1 Zyklische Gruppen

1.1 Definition (Zyklische Gruppen der Ordnung n)
$Z_n := \langle a \mid a^n = e \rangle = \{a^0, a^1, \dots a^{n-1}\}$

1.2 Lemma
Z_n ist isomorph zu $\mathbb{Z}/n\mathbb{Z}$, d.h. es existiert ein Isomorphismus $f : \mathbb{Z}/n\mathbb{Z} \to Z_n, i \mapsto a^i$.

Beweis. a) f ist bijektiv: Es genügt zu zeigen, dass f injektiv ist.

$$f(a^i) = f(a^j) \;\Rightarrow\; i + n\mathbb{Z} = j + n\mathbb{Z} \overset{i,j \in \mathbb{Z}/n\mathbb{Z}}{\Rightarrow} i = j \;\Rightarrow\; f \text{ bijektiv}$$

b) $f(i + j) = f(i) + f(j) \forall i, j \in \mathbb{Z}/n\mathbb{Z}$

$$f(i + j) = a^{i+j} = a^i \cdot a^j = f(i) \cdot f(j)$$

1.3 Bemerkung (Eigenschaften von Z_n)

- ▷ Z_n ist abelsch.
- ▷ Zu jedem Teiler t von n gibt es genau eine Untergruppe der Ordung t, nämlich $\langle a^{\frac{n}{t}} \rangle$.
- ▷ Untergruppen von zyklischen Gruppen sind wieder zyklisch.

1.4 Lemma
Sei $(G, \circ)$ eine zyklische Gruppe der Ordnung n mit $G = \langle n \rangle$. Sei weiter U eine Untergruppe von G. Dann ist U zyklisch, d.h. es gibt ein Element a^k mit $U = \langle a^k \rangle$.

Beweis. Wir zerlegen die Behauptung in zwei Fälle.

a) Ist $\#U = 1$, d.h. $U = \{e = a^0\}$ ist zyklisch.

b) Sei $\#U > 1$. Somit enthält U ein Element a^i mit $i > 0, i$ minimal. Wir zeigen, dass $U = \langle a^i \rangle$.
Sei $a^j \in U$ beliebig. Dann gilt $a^j \in \langle a^i \rangle$, denn:
Es gibt $q, r \in \mathbb{N}$ mit $j = q \cdot i + r$ und $0 \leq r < i$. Dann ist $a^j = a^{q \cdot i + r} = (a^i)^q \cdot a^r$ mit $a^i, a^j \in U$ und somit auch $(a^i)^q \in U$ sowie schlussendlich auch $a^r \in U$. Da i minimal ist, folgt $r = 0$ und dann $a^r = e$, sodass $a^j = (a^i)^q \cdot e = (a^i)^q \in \langle a^i \rangle$ □

1.5 Definition
Seien $(G_1, \circ_1), (G_2, \circ_2)$ Gruppen und $g_1, g_1' \in G_1$ und $g_2, g_2' \in G_2$. Durch

$$(g_1, g_2) \circ (g_1', g_2') = (g_1 \circ_1 g_1', g_2 \circ_2 g_2')$$

wird eine Operation in $G_1 \times G_2$ erklärt. Man nennt $(G_1 \times G_2, \circ)$ das direkte Produkt der Gruppen G_1 und G_2.

1.6 Bemerkung
Offensichtlich ist $(G_1 \times G_2, \circ)$ eine Gruppe.

1.7 Satz
$(G_1, \circ_1), (G_2, \circ_2)$ seien Gruppen.

a) $G_1 \times G_2 \cong G_2 \times G_1$

b) Sind G_1 und G_2 abelsch, so ist auch $G_1 \times G_2$ abelsch.

c) Ist $G_1 \times G_2$ zyklisch, so sind auch G_1 und G_2 zyklisch.

1.8 Beispiel
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \neq \mathbb{Z}/4\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$, denn $\langle(1,1)\rangle = \{(1,1),(0,2),(1,0),(0,1),(1,2),(0,0)\}$.

