# I. Zyklische Gruppen

**Wdh.:**

Sei $G$ eine Gruppe. $G$ heißt zyklisch, wenn gilt:

$$\exists\, g \in G \text{ mit } \langle g \rangle = \{ g, g^2, \dots \} = G.$$

Man nennt $g$ erzeugendes Element von $G$.

Für eine Gruppe $G$ und $g \in G$ ist

$$\operatorname{ord}(G) := |G|$$

und $\operatorname{ord}(g) := \operatorname{ord}(\langle g \rangle)$.

Bsp.: Sei $G := (\mathbb{Z}/5\mathbb{Z})^*$,

Dann ist $\operatorname{ord}(G) = 4$,
$\operatorname{ord}(1) = 1$, $\operatorname{ord}(4) = 2$, $\operatorname{ord}(2) = 4$.
Also ist $G$ zyklisch.

**I.1 Def.:** Sei $(G, \cdot)$ eine abelsche Gruppe, $H \leq G$.
$\pi: G \longrightarrow G/H$, $g \longmapsto gH$,
wobei $gH := \{ x \in G \mid x = g \cdot h, h \in H \}$,
heißt Quotienten-Abbildung.

Dann ist $G/H$ mit der Verknüpfung
$(xH) \cdot (yH) := xyH = yxH$
wiederum eine abelsche Gruppe.

# I. Zyklische Gruppen

**Wdh.:**

Sei $G$ eine Gruppe. $G$ heißt zyklisch, wenn gilt:

$$\exists\, g \in G \text{ mit } \langle g \rangle = \{ g, g^2, \dots \} = G.$$

Man nennt $g$ erzeugendes Element von $G$.

Für eine Gruppe $G$ und $g \in G$ ist

$$\operatorname{ord}(G) := |G|$$

und $\operatorname{ord}(g) := \operatorname{ord}(\langle g \rangle)$.

Bsp.: Sei $G := (\mathbb{Z}/5\mathbb{Z})^*$,

Dann ist $\operatorname{ord}(G) = 4$,
$\operatorname{ord}(1) = 1$, $\operatorname{ord}(4) = 2$, $\operatorname{ord}(2) = 4$.
Also ist $G$ zyklisch.

**I.1 Def.:** Sei $(G, \cdot)$ eine abelsche Gruppe, $H \leq G$.
$\pi: G \longrightarrow G/H$, $g \longmapsto gH$,

wobei $gH := \{ x \in G \mid x = g \cdot h, h \in H \}$,

heißt Quotienten-Abbildung.

Dann ist $G/H$ mit der Verknüpfung
$(xH) \cdot (yH) := xyH = yxH$
wiederum eine abelsche Gruppe.

## I.2 Satz:

Sei $(G, \cdot)$ eine abelsche Gruppe, $H \leq G$. Dann ist $ord(H) \mid ord(G)$.

## I.3 Corollar:

Sei $(G, \cdot)$ eine Gruppe, $g \in G$. Dann ist $g^{ord(G)} = e$.

**Ziel:**

Sei $K$ Körper, $(G, \cdot) \leq K^*$ endlich. Dann ist $G$ zyklisch.

## I. 4 Satz:

Seien $(G_i, \cdot)$ zykl. Gruppen mit Ordnung $m_i$ für $i \in \underline{r}$.

Weiterhin seien alle $m_i$ paarweise teilerfremd. Dann ist

$G_1 \times \ldots \times G_r$, mit komponentenweiser Multiplikation, eine zyklische Gruppe von Ordnung

$$m = m_1 \cdot \ldots \cdot m_r.$$

## I.5 Satz:

Sei $G$ endl. abelsche Gruppe mit $\text{ord}(G) = m$.

Für $i \in I$ seien $G_i \leq G$, $\text{ord}(G_i) =: m_i$
und alle $m_i$ paarw. teilerfremd und $m = m_1 \cdot \ldots \cdot m_r$.

Dann ist $G_1 \times \ldots \times G_r \cong G$ mit Isomorphismus
$\varphi : (x_1, \ldots, x_r) \longmapsto x_1 \cdot \ldots \cdot x_r$.

## I.6 Satz:

Sei $(G, \cdot)$ endl. abelsche Gruppe,
$p \in \mathbb{N}$ prim mit $p \mid \text{ord}(G)$.

Dann $\exists x \in G$ mit $\text{ord}(x) = \text{ord}(\langle x \rangle) = p$.

## I.7 Satz:

Sei $(G, \cdot)$ endl. abelsche Gruppe,
$p^k$ eine Primzahlpotenz mit $p^k \mid \text{ord}(G)$.

Dann hat $G$ eine Untergruppe der Ordnung $p^k$.

## I.8 Satz:

Sei $K$ ein Körper, $(G, \cdot) \leq K^*$ endlich.

Dann ist $G$ zyklisch.

# II. Quadratische Erweiterungen.

## II.1 Definition:

Sei $R$ ein kommutativer Ring, $D \in R$.

Dann ist $Q(R,D) := \left\{ \begin{pmatrix} x & Dy \\ y & x \end{pmatrix} \in R^{2\times 2} \mid x, y \in R \right\}$

ein kommutativer Ring.

