Universität Ulm

Prof. Dr. S. Wewers
WS 2013/2014

Elemente der Algebra: Blatt 15

A1. Zerlegen Sie das Polynom f im Ring R in irreduzible Faktoren.

(a) $f = x^4 + x^2 + 1$, $R = \mathbb{F}_2[x]$ (+4)

(b) $f = x^4 + x^2 + 1$, $R = \mathbb{F}_4[x]$ (+4)

(c) $f = x^3 + x + 1$, $R = \mathbb{F}_3[x]$ (+4)

(d) $f = x^4 - x^2 + 1$, $R = \mathbb{F}_5[x]$ (+4)

(e) $f = x^6 - 1$, $R = \mathbb{F}_{25}[x]$ (+4)

A2. (a) Bestimmen Sie alle irreduziblen Polynome in $\mathbb{F}_2[x]$ von Grad 4. (Hinweis: Beachten Sie Aufgabe A3.) (+8)

(b) Betrachten Sie das irreduzible Polynom $f := x^4 + x + 1 \in \mathbb{F}_2[x]$. Sei α eine Nullstelle von f in $\mathbb{F}_{16}$. Wie Sie in der Vorlesung gesehen haben ist dann $\mathbb{F}_{16} = \mathbb{F}_2[\alpha]$, da f irreduzibel ist. Bestimmen Sie über $\mathbb{F}_2$ das Minimalpolynom von α^2 und α^4. (+5)

(c) Finden Sie einen Erzeuger der zyklischen Gruppe $\mathbb{F}_{16}^\times$. (+5)

(d) Nach Aufgabe A4 gilt $\mathbb{F}_4 \subseteq \mathbb{F}_{16}$. Finden Sie ein Element $\gamma \in \mathbb{F}_{16}$ sodass $\mathbb{F}_4 = \mathbb{F}_2[\gamma]$. (+5)

A3. Sei p eine Primzahl. Es bezeichne $P(n)$ die Menge der normierten irreduziblen Polynome vom Grad n in $\mathbb{F}_p[x]$.

(a) Sei $n \in \mathbb{N}$ und $f \in P(n)$. Zeigen Sie, dass f das Polynom $x^{p^n} - x$ teilt. (Hinweis: Betrachten Sie die Polynome als Elemente von $\mathbb{F}_{p^n}[x]$.) (+7)

(b) Sei $n \in \mathbb{N}$, d ein Teiler von n und sei f in $P(d)$. Zeigen Sie, dass f das Polynom $x^{p^n} - x$ teilt. (Hinweis: Verwenden Sie das Ergebnis aus Aufgabe A4.) (+3)

(c) Sei $n \in \mathbb{N}$. Zeigen Sie, dass gilt (+7)

$$x^{p^n} - x = \prod_{d|n} \prod_{f \in P(d)} f.$$

(d) Bestimmen Sie für $p = 2$ die Mächtigkeit von $P(4)$. (+3)

(e) Bestimmen Sie für $p = 3$ die Mächtigkeit von $P(3)$. (+3)

A4. Sei p eine Primzahl, n, m in $\mathbb{N}$. In dieser Aufgabe soll gezeigt werden, dass der Körper $\mathbb{F}_{p^m}$ genau dann im Körper $\mathbb{F}_{p^n}$ enthalten ist, wenn $m|n$.

(a) Sei $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ der durch $\alpha \mapsto \alpha^p$ gegebene Automorphismus von $\mathbb{F}_{p^n}$ (siehe Satz 1 (iii) aus der Vorlesung vom 4.2.). Es lässt sich φ als Gruppenelement in der Gruppe der Automorphismen von $\mathbb{F}_{p^n}$ auffassen. Zeigen Sie, dass φ in dieser Gruppe Ordnung n hat, d.h. zeigen Sie, dass (+6)

$$n = \min\{k \in \mathbb{N} : \varphi^k = \mathrm{Id}\}.$$

(b) Nehmen Sie an, dass $\mathbb{F}_{p^m}$ ein Teilkörper von $\mathbb{F}_{p^n}$ ist. Zeigen Sie, dass m dann n teilt. (Hinweis: Verwenden Sie die Einschränkung von φ auf $\mathbb{F}_{p^m}$ und die vorige Teilaufgabe.) (+6)

(c) Nehmen Sie nun an, dass $m|n$. Zeigen Sie, dass dann $\mathbb{F}_{p^m}$ ein Teilkörper von $\mathbb{F}_{p^n}$ ist. (Hinweis: Argumentieren Sie wie im Beweis des Satzes aus der Vorlesung: Die Teilmenge der $\alpha \in \mathbb{F}_{p^n}$ mit $\alpha^{p^m} = \alpha$ ist ein Teilkörper.) (+10)

Abgabe bitte nur zu zweit am 10.2.2014 in der Übung. Beschriften Sie ihre Abgabe mit Namen und Matrikelnummer (oder SLC-Namen) beider Studenten. **Achten Sie auf einen ausreichenden Seitenrand für die Korrektur.**