1.9 Satz
Die Gruppe $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ ist genau dann zyklisch, wenn $\mathrm{ggT}(n,m) = 1$.

Beweis. $\mathrm{ggT}(n,m) = 1 \;\Rightarrow\; \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/n \cdot m\mathbb{Z} = \langle(1,1)\rangle$
Sei $\mathrm{ggT}(n,m) = d > 1$ und $(a,b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Dann ist $\mathrm{ord}(a,b) = \#\langle(a,b)\rangle < n \cdot m = \#\mathbb{Z}/(\mathbb{Z}n) \times \mathbb{Z}/m\mathbb{Z}$.
Sei nun $n = n' \cdot d$ und $m = m' \cdot d$. Dann ist

$$\underbrace{(a,b) + \cdots (a,b)}_{n' \cdot m' \cdot d < n \cdot m \text{ Summanden}} = (0,0)$$

1.10 Theorem (Basissatz für endliche abelsche Gruppen)
Jede endliche abelsche Gruppe ist isomorph zu einem direkten Produkt zyklischer Gruppen von Primzahlpotenzordnung

$$Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_k} \quad \text{mit } m_1 \mid m_2, m_2 \mid m_3, \ldots, m_{k-1} \mid m_k$$

Diese Darstellung ist eindeutig bis auf die Reihenfolge der Faktoren im direkten Produkt.

1.11 Beispiel
Suche alle abelschen Gruppen der Ordnung 8.
$8 = 2^3 = 2^1 \cdot 2^1 \cdot 2^1$
$Z_8 = Z_{2^3}$
$Z_{2^2} \times Z_{2^1} = Z_4 \times Z_2$
$Z_{2^1} \times Z_{2^1} \times Z_{2^1} = Z_2 \times Z_2 \times Z_2$
$\Rightarrow$ Es gibt bis auf Isomorphie genau 3 abelsche Gruppen der Ordnung 8.

1.12 Beispiel
Alle abelschen Gruppen der Ordnung 360 enthalten ein Element der Ordnung 30.
$360 = 2^3 \cdot 3^2 \cdot 5$

2 Ringe

2.1 Definition
Sei $R \neq \emptyset$. $(R, +, \cdot)$ heißt *Ring*, falls gilt:

a) $(R, +)$ ist eine abelsche Gruppe.

b) $R, \cdot)$ ist eine Halbgruppe.

c) Distributivgesetze: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ und $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ für alle $a, b, c \in R$.

d) Gilt zusätzlich
$a \cdot b = b \cdot a$ für alle $a, b \in R$,
dann wird $(R+, \cdot)$ kommutativer Ring genannt.

2.2 Definition
Sei $(R, +, \cdot)$ ein Ring und $U \subseteq R$. U heißt *Unterring* von $(R, +, \cdot)$, wenn gilt:

a) $U \neq \emptyset$ $(0_R \in U)$

b) $a, b, \in U \quad \Rightarrow \quad a + b \in U$ für alle $a, b \in U$ (Abgschlossenheit unter Addition)

c) $a \in U \quad \Rightarrow \quad -a \in U$ für alle $a \in U$ (Abgeschlossenheit unter additiven Inversen)

2.3 Beispiel
$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ sind kommutative Ringe.
$\mathbb{R}^{n \times n}$, der Matrizenring (über $\mathbb{R}$)
$\mathbb{Z}/n\mathbb{Z}$, der Restklassenring modulo n
$2\mathbb{Z} = \{2 \cdot z : z \in \mathbb{Z}\}$ ist ein Unterring von $\mathbb{Z}$ $\{a + bi : a, b \in \mathbb{Z}\}$ ist Unterring von $\mathbb{C}$

2.4 Bemerkung
Allgemein gilt:

$$a \cdot (b_1 + \cdots + b_n) = a \cdot b_1 + \cdots + a \cdot b_n$$

für alle $a, b_i \in R$.

