Musterlösung Serie 17

ENDLICHE KÖRPER

---

95. (a) Zeige: 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) Zeige: 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.

96. Bestimme 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 $r_6 = 116$.

97. Das Polynom $f = X^3 + X + 1$ ist irreduzibel über $\mathbb{F}_7$.

Berechne $(X^2 + 2)^{-1}$ 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

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

98. Sei $\mathbb{F}_q$ ein Körper der Ordnung $q = p^n$ für $n \geqslant 1$ und p prim, und seien $a, b \in \mathbb{F}_q$. Zeige, 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 $\mathbb{F}_p$.