# Musterlösung Serie 18

ENDLICHE KÖRPER II

---

**99**. Sei $p$ eine Primzahl und sei $q = p^n$ für eine positive ganze Zahl $n$.

(a) Zeige: Ein irreduzibles Polynom $f \in \mathbb{F}_p[X]$ teilt $X^q - X$ in $\mathbb{F}_p[X]$ genau dann, wenn sein Grad ein Teiler von $n$ ist.

(b) Sei $I_d$ die Menge der normierten, irreduziblen Polynome vom Grad $d$ in $\mathbb{F}_p[X]$. Beweise die Gleichung

$$X^q - X = \prod_{d|n} \prod_{f \in I_d} f.$$

(c) Sei $r_d := |I_d|$. Folgere aus (b), dass $\sum_{d|n} \big(d \cdot r_d\big) = q$ gilt.

(d) Zeige: Das Polynom $X^q - X$ ist über $\mathbb{F}_p$ das Produkt aller normierten irreduziblen Polynome vom Grad $m$ mit $m \mid n$.

(e) Zeige: Die Summe der Grade der irreduziblen Polynome aus (d) ist gleich $q$.

*Lösung*: (a) Mit Satz 16.5 besitzt ein irreduzibles Polynom $f \in \mathbb{F}_p[X]$ im Zerfällungskörper keine mehrfachen Nullstellen. Also ist $f$ genau dann ein Teiler von $X^q - X$, wenn $f$ und $X^q - X$ eine gemeinsame Nullstelle $\alpha$ in einem Zerfällungskörper von $X^q - X$ haben. Aber die Nullstellen von $X^q - X$ sind genau die Elemente des Körpers $\mathbb{F}_q$ der Ordnung $q$. F"ur diese ist $[\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ ein Teiler von $[\mathbb{F}_q : \mathbb{F}_p] = n$. Damit ist gezeigt, dass aus $f | X^q - X$ tatsächlich $\deg(f) | n$ folgt.

Nimm umgekehrt $\deg(f) | n$ an. Sei $\alpha$ eine Nullstelle von $f$ in einem Zerfällungskörper von $f$. Dann ist $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg(f)$ und somit ist $\mathbb{F}_p(\alpha)$ der Zerfällungskörper von $X^{p^{\deg(f)}} - X$. Dies impliziert $\alpha^{p^{\deg(f)}} = \alpha$ und mit $\deg(f) | n$ folgt $\alpha^q = \alpha$.

(b) Wegen (a) teilt die rechte Seite die linke, denn die $f$ sind alle zueinander teilerfremd. Sei umgekehrt $a \in \mathbb{F}_q$ eine Nullstelle von $X^q - X$. Sei $m_{a,\mathbb{F}_p}$ das normierte Minimalpolynom von $a$ über $F_p$. Dann gilt $m_{a,\mathbb{F}_p} | X^q - X$ und $\deg(m_{a,\mathbb{F}_p}) \leqslant [\mathbb{F}_q : \mathbb{F}_p] = n$, also ist das Polynom auf der rechten Seite ein annullierendes Polynom für $a$ und $m_{a,\mathbb{F}_p}$ muss einer der Faktoren sein. Da $X^q - X$ nur einfache Nullstellen hat, folgt die Aussage.

(c) Vergleiche den Grad auf der rechten und linken Seite in (b).

(d) und (e) folgen direkt aus (b) bzw. (c).

**100**. Sei $p$ eine Primzahl, sei $K$ ein Körper der Charakteristik $p$ und sei $K \to K, x \mapsto x^p$ der Frobeniushomomorphismus.

(a) Zeige: Der Frobeniushomomorphismus ist injektiv.

(b) Zeige: Ist $K$ ein endlicher Körper, so ist der Frobeniushomomorphismus ein Automorphismus des Körpers $K$.

*Lösung*: (a) Aus Satz 16.5.(a) folgt, dass der Frobeniushomomorphismus eine Körperhomomorphismus ist. Somit ist der Frobeniushomomorphismus injektiv.

(b) Mit Satz 16.5 wissen wir, dass der Frobeniushomomorphismus die Nullstellen der Minimalpolynome der Elemente $a \in K$ zyklisch vertauscht. Somit ist der Frobeniushomomorphismus surjektiv und mit (a) also bijektiv, d.h. ein Automorphismus.

**101**. Finde für $q = 8, 9, 16$ das Minimalpolynom über $\mathbb{F}_2$ *bzw.* $\mathbb{F}_3$ eines Erzeugers von $\mathbb{F}_q^*$.

*Lösung*: Sei $p^r = 8$. Dann ist $\mathbb{F}_8$ isomorph zu $\mathbb{F}_2[X]/(X^3 + X + 1)$, da $X^3 + X + 1$ ein irreduzibles Polynom vom Grad 3 über $\mathbb{F}_2$ ist. Ausserdem ist $\mathbb{F}_8^*$ zyklisch der Ordnung 7, also ist jedes von 1 verschiedene Element ein Erzeugendes. Zum Beispiel können wir das Bild von $X$ in $\mathbb{F}_2[X]/(X^3+X+1)$ als erzeugendes Element wählen. Sein Minimalpolynom ist natürlich $X^3 + X + 1$.

