Algebra: Blatt 2

Irene Bouw
Michael Eskin

Abgabe: 08.11.2013, vor der Übung

Aufgabe 1 *(1+2+1+3 Punkte)*
Sei $\ell \in \mathbb{N}$ eine Primzahl und

$$\Phi_\ell(X) = \frac{X^\ell - 1}{X - 1} = X^{\ell-1} + \ldots + 1 \in \mathbb{Z}[X].$$

In der Vorlesung wurde gezeigt, dass $\Phi_\ell \in \mathbb{Z}[X]$ irreduzibel ist. Wir bestimmen die Faktorisierung von $\Phi_\ell(X) \in \mathbb{F}_p[X]$.

(a) Sei $p = \ell$. Zeigen Sie, dass $\Phi_\ell(X) \equiv (X-1)^{\ell-1} \in \mathbb{F}_\ell[X]$.

(b) Sei $p \neq \ell$ und sei $f > 0$ minimal sodass $p^f \equiv 1 (\operatorname{mod} \ell)$ (d.h. $f = \operatorname{ord}_\ell(p)$ ist die Ordnung von p in $(\mathbb{Z}/\ell\mathbb{Z})^*$). Zeigen Sie, dass f die kleinste natürliche Zahl ist, sodass $\mathbb{F}_{p^f}$ eine primitive ℓ-te Einheitswurzel $\zeta \in \mathbb{F}_{p^f}^*$ enthält. Was ist der Zerfällungskörper von Φ_ℓ über $\mathbb{F}_p$?

(c) Sei $a \in \mathbb{Z}$ teilerfremd zu ℓ und $p \neq \ell$. Zeigen Sie, dass $\mathbb{F}_{p^f} \simeq \mathbb{F}_p(\zeta) = \mathbb{F}_p(\zeta^a)$.

Hinweis: Zeigen Sie, dass die Ordnung von ζ^a genau ℓ ist.

(d) Sei $p \neq \ell$. Schließen, dass Φ_ℓ in $\mathbb{F}_p[X]$ in $\frac{\ell-1}{f}$ irreduzible Faktoren von Grad f zerfällt.

Hinweis: Sei k ein endlicher Körper mit $\operatorname{Char}(k) = p > 0$, $\operatorname{Frob}_p : k \to k$ der Frobeniushomomorphismus sowie $\operatorname{Frob}_p : k[X] \to k[X]$ der induzierte Frobeniushomomorphismus angewandt auf die Koeffizienten eines Polynoms. Zeigen Sie: $f \in \mathbb{F}_p[X]$ genau dann, wenn $\operatorname{Frob}_p(f) = f$.

Aufgabe 2 *(2 Punkte)*
Bestimmen Sie den Zerfällungskörper L des Polynoms $X^4 + 2X^2 - 2$ über $\mathbb{Q}$ sowie den Grad der Körpererweiterung $L/\mathbb{Q}$.

Aufgabe 3 *(5 Punkte)*
Sei L der Zerfällungskörper eines Polynoms $f \in K[X]$ über K.

Zeigen Sie, dass jedes irreduzible Polynom $g \in K[X]$, welches eine Nullstelle in L besitzt, bereits über L in Linearfaktoren zerfällt.

Hinweis: Benutzen Sie Satz 1.1.8 und Satz 2.2.5.

Anmerkung: Eine Körpererweiterung L/K mit der obigen Eigenschaft wird *normale Körpererweiterung* genannt.

Bitte wenden!

Aufgabe 4 *(1+1+1+1+1 Punkte)*
Seien $D_1, D_2 \in \mathbb{Q}$ keine Quadrate und $D_1 D_2$ sei ebenfalls kein Quadrat.

(a) Zeigen Sie: $L := \mathbb{Q}(\sqrt{D_1} + \sqrt{D_2}) = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$.

(b) Bestimmen Sie alle Elemente von $\mathrm{Aut}_{\mathbb{Q}}(L)$.

(c) Zeigen Sie, dass $\mathrm{Aut}_{\mathbb{Q}}(L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Es sei $f = X^4 + X + 1 \in \mathbb{F}_2[X]$. Dieses Polynom ist nach Vorlesung irreduzibel.

(d) Bestimmen Sie alle Nullstellen von f in $L = \mathbb{F}_{2^4} \simeq \mathbb{F}_2[X]/(f)$.

(e) Zeigen Sie, dass $\mathrm{Frob}_p : \mathbb{F}_{2^4} \to \mathbb{F}_{2^4}, a \mapsto a^2$ ein Erzeuger von $\mathrm{Aut}_{\mathbb{F}_2}(\mathbb{F}_{2^4})$ ist. Schließen Sie, dass $\mathrm{Aut}_{\mathbb{F}_2}(\mathbb{F}_{2^4}) \simeq \mathbb{Z}/4\mathbb{Z}$.