

1.3.11 Def

Sei $n \in \mathbb{N} (= \mathbb{N} \setminus \{0\})$. Die Eulersche φ -Funktion ist

$$\begin{aligned}\varphi(n) &= \# \{ \tilde{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{ggT}(\tilde{a}, n) = 1 \} \\ &= \# \{ a \in \mathbb{Z} \mid 0 \leq a < n, \text{ggT}(a, n) = 1 \}.\end{aligned}$$

Schreibweise: $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \cong \{0, 1, \dots, n-1\}$, $a+b \bmod n$

Sei $\mathbb{Z}_n^* = \{ \tilde{a} \in \mathbb{Z}_n \mid \exists \tilde{b} \in \mathbb{Z}_n : \tilde{b} \tilde{a} = \tilde{1} \}$

die Menge der bzgl. Multiplikation invertierbaren Elemente (Einheiten).
Bem. $(\mathbb{Z}_n^*, \cdot)$ ist Gruppe.

1.3.12 Lemma

$$\mathbb{Z}_n^* = \{ \tilde{a} \in \mathbb{Z}_n \mid \text{ggT}(\tilde{a}, n) = 1 \}$$

und somit $\text{ord } \mathbb{Z}_n^* = \varphi(n)$, ($\leq n-1$)

Bew.

$$\tilde{a} \in \mathbb{Z}_n \text{ invertierbar bzgl. Mult.} \Leftrightarrow \exists \tilde{b} \in \mathbb{Z}_n : \tilde{b} \cdot \tilde{a} = \tilde{1}$$

$$\Leftrightarrow \exists b \in \mathbb{Z} : b \cdot a \equiv 1 \bmod n \Leftrightarrow \exists b, d \in \mathbb{Z} : b \cdot a + d \cdot n = 1$$

$$\Leftrightarrow \text{ggT}(a, n) = 1$$

□

1.3.13 Eulerscher Satz

Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$.

Dann gilt

$$a^{\varphi(n)} \equiv 1 \bmod n$$

Bew.

$$\text{ggT}(a, n) = 1 \Rightarrow \tilde{a} \in \mathbb{Z}_n^* \xrightarrow[\text{Bem. Fermat 1.3.5}]{\text{Lagrange 1.2.6}} \text{ord } \mathbb{Z}_n^* = \varphi(n) \Rightarrow \tilde{a}^{\varphi(n)} = \tilde{1}$$

□

1.3.14 Kleiner Fermatischer Satz II

Sei $p \in \mathbb{N}$ prim und $a \in \mathbb{N}$ mit $p \nmid a$.

Dann gilt $a^{p-1} \equiv 1 \bmod p$ (und $a^p \equiv a \bmod p$).

Bew.

p prim $\Rightarrow \varphi(p) = p-1$, denn $\text{ggT}(q, p) = 1$ für $0 < q < p$.

Zudem p prim und $p \nmid a \Rightarrow \text{ggT}(a, p) = 1$.

Zusammen $a^{p-1} = a^{\varphi(p)} \equiv 1 \bmod p$.

$$\left\{ \begin{array}{l} p \text{ prim} \Rightarrow \exists d \mid p \Rightarrow d=1 \text{ oder } d=p \\ \downarrow \\ \text{ggT}(a, p) \in \{1, p\} \\ \text{Wenn } p \nmid a, \text{ dann} \\ \text{ggT}(a, p) = 1 \end{array} \right.$$

§ 1.4 Operationen von Gruppen auf Mengen

(2)

1.4.1 Def

Sei G eine Gruppe und X eine Menge. Eine Operation oder Aktion oder Wirkung von G auf X ist eine Abbildung

$$\tau : G \times X \rightarrow X, (a, x) \mapsto \tau_a(x),$$

mit

$$\tau_{ab}(x) = \tau_a(\tau_b(x))$$

und

$$\tau_e(x) = x \quad \text{für alle } a, b \in G \text{ und } x \in X.$$

Man schreibt auch

$$\tau_g(x) = g \cdot x \quad (\text{besitzt, wenn } X = G \text{ oder } G \subseteq X.)$$

1.4.2 Lemma

Für jedes $a \in G$ ist $\tau_a : X \rightarrow X$ bijektiv.

Bew.

$$\tau_{a^{-1}}(\tau_a(x)) = \tau_{e}(x) = x = \tau_a(\tau_{a^{-1}}(x)) \Rightarrow (\tau_a)^{-1} = \tau_{a^{-1}} \text{ ist links- und rechtsinverses.}$$

Es folgt: $G \rightarrow S(X), g \mapsto \tau_g$, ist ein Homomorphismus

und umgekehrt: Ist $\tau : G \rightarrow S(X), g \mapsto \tau_g$, ein Homomorphismus,

dann ist $G \times X \rightarrow X, (g, x) \mapsto \tau_g(x)$, eine Operation.

τ operiert transitiv, wenn es zu $x, y \in X$ ein $g \in G$ gibt mit

$$\tau_g(x) = y.$$

1.4.3 Def

Operiert G auf X , so heißt

(i) $Gx = \{g \cdot x \in X \mid g \in G\}$ Bahn oder Orbit von x ,

(ii) $G_x = \{g \in G \mid g \cdot x = x\}$ Isotropiegruppe oder Stabilisator oder Standgruppe von x .

Bem. (i) Die Bahnen sind disjunkt oder gleich, $Gx \cap Gy \neq \emptyset \Rightarrow Gx = Gy$.

Die Bahnen liefern eine disjunkte Zerlegung von X . Durch $x \sim_a y \Leftrightarrow y \in Gx$ ist eine Äquivalenzrelation auf X erklärt.

