Beispiel $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3 + X + 1)$

Bsp: Wir konstruieren einen Körper $\mathbb{F}_8 = \mathbb{F}_{2^3}$.

- Das Polynom $h = X^3 + X + 1$ ist irreduzibel über $\mathbb{F}_2$, da es weder 0 noch 1 als Nullstelle besitzt, d.h. kein Linearfaktor teilt h.
- Damit erhalten wir $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3 + X + 1)$. D.h. in $\mathbb{F}_8$ gilt
$$X^3 + X + 1 \equiv 0 \bmod 2 \text{ bzw. } X^3 \equiv -X - 1 \equiv X + 1 \bmod 2.$$
- Wir bestimmen $(X + 1)^{-1}$ in $\mathbb{F}_8$. D.h. wir bestimmen $a, b, c \in \mathbb{F}_2$ mit $(X+1)(aX^2+bX+c) \equiv 1 \Leftrightarrow a(X+1)+bX^2+cX+aX^2+bX+c \equiv 1$.
- Koeffizientenvergleich liefert
$$\left|\begin{array}{cc} a+b & \equiv 0 \\ a+b+c & \equiv 0 \\ a+c & \equiv 1 \end{array}\right| \text{ bzw. } a \equiv 1,\ b \equiv 1 \text{ und } c \equiv 0.$$
- Test: $(X + 1)(X^2 + X) \equiv X^3 + 2X^2 + X \equiv 2X^2 + 2X + 1 \equiv 1$.

Hinweis: Verschiedene irreduzible h liefern isomorphe Körper.

Satz von Wilson

Satz von Wilson

Eine Zahl $p \in \mathbb{N}$ ist prim gdw $(p-1)! \equiv (-1) \bmod p$.

Beweis:

$\Leftarrow$ Sei $p = ab$ mit $1 < a, b < p$.

- Fall 1 ($a \neq b$): Es gilt $ab|(p-1)!$ und daher $(p-1)! \equiv 0 \bmod p$.
- Fall 2 ($p = 4$:) Es gilt $3! \equiv 2 \bmod 4$.
- Fall 3 ($p = a^2$ mit $a > 2$:) Wegen $2a < p$ gilt $a \cdot 2a|(p-1)!$.
- Damit folgt $(p-1)! \equiv 0 \bmod 2a^2$ bzw. $(p-1)! \equiv 0 \bmod p$.

$\Rightarrow$ Sei $p \in \mathbb{P}$. Dann ist $\mathbb{F}_p$ ein Körper.

- D.h. jedes $\bar{a} \in \mathbb{F}_p \setminus \{\bar{0}\}$ besitzt ein Inverses $\bar{a}^{-1} \in \mathbb{F}_p \setminus \{\bar{0}\}$.
- Nur $\bar{1}$ und $\overline{-1} = \overline{p-1}$ sind selbstinvers, da $X^2 - 1$ über einem Körper nur maximal zwei Nullstellen besitzen kann.
- D.h. im Produkt $(p-1)!$ in $\mathbb{F}_p$ sind außer $1, p-1$ je zwei Elemente paarweise 1. Damit folgt $(p-1)! \equiv p-1 \equiv (-1) \bmod p$.

Erzeuger von Gruppen

Definition Erzeuger

Sei G eine Gruppe und $S \subseteq G$.

1. Wir bezeichnen mit $\langle S \rangle$ die von S *erzeugte* Untergruppe, d.h. die kleinste Untergruppe von G, die S enthält.
   Die Elemente von S heißen Erzeuger von $\langle S \rangle$.
2. G heißt *zyklisch*, falls $G = \langle g \rangle$ für ein $g \in G$.
3. G heißt *endlich erzeugt*, falls $G = \langle S \rangle$ für ein endliches S.

Bsp:

- $(\mathbb{Z}, +) = \langle 1 \rangle$
- $(\mathbb{Z}/n\mathbb{Z}, +) = \langle \bar{1} \rangle = \langle \bar{a} \rangle$ für alle a mit $\mathrm{ggT}(a, n) = 1$.

Lemma G besitzt $\mathbb{Z}$-Modulstruktur

Sei $(G,+)$ eine abelsche Gruppe und $g \in G$, $n \in \mathbb{N}_0$. Dann ist G zusammen mit folgender Skalarmultiplikation ein $\mathbb{Z}$-Modul:

$$n \cdot g := \underbrace{g + \ldots + g}_{n-mal},\ 0g := 0 \text{ und } (-n)g := -(ng).$$

Beweis:

- Offenbar gilt für alle $r, s \in \mathbb{N}_0$
$$1 \cdot g = g,\ r(sg) = (rs)g \text{ und } (r+s)g = rg + sg.$$
- Aus der Kommutativität von G folgt für $g, g' \in G$ und $r \in \mathbb{N}_0$
$$r(g+g') = \underbrace{g + g' + \ldots + g + g'}_{r-\text{mal}} = rg + rg'.$$

Erzeugung aus endlichen Mengen

Lemma Erzeugung aus endlichen Mengen

Sei $(G,+)$ eine abelsche Gruppe und $S \subseteq G$. Dann gilt

$$\langle S \rangle = \left\{ \sum_{g \in S'} n_g g \mid S' \subseteq S \text{ endlich}, n_g \in \mathbb{Z} \right\}.$$

Beweis:

$\supseteq$ Es gilt $g \in S' \subseteq S \subseteq \langle S \rangle$.

