Université du Luxembourg
Faculté des Sciences, de la Technologie et de la Communication

Bachelorarbeit

Konstruktion und Struktur endlicher Körper

Hoeltgen Laurent

Luxemburg den 28. Mai 2008

Betreuer:
Prof. Dr. Martin Schlichenmaier

Inhaltsverzeichnis

Einführung

Endliche Körper sind endliche Zahlbereiche, auf denen man die elementaren Rechenoperationen Addition, Multiplikation, Substraktion und Division benutzen kann. Sie wurden zum ersten Mal von Évariste Galois[1] (1811-1832) angegeben und heißen deshalb auch noch Galoiskörper. Endliche Körper spielen eine wichtige Rolle in der Zahlentheorie, algebraischer Geometrie, Kryptographie und Codierungstheorie. Ihre Anwendung in der Kryptographie beruht auf der Tatsache, dass es sehr einfach ist in einem endlichen Körper a^x auszurechnen, jedoch kein Algorithmus bekannt ist, welcher für gegebene a und b ein x auf effiziente Art bestimmen kann, so dass $a^x = b$ gilt. Die Zahl x wird auch noch diskreter Logarithmus von b mit Basis a genannt. Das Diffie-Hellman Verfahren zum Schlüsselaustausch benutzt dieses Prinzip. In der Codierungstheorie benutzt man endliche Körper um Fehler in der Datenübertragung, welche durch Störsignale verursacht werden, zu korrigieren. Damit wird es möglich Informationen selbst über sehr weite Strecken fehlerlos zu übermitteln. Das populärste Beispiel hierfür wäre wahrscheinlich der Reed-Solomon Code, welcher von der Raumfahrtagentur NASA benutzt wird, um die Datenübertragung zu den Voyager Raumsonden zu ermöglichen.
Wir werden uns in dieser Arbeit hauptsächlich mit der Existenz und Eindeutigkeit endlicher Körper beschäftigen. Dazu werden wir als erstes zeigen, dass es endliche Körper mit p Elementen gibt, wobei p eine Primzahl ist. Diese Erkenntnis werden wir dann nutzen um schrittweise zu zeigen, dass wenn ein Körper endlich ist, dann muss dieser p^n Elemente besitzen, wobei p wiederum eine Primzahl und n eine natürliche Zahl ist. Danach beweisen wir die Eindeutigkeit und etwas später die Existenz endlicher Körper mit p^n Elementen für jede Primzahl p und jede natürliche Zahl n. Mit Hilfe der Galoistheorie wird es uns dann möglich sein alle Unterkörper eines solchen Körpers zu bestimmen. Als letztes wollen wir eine explizite Konstruktion von zwei endlichen Körpern angeben und zeigen wie man in diesen rechnet.

[1] É. Galois: Sur la théorie des nombres, Bulletin des sciences mathématiques de Ferussac XIII, 1830, §218

1 Endliche Körper

In diesem ersten Kapitel wollen wir endliche Körper definieren und einige allgemeine Aussagen über endliche Körper beweisen. Wir werden zeigen, dass falls ein Körper endlich ist, dann muss dieser p^n Elemente besitzen, wobei p eine Primzahl und n eine natürliche Zahl ist.
Wir setzen Satz 1.1 als bekannt voraus und geben ihn hier ohne Beweis an. Der Beweis kann zum Beispiel in [9] nachgelesen werden.

Satz 1.1 (Satz von Lagrange)
Sei G eine endliche Gruppe.

(1) Ist H eine Untergruppe von G, so ist die Kardinalität von H ein Teiler der Kardinalität von G.

(2) Insbesondere teilt die Ordnung von $x \in G$ die Kardinalität von G.

Definition 1.2
Es seien eine nicht leere Menge K gegeben sowie zwei Abbildungen $+,\cdot : K \times K \to K$. Es gelte

K1 K ist bezüglich + eine kommutative Gruppe. Das neutrale Element bezeichnen wir mit 0.

K2 $K\backslash\{0\}$ ist bezüglich $\cdot$ eine kommutative Gruppe. Das neutrale Element bezeichnen wir mit 1. Wir schreiben K^* für diese Gruppe. Wir nennen sie die multiplikative Gruppe von K.

K3 $x \cdot (y + z) = x \cdot y + x \cdot z \; \forall \; x, \; y, \; z \; \in K$ (Distributivgesetz)

Dann nennen wir $(K, + ,\cdot)$ einen Körper.

Proposition 1.3
Die Menge $(\mathbb{Z}/p\mathbb{Z}, + ,\cdot)$ bildet für jede Primzahl p einen Körper.