Sei $p^r = 9$. Dann ist $\mathbb{F}_9$ isomorph zu $\mathbb{F}_3[X]/(X^2 + 1)$, da $X^2 + 1$ ein irreduzibles Polynom vom Grad 2 über $\mathbb{F}_3$ ist. Eine $\mathbb{F}_3$-Basis von $\mathbb{F}_9$ ist also $\{1, a\}$ mit $a^2 = -1$. Da $\mathbb{F}_9^*$ zyklisch der Ordnung $8$ ist, suchen wir ein Element der Ordnung $8$. Die Elemente der Ordnungen $1$, $2$ und $4$ sind respektive $1$, $-1$ und $\pm a$. Somit kann zum Beispiel $a + 1$ nur noch die Ordnung $8$ haben. (Wir k"onnen dies auch direkt nachrechnen vermittels $(a + 1)^2 = 2a$ und $(a + 1)^4 = (2a)^2 = -4 = -1 \neq 1$.) Wegen $(a + 1)^2 + (a + 1) - 1 = 0$ und $a + 1 \notin \mathbb{F}_3$ ist $X^2 + X - 1$ das Minimalpolynom von $a + 1$ über $\mathbb{F}_3$.

Sei $p^r = 16$. Das Polynom $X^4 + X + 1$ ist irreduzibel vom Grad $4$ über $\mathbb{F}_2$, folglich ist $\mathbb{F}_{16} = \mathbb{F}_2(a)$ f"ur ein Element $a$ mit Minimalpolynom $X^4 + X + 1$ "uber $\mathbb{F}_2$. Da $\mathbb{F}_{16}^*$ zyklisch der Ordnung $16 - 1 = 3 \cdot 5$ ist, ist schon $a$ selbst ein Erzeuger, sofern nicht $a^3 = 1$ oder $a^5 = 1$ ist. In diesem Fall w"are $a$ eine Nullstelle des Polynoms $X^3 - 1$ oder des Polynoms $X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1)$. Allerdings ist aus Gradgr"unden jedes dieser Polynome teilerfremd zum irreduziblen Polynom $X^4 + X + 1$. Dies kann also nicht sein, und $a$ ist ein Erzeuger von $\mathbb{F}_{16}^*$ mit dem Minimalpolynom $X^4 + X + 1$.

**102**. Sei $q = 3^3$ und sei $\mathbb{F}_q := \mathbb{F}_3[X]/(X^3 + X^2 + X + 2)$ ein Körper der Ordnung $q$.

(a) Bestimme die Nullstellen des Polynoms $(Y^3 + Y^2 + Y + 2) \in \mathbb{F}_q[Y]$.

(b) $Y = (2\,X + 1)$ ist eine Nullstelle des Polynoms $g = (Y^3 + 2\,Y^2 + 1) \in \mathbb{F}_q[Y]$. Bestimme die anderen Nullstellen von $g$.

(c) Zeige, dass das Polynom $(Y^2 + Y + 2) \in \mathbb{F}_q[Y]$ keine Nullstellen in $\mathbb{F}_q$ hat.

*Lösung*: (a) Offensichtlich ist $X$ eine Nullstelle von $Y^3 + Y^2 + Y + 2$. Mit Satz 16.8 sind dann $X^3$ und $X^{3^2} = X^9$ die anderen beiden Nullstellen. In $\mathbb{F}_q$ gilt $X^3 \equiv 2\,X^2 + 2\,X + 1$ und $X^9 \equiv X^2 + 1$, d.h.

$$X, \quad 2\,X^2 + 2\,X + 1, \quad X^2 + 1$$

sind die drei Nullstellen von $Y^3 + Y^2 + Y + 2$.

(b) Mit Satz 16.8 sind die anderen beiden Nullstellen von $g$

$$(2\,X + 1)^3 \equiv X^2 + X \quad \text{und} \quad (2\,X + 1)^9 \equiv 2\,X^2.$$

(c) Das Polynom $h = (Y^2 + Y + 2)$ ist irreduzibel über $\mathbb{F}_q$, weil $\deg(h) = 2$ und $2 \nmid 3$.

**103**. Zeige, dass ein endlicher Körper nie algebraisch abgeschlossen ist.

*Lösung*: Wir orientieren uns an Euklids Beweis für die Existenz unendlich vieler Primzahlen. Sei $\mathbb{F}$ ein endlicher Körper. Dann ist

$$f(X) \ := \ 1 + \prod_{a \in \mathbb{F}} (X - a) \ \in \ \mathbb{F}[X]$$

ein wohldefiniertes normiertes Polynom über $K$. Nach Konstruktion gilt $f(a) = 1$ für alle $a \in \mathbb{F}$, also hat $f$ keine Nullstelle in $\mathbb{F}$. Dies zeigt, dass $\mathbb{F}$ nicht algebraisch abgeschlossen ist.