# Lösung 11

## Kreisteilungspolynome

1. Berechnen Sie die Zerlegung in irreduzible Faktoren von $\Phi_7(X)$ in $\mathbb{F}_{29}[X]$, wobei $\Phi_n(X)$ das $n$-te Kreisteilungspolynom bezeichnet.

2. Seien $p$ eine ungerade Primzahl und $r \geqslant 1$. Zeigen Sie, dass
$$(\mathbb{Z}/p^r\mathbb{Z})^\times \cong \left(\mathbb{Z}/p^{r-1}\mathbb{Z}\right) \times (\mathbb{Z}/(p-1)\mathbb{Z})\,.$$
Ist diese Gruppe zyklisch?

3. Zeigen Sie, dass
$$\Phi_n(X) = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)},$$
wobei $\mu : \mathbb{N}^\times \to \{-1, 0, 1\}$ die Möbiusfunktion bezeichnet.

4. Seien $E = \mathbb{F}_p(X, Y)$ und $K = \mathbb{F}_p(X^p, Y^p)$. Zeigen Sie, dass
   (a) $[E : K] = p^2$, und
   (b) $f^p \in K$ für alle $f \in E$.

   Folgern Sie, dass $E|K$ keine einfache Körpererweiterung ist.

   *Lösung*:

   (a) Wir zeigen, dass die Zwischenerweiterung $L := \mathbb{F}_p(X, Y^p)$ über $K$ gerade Grad $p$ hat. Das Polynom $(T - X)^p = T^p - X^p$ ist irreduzibel über $\mathbb{F}_p(Y^p)[X^p]$ nach Eisenstein und nach Gauss auch über dem Quotientenkörper $\mathbb{F}_p(X^p, Y^p)$. Daraus folgt, dass $L$ über $K$ Grad $p$ hat. Ein ähnliches Argument gibt, dass $E$ über $L$ Grad $p$ hat, und damit ist nach der Multiplizität der Grade $[E : K] = p^2$.

   (b) Sei $f \in \mathbb{F}_p(X, Y)$ und schreibe
$$f = \frac{\sum_{i,j} a_{i,j} X^i Y^j}{\sum_{i,j} b_{i,j} X^i Y^j}$$
mit $a_{i,j}$ und $b_{i,j} \in \mathbb{F}_p$. Dann ist
$$f^p = \frac{\sum_{i,j} a_{i,j}^p X^{ip} Y^{jp}}{\sum_{i,j} b_{i,j}^p X^{ip} Y^{jp}},$$
und somit in $K$.

Daraus folgt direkt, dass für jedes $f \in E$

$$[K(f) : K] \leqslant p,$$

und damit kann die Erweiterung $E|K$ nicht einfach sein.

5. Sei $p$ eine Primzahl mit $\mathrm{ggT}(p, n) = 1$. Zeigen Sie, dass

$$\Phi_{pn}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)}.$$

*Lösung*: Wir müssen zeigen, dass

$$\Phi_n(X)\Phi_{pn}(X) = \Phi_n(X^p).$$

Die linke Seite ist quadratfrei und die Nullstellen sind gerade die primitiven $n$-ten und $np$-ten Einheitswurzeln. Ist $\zeta$ eine primitive $n$-te Einheitswurzel, so gilt dies auch für $\zeta^p$ da $p \nmid n$. Ist $\zeta$ eine primitive $np$-te Einheitswurzel, so ist $\zeta^p$ eine primitive $n$-te Einheitswurzel. Andererseits, ist $\zeta^p$ eine primitive $n$-te Einheitswurzel, so hat $\zeta$ Ordnung $n$ oder $np$.

Zusammenfassend sind die Nullstellen von $\Phi_n(X)\Phi_{pn}(X)$ die $p$-ten Wurzeln der primitive $n$-ten Einheitswurzeln. Aber diese sind genau die Nullstellen von $\Phi_n(X^p)$.

Aus der Vorlesung (siehe Seite IV-50) wissen wir, dass $\deg(\Phi_n) = \varphi(n)$. Damit gilt

$$\begin{aligned} \deg(\Phi_n(X)\Phi_{pn}(X)) &= \varphi(n) + \varphi(n)\varphi(p) = \varphi(n) + \varphi(n)(p-1) = \varphi(n)p \\ \deg(\Phi_n(X^p) &= \varphi(n)p, \end{aligned}$$

und somit haben die beiden Polynome den gleichen Grad, sind monisch und haben die gleichen Nullstellen. Damit sind sie gleich.

6. Sei $p$ eine Primzahl mit $\mathrm{ggT}(p, n) = 1$. Zeigen Sie, dass die monischen irreduziblen Faktoren von $\Phi_n(X)$ in $\mathbb{F}_p[X]$ verschieden sind, den gleichen Grad haben und, dass dieser gerade gleich der Ordnung von $p \bmod n$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ ist.

*Lösung*: Siehe Vorlesung 12, Theorem IV.34.