Beweis. Zeige die Aussage mittels vollständiger Induktion über n. □

2.5 Bemerkung
Addition ist in jedem Ring kommutativ.
"Punktrechnung vor Strichrechnung."
Inverse Elemente in Ringen existieren immer bzgl. der Addition (Bezeichnung $-a$), und sofern sie bzgl. der Multiplikation existieren schreibe a^{-1}.

2.6 Bemerkung
Jeder Ring hat ein neutrales Element bezüglich der Addition. Nenne dieses auch *Nullelement* und bezeichne es mit 0.
Das Nullelement ist eindeutig bestimmt, denn: $0_1 = 0_1 + 0_2 = 0_2$.

2.7 Definition
Sei $(R, +, \cdot)$ ein Ring mit Nullelement 0. Existiert ein Element $1 \in R \backslash \{0\}$ mit $a \cdot 1 = 1 \cdot a = 1$ für alle $a \in R$, dann wird 1 *Einselement* genannt.

2.8 Bemerkung
Nicht jeder Ring hat ein Einselement! Falls ein solches aber existiert, dann ist es auch eindeutig bestimmt, denn: $1_1 = 1_1 \cdot 1_2 = 1_2$.

2.9 Beispiel

- ▷ $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Ringe mit Nullelement 0 und Einselement 1.
- ▷ $\mathbb{Z}/n\mathbb{Z}$ ist ein Ring mit Nullelement 0 und Einselement 1.
- ▷ $\mathbb{R}^{n\times n}$ ist ein Ring mit Nullelement $0_{n\times n}$ und Einselement $\mathbb{1}_n$.
- ▷ Sei $M \neq \emptyset$ und $(\mathcal{P}(M); \triangle, \cap)$ ist dann ein Ring mit Nullelement $\emptyset$ und Einselement M.

2.10 Bemerkung
Sei $(R, +, \cdot)$ ein Ring mit Nullelement 0 und $a \in R$. Dann gilt $0 \cdot a = 0$ und $a \cdot 0 = 0$.

Beweis. $0 \cdot a = (0+0) \cdot a = (0 \cdot a) + (0 \cdot a) \quad\Rightarrow\quad (0 \cdot a) + (-0 \cdot a) = (0 \cdot a) + (0 \cdot a) + (-0 \cdot a) \quad\Rightarrow$
$0 = 0 \cdot a + 0 = 0 \cdot a$ □

2.11 Definition
Sei $(R, +, \cdot)$ ein kommutativer Ring mit $a, b \in R\backslash\{0\}$. Gilt $a \cdot b = 0$, dann werden a, b *Nullteiler* in $(R, +, \cdot)$ genannt.

2.12 Beispiel
Der Ring $\mathbb{Z}/6\mathbb{Z}$ hat die Nullteiler 2 und 3, denn $2 \cdot 3 = 3 \cdot 2 = 0$.
Die Ringe $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ besitzen keine Nullteiler, sind also nullteilerfrei.
In Matrizenringen gibt es Nullteiler, z.B.

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

In $\mathbb{Z}/p\mathbb{Z}$ mit p prim gibt es keine Nullteiler, denn: Sei $a \in \mathbb{Z}/p\mathbb{Z}\backslash\{0\}$. Angenommen es existiert ein $b \in \mathbb{Z}/p\mathbb{Z}\backslash\{0\}$ mit $a \cdot b = 0 \pmod p$. Dann folgt $(a^{-1} \cdot a) \cdot b = a^{-1} \cdot 0$ und $1 \cdot b = b = 0$. ↯

2.13 Definition
Sei $(R, +, \cdot)$ ein kommutativer Ring mit Einselement, in dem es keine Nullteiler gibt (nullteiiler-frei). Dann wird $(R, +, \cdot)$ ein *Integritätsring* genannt.