Denn $\begin{pmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 & Dy_2 \\ y_2 & x_2 \end{pmatrix} = \begin{pmatrix} x_1x_2 + Dy_1y_2 & D(x_1y_2 + x_2y_1) \\ x_1y_2 + x_2y_1 & x_1x_2 + Dy_1y_2 \end{pmatrix}$

Ferner seien $E := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $W := \begin{pmatrix} 0 & D \\ 1 & 0 \end{pmatrix}$

$\varepsilon : R \to Q(R,D)$, $x \mapsto x \cdot E$ ist

eine Einbettung von $R$ in $Q(R,D)$.

Wir schreiben für $\xi \in Q(R,D)$

$$\xi = xE + yW = x + yW.$$

Dann ist $W^2 = D \cdot E = D$

Hat $D$ keine Quadratwurzel in $R$, so schreibt man auch $Q(R,D) = R[\sqrt{D}]$.

Auf $Q(R,D)$ definieren wir

Konjugation:

$$\overline{(-)} : Q(R,D) \to Q(R,D),\ \xi \mapsto \bar{\xi} = x - yW$$

Spur:

$$Tr : Q(R,D) \to R,\ \xi \mapsto \xi + \bar{\xi} = 2x$$

Norm:

$$N : Q(R,D) \to R,\ \xi \mapsto \xi \cdot \bar{\xi} = x^2 - Dy^2 = \det(\xi)$$

$$N(Q(R,D)^*) \subseteq R^*.$$

## II.2 Satz:

Sei $R$ kommut. Ring, $D \in R$ so dass es ein $a \in R$ gibt mit $a^2 = D$.
Außerdem seien 2, $a$ invertierbar in $R$.
Dann ist $\phi : Q(R, D) \to R \times R$, $x + y\sqrt{D} \mapsto (x + ay, x - ay)$
ein Ring-Isomorphismus.

## II.3 Satz:

Sei $K$ ein Körper, $D \in K$ mit
$a^2 \neq D \quad \forall a \in K$.
Dann ist $K[\sqrt{D}]$ ein Körper

**Bemerkung:**
Sei $p > 2$ prim, $D_1, D_2 \in \mathbb{F}_p^*$ ohne Quadratwurzeln
$D$ aus kann man zeigen, dass $\mathbb{F}_p[\sqrt{D}] \cong \mathbb{F}_p[\sqrt{D_1}]$.
Dann bezeichnen wir $\mathbb{F}_{p^2} = \mathbb{F}_p[\sqrt{D}]$ unabhängig von $D$.

## II.4 Definition:

Sei $p > 2$ prim. Dann ist
$\varphi_p : \mathbb{F}_{p^2} \to \mathbb{F}_{p^2}$, $\xi \mapsto \xi^p$ ein Körper-Autom.
genannt Frobenius-Automorphismus.

## II.5 Satz:

Sei $p > 2$ prim. Dann gilt
$$\varphi_p(\xi) = \overline{\xi} \quad \forall \xi \in \mathbb{F}_{p^2}.$$
Insbesondere ist also $N(\xi) = \xi^{p+1} \quad \forall \xi \in \mathbb{F}_{p^2}$.

## II. 6 Satz:

Sei $p > 2$ prim. Dann ist

$$N : \mathbb{F}_{p^2}^* \longrightarrow \mathbb{F}_p^* \quad \text{surjektiv}$$

und $\text{Kern}(N) = \{ \xi \in \mathbb{F}_{p^2}^* : N(\xi) = 1 \}$
ist zyklische Gruppe von Ordnung $p+1$.

## II. 7 Satz:

Sei $p > 2$ prim, $n \geq 2$ und $a \in \mathbb{Z}$ so dass es ein $x_0 \in \mathbb{Z}$ gibt mit $x_0^2 \equiv a \bmod p$.

Dann existiert ein $x \in \mathbb{Z}$ mit

$$x^2 \equiv a \bmod p^n$$

und $x \equiv x_0 \bmod p$.

## Bemerkung:
(Legendre-Symbol)

Hat $a$ eine (bzw. keine) Quadratwurzel in $\mathbb{Z}/p\mathbb{Z}$, wobei $a, p$ teilerfremd sein müssen,

schreibt man $\left(\frac{a}{p}\right) = 1$ (bzw. $\left(\frac{a}{p}\right) = -1$).

Das Legendre-Symbol ist - bei festem $p$ - multiplikativ.

II.2.

