8. Übung zur Vorlesung

Algebra I: Körper, Ringe, Moduln

im Wintersemester 2015/2016

Erinnerung: Eine *primitive* n-te Einheitswurzel in einem Körper K ist ein Element $\zeta \in K^*$ mit multiplikativer Ordnung n. Äquivalent kann man fordern, dass

- $\zeta^n = 1$ und $\zeta^d \neq 1$ für jeden echten Teiler d von n, oder
- $\zeta^n = 1$ und $\zeta^{n/p} \neq 1$ für jeden Primteiler p von n, oder
- die multiplikativ aufgespannte Gruppe $\langle\zeta\rangle \subset K^*$ hat Ordnung n.

Aufgabe 1 (Kreisteilungspolynome) — Das n-te *Kreisteilungspolynom* $\Phi_n(x)$ ist das Polynom

$$\Phi_n(x) := \prod_{\substack{\zeta \text{ primitive n-te} \\ \text{Einheitswurzel von } \mathbb{C}}} (x - \zeta).$$

(a) Zeige die (Rekursions-)gleichung
$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

(b) Bestimme die ersten 12 Kreisteilungspolynome.

(c) Zeige, dass $\Phi_n(x) \in \mathbb{Z}[x]$ ganzzahlige Koeffizienten besitzt.

(d) Zeige, dass Φ_n den Grad $\varphi(n)$ besitzt und folgere ein weiteres Mal die Gleichung $n = \sum_{d|n} \varphi(d)$.

[Wir zeigen später, dass Φ_n irreduzibel in $\mathbb{Q}[x]$ ist.] Ausgehend von den Berechnungen in b) kann man auf die folgenden Vermutungen kommen. Beweise sie.

(e) Für n ungerade ist $\Phi_{2n}(x) = \Phi_n(-x)$. Für n gerade ist $\Phi_{2n}(x) = \Phi_n(x^2)$.

Aufgabe 2 (Separabilität) — Teste die folgenden Polynome auf Separabilität:

(a) $x^4 + 3x^3 - 12x^2 - 20x + 48 \in \mathbb{Q}[x]$.

(b) $x^3 + 5x^2 - 2x - 24 \in \mathbb{Q}[x]$.

(c) $x^3 + 5x^2 - 2x - 24 \in \mathbb{F}_5[x]$.

(d) $x^{15} + 5x^{10} - 2x^5 - 25 \in \mathbb{F}_5[x]$.

Aufgabe 3 (Das Kompositum zweier Erweiterungen) — Es seien L/K und L'/K zwei Körpererweiterungen eines Körpers K, die in einem gemeinsamen Oberkörper F enthalten sind. Zeige, dass das *Kompositum* $LL' := \{xx' \mid x \in L, x' \in L'\}$ eine Körpererweiterung von K, L und L' ist. Zeige außerdem, dass das Kompositum algebraisch/separabel/endlich über K ist, falls L, L' algebraisch/separabel/endlich über K sind. Außerdem gilt $[LL' : K] \leq [L : K] \cdot [L' : K]$.