2.14 Beispiel
$(\mathbb{Z}, +, \cdot)$ ist ein Integritätsring.

2.15 Definition
Sei $(R, +, \cdot)$ ein Ring mit Nullelement 0. Ist $(R\backslash\{0\}), +, \cdot)$ eine abelsche Gruppe, dann nennt man $(R, +, \cdot)$ einen *Körper*.

3 Endliche Körper

3.1 Definition
Ein endlicher Körper mit p^k Elementen (p prim, $k \in \mathbb{N}\backslash\{0,1\}$), in Zeichen $\mathrm{GF}(p^k)$ ist $(\mathrm{GF}(p^k)[x]/f(x), \oplus, \otimes)$ mit $f(x) \in \mathrm{GF}(p)[x], \mathrm{grad}(f) = k$ und f ist irreduzibel.

3.2 Definition
Sei K ein Körper, $f(x) \in K[x]$. Dann heißt $f(x)$ irreduzibel über K, wenn es keine Polynome $a(x), b(x) \in K[x]$ gibt, sodass $f(x) = a(x) \cdot b(x)$ und $0 < \mathrm{grad}(a(x)) \leq \mathrm{grad}(b(x)) < \mathrm{grad}(f(x))$ gilt.

3.3 Beispiel
- ▷ Sei $K = \mathrm{GF}(2)$, dann ist $x^4 + 1 = (x-1)^4$ nicht irreduzibel.
- ▷ Sei $K = \mathrm{GF}(2)$, dann ist $x^3 + x + 1$ irreduzibel.
- ▷ Sei $K = \mathrm{GF}(2)$, dann sind $x^4 + x^3 + 1$, $x^4 + x + 1$, $x^4 + x^3 + x^2 + x + 1$ irreduzibel.

3.4 Bemerkung
Aber für $K = \mathrm{GF}(3)$ ist $2x + 1 = 2x + 1$ ist irreduzibel, d.h. konstante Faktore können immer ausgeklammert werden ohne die Irreduzibiliät zu verändern.

3.5 Beispiel
Wir betrachten einen endlichen Körper mit 2^4 Elementen. Dann ist $\mathrm{GF}(2) = \mathbb{Z}/2\mathbb{Z} = \{0,1\}$. Menge

$$\begin{aligned}\mathrm{GF}(2)[x]/(x^4 + x^3 + 1) &= \{a_3x^3 + a_2x^2 + a_1x + a_0 : a_0, a_1, a_2, a_3 \in \mathrm{GF}(2)\} \\ &= \{\underbrace{0,1}_{\text{Grad } 0}, \underbrace{x, x+1}_{\text{Grad } 1}, \underbrace{x^2, x^2+1, x^2+x, x^2+x+1}_{\text{Grad } 2}, \underbrace{x^3, \ldots, x^3+x^2+x+1}_{\text{8 Polynome vom Grad 3}}\}\end{aligned}$$

3.6 Bemerkung
$\mathrm{GF}(2)[x]/(x^4 + x^3 + 1) = \mathrm{GF}(2)[x]/(x^4 + x + 1) = \mathrm{GF}(2)[x]/(f(x))$ mit $\mathrm{grad}\, f(x) = 4$ über $\mathrm{GF}(2)$.

3.7 Bemerkung
$a(x)^{-1} = (x^3 + x + 1)1{-}1 = x^3 + x$ in $\mathrm{GF}(2)[x]$.
Berechnung von $a(x)^{-1}$ mit erweitertem euklidischen Algorithmus:

$$1 \cong \mathrm{ggT}(a(x), \underbrace{(x^4 + x^3 + 1)}_{\text{irreduzibel}}) = \alpha(x) \odot a(x) + \beta(x) \odot (x^4 + x^3 + 1)$$

mod $(x^4 + x^3 + 1)$:

$$\begin{aligned} 1 &\equiv \alpha(x) \odot a(x) \mod (x^4 + x^3 + 1) \\ \Rightarrow\ a(x)^{-1} &= \alpha(x) \mod (x^3 + x^3 + 1)\end{aligned}$$