Beweis: Die Menge $(\mathbb{Z}/p\mathbb{Z},+)$ ist eine kommutative Gruppe, denn seien $\overline{a}$, $\overline{b}$, $\overline{c} \; \in \mathbb{Z}/p\mathbb{Z}$

$$\begin{aligned}\overline{a} + \left(\overline{b} + \overline{c}\right) &= a + pk_1 + (b + pk_2 + c + pk_3) \\ &= (a + pk_1 + b + pk_2) + c + pk_3 \text{ (Assoziativität in } \mathbb{Z}) \\ &= \left(\overline{a} + \overline{b}\right) + \overline{c}\end{aligned}$$

Das neutrale Element ist offensichtlich $\overline{0} = 0 + kp = kp$ und das zu $\overline{a}$ inverse Element ist klarerweise $\overline{-a} = -a + kp$. Die Kommutativität ist ebenfalls klar, es genügt analog wie zum Beweis zur Assoziativität den Fall zurück nach $\mathbb{Z}$ zu führen.
Die Menge $((\mathbb{Z}/p\mathbb{Z}) \setminus \{0\} ,\cdot)$ ist eine kommutative Gruppe denn seien $\overline{a}$, $\overline{b}$, $\overline{c} \; \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$

$$\begin{aligned}\overline{a} \cdot \left(\overline{b} \cdot \overline{c}\right) &= (a + pk_1) \cdot ((b + pk_2) \cdot (c + pk_3)) \\ &= ((a + pk_1) \cdot (b + pk_2)) \cdot (c + pk_3) \text{ (Assoziativität in } \mathbb{Z}) \\ &= \left(\overline{a} \cdot \overline{b}\right) \cdot \overline{c}\end{aligned}$$

Das neutrale Element ist offensichtlich $\overline{1} = 1 + kp$. Zudem ist p eine Primzahl und keines der Elemente mit Ausnahme der 1 in $(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ ist ein Teiler von p. Daraus folgt mit dem euklidischen Algorithmus für $0 < a < p$ in $\mathbb{Z}$, dass es ein b und ein k in $\mathbb{Z}$ gibt mit:

$$\begin{aligned} 1 &= ggT\,(a,p) = ab + kp \\ &\Leftrightarrow \overline{1} = \overline{a}\overline{b} \end{aligned}$$

Damit ist b das Inverse zu a in $\mathbb{Z}/p\mathbb{Z}$. Die Kommutativität ist auch klar, es genügt analog wie zum Beweis zur Assoziativität den Fall zurück nach $\mathbb{Z}$ zu führen.
Schlussendlich kann man das Distributivgesetz ebenfalls beweisen in dem man den Fall zurück nach $\mathbb{Z}$ führt. Somit ist $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ ein Körper.

Definition 1.4
Ein Unterkörper ist eine Teilmenge eines Körpers, die mit den Operationen des Oberkörpers wieder einen Körper bildet. Dazu müssen folgende Aussagen für einen Unterkörper U eines Körpers K gelten.

(1) $1_K,\, 0_K \in U$

(2) $a,\, b \in U \Rightarrow a + b \in U,\, a \cdot b \in U$

(3) $a \in U \Rightarrow -a \in U$

(4) $a \in U \setminus \{0\} \Rightarrow a^{-1} \in U \setminus \{0\}$

Definition 1.5
Ein endlicher Körper ist ein Körper K mit endlich vielen Elementen. Wir schreiben $\mathbb{F}_p$ für einen Körper mit p Elementen.

Proposition 1.6
Sei K ein endlicher Körper, dann besitzt K einen kleinsten Unterkörper P.

Beweis: Da K nur endlich viele Elemente besitzt, gibt es nur endlich viele Möglichkeiten um Untermengen zu bilden. Also gibt es auch nur höchstens endlich viele Unterkörper. Seien nun K_i für $i \in \{1, \ldots, n\}$ alle Unterkörper von K. Es folgt, dass $\cap_{i=1}^{n} K_i \neq \emptyset$, denn $1_K,\, 0_K \in K_i$ für jedes i. Seien nun $a,\, b \in \cap_{i=1}^{n} K_i$, dann sind $a,\, b \in K_i\ \forall i$ und somit auch $a + b,\, a \cdot b,\ -a \in K_i\ \forall i$. Zudem gilt, dass $\cap_{i=1}^{n} K_i$ mindestens ein Element a enthält welches von 0_K verschieden ist. Für dieses Element gilt $a^{-1} \in K_i \setminus \{0\}\ \forall i$. Hieraus folgt, dass $\cap_{i=1}^{n} K_i$ ein Unterkörper ist, der in allen anderen Unterkörpern enthalten ist.

