3.5.3 Berechnung der inversen diskreten Fouriertransformation

Satz 151
Es gilt

$$\mathcal{F}_{n,\omega}^{-1} = \frac{1}{n}\mathcal{F}_{n,\omega^{-1}}.$$

Bemerkung: ω^{-1} ist ebenso eine primitive n-te Einheitswurzel.
Zum Beweis von Satz 151 benötigen wir folgendes Lemma:

Lemma 152
Ist ω eine primitive n-te Einheitswurzel, so gilt

$$\sum_{j=0}^{n-1} \omega^{kj} = 0$$

für alle $k = 1, \ldots, n-1$.

Beweis:
Für jedes $a \in \mathbb{C}$, $a \neq 1$, gilt $\sum_{j=0}^{n-1} a^j = \frac{a^n-1}{a-1}$. Speziell für $a = \omega^k$ ist $a^n = \omega^{kn} = 1$, $(k = 1, \ldots, n-1)$. □

Nun zum Beweis von Satz 151.

Beweis:
Sei $\vec{e} = \mathcal{F}_{n,\omega}(\vec{a}) = (e_0, \ldots, e_{n-1})$. Wir zeigen, dass gilt:

$$\frac{1}{n}\mathcal{F}_{n,\omega^{-1}}(\vec{e}) = \vec{a}$$

$$\begin{aligned} P_{\vec{e}}(\omega^{-k}) &= \sum_{j=0}^{n-1} e_j \omega^{-kj} = \sum_{j=0}^{n-1} P_{\vec{a}}(\omega^j)\omega^{-kj} \\ &= \sum_{j=0}^{n-1}\sum_{i=0}^{n-1} a_i \omega^{ij}\omega^{-kj} = \sum_{i=0}^{n-1} a_i \sum_{j=0}^{n-1} \omega^{(i-k)j} = na_k, \end{aligned}$$

denn nach Lemma 152 ist $\sum_{j=0}^{n-1} \omega^{(i-k)j} = 0$, falls $i \neq k$.
Im Fall $i = k$ gilt $\sum_{j=0}^{n-1} \omega^{(i-k)j} = n$. □

3.6 Restklassen in Polynomringen

3.6.1 Einführung und Definitionen

Der Begriff der Restklasse stammt ursprünglich aus der Teilbarkeitslehre in $\mathbb{Z}$;
($\mathbb{Z} = \langle \mathbb{Z}, +, \cdot \rangle$ ist ein kommutativer Ring).

Definition 153
Sei n eine fest gewählte ganze Zahl $\neq 0$. Für jedes $\ell \in \mathbb{Z}$ heißt die Menge

$$[\ell]_n := \{m \in \mathbb{Z} : m - \ell \text{ ist durch } n \text{ teilbar}\}$$

die Restklasse von ℓ modulo n.

Bemerkungen

1. Für $\ell, m \in \mathbb{Z}$ gilt:
$$m \in [\ell]_n \iff m \bmod n = \ell \bmod n\,.$$
Gilt $m \in [\ell]_n$, so schreibt man auch $m \equiv \ell \bmod n$ oder $m = \ell \bmod n$ und spricht „m kongruent ℓ modulo n“.
2. Es gilt $[\ell]_n = \{\ell + kn : k \in \mathbb{Z}\} =: \ell + n\mathbb{Z} =: \ell + (n)$.
3. Da es genau n verschiedene Reste $0, 1, \ldots, n-1$ gibt, gibt es auch genau n verschiedene Restklassen $[0]_n, [1]_n, \ldots, [n-1]_n$.

Bemerkungen

4. Kongruenz modulo n definiert auf $\mathbb{Z}$ eine Äquivalenzrelation $\sim_n$: $m \sim_n \ell :\iff n$ teilt $m - \ell$, und $[\ell]_n$ ist die Äquivalenzklasse von ℓ.
5. Auf der Menge aller Restklassen $[\ell]_n$ kann man Addition und Multiplikation wie folgt definieren

$$[\ell]_n +_n [m]_n := [\ell + m]_n, \qquad [\ell]_n \cdot_n [m]_n := [\ell \cdot m]_n,$$

   und erhält einen kommutativen Ring; er heißt der Restklassenring $\mathbb{Z}$ modulo n und wird mit $\mathbb{Z}/(n)$ oder $\mathbb{Z}/n\mathbb{Z}$ oder $\mathbb{Z}_n$ bezeichnet.
6. Die Abbildung $\langle \mathbb{Z}, +, \cdot \rangle \to \langle \mathbb{Z}_n, +_n, \cdot_n \rangle$, $\ell \mapsto$ „Rest der Division von ℓ durch n“ ist ein Ringhomomorphismus.

Restklassen können auch im Polynomring $K[x]$ (K ein Körper) gebildet werden.

Definition 154

Sei $g \in K[x]$ ein Polynom, $\text{grad}(g) \geq 1$. Für jedes $f \in K[x]$ heißt die Menge

$$[f]_g := \{h \in K[x] : h - f \text{ ist durch } g \text{ teilbar}\}$$

die Restklasse von f modulo g.

Bemerkung: Wie in $\mathbb{Z}$ gilt nun auch im Polynomring $K[x]$:

1. $h \in [f]_g \iff h$ und f haben bei Polynomdivision durch g denselben Rest.
2. $[f]_g = \{f + hg \ : \ h \in K[x]\} =: f + (g)$ mit $(g) := \{hg : h \in K[x]\} =$ Menge aller Polynome, die durch g teilbar sind.