3.8 Definition
Seo $K = \mathrm{GF}(p)$ ein Körper, $f(x) \in K[x]$ irreduzibel. $f(x)$ heißt *primitiv*, wenn gilt

$$\min\{l \in \mathbb{N}\backslash\{0\} : x^l \equiv 1(\mod f(x))\} = p^k - 1$$

3.9 Beispiel
Sei $K = \mathrm{GF}(2)$ und $f(x) = x^3 + x + 1$. Also ist $\min\{\dots\} = 7 = 2^3 - 1$ und damit $x^3 + x + 1$

l	$x^l \mod (x^3 + x + 1)$
0	1
0	x
2	x^2
3	$x^3 = x + 1$
4	$x^4 = x(x+1) = x^2 + x$
5	$x^5 = x(x^2 + x) = x^3 + x^2 = x^2 + x + 1$
6	$x^6 = x^2 + 1$
7	$x^7 = 1$

primitiv über GF(2)

3.10 Bemerkung
Ist $f(x) \in \mathrm{GF}(p)[x]$ mit $\mathrm{grad}(f(x)) = k$ ein primitives Polynom, dann kann man alle Elemente von $\mathrm{GF}(p)[x]/f(x)\setminus\{0\}$ in der Form $x^l \mod f(x)$ notieren, wobei $k \in \{0, 1, \dots, p^k - 2\}$. Man stellt fest, dass sowohl $\mathrm{GF}(p)[x]/f(x)\setminus\{0\}$ als auch $x^l \mod f(x)$ genau $p^k - 1$ Elemente besitzen ($\mathrm{GF}(p)[x]$ hat p^k Elemente).

4 Fourier-Transformationen

4.1 Diskrete Fourier-Transformation (DFT)

4.1 Beispiel
Sei $p(x) = 1 + 2x + 0x^2 + x^3$. Auwertung an $\omega^0, \omega^1, \omega^2, \omega^3$ einer primitiven 4-ten Einheitswurzel ω in $\mathbb{C}$. Wähle $\omega = i$, also an $1, i, -1, -i$

$$DFT_{4,i} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

$$DFT_{4,i} \cdot \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 1+i \\ -2 \\ 1-i \end{pmatrix}$$

Also ist $p(1) = 4$, $p(i) = 1 + i$, $p(-1) = -2$, $p(-i) = 1 - i$.

4.2 Schnelle Fourier-Transformation (FFT)

4.2 Bemerkung (Polynommultiplikation)
Gegeben seine Polynome a, b und wir suchen das Polynom $a \cdot b$. Wende zuerst DFT auf beide Polynome a und b an. Mit komponentenweiser Multiplikation im Körper und inverser DFT erhält man $a(x) \cdot b(x)$.

4.3 Bemerkung (Multiplikation großer natürlicher Zahlen)
Gegeben seien zwei natürliche Zahlen $a, b \in \mathbb{N}$.

$$a = a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots + a_n \cdot 2^n = \sum_{i=0}^{n} a_i \cdot 2^i$$

$$b = b_0 + b_1 \cdot 2 + b_2 \cdot 2^2 + \cdots + b_n \cdot 2^n = \sum_{i=0}^{n} b_i \cdot 2^i$$

Daraus basteln wir nun Polynomfunktionen

$$a(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \cdots + a_n \cdot x^n$$
$$b(x) = b_0 + b_1 \cdot x + b_2 \cdot x^2 + \cdots + b_n \cdot x^n$$

Mit DFT erhält man dann $a(x) \cdot b(x) = p(x)$, und für die Multiplikation

$$a \cdot b = p(x) = p(2) = a(2) \cdot b(2)$$

4.4 Bemerkung
ω ist primitive $(n+1)$-te Einheitswurzel $\Rightarrow$ ω^2 ist primitive $\frac{n+1}{2}$-te Einheitswurzel.

