Algebra II

Serie 24

Galoisgruppen von Kreisteilungspolynomen — Besprechung 31. Mai

---

142. Zeige: Die Nullstellen des Polynoms $X^5 - 6X + 3 \in \mathbb{Q}[X]$ sind nicht durch Radikale ausdrückbar.

Sei d eine positive natürliche Zahl. Sei μ_d die Menge der primitiven d-ten Einheitswurzeln in $\mathbb{C}$. Definiere das d-te Kreisteilungspolynom als

$$\Phi_d := \prod_{\xi \in \mu_d} (X - \xi).$$

143. *(Irreduzibilität des Kreisteilungspolynoms)* Sei n eine positive ganze Zahl und sei $f \in \mathbb{Z}[X]$ ein normierter irreduzibler Faktor von $X^n - 1$ mit Nullstelle $\xi \in \mathbb{C}$.

(a) Zeige: Für jede natürliche Zahl k existiert ein eindeutiges Polynom $g_k \in \mathbb{Z}[X]$ mit $\deg(g_k) < \deg(f)$ und $f(\xi^k) = g_k(\xi)$.
Zeige ausserdem, dass die Menge $\{g_k : k \in \mathbb{Z}_{\geq 0}\}$ endlich ist.

(b) Sei $a := \sup\{|u| : u \text{ ist Koeffizient eines } g_k\}$. Zeige: Ist $k = p$ prim, so teilt p alle Koeffizienten von g_p. Schliesse daraus, dass für alle $p > a$ das Polynom g_p gleich Null ist. [*Hinweis:* $f(\xi^p) = f(\xi^p) - f(\xi)^p$]

(c) Folgere: Wenn alle Primfaktoren einer ganzen Zahl m grösser als a sind, dann gilt $f(\xi^m) = 0$.

(d) Zeige: Für jede zu n teilerfremde ganze Zahl r gilt $f(\xi^r) = 0$. [*Hinweis:* Betrachte $m := r + n \prod_{p \leq a, p \nmid r} p$]

(e) Sei Φ_n das n-te Kreispolynom, das heisst das normierte Polynom, das genau die primitiven n-ten Einheitswurzeln als einfache Nullstellen hat.
Zeige:
$$\prod_{0<d,\, d|n} \Phi_d(X) = X^n - 1$$
und folgere, dass für alle n das Polynom Φ_n ganzzahlige Koeffizienten hat.

(f) Zeige, dass das n-te Kreisteilungspolynom Φ_n irreduzibel ist.

144. Ziel dieser Aufgabe ist zu zeigen, dass für primitive n-te Einheitswurzeln ξ gilt

$$\operatorname{Gal}(\mathbb{Q}(\xi) : \mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

Insbesondere erhalten wir $|\operatorname{Gal}(\mathbb{Q}(\xi) : \mathbb{Q})| = \varphi(n)$. Im Folgenden sei $n \geq 2$ eine natürliche Zahl und $\xi \in \mathbb{C}$ eine primitive n-te Einheitswurzel. Sei G die Galoisgruppe von $X^n - 1$ über $\mathbb{Q}$.

(a) Zeige: $G \leq (\mathbb{Z}/n\mathbb{Z})^*$. Insbesondere ist G abelsch.

(b) Bestimme $\varPhi_d$ für $d = 1, 2, 3, 4, 8$.

(c) Zeige: $G \cong (\mathbb{Z}/n\mathbb{Z})^*$.

145. Sei n eine positive ganze Zahl und sei $\xi \in \mu_n$.

(a) Zeige: Für jeden Zwischenkörper K der Erweiterung $\mathbb{Q}(\xi) : \mathbb{Q}$ ist die Erweiterung $K : \mathbb{Q}$ normal und hat abelsche Galoisgruppe.

(b) Folgere: Falls $\varphi(n)$ eine Zweierpotenz ist, so ist das regelmässige n-Eck konstruierbar (dies vervollständigt den Beweis von Satz 21.6 der Vorlesung).