§ 20. Kreisteilungspolynome

Definition (20.1)

Sei $n \in \mathbb{N}$. Eine *n*-te Einheitswurzel in $\mathbb{C}$ ist ein Element $\zeta \in \mathbb{C}$ mit $\zeta^n = 1$. Mit μ_n bezeichnen wir die Menge aller n-ten Einheitswurzeln. Es handelt sich um eine Untergruppe von $\mathbb{C}^\times$.

Lemma (20.2)

Sei $k \in \mathbb{Z}$. Genau dann gilt $\mu_n = \langle \zeta_n^k \rangle$, wenn $\mathrm{ggT}(k, n) = 1$ ist.

Definition der Kreisteilungspolynome

Definition (20.3)

Sei $n \in \mathbb{N}$, $n \geq 2$.

- Eine primitive n-te Einheitswurzel ist ein Element $\zeta \in \mu_n$ mit $\mu_n = \langle \zeta \rangle$.
- Wir bezeichnen mit $\mu_n^\times \subseteq \mu_n$ die Menge der primitiven n-ten Einheitswurzeln.
- Das Polynom $\Phi_n \in \mathbb{C}[x]$ gegeben durch

$$\Phi_n \quad = \quad \prod_{\zeta \in \mu_n^\times} (x - \zeta)$$

wird das n-te Kreisteilungspolynom genannt.

Die Ganzzahligkeit der Kreisteilungspolynome

- Aus technischen Gründen setzen wir $\Phi_1 = x - 1$, obwohl wir für $n = 1$ keine primitiven n-ten Einheitswurzeln definiert haben.
- Für alle $n \in \mathbb{N}$ ist $\varphi(n) = \operatorname{grad} \Phi_n$.

Lemma (20.4)

Für alle $n \in \mathbb{N}$ gilt $x^n - 1 = \prod_{d|n} \Phi_d$, wobei d die natürlichen Teiler von n durchläuft.

Satz (20.5)

Es gilt $\Phi_n \in \mathbb{Z}[x]$ für alle $n \in \mathbb{N}$.

Beweis von Satz 20.5

Zeige durch vollständige Induktion über n: $\Phi_n \in \mathbb{Z}[x]$

Ind.-Anf. $n = 1$: $\Phi_1 = x - 1 \in \mathbb{Z}[x]$

Ind.-Schritt: Sei $n \in \mathbb{N}$, $n > 1$, setze die Aussage für Zahlen $< n$ voraus. Lemma 2.4 $\Rightarrow x^n - 1 = \Phi_n \cdot g$

mit $g = \prod_{d \in S} \Phi_d$, wobei $S = \{ d \in \mathbb{N} \mid d \mid n, d < n \}$.

Nach Induktionsvoraussetzung gilt $g \in \mathbb{Z}[x]$.

Zeige zunächst $\Phi_n \in \mathbb{Q}[x]$. $\mathbb{Q}[x]$ ist euklidisches Ring

Division mit Rest $\Rightarrow \exists q, r \in \mathbb{Q}[x]$ mit $x^n - 1 = qg + r$

wobei $r = 0$ oder $\text{grad}(r) < \text{grad}(g)$ gilt (*)

$r = x^n - 1 - qg = \Phi_n g - qg = (\Phi_n - q)g$ Wegen (*) Kürzungsregel $\Longrightarrow$ in $\mathbb{C}[x]$

folgt daraus $r = 0 \Rightarrow qg = x^n - 1 = \Phi_n g$

$\Phi_n = q \Rightarrow \Phi_n \in \mathbb{Q}[x]$

Es gilt $x^n - 1, g \in \mathbb{Z}[x]$. $x^n - 1 = \Phi_n g$, mit $\Phi_n \in \mathbb{Q}[x]$

$\rightarrow$ g ist ein Teiler von $x^n - 1$ im Polynomring $\mathbb{Q}[x]$

Da das Polynom g normiert und damit primitiv ist, ist g Teiler von $x^n - 1$ in $\mathbb{Z}[x]$ (Folgerung aus dem Gauß'schen Lemma)

$\Rightarrow \exists h \in \mathbb{Z}[x]$ mit $hg = x^n - 1 = \Phi_n g$ $\overset{\text{Kürzungs-regel in } \mathbb{Q}[x]}{\Longrightarrow}$

$\Phi_n = h \Rightarrow \Phi_n \in \mathbb{Z}[x]$. □

Beispiele für die Berechnung von Kreisteilungspolynomen:

