Prof. Dr. Benjamin Klopsch
Dr. Philip Möller
Wintersemester 2024–25

Zahlentheorie I – Blatt 6

Vorstellung/Abgabe der Lösungen in der Übungsstunde am 18.11.2024, ab 14.30 Uhr

Bitte reichen Sie Lösungen zu der Aufgabe 6.1 ein; weitere Informationen auf

`http://reh.math.uni-duesseldorf.de/~internet/ZahlenI_WS2425/`.

Aufgabe 6.1 (8 Punkte)

Für $n \in \mathbb{N}$ sei $\zeta = \exp(2\pi i/n)$, und es bezeichne Φ_n das $n$te Kreisteilungspolynom, also

$$\Phi_n = \prod_{\substack{1 \le k \le n \\ \mathrm{ggT}(k,n)=1}} \left(X - \zeta^k\right) \in \mathbb{C}[X] \qquad \text{vom Grad } \varphi(n).$$

(a) Erläutern Sie, wieso $X^n - 1 = \prod_{d|n} \Phi_d$ gilt, und folgern Sie, daß $\Phi_n \in \mathbb{Z}[X]$ ist.

(b) Es bezeichne $\mu\colon \mathbb{N} \to \{0, 1, -1\}$ die Möbiusfunktion.[1] Zeigen Sie: In $\mathbb{Q}(X)$, dem Quotientenkörper von $\mathbb{Z}[X]$, gilt die Umkehrformel

$$\Phi_n = \prod_{d|n} \left(X^d - 1\right)^{\mu(n/d)}.$$

Hinweis. Es genügt, zu zeigen, daß die vermuteten Ausdrücke Ψ_d für Φ_d die definierende Gleichung $X^n - 1 = \prod_{d|n} \Psi_d$ erfüllen.

(c) Folgern Sie aus (b): Ist n_0 der quadratfreie Anteil von n, d. h. das Produkt der verschiedenen Primteiler von n, und $n = n_0 m$, so gilt $\Phi_n = \Phi_{n_0}(X^m)$.

(d) Leiten Sie aus (b) die folgende praktische Beziehung her:

$$\Phi_n \equiv \prod_{d|n} \left(1 - X^d\right)^{\mu(n/d)} \qquad \text{in } \mathbb{Z}[[X]] \text{ modulo } X^{\varphi(n)+1}\mathbb{Z}[[X]].$$

(e) Zeigen Sie, daß Φ_n für $n \ge 2$ palindromisch ist, d. h., $X^{\varphi(n)}\Phi_n(X^{-1}) = \Phi_n$ gilt, und bestimmen Sie für $n \ge 3$ mittels der Formel aus (c) die äußersten drei Koeffizienten von $\Phi_n = f_0 X^{\varphi(n)} + f_1 X^{\varphi(n)-1} + f_2 X^{\varphi(n)-2} + \ldots + f_2 X^2 + f_1 X + f_0$ als

$$f_0 = 1, \qquad f_1 = -\mu(n), \qquad f_2 = \begin{cases} \frac{1}{2}\big(\mu(n) - 1\big)\mu(n) - \mu(n/2) & \text{falls } n \equiv_2 0, \\ \frac{1}{2}\big(\mu(n) - 1\big)\mu(n) & \text{falls } n \equiv_2 1. \end{cases}$$

Folgern Sie: $f_0, f_1, f_2 \in \{0, 1, -1\}$.

(f) Bestimmen Sie mithilfe der Formel aus (c) den Koeffizienten von X^7 in Φ_{105} und verifizieren Sie so, daß dieser nicht in $\{0, 1, -1\}$ liegt.[2]

Hinweis. Hier können Sie sogar modulo X^8 rechnen!

[1] Es ist $\mu(n) = (-1)^r$, falls $n = p_1 \cdots p_r$ quadratfrei und Produkt von $r \in \mathbb{N}_0$ paarweise verschiedenen Primzahlen ist, und $\mu(n) = 0$, falls n nicht quadratfrei ist.

[2] Schur zeigte 1931 (in einem Brief an Landau), daß Koeffizienten von Kreisteilungspolynomen betragsmäßig beliebig große Werte annehmen können.

Aufgabe 6.2

Für $n \in \mathbb{N}$ sei $\zeta = \exp(2\pi i/n)$, wie in der vorherigen Aufgabe, und $\Phi_n \in \mathbb{Z}[X]$ bezeichne das $n$te Kreisteilungspolynom.

(a) Zeigen Sie, daß Φ_n irreduzibel über $\mathbb{Q}$ ist, oder gleichbedeutend: $\Phi_n = \mathrm{Minpol}_{\mathbb{Q}}(\zeta)$.

Hinweis. Sei $f = \mathrm{Minpol}_{\mathbb{Q}}(\zeta)$ und $X^n - 1 = fg$; nach dem Lemma von Gauß (welchem?) sind $f, g \in \mathbb{Z}[X]$. Es genügt, zu zeigen: Für Primzahlen p mit $p \nmid n$ gilt $f(\zeta^p) = 0$. (Wieso?) Widerspruchsannahme: $f(\zeta^p) \neq 0$. Dann ist ζ Nullstelle von $g(X^p)$, also $g(X^p) = fh$ für geeignetes $h \in \mathbb{Z}[X]$. Rechnen Sie nun modulo p, um einen Widerspruch herzuleiten.

(b) Folgern Sie: $K = \mathbb{Q}(\zeta)$ ist galoissch über $\mathbb{Q}$ und $\mathrm{Gal}(K\,|\,\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

(c) Bestimmen Sie einen Zahlkörper k dergestalt, daß k galoissch über $\mathbb{Q}$ mit $\mathrm{Gal}(k\,|\,\mathbb{Q}) \cong C_{10} \times C_{20}$ ist. Geben Sie explizit $\alpha \in k$ mit $k = \mathbb{Q}(\alpha)$ an.

Aufgabe 6.3

Sei $K\,|\,k$ eine endliche galoissche Körpererweiterung mit unendlichem Grundkörper, und sei $G = \mathrm{Gal}(K\,|\,k)$. Zeigen Sie: Dann existiert eine *Normalbasis* für $K\,|\,k$, d. h., es existiert ein $\alpha \in K$ dergestalt, daß die Konjugierten von α über k – also die Elemente α^σ, $\sigma \in G$ – eine k-Basis für K bilden.

Hinweis. Überlegen Sie sich zunächst, daß es genügt, ein $\alpha \in K$ zu finden, für das gilt:

$$\det\big((\alpha^{\sigma\tau^{-1}})_{\sigma,\tau\in G}\big) \neq 0.$$

Schreiben Sie $K = k(\beta)$ und $f = \mathrm{Minpol}_k(\beta) \in k[X]$. Setzen Sie $g = f/(X-\beta) \in K[X]$ und verifizieren Sie, daß das Polynom

$$h = \det\big((g(X)^{\sigma\tau^{-1}})_{\sigma,\tau\in G}\big) \in K[X]$$

an der Stelle β nicht verschwindet; hierbei sind Körperautomorphismen koeffizientenweise auf Polynome anzuwenden. Beenden Sie den Beweis ähnlich wie für den Satz vom primitiven Element.

Bemerkung. Die Existenz von Normalbases ist auch für galoissche Erweiterungen endlicher Körper gegeben, verlangt aber eine andersgeartete Beweisführung.