operation** von G auf M.
Man nennt die Menge M ausgestattet mit der Operation der Gruppe G auch $G-$Menge.

Definition 5. G operiere auf M, $m \in M$. $Gm := \{gm \mid g \in G\}$ heißt die **Bahn** von m unter G.
Bemerkung: Gm ist endlich, wenn G oder M endlich ist.

Definition 6. Sei $M \subseteq G$, G Gruppe.

1. $$\langle M \rangle := \bigcap_{U \leq G, M \subseteq U} U$$
   heißt das **Erzeugnis** von M. $\langle M \rangle$ ist die kleinste Untergruppe, die M enthält.
   Falls $M = \{g_1, \cdots, g_n\}$, schreibt man auch: $\langle M \rangle := \langle g_1, \cdots, g_n \rangle$
2. Falls $G = \langle M \rangle$, so heißt M ein **Erzeugendensystem** von G.
3. Eine Gruppe, die von einem Element erzeugt wird, heißt **zyklisch**.

Alternative Definition:
Sei $M \subseteq G$, G Gruppe.

1. $\langle M \rangle := \{m_1 \cdots m_n \mid m_i \in M \text{ oder } m_i^{-1} \in M, n \in \mathbb{N}_0\}$
2. das leere Produkt ist als 1 definiert
3. algorithmisch besser nutzbar

Algorithm 1 einfacher Bahnenalgorithmus

Eingabe: $E = \{g_1, \ldots, g_n\}$ Gruppe $G = \langle E \rangle$, Operation von G auf M, $m \in M$.
Ausgabe: Die Bahn Gm

```
Bahn := {m}
for each e ∈ Bahn do
  for each g ∈ E do
    newElement := g · e
    if newElement ∉ Bahn then
      Bahn := Bahn ∪ {newElement}
    end if
  end for
end for
```

Bemerkung 2. Falls $|\ G\ | = \infty$, so füge zu E noch die inversen Elemente der Erzeuger hinzu: $E = \{g_1, \dots\ g_n, g_1^{-1} \dots g_n^{-1}\}$

Bemerkung 3.
- $U \leq G$ operiert auf G durch inverse Rechtsmultiplikation: $U \times G \to G : (u, g) \mapsto gu^{-1}$.
- Die Bahn $gU := \{gu \mid u \in U\}$ von $g \in G$ unter der Operation heißt **Restklasse** von g nach U.
- Menge der Restklassen von G nach U bezeichnet man als G/U
- ein Restklassenvertretersystem bezeichnet man als **Transversale**.

Definition 7. G operiere auf M, $m \in M$. $\text{Stab}_G(m) := \{g \in G \mid gm = m\}$ heißt **Stabilisator** von m in G.

Bemerkung 4. $\text{Stab}_G(m) \leq G$.

Satz 1. $|\ Gm\ | \cdot |\ Stab_G(m)\ | = |\ G\ |$

Beweis. $m = m_0,\ Gm = \{m_0, ..., m_{b-1}\}$

1. $G = G_0 \dot\cup ... \dot\cup G_{b-1},\ G_i := \{g \in G \mid gm_0 = m_i\}$
   $\supseteq$: $g \in G_i \Rightarrow g \in G \Rightarrow \cup_{i=0}^{b-1} G_i \subseteq G$
   $\subseteq$: $g \in G \Rightarrow gm_0 \in Gm$, dh $\exists!\ m_i : gm_0 = m_i \Rightarrow g \in G_i$ für ein $i \Rightarrow G \subseteq \cup_{i=0}^{b-1} G_i$
   Disjunktheit klar
2. $G_0 = Stab_G(m_0)$ (klar)
3. Bijektion zwischen G_0 und G_i:
   $g_i \in G_i$ bel., dann $\varphi_i : G_0 \to G_i,\ g \mapsto g_i g$ ist Bijektion.
   Dazu: wohldef.: $\varphi_i(g)m = g_i \underbrace{gm}_{=m,\ \text{da}\ g \in G_0} = g_i m = m_i \Rightarrow \varphi_i(g) \in G_i$
   Umkehrabb.: $\varphi_i^{-1} : G_i \to G_0,\ h \mapsto g_i^{-1} h$
   $\varphi_i^{-1}(\varphi_i(g)) = \varphi_i^{-1}(g_i g) = g_i^{-1}(g_i g) = g$
   $\varphi_i(\varphi_i^{-1}(h)) = \varphi_i(g_i^{-1} h) = g_i(g_i^{-1} h) = h$
   $\Rightarrow |G_0| = |G_1| = ... = |G_{b-1}| \Rightarrow |G| = \sum_{i=0}^{b-1} |G_i| = |Gm||Stab_G(m)|$

