Übungen zur Vorlesung Algebra 2

Institut für Reine Mathematik SS 08 – Blatt 01

Abgabetermin: Donnerstag 24.04.2008 um 12:15 Uhr vor Beginn der Vorlesung

---

1. Zeigen Sie:

   (a) $\mathbb{F}_{q^m} \cap \mathbb{F}_{q^n} = \mathbb{F}_{q^d}$, wobei $d := \mathrm{ggT}(m,n)$.

   (b) $\mathbb{F}_{q^m}\mathbb{F}_{q^n} = \mathbb{F}_{q^k}$, wobei $k := \mathrm{kgV}(m,n)$.

2. Sei q eine Primzahlpotenz. Wir definieren *Norm*, *Spur* und *Frobenius* wie folgt:

$$\begin{array}{rlll} & l_x : & \mathbb{F}_{q^m} \to \mathbb{F}_{q^m} ; & z \mapsto x \cdot z, \\ \textit{(Spur)} & \mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}} : & \mathbb{F}_{q^m} \to \mathbb{F}_q ; & x \mapsto \mathrm{Tr}(l_x), \\ \textit{(Norm)} & \mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}} : & \mathbb{F}_{q^m} \to \mathbb{F}_q ; & x \mapsto \det(l_x), \\ \textit{(Frobenius)} & F_q : & \mathbb{F}_{q^m} \to \mathbb{F}_{q^m} ; & x \mapsto x^q. \end{array}$$

   Zeigen Sie die folgenden Aussagen:

   (a) Für alle $x \in \mathbb{F}_{q^m}$ gilt:

$$\mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}}(x) = \sum_{i=1}^{m} F_q^i(x) = x^q + x^{q^2} + \cdots + x^{q^m}.$$

   (b) Für alle $x \in \mathbb{F}_{q^m}$ gilt:

$$\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}}(x) = \prod_{i=1}^{m} F_q^i(x) = x^q \cdot x^{q^2} \cdots x^{q^m} = x^{(q^m-1)/(q-1)}.$$

   (c) Bestimmen Sie $\mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}}(x)$ und $\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}}(x)$ für $x \in \mathbb{F}_q$.

   (d) $\mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ ist surjektiv.

   (e) $\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}} : \mathbb{F}_{q^m}^\times \to \mathbb{F}_q^\times$ ist surjektiv.

3. Betrachten Sie das Polynom

$$\Phi(T) := T^6 + T^3 + 1 \in \mathbb{F}_2[T].$$

   (a) Zeigen Sie zunächst, dass $\Phi(T)$ irreduzibel ist.

   Betrachten Sie nun den Körper

$$\mathbb{F}_{64} := \mathbb{F}_2[T]/(\Phi(T)), \text{ und } \alpha := \overline{T} \in \mathbb{F}_{64}.$$

   (b) Bestimmen Sie $\mathrm{ord}_{\mathbb{F}_{64}^\times}(\alpha)$. Ist α Erzeuger von $\mathbb{F}_{64}^\times$?

   (c) Stellen Sie $1/(1+\alpha^7)$ und $\alpha^{37} + \alpha^{51}$ jeweils als Polynom in α von möglichst kleinem Grad dar.

   (d) Bestimmen Sie $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_{64}}(\alpha)$ und $\mathrm{N}_{\mathbb{F}_2}^{\mathbb{F}_{64}}(\alpha^{13})$.