

Musterlösung Serie 19

ENDLICHE KÖRPER II

96. Sei p eine Primzahl, sei K ein Körper der Charakteristik p und sei $K \rightarrow K, x \mapsto x^p$ der Frobeniushomomorphismus.

- (a) Zeigen Sie: Der Frobeniushomomorphismus ist injektiv.
- (b) Zeigen Sie: Ist K ein endlicher Körper, so ist der Frobeniushomomorphismus ein Automorphismus des Körpers K .

Lösung:

- (a) Der Frobenius ist ein Körperhomomorphismus. Somit ist der Frobeniushomomorphismus injektiv.
- (b) Aus Aufgabe (a) wissen wir, dass der Frobeniushomomorphismus ein injektiver Endomorphismus einer endlichen Menge ist. Somit hat das Komplement des Bildes des Frobenius Kardinalität 0, ist also leer. Somit ist der Frobenius surjektiv, somit ist er ein Automorphismus.

97. Finden Sie 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 können 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 $\mathbb{F}_{16} = \mathbb{F}_2(a)$ für ein Element a mit Minimalpolynom $X^4 + X + 1$ über $\mathbb{F}_2$. 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 wäre a eine Nullstelle des Polynoms $X^3 - 1$ oder des Polynoms $X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1)$. Jedes dieser Polynome ist teilerfremd zum irreduziblen Polynom $X^4 + X + 1$, weil sie nicht konstant sind, deren Grad kleiner gleich 4 ist und sie nicht gleich $X^4 + X + 1$ sind. Somit ist a ein Erzeuger von $\mathbb{F}_{16}^*$ mit dem Minimalpolynom $X^4 + X + 1$.

98. 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) Bestimmen Sie die Nullstellen des Polynoms $Y^3 + Y^2 + Y + 2 \in \mathbb{F}_q[Y]$.
- (b) $Y = 2X + 1$ ist eine Nullstelle des Polynoms $g = Y^3 + 2Y^2 + 1 \in \mathbb{F}_q[Y]$.
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 $X^3 \equiv 2X^2 + 2X + 1$ und $X^9 \equiv X^2 + 1$, d.h.

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

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

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

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

(c) Die Diskriminante von $Y^2 + Y + 2$ ist $1 - 4 \cdot 2 = 2$. Da keine Wurzel von 2 in $\mathbb{F}_3$ existiert, kann auch keine Wurzel von 2 in $\mathbb{F}_q$ existieren, da diese Erweiterung ungeraden Grad hat. Wir nehmen nun an es existiert eine Nullstelle von $Y^2 + Y + 2$ in $\mathbb{F}_q$. Dann impliziert die Mitternachtsformel, dass eine Wurzel von 2 in $\mathbb{F}_q$ liegt. Dies ist ein Widerspruch. Also existiert keine Nullstelle von $Y^2 + Y + 2$ in $\mathbb{F}_q$.

99. Zeigen Sie, 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.