Beweis. ω ist eine primitive $(n+1)$-te Einheitswurzel, wenn

- $\omega^{n+1} = 1$ und
- $|\langle \omega \rangle| = \left| \{\omega^0, \omega^1, \omega^2, \dots, \omega^n\} \right| = n + 1$.

Damit ist die Aussage klar. □

4.5 Bemerkung
ω^k ist primitive $(n+1)$-te Einheitswurzel
$\Rightarrow \quad -\omega^k$ ist primitive $(n+1)$-te Einheitswurzel, falls ω primitive $(n+1)$-te Einheitswurzel ist.

Beweis. $(\omega^k)^{n+1} = 1 \quad \Rightarrow \quad (-\omega^k)^{n+1} = (-1)^{n+1} \cdot (\omega^k)^{n+1} = 1 \cdot 1$, da $n+1 = 2^r$ vorausgesetzt war. □

4.6 Satz (Aufwand $A(r)$ für Algorithmus von Cooley-Tukey)
Seien $n+1 = 2^r$, ω eine primitive $(n+1)$-te Einheitswurzel und

$$p(x) = a_0 \cdot a_1 \cdot x + \cdots + a_n \cdot x^n = (a_0 + a_2 \cdot y + \cdots) + x \cdot (a_1 + a_3 \cdot y + \cdots) \text{ mit } y = x^2$$

Dabei wird der linke Summand an den Stellen $\omega^0, \ldots, \omega^n$ und der rechte Summand an $(\omega^2)^0, \ldots, (\omega^2)^{\frac{n+1}{2}}$ ausgewertet wird.

4.7 Beispiel

- $\triangleright$ $r = 0 \quad \Rightarrow \quad n+1 = 1 \quad \Rightarrow \quad n = 0 \quad \Rightarrow \quad p(x) = a_0 \quad \Rightarrow \quad A(r) = 0$
- $\triangleright$ $r = 1 \quad \Rightarrow \quad n+1 = 2 \quad \Rightarrow \quad n = 1 \quad \Rightarrow \quad p(x) = a_0 + a_1 \cdot x \quad \Rightarrow \quad A(1) = 2 \cdot 0 + 2 + 1 = 3.$
- $\triangleright$ $r = 2 \quad \Rightarrow \quad n+1 = 4 \quad \Rightarrow \quad n = 3$
  $\Rightarrow \quad p(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + a_3 \cdot x^3 = (a_0 + a_2 \cdot y) + x \cdot (a_1 + a_3 \cdot y)$ mit $y = x^2$.
  $\Rightarrow \quad A(2) = 2 \cdot 3 + 4 + 2 = 12$

Allgemein ist damit

$$A(r) = 2 \cdot A(r-1) + \underbrace{2^r}_{\text{Addition}} + \underbrace{2^{r-1}}_{\text{Multiplikation}}$$

4.8 Satz
Für den Aufwand gilt

$$A(r) = \frac{3}{2} \cdot r \cdot 2^r$$

Beweis. Für $r = 0$ ist $A(0) = 0$ ✓
Für $r > 0$ ist

$$\begin{aligned} A(r) = 2 \cdot A(r-1) + 2^r + 2^{r+1} &= 2 \cdot \frac{3}{2}(r-1) \cdot 2^(r-1) + 2^r + 2^{r+1} \\ &= \frac{3}{2} \cdot r \cdot 2^r - \frac{3}{2} \cdot 2^r + 2^r + 2^{r+1} \\ &= \frac{3}{2} \cdot r \cdot 2^r \end{aligned}$$

4.9 Bemerkung
Außerdem erhält man

$$n+1 = 2^r \quad \Rightarrow \quad r = \log_2(n+1) \quad \Rightarrow \quad \frac{3}{2} \cdot \log_2(n+1)(n+1)$$

und damit ist der Aufwand für FFT $\mathcal{O}(n \cdot \log(n))$.