(1) Sei p eine Primzahl. Lemma 20.4

$$\Rightarrow x^p - 1 = \Phi_1 \Phi_p = (x-1)\Phi_p \Rightarrow$$

$$\Phi_p = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

(2) Berechnung von Φ_6: $x^6 - 1 = \Phi_1 \Phi_2 \Phi_3 \Phi_6$

$$\Rightarrow \Phi_6 = \frac{x^6 - 1}{\Phi_1 \Phi_2 \Phi_3} = \frac{(x^6-1)(x-1)}{\Phi_1 \Phi_2 (x^3 - 1)}$$

$$= \frac{(x^3)^2 - 1}{(x^3-1)\cdot \Phi_2} = \frac{x^3+1}{\Phi_2} = \frac{x^3+1}{x+1} = x^2 - x + 1$$

Die Irreduzibilität der Kreisteilungspolynome

Lemma (20.6)

Für jedes Polynom $f \in \mathbb{F}_p[x]$ gilt $f^p = f(x^p)$.

Satz (20.7)

Für jedes $n \in \mathbb{N}$ ist das Kreisteilungspolynom Φ_n in $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$ irreduzibel.

Beweis von Lemma 20.6

geg: Primzahl p, $f \in \mathbb{F}_p[x]$

Schreibe $f = \sum_{k=0}^{n} a_k x^k$, $n \in \mathbb{N}_0$, $a_k \in \mathbb{F}_p$ $(0 \le k \le n)$

Es gilt $a^p = a \; \forall a \in \mathbb{F}_p$ (Kl. Satz von Fermat)

$$\Rightarrow f^p = \left(\sum_{k=0}^{n} a_k x^k\right)^p = \sum_{k=0}^{n} a_k^p x^{kp}$$

↑ Freshman's Dream

$$= \sum_{k=0}^{n} a_k (x^p)^k = f(x^p)$$

□

Beweis von Satz 20.7

Sei $n \in \mathbb{N}$. z.zg: Φ_n ist irreduzibel in $\mathbb{Z}[x]$ (und damit auch in $\mathbb{Q}[x]$). O.B.d.A. sei $n > 1$.

Ang. Φ_n ist reduzibel in $\mathbb{Z}[x] \Rightarrow$ $\exists$ nicht-konst. Polynome $f, g \in \mathbb{Z}[x]$ mit $\Phi_n = f g$.

Dabei können wir annehmen, dass f in $\mathbb{Z}[x]$ irreduzibel ist. Sei p eine Primzahl mit $p \nmid n$.

Zeige: Ist $\zeta \in \mathbb{C}$ eine Nullstelle von f, dann ist auch ζ^p eine Nullstelle von f. (Δ)

Ang. $f(\zeta^p) \neq 0$. $f(\zeta) = 0 \Rightarrow \Phi_n(\zeta) = 0$

$\Rightarrow \zeta \in \mu_n^\times$ $\overset{ggT(n,p)=1}{\Rightarrow}$ $\zeta^p \in \mu_n^\times \Rightarrow \Phi_n(\zeta^p) = 0$

$\rightarrow f(\zeta^p)\, g(\zeta^p) = 0$ $\overset{f(\zeta^p)\neq 0}{\Rightarrow}$ $g(\zeta^p) = 0 \Rightarrow$

ζ ist Nullstelle von $g(x^p)$ Da $f = \mu_{\zeta,\mathbb{Q}}$ gilt,

ist f in $\mathbb{Q}[x]$ ein Teiler von $g(x^p)$. $\overset{f \text{ normiert}}{\Rightarrow}$

f ist Teiler von $g(x^p)$ in $\mathbb{Z}[x] \rightarrow$ Folg. aus Lemma v. Gauß

$\exists h \in \mathbb{Z}[x]$ mit $f h = g(x^p)$.

Seien nun $\bar{f}, \bar{g}, \bar{h}$ die Bilder von f, g, h in $\mathbb{F}_p[x]$.

Lemma 20.6 $\Rightarrow$ $\bar{f} \cdot \bar{h} \overset{(**)}{=} \bar{g}^p$ Sei $\bar{f}_1 \in \mathbb{F}_p[x]$

ein irreduzibler Faktor von $\bar{f}$. $(**) \Rightarrow \bar{f}_1 \mid \bar{g}^p$

$\overset{\bar{f}_1 \text{ irred}}{\Rightarrow}$ $\bar{f}_1 \mid \bar{g}$ s.o. $\Rightarrow f \cdot g = \Phi_n$ Weil Φ_n

$0 \leq k \leq$)

t)

□

ein Teiler von $x^n - 1$ ist, gilt dasselbe für f g

$\Rightarrow \exists\, h_1 \in \mathbb{Z}[x] : f g \cdot h_1 = x^n - 1 \Rightarrow \bar{f}\bar{g}\bar{h}_1 = x^n - \bar{1}$

