Lösung 12

Kreisteilungspolynome

1. Sei p eine ungerade Primzahl. Zeigen Sie, dass es genau eine Zwischenerweiterung $\mathbb{Q} \subset L \subset \mathbb{Q}[p]$ gibt mit $[L : \mathbb{Q}] = 2$.

2. Zeigen Sie, dass $\Phi_8(X) = X^4 + 1$ gilt, und dass Φ_8 reduzibel in $\mathbb{F}_p[X]$ für jede Primzahl p ist.

3. Zeigen Sie, dass
$$(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \left(\mathbb{Z}/2^{r-2}\mathbb{Z}\right)$$
für $r \geqslant 2$.

4. Sei $f \in K[X]$ ein separables Polynom, $g \in K[X]$ ein irreduzibler Faktor sowie $K \subset L \subset F$, wobei F bzw. L ein Zerfällungskörper von f bzw. g sind. Zeigen Sie, dass $\mathrm{Gal}(F|K)$ transitiv auf $R(g)$ wirkt.

   Lösung: Seien α und β Nullstellen von g in L. Da f separabel ist hat g nur verschiedene Nullstellen. Nach Korollar II.23 existiert $\varphi : L \to L$ mit $\varphi(\alpha) = \beta$ und φ erweitert die Identität auf K. Da sowohl F als auch L normale Erweiterungen sind folgt aus Theorem II.26, dass der Homomorphismus $\mathrm{Gal}(F|K) \to \mathrm{Gal}(L|K)$ surjektiv ist. Damit existiert $\Phi \in \mathrm{Gal}(F|K)$ der eingeschränkt auf L gleich φ ist. Daraus folgt, $\Phi(\alpha) = \varphi(\alpha) = \beta$, was zu zeigen war.

5. Sei p eine Primzahl und $r \geqslant 1$. Zeigen Sie, dass
$$\Phi_{p^r}(T) = \frac{T^{(p^r)} - 1}{T^{(p^{r-1})} - 1}.$$

   Lösung: Wir bemerken zunächst, dass die rechte Seite gleich $\Phi_p(T^{p^{r-1}})$ ist. Wir machen eine Induktion über r. Für $r = 1$ ist die Aussage bewiesen (siehe Algebra 1, Serie 13, Aufgabe 6 (f)). Es gilt
$$\Phi_{p^r}(T) = \frac{\prod_{d|p^r} \Phi_{p^r}(T)}{\prod_{d|p^r, d<p^r} \Phi_{p^r}(T)} = \frac{T^{p^r} - 1}{\prod_{k=0}^{r-1} \Phi_{p^k}(T)}.$$
   Nun wenden wir die Induktionsannahme an und erhalten für alle $k = 1, \ldots, r-1$
$$\Phi_{p^k}(T) = \frac{T^{p^k} - 1}{T^{p^{k-1}} - 1}.$$

Das Produkt im obigen Nenner vereinfacht sich also zu

$$\prod_{k=0}^{r-1} \Phi_{p^k}(T) = (T-1) \prod_{k=1}^{r-1} \frac{T^{p^k}-1}{T^{p^{k-1}}-1} = T^{p^{r-1}},$$

was zu zeigen war.

6. Zeigen Sie, dass $\Phi_{p^r}(X) \in \mathbb{Q}[X]$ irreduzibel ist.

   Hinweis: Wenden Sie das Eisensteinkriterium auf $\Phi_{p^r}(X+1)$ an.

   Lösung: Aus Aufgabe 5 wissen wir bereits, dass

   $$\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$$

   Wir wollen das Eisensteinkriterium mit der Primzahl p auf $\Phi_{p^r}(X+1)$ anwenden. Es ist

   $$\Phi_{p^r}(X+1) = \frac{(X^{p^{r-1}}+1)^p - 1}{(X^{p^{r-1}}+1)-1} \equiv \frac{(X^{p^r}+1)-1}{X^{p^{r-1}}} \bmod p \equiv X^{p^{r-1}(p-1)} \bmod p.$$

   Daraus folgt, dass p alle Koeffizienten ausser den Leitkoeffizienten teilt. Es bleibt zu zeigen, dass p^2 nicht den konstanten Koeffizienten a_0 von $\Phi_{p^r}(X+1)$ teilt. Es ist $a_0 = \Phi_{p^r}(0+1) = \Phi_{p^r}(1) = \Phi_p(1) = \sum_{i=0}^{p-1} 1 = p$, und damit teilt p^2 nicht a_0 und wir haben gezeigt, dass $\Phi_{p^r}(X)$ irreduzibel ist.