$\phi$ ist Bijektion mit Inverser

$$\phi^{-1}: (u,v) \longmapsto \frac{u+v}{2} + \frac{u-v}{2a} W.$$

$\phi$ ist Homomorphismus, denn

$x + ay$ und $x - ay$ sind die Eigenwerte von $\begin{pmatrix} x & ya^2 \\ y & x \end{pmatrix}$ zu den Eigenvektoren $\begin{pmatrix} a \\ 1 \end{pmatrix}$ und $\begin{pmatrix} -a \\ 1 \end{pmatrix}$.

$$\begin{pmatrix} x & ya^2 \\ y & x \end{pmatrix} \begin{pmatrix} a \\ 1 \end{pmatrix} = \begin{pmatrix} xa + ya^2 \\ x + ya \end{pmatrix} = (x+ay) \begin{pmatrix} a \\ 1 \end{pmatrix}.$$

II.4:

$$f_p(\xi \cdot \eta) = (\xi \cdot \eta)^p = \xi^p \cdot \eta^p$$

$$f_p(\xi + \eta) = (\xi + \eta)^p = \sum_{k=1}^{p} \frac{p!}{k!(p-k)!} \xi^k \eta^{p-k}$$

$$= \xi^p + \eta^p.$$

# III Mersenne - Primzahlen

## III. 1. Definition:

Sei $R$ ein kommutativer Ring, $D \in R$.

Dann ist $U_1(R,D) := \{ A \in Q(R,D) : N(A) = 1 \} = \text{Kern}(N)$.
Untergruppe von $Q(R,D)^*$.

## III. 2 Satz:

Sei $p > 2$ prim, $n \geq 1$, $D \in \mathbb{Z}$ mit $p \nmid D$.

a) Ist $\left(\frac{D}{p}\right) = 1$, so ist $U_1(\mathbb{Z}/p^n\mathbb{Z}, D) \cong (\mathbb{Z}/p^n\mathbb{Z})^*$
also zyklisch mit Ordnung $p^n - p = p^{n-1}(p-1)$

b) Ist $\left(\frac{D}{p}\right) = -1$, so ist $U_1(\mathbb{Z}/p^n\mathbb{Z}, D)$ zyklisch
und von Ordnung $p^{n-1}(p+1)$.

## III. 3 Satz:

Sei $N \geq 3$ ungerade und $D \in \mathbb{Z}$ mit $\left(\frac{D}{N}\right) = -1$.

Genau dann ist $N$ eine Primzahl, wenn:

$\exists\, \xi \in (\mathbb{Z}/N\mathbb{Z})[\sqrt{D}]$ mit

$$\xi \cdot \bar{\xi} = 1,$$

$$\xi^{N+1} = 1$$

und $\xi^{\left(\frac{N+1}{q}\right)} \neq 1$ für alle Primteiler $q$ von $N+1$.

II. 2. a)

Beweis:

Da $\left(\frac{D}{p}\right) = 1$ $\exists\, a \in \mathbb{Z}$ mit $a^2 \equiv D \bmod p^n$

nach Satz II. 7.

Nach II. 2 ist dann

$$Q(\mathbb{Z}/p^n\mathbb{Z}, D) \cong (\mathbb{Z}/p^n\mathbb{Z}) \times (\mathbb{Z}/p^n\mathbb{Z}).$$

Da unter dem Isomorphismus

$$\varphi(\xi) = \varphi(x + ya) = (x+ya, x-ya) = (\xi, \bar{\xi})$$

$U_1(\mathbb{Z}/p^n\mathbb{Z}, D)$ abgebildet wird auf

$$\{(\xi, \bar{\xi}) \mid \xi \cdot \bar{\xi} = 1\} \subseteq (\mathbb{Z}/p^n\mathbb{Z})^* \times (\mathbb{Z}/p^n\mathbb{Z})^*,$$

ist $U_1(\mathbb{Z}/p^n\mathbb{Z}, D) \cong (\mathbb{Z}/p^n\mathbb{Z})^*$.

## III.4 Definition:

Sei $n \in \mathbb{N}$. Dann ist

$$M_n := 2^n - 1.$$

Falls $M_n$ prim ist nennt man $M_n$ Mersenne'sche Primzahl.

Ist $M_n$ prim so muss auch $n$ prim sein.

**Bemerkung:**

Für $n \geq 3$ ungerade gilt (u.a. nach dem Quadratischen Reziprozitätsgesetz):

$$\left(\frac{2}{M_n}\right) = 1 \quad , \quad \left(\frac{3}{M_n}\right) = -1.$$

## III.5 Satz:

Sei $M_p = 2^p - 1$, $p > 2$, eine Mersenne-Primzahl. Dann hat das Element

$$2 + \sqrt{3} \in (\mathbb{Z}/M_p\mathbb{Z})[\sqrt{3}]^*$$

die Ordnung $M_p + 1 = 2^p$, ist also erzeugendes Element von $U_1(\mathbb{Z}/M_p\mathbb{Z}, 3)$.

## III. 6 Satz:

Sei $n \geq 3$ ungerade. Genau dann ist $M_n = 2^n - 1$ eine Primzahl wenn für die rekursiv definierte Folge $(v_k) \in \mathbb{Z}^{\mathbb{N}_0}$

$$v_0 := 4 \quad \text{und}$$
$$v_k := v_{k-1}^2 - 2 \quad \forall k \in \mathbb{N}$$

gilt:

$$v_{n-2} \equiv 0 \mod M_n .$$

## III. 7 Satz:

Sei $p \geq 2$ prim und $q \in \mathbb{Z}$ mit

$$q \mid M_p .$$

Dann $\exists k \in \mathbb{Z}$ mit $q = 2kp + 1$.