$\bar{f}_1 \mid \bar{f}$, $\bar{f}_1 \mid \bar{g} \Rightarrow \bar{f}_1^2 \mid (x^n - \bar{1}) \Rightarrow$ Das Polynom $x^n - \bar{1}$ hat in einem alg Abschluss $\mathbb{F}_p^{alg}$ von $\mathbb{F}_p$ mehrfache Nullstellen (nämlich die Nullst. von $\bar{f}_1$). andererseits: $\bar{f}_n = x^n - \bar{1} \Rightarrow$

$\bar{f}_n' = n \cdot x^{n-1} \neq \bar{0}$ (wg. $p \nmid n$) $\Rightarrow ggT(\bar{f}_n, \bar{f}_n') = \bar{1}$

$\Rightarrow x^n - \bar{1}$ hat keine mehrfachen Nullst. in $\mathbb{F}_p^{alg}$ $\lightning$

Jede primitive Einheitswurzel hat die Form ζ^m mit $m \in \mathbb{N}$, $ggT(m, n) = 1$. Schreibe m als Produkt $p_1 \cdot \ldots \cdot p_r$ von

Primzahlen. $ggT(m,n)=1 \Rightarrow p_i \nmid n$ für $1 \leq i \leq r$

Aus (Δ) folgt, dass mit g auch g^{p_1}, $g^{p_1 p_2}$, ... g^m Nullstellen von f sind. $\Rightarrow$ Jede Nullst. von Φ_n ist Nullst. von f. $\Rightarrow$

$f = \Phi_n \cdot g = 1$ $\lightning$

$\square$

Quadratische Reste und Nichtreste

Definition (20.8)

Sei p eine Primzahl und $a \in \mathbb{Z}$. Man nennt a einen quadratischen Rest modulo p, wenn eine Zahl $c \in \mathbb{Z}$ mit

$$a \equiv c^2 \mod p \qquad \text{existiert.}$$

Andernfalls spricht man von einem quadratischen Nichtrest.

Definition des Legendre-Symbols

Definition (20.9)

Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$. Das Legendre-Symbol modulo p ist definiert durch

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{falls } a \text{ quadratischer Rest modulo } p \text{ und } p \nmid a \\ 0 & \text{falls } p \mid a \\ -1 & \text{falls } a \text{ quadratischer Nichtrest modulo } p. \end{cases}$$

Elementare Rechenregeln für das Legendre-Symbol

Lemma (20.10)

Sei p eine ungerade Primzahl, und seien $a, b \in \mathbb{Z}$. Dann gelten für das Legendre-Symbol die folgenden Regeln:

(i) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$ *(Eulersches Kriterium)*

(ii) Aus $a \equiv b \mod p$ folgt $\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)$.

(iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

Ergänzungssätze zum Quadratischen Reziprozitätsgesetz

Satz (20.11)

Für jede ungerade Primzahl p gilt

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{falls } p \equiv 1 \mod 4 \\ -1 & \text{falls } p \equiv 3 \mod 4 \end{cases}$$

und

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{falls } p \equiv 1, 7 \mod 8 \\ -1 & \text{falls } p \equiv 3, 5 \mod 8 \end{cases}$$

Beweis von Satz 20.11, Teil (ii)

zeige noch: $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1, 7 \ (8) \\ -1 & p \equiv 3, 5 \ (8) \end{cases}$ p ungerade Primzahl

$2 = (-i)(2i) = (-i)(1+i)^2$

Eulersches Kriterium $\Rightarrow \left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} = (-i)^{(p-1)/2} (1+i)^{p-1}$

$\equiv (-i)^{(p-1)/2} \frac{(1+i)^p}{(1+i)} \equiv (-i)^{(p-1)/2} \frac{(1-i)}{(1+i)(1-i)} (1+i)^p \equiv$

$\left(\frac{1}{2}(-i)^{(p-1)/2} + \frac{1}{2}(-i)^{(p+1)/2}\right)(1+i^p) \mod p$

Ist $p \equiv 1 \mod 8$, dann folgt $\left(\frac{2}{p}\right) \equiv \left(\frac{1}{2} + \frac{1}{2}(-i)\right)(1+i)$

$\equiv \frac{1}{2}(1-i)(1+i) \equiv \frac{1}{2} \cdot 2 \equiv 1 \mod p \Rightarrow \left(\frac{2}{p}\right) = 1$

Die Behandlung der Fälle $p \equiv k \bmod 8$ für $k \in \{3, 5, 7\}$ läuft analog. $\square$

Das Quadratische Reziprozitätsgesetz

Satz (20.12)

Für zwei beliebige voneinander verschiedene ungerade Primzahlen p, q gilt

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

$$= \begin{cases} 1 & \text{falls } p \equiv 1 \bmod 4 \text{ oder } q \equiv 1 \bmod 4 \\ -1 & \text{falls } p \equiv q \equiv 3 \bmod 4. \end{cases}$$