- Mit der $\mathbb{Z}$-Modulstruktur und Abgeschlossenheit von $\langle S \rangle$ sind auch
$$n_g g \in \langle S \rangle \text{ und } \sum_{g \in S'} n_g g \in \langle S \rangle.$$

$\subseteq$ Die linke Seite ist die kleinste Untergruppe, die S enthält.

- Wir bezeichnen die Menge auf der rechten Seite mit H.
- Da $S \subseteq H$, folgt $\langle S \rangle \subseteq H$, wenn H eine Untergruppe ist.
- Abgeschlossenheit: Seien $h = \sum_{g \in S'} n_g g$ und $h' = \sum_{g \in S''} n'_g g$.
- Wir schreiben $h = \sum_{g \in S' \cup S''} n_g g$ mit $n_g = 0$ für $g \in S'' \setminus S'$.
- Analog ist $h' = \sum_{g \in S' \cup S''} n'_g g$ mit $n'_g = 0$ für $g \in S' \setminus S''$.
- Dann gilt $h - h' = \sum_{g \in S' \cup S''} (n_g - n'_g) g \subseteq H$.

Zyklische Gruppen

Lemma

Sei $(G, +)$ eine Gruppe. Dann gilt $\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}$ für alle $g \in G$.

Beweis:

- Wie zuvor mit $S' = S = \{g\}$ als einziger nichtleerer Teilmenge.
- Kommutativität wird nicht benötigt, da nur g aufsummiert wird.

Satz zyklisch $\Rightarrow$ abelsch

Jede zyklische Gruppe G ist abelsch.

Beweis:

- Sei $G = \langle g \rangle = \{ng \mid n \in \mathbb{Z}\}$ für einen Erzeuger $g \in G$.
- Kommutativität folgt aus

$$ng + mg = (n + m)g = (m + n)g = mg + ng.$$

Isomorphiesatz

Satz Isomorphiesatz für zyklische Gruppen

Jede zyklische Gruppe ist isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z}$ für ein $n \in \mathbb{N}$.

Beweis:

- Wir betrachten den Gruppenhomorphismus
$$\Phi : \mathbb{Z} \to G, m \mapsto mg.$$
- Der Kern $\mathrm{Ker}(\Phi) \subseteq \mathbb{Z}$ ist ein Ideal, denn $0 \in \mathrm{Ker}(\Phi)$ und für $a, b \in \mathrm{Ker}(\Phi)$ gilt $a + b \in \mathrm{Ker}(\Phi)$ und $ma \in \mathrm{Ker}(\Phi)$ für $m \in \mathbb{Z}$.
- Da $\mathbb{Z}$ ein Hauptidealring ist, gilt $\mathrm{Ker}(\Phi) = n\mathbb{Z}$ für ein $n \geq 0$.
- Nach Homomorphiesatz gilt für einen Homomorphismus $f : A \to B$
$$\mathrm{Im}(f) \cong A/\mathrm{Ker}(f).$$
- D.h. $G \cong \mathbb{Z}$ für $n = 0$ bzw. $G \cong \mathbb{Z}/n\mathbb{Z}$ für $n \geq 1$.

Erzeuger besitzen Ordnung G.

Lemma Ordnung eines Erzeugers

Sei $(G, +)$ eine endliche zyklische Gruppe. Für ein $g \in G$ gilt

$$G = \langle g \rangle \text{ gdw } \mathrm{ord}(g) = |G|.$$

Beweis:

$\Rightarrow$ Sei $G = \langle g \rangle = \{g, 2g, \ldots, \mathrm{ord}(G)g\}$.

- Alle Elemente in $\{g, 2g, \ldots, \mathrm{ord}(G)g\}$ sind verschieden.
- Annahme: $ig = jg$ für $1 \leq i < j \leq \mathrm{ord}(G)$.
- Dann gilt $(j - i)g = 1$ mit $0 < j - i < \mathrm{ord}(G)$. (Widerspruch)
- Damit gilt $|G| = |\{g, 2g, \ldots, \mathrm{ord}(G)g\}| = \mathrm{ord}(g)$.

$\Leftarrow$ Sei $\mathrm{ord}(g) = |G|$.

- In $\langle g \rangle = \{g, 2g, \ldots, \mathrm{ord}(G)g\}$ sind je zwei Elemente verschieden.
- Da $|\langle g \rangle| = |G|$, muss $\langle g \rangle$ alle Elemente aus G enthalten.