Algorithm 2 verfeinerter Bahnenalgorithmus

Eingabe: $E = \{g_1, \dots, g_n\}$ Gruppe $G = \langle E \rangle$, Operation von G auf M, $m \in M$.
Ausgabe: 1. Die Bahn Gm, 2. Erzeugendensystem E_S von $Stab_G(m)$, 3. Eine Abbildung $\omega : Gm \to G$ mit $\omega(e)m = e$

```
Bahn := {m}
ω(m) = id
E_S = ∅
for each e ∈ Bahn do
  for each g ∈ E do
    newElement := g · e
    if newElement ∉ Bahn then
      Bahn := Bahn ∪ {newElement}
      ω(newElement) := g · ω(e)
    else
      E_S := E_S ∪ {ω(ge)^{-1} · g · (ω(e))}
    end if
  end for
end for
```

Beweis. Zu zeigen: $\langle E_S \rangle = Stab_G(m) =: S$.
Man führt einen Inklusionsbeweis.

- „$\subseteq$“

  Sei $s \in E_s$
  $sm = \omega(gx)^{-1} g\omega(x)m = w(gx)^{-1}gx = m$

- „$\supseteq$“

  Sei $g \in S$, $g = h_k \cdots h_1$ mit $h_i \in E, i = 1, \ldots, k$

  Induktion nach k:

  IA: $k = 0 \Rightarrow g = 1 \Rightarrow g \in \langle E_S \rangle$.
  IV: Es sei $g = h_i \cdots h_1 \in \langle E_S \rangle$ für alle $i < k$

  IS: $k \to k+1$
  Da $g \in Stab_G(m)$ ist, gilt $gm = h_k \cdots h_1 m = m$.
  Sei nun $h_i \cdots h_1$ das größte Endteilwort von $h_k \cdots h_1$ mit $\omega(h_i \cdots h_1 m) = h_i \cdots h_1$. Dies entspricht dem längsten Teilpfad von $h_1 \cdots h_k$ beginnend an der Wurzel m im Schreierbaum.
  Dann gilt $i < k$ (da $\omega(h_k \cdots h_1 m) = \omega(m) = 1$ die Bedingung nicht erfüllt).

  Wir setzen $v := \omega(h_{i+1} \cdots h_1 m) = h'_j \cdots h'_1$ mit $j \leq i+1 \leq k$, $h'_i \in E, i = 1, \ldots, j$.
  Da der nächstlängere Pfad nicht im Baum enthalten ist, wurde mit ihm ein Stabilisatorelement gefunden und es gilt:
  $w_2 = v^{-1} h_{i+1} \cdots h_1 = \omega(h_{i+1} \cdots h_1 m)^{-1} h_{i+1} \omega(h_i \cdots h_1 m) \in E_S$.
  Da in $g = h_k \cdots h_1 = h_k \cdots h_{i+2} v v^{-1} h_{i+1} \cdots h_1$ der hintere Teil w_2 in E_S enthalten ist, folgt aus $w_1 := h_k \cdots h_{i+2} v \in \langle E_S \rangle$ (zu zeigen) auch $g \in \langle E_S \rangle$.
  Wegen $gm = m$ und $w_2 m = m$ muss natürlich auch $w_1 m = m$ gelten. Um zu zeigen, dass $w_2 \in \langle E_S \rangle$ gilt muss man zwei Fälle unterscheiden.

  1. Fall $j < i + 1 \leq k$
     $w_2 = h_k \cdots h_{i+2} v$ hat eine Länge $< k$, also greift die IV und es gilt $h_k \cdots h_{i+2} v \in \langle E_S \rangle$.

  2. Fall $j = i + 1 \leq k$
     Im Fall $j < k$ greift die IV analog zu Fall 1. Im Fall $j = k$ ist die Länge von w_2 erneut k, jedoch hat w_2 ein echt längeres Endteilwort mit $\omega(h'_{i+1} \cdots h'_1 m) = h'_{i+1} \cdots h'_1$. Da das Endteilwort echt länger ist, muss man die Argumentation maximal $k - i$ mal wiederholen bis die Induktionsvorraussetzung greift.

  Aus beiden Fällen zusammen folgt $g = h_k \cdots h_1 \in \langle E_S \rangle$ und die Behauptung gilt für $k+1$. Nach dem Prinzip der vollständigen Induktion gilt $g = h_k \cdots h_1 \in \langle E_S \rangle$ für alle $k \in \mathbb{N}_0$.