Musterlösung Serie 18

ENDLICHE KÖRPER I

---

91. (a) Zeigen Sie: Ist K ein endlicher Körper mit $|K| = p^n$ (für $n \geqslant 1$ und p prim), so ist K der Zerfällungskörper von $X^{p^n} - X$ über $\mathbb{F}_p$.

(b) Zeigen Sie: Sind K und K' endliche Körper mit $|K| = |K'|$, so sind K und K' isomorph.

Lösung: (a) Da K ein Körper ist, ist $K^* = K\backslash\{0\}$. D.h. die multiplikative Gruppe von $|K^*|$ hat die Ordnung $p^n - 1$ und somit gilt für jedes $a \in K^*$, $a^{p^n-1} = 1$ bzw. $a^{p^n} = a$. Weil auch $0^{p^n} = 0$ gilt, ist jedes der p^n Elemente $a \in K$ eine Nullstelle von $X^{p^n} - X$. Das Polynom $X^{p^n} - X$ hat also p^n verschiedene Nullstellen in K und somit ist K ein Zerfällungskörper von $X^{p^n} - X$ über $\mathbb{F}_p$.

(b) Aus (a) folgt, dass K und K' Zerfällungskörper sind von $X^{p^n} - X$ über $\mathbb{F}_p$, und mit Satz 15.2 folgt, dass K und K' isomorph sind.

92. Bestimmen Sie die Anzahl der irreduziblen Polynome $f \in \mathbb{F}_3[X]$ vom Grad 6.

Lösung: Allgemein gilt für p:

- $r_1 = p$
- $r_2 = \frac{1}{2}(p^2 - p)$
- $r_3 = \frac{1}{3}(p^3 - p)$
- $r_4 = \frac{1}{4}(p^4 - p^2)$
- $r_5 = \frac{1}{5}(p^5 - p)$
- $r_6 = \frac{1}{6}(p^6 - p^3 - p^2 + p)$

Für $p = 3$ ist $r_6 = 116$.

93. Wir definieren das irreduzible Polynom $f := X^3 + X + 1$ über $\mathbb{F}_7$. Berechnen Sie $(X^2+2)^{-1}$ im Körper $\mathbb{F}_7[X]/(f)$.

Lösung: Wir rechnen in $\mathbb{F}_7$ und wenden den verallgemeinerten Euklid'schen Algorithmus an: Es ist

$$\begin{array}{rcll} (X^3 + X + 1) : (X^2 + 2) & = & X & \text{Rest: } (-X + 1) \\ (X^2 + 2) : (-X + 1) & = & -X - 1 & \text{Rest: } 3 \\ (-X + 1) : 3 & = & -5X & \text{Rest: } 1 \\ 3 : 1 & = & 3 & \text{Rest: } 0 \end{array}$$

mit $b_0 = X$, $b_1 = -X - 1$, $b_2 = -5X$, $b_3 = 3$.

Nun wenden wir das Schema an:

		X	$-X-1$	$-5X$	3
0	**1**	X	$-X^2-X+1$	$5X^3+5X^2-4X$	f
1	**0**	$\ldots$	$\ldots$	h	X^2+2

Wir erhalten daraus

$$h \cdot f - (5X^3 + 5X^2 - 4X) \cdot (X^2 + 2) = 1$$

bzw.

$$(2X^3 + 2X^2 + 4X) \cdot (X^2 + 2) \equiv 1 \pmod{f},$$

und weil

$$(2X^3 + 2X^2 + 4X) - 2 \cdot f = 2X^2 + 2X + 5$$

ist

$$(X^2 + 2)^{-1} \equiv 2X^2 + 2X + 5 \pmod{f}.$$

94. Sei $\mathbb{F}_q$ ein Körper der Ordnung $q = p^n$ für $n \geqslant 1$ und p prim, und seien $a, b \in \mathbb{F}_q$. Zeigen Sie, dass in $\mathbb{F}_q$ folgendes gilt:

(a) $(a + b)^p = a^p + b^p$.

(b) $a^p = a \iff a \in \mathbb{F}_p$.

Lösung: (a) Es ist

$$(a + p)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k,$$

und weil

$$\binom{p}{k} = \frac{p \cdot (p-1) \cdots (p-k+1)}{1 \cdot 2 \cdots k},$$

gilt für alle $1 \leqslant k \leqslant p-1$, $p \mid \binom{p}{k}$, d.h. $\binom{p}{k} \equiv 0 \pmod{p}$. Somit gilt in $\mathbb{F}_q$:

$$(a + b)^p = a^p b^0 + a^0 b^p = a^p + b^p$$

(b) ($\Leftarrow$) Ist $a = 0$, so ist $a^p = a$. Ist $a \in \mathbb{F}_p^*$, so ist, weil $|\mathbb{F}_p^*| = p - 1$, $a^{p-1} = 1$, also $a^p = a$.
($\Rightarrow$) Ist $a^p = a$, so ist a eine Nullstelle von $X^p - X$. Die p Elemente aus $\mathbb{F}_p$ sind, wie oben gezeigt, paarweise verschiedene Nullstellen von $X^p - X$, und weil $X^p - X$ höchstens p Nullstellen besitzt, sind alle Nullstellen von $X^p - X$ in $\mathbb{F}_p$.

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

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

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

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

(c) Sei $r_d := |I_d|$. Schliessen Sie $\sum_{d|n} \big(d \cdot r_d\big) = q$ aus (b).

(d) Zeigen Sie: Die Summe der Grade aller normierten, irreduziblen Polynome, deren Grad n teilt, 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 α 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. Für 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.

Sei nun $f \in \mathbb{F}_p[X]$ ein irreduzibles Polynom mit $\deg(f)|n$. Sei α eine Nullstelle von f in einem Zerfällungskörper von f. Dann ist $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg(f)$ und somit gilt $\alpha^{p^{\deg(f)}} = \alpha$. Aus $\deg(f)|n$ folgt nun $\alpha^q = \alpha$.

(b) Wegen (a) teilt die rechte Seite die linke, denn die f sind alle zueinander teilerfremd. Der Zerfallungskörper von $X^q - X$ ist $\mathbb{F}_q$ und wir haben bereits in Aufgabe 91

$$X^q - X = \prod_{x \in \mathbb{F}_q} (X - x)$$

bewiesen. Also hat $X^q - X$ keine doppelten Nullstellen. Insbesondere kann kein irreduzibles Polynom $X^q - X$ mehr als zweimal teilen. Also muss die linke Seite gleich der rechten sein, weil wir wissen welche irreduziblen Faktoren in der Faktorisierung von $X^q - X$ vorkommen müssen und weil keiner doppelt vorkommen kann, müssen alle Faktoren einfach vorkommen.

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

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