$X / \sim_a (= X / G)$ heißt Bahnenraum, $x \in Gx$ heißt auch Vertreter.

G transitiv $\Leftrightarrow Gx = X$

| Vertreter: je ein Vertreter für jede Bahn

(ii) G_x ist Untergruppe von G : $1 \in G_x$; sind $a, b \in G_x$,

d.h. $ax = x = bx \Rightarrow ab^{-1}x = a(b^{-1}bx) = ax = x$, also $ab^{-1} \in G_x$.

Beispiele Die Gruppe G operiert auf sich, $G \times G \rightarrow G$, durch

(i) $(g, h) \mapsto gh$ (Linkstranslation)

(ii) $(g, h) \mapsto \text{int}_g(h) = ghg^{-1}$ (Konjugation / ^{1.1.10 (iv)}innere Automorphismen)

(iii) $H \leq G$ Untergruppe, $H \times G \rightarrow G$, $(h, g) \mapsto hg$
 $g \in G$: Bahnen Hg sind Rechtsnebenklassen, $G/H = H \backslash G$ (Vorsicht! $X_n = \frac{X}{n}$)

(iv) $SO(2) \times D^2$, $SO(3) \times S^2$ (transitiv), $SO(2) \times S^2$ (Drehung um Achse $\times S^2$)

14.4. Lemma (Bahn-Lemma)

G operiert auf X . Für $x \in X$ induziert die Abbildung

$G \rightarrow X, g \mapsto gx$, eine Bijektion $G/G_x \xrightarrow{\sim} Gx$

von der Menge der Linksnebenklassen von G modulo G_x auf die Bahn Gx von x . Insbesondere

$$\begin{aligned} \text{ord } Gx &= \text{ord } G/G_x = (G : G_x) \\ (\text{mit } \text{ord } G &= \text{ord}(Gx) \cdot \text{ord}(G_x)). \end{aligned}$$

Bew.

$\varphi: G \rightarrow Gx, g \mapsto gx$, ist surjektiv.

Weiter gilt für $H = G_x$: $\varphi(a) = \varphi(b) \Leftrightarrow$

$\Leftrightarrow ax = bx \Leftrightarrow b^{-1}ax = x \Leftrightarrow b^{-1}a \in G_x = H \Leftrightarrow aH = bH$

d.h.

$G/H \rightarrow Gx$ ist wohldefiniert ($\Leftarrow$) und injektiv ($\Rightarrow$).

Bch. folgt mit 1.2.4 (Lagrange)

□

Bsp. $G = SO(3)$ operiert transitiv auf S^2 .

Wähle $x \in S^2$. $G_x = \{g \in SO(3) \mid gx = x\} \cong SO(2)$

sind Drehungen um die Achse, die von x aufgespannt wird; x ist Eigenvektor mit Eigenwert 1.

$SO(n)$ sind Liegruppen und

$\frac{SO(3)}{SO(2)}$ ist diffeomorph zu $Gx = S^2$ (transitiv).

Aus dem Bahn-Lemma (1.4.4) folgt

1.4.5 Bahnengleichung

G operiere auf einer endlichen Menge X .

$x_1, \dots, x_n$ sei ein Vertretersystem der Bahnen von X .

Dann gilt

$$\text{ord } X = \sum_{j=1}^n \text{ord } Gx_j = \sum_{j=1}^n (G : G_{x_j}).$$

Bem. Vertretersystem bedeutet, daß $Gx_j \cap Gx_k = \emptyset$, $j \neq k$.

Weiter gilt $X = \bigcup_{j=1}^n Gx_j$.

1.4.6 Def Sei G eine Gruppe und $S \subset G$ eine Teilmenge.

Dann heißt

$$Z_S = \{x \in G \mid xs = sx \ \forall s \in S\} \quad \text{Zentralisator von } S \text{ in } G$$

und

$$Z = Z_G = \{x \in G \mid xs = sx \ \forall s \in G\} \quad \text{Zentrum von } G.$$

Es gilt (i) $Z < Z_S < G$ sind Untergruppen.

(ii) Z ist abelsch und $Z \trianglelefteq G$ // Normalteiler von G .

(iii) G/Z ist isomorph zur Gruppe der inneren Automorphismen, denn Z ist der Kern von $G \rightarrow \text{Aut}(G)$, $g \mapsto \text{int}_g$.

Betrachte die Operation einer Gruppe G auf sich unter Konjugation,

$$G \times G \rightarrow G, \quad (g, x) \mapsto gxg^{-1}.$$

Dann ist

$$G_x = Z_{G \setminus \{x\}}$$

und $x \in Z \Leftrightarrow Gx = \{x\}$ (Im Zentrum liegen genau die ein-elementigen Bahnen)
 $\Rightarrow \text{ord } Gx = (G : Z_{G \setminus \{x\}}) = 1$.

Ist $x \notin Z$, dann $G_x = Z_{G \setminus \{x\}} \neq G \Rightarrow \text{ord } Gx = (G : Z_{G \setminus \{x\}}) > 1$.

Aus der Bahnengleichung wird dann:

1.4.7 Klassengleichung: Sei G endliche Gruppe mit Konjugation als Operation auf sich.

$Z \neq x_1, \dots, x_k$ Vertretersystem der mehr-elementigen Bahnen ($Z = \{x_{k+1}, \dots, x_n\}$).

Dann gilt
$$\text{ord } G = \text{ord } Z + \sum_{j=1}^k (G : Z_{G \setminus \{x_j\}}).$$