Anwendungsbeispiel für das QRG

Frage: Ist 103 ein quadratischer Rest modulo 449? (beides Primzahlen)

$$\left(\frac{103}{449}\right) \overset{\uparrow 449 \equiv 1 \,(4)}{=} \left(\frac{449}{103}\right) = \left(\frac{37}{103}\right) \overset{\uparrow 37 \equiv 1 \,(4)}{=}$$

$$\left(\frac{103}{37}\right) \equiv \left(\frac{-8}{37}\right) \equiv \left(\frac{-1}{37}\right)\left(\frac{2}{37}\right)^3 \overset{\uparrow 37 \equiv 1 \,(4)}{=}$$

$$1 \cdot \left(\frac{2}{37}\right) \overset{\uparrow 37 \equiv 5 \,(8)}{=} -1$$

Antwort: nein

Ringe erzeugt durch eine primitive p-te Einheitswurzel

Lemma (20.13)

Seien p und q zwei verschiedene ungerade Primzahlen. Weiter sei

$$\zeta_p = e^{2\pi i/p} \in \mathbb{C}^\times \quad , \quad R = \mathbb{Z}[\zeta_p] \quad \text{und} \quad (q) = qR \ ,$$

das von q in R erzeugte Hauptideal. Dann gelten die folgenden Gleichungen.

(i) $R = \{a_0 + a_1\zeta_p + ... + a_{p-2}\zeta_p^{p-2} \mid a_0, a_1, ..., a_{p-2} \in \mathbb{Z}\}$

(ii) $(q) \cap \mathbb{Z} = q\mathbb{Z}$

Definition der Gauß'schen Summen

Definition (20.14)

Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$. Dann ist die Gauß'sche Summe $g_{a,p} \in \mathbb{Z}[\zeta_p]$ gegeben durch

$$g_{a,p} = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{na}.$$

Rechenregeln für Gauß'sche Summen

Lemma (20.15)

Es seien p, q zwei verschiedene ungerade Primzahlen und $a \in \mathbb{Z}$ mit $p \nmid a$. Dann gelten für die Gauß'schen Summen die folgenden Rechenregeln.

(i) $g_{a,p} = \left(\frac{a}{p}\right) g_{1,p}$

(ii) $g_{1,p}^2 = \left(\frac{-1}{p}\right) p = p^*$

(iii) $g_{1,p}^q \equiv g_{q,p} \bmod (q)$

Dabei bezieht sich die Kongruenz unter (iii) auf den Ring $\mathbb{Z}[\zeta_p]$.

Herleitung des QRG aus Lemma 20.15.

geg: verschiedene ungerade Primzahlen p, q

$$\left(\frac{q}{p}\right) g_{1,p} \overset{(i)}{\equiv} g_{q,p} \overset{(iii)}{\equiv} g_{1,p}^{q} \equiv g_{1,p} \left(g_{1,p}^{2}\right)^{(q-1)/2}$$

$$\overset{(iii)}{\equiv} g_{1,p} (p^*)^{(q-1)/2} \underset{\text{Euler}}{\equiv} g_{1,p} \left(\frac{p^*}{q}\right) \bmod q$$

$$\overset{g_{1,p}}{\Longrightarrow} \left(\frac{q}{p}\right) g_{1,p}^{2} = \left(\frac{p^*}{q}\right) g_{1,p}^{2} \bmod q \overset{(iii)}{\Longrightarrow}$$

$$\left(\frac{q}{p}\right) \cdot p^* \equiv \left(\frac{p^*}{q}\right) \cdot p^* \bmod q \quad (\Delta_2)$$

Sei $l \in \mathbb{Z}$ mit $l \cdot p^* \equiv 1 \bmod q$, multipliziere (Δ_2) mit l.

$\left(\frac{2}{\cdot}\right) = -1$ Antarktis rein

15.

$p \cdot q$

$(g^{2})^{(q-1)/2}$

od q

$q \overset{(iii)}{\Longrightarrow}$

$\Delta_2)$

multi –

$$\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \bmod q \Longrightarrow \left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = \left(\frac{\left(\frac{-1}{p}\right)}{q}\right) \cdot \left(\frac{p}{q}\right)$$

$\uparrow$ $p^* = \left(\frac{-1}{p}\right) \cdot p$

$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) \in \{\pm 1\}$

$\Longrightarrow$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{\left(\frac{-1}{p}\right)}{q}\right) = \begin{cases} 1 & \text{falls } p \equiv 1 \bmod 4 \\ & \text{oder } q \equiv 1 \bmod 4 \\ -1 & p \equiv q \equiv 3 \bmod 4 \end{cases}$$