Definition 1.7
Ein Primkörper ist ein Körper welcher keinen echten Unterkörper besitzt.

Definition 1.8
Die Charakteristik eines Körpers ist die kleinste natürliche Zahl $n > 0$ für welche gilt:

$$n \cdot 1 := \underbrace{1 + 1 + \ldots + 1}_{n\ mal} = 0$$

Falls es keine solche Zahl gibt, dann wird die Charakteristik des Körpers als 0 definiert.

Proposition 1.9
Die Charakteristik eines Körpers K ist entweder 0 oder eine Primzahl. Die Charakteristik eines endlichen Körpers ist immer eine Primzahl.

Beweis: Angenommen die Charakteristik von K sei $n \in \mathbb{N}$, wobei n keine Primzahl ist. Das heißt es gilt $n = rs$, wobei $1 < r < n$ und $1 < s < n$ sind. Es folgt:

$$(r \cdot 1)(s \cdot 1) = \underbrace{(1 + 1 + \ldots + 1)}_{r\ mal}\underbrace{(1 + 1 + \ldots + 1)}_{s\ mal} = n \cdot 1 = 0$$

Da K ein Körper ist, folgt, dass entweder $r \cdot 1 = 0$ oder $s \cdot 1 = 0$. Dies ist ein Widerspruch zur Minimalität von n. Somit ist $n = 0$ oder n ist eine Primzahl. Wir bemerken zudem, dass $n = 1$ nicht möglich ist, da $0 \neq 1$ gelten muss. Angenommen K ist ein endlicher Körper. Dann folgt, dass die Folge: $0,\ 1,\ 1+1,\ 1+1+1,\ \ldots$ mindestens einen sich wiederholenden Term besitzt. Angenommen $r \cdot 1 = s \cdot 1$ mit $r < s$. Daraus folgt: $(s - r) \cdot 1 = 0$. Somit hat K eine von 0 verschiedene Charakteristik, da $r - s < \infty$ und wegen des ersten Teils des Beweises ist diese sogar eine Primzahl.

Proposition 1.10
Sei K ein Körper mit Charakteristik p. Dann besitzt K einen Primkörper U welcher isomorph zu $\mathbb{Z}/p\mathbb{Z}$ ist.

Beweis: Hat K die Charakteristik p, so können wir folgende Abbildung definieren:

$$\Theta : \mathbb{Z}/p\mathbb{Z} \to K$$
$$r \mapsto r \cdot 1$$

Diese Abbildung ist ein Homomorphismus. Denn

$$\Theta(r + s) = (r + s) \cdot 1 = r \cdot 1 + s \cdot 1 = \Theta(r) + \Theta(s)$$
$$\Theta(r \cdot s) = (r \cdot s) \cdot 1 = (r \cdot 1) \cdot (s \cdot 1) = \Theta(r) \cdot \Theta(s)$$

Außerdem ist Θ injektiv denn

$$\Theta(r) = 0 \Leftrightarrow r \cdot 1 = 0 \Leftrightarrow r = k \cdot p \Leftrightarrow r = \overline{0} \in \mathbb{Z}/p\mathbb{Z}$$
$$\Rightarrow \ker\Theta = \{\overline{0}\}$$

Somit bildet Θ einen Isomorphismus zwischen $\mathbb{Z}/p\mathbb{Z}$ und $\mathrm{Im}\Theta$. Da Θ ein Isomorphismus und $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, folgt, dass $\mathrm{Im}\Theta$ einen Unterkörper von K bildet. Da jeder Unterkörper von K das Element 1 enthält, enthält jeder Unterkörper auch $r \cdot 1 = 1 + 1 + \ldots + 1$. Also ist der Körper $\mathrm{Im}\Theta$ in jedem Unterkörper enthalten und somit mit dem Primkörper U in K identisch. Des weiteren gibt es nur einen einzigen solchen Isomorphismus denn sei Θ' ein weiterer Isomorphismus:

$$\Theta'(1) = 1 \Rightarrow \Theta'(r) = \Theta'\underbrace{(1 + 1 + \ldots + 1)}_{r\ mal} = \underbrace{\Theta'(1)}_{=1} + \ldots + \underbrace{\Theta'(1)}_{=1} = r \cdot 1 = \Theta(r)$$

Korollar 1.11
Der Primkörper eines endlichen Körpers besitzt immer p Elemente, wobei p eine Primzahl ist.

Beweis: Dies ist offensichtlich, da nach Proposition 1.10 der Primkörper Isomorph zu $\mathbb{Z}/p\mathbb{Z}$ ist, und dieser p Elemente besitzt.

Korollar 1.12
$\mathbb{Z}/p\mathbb{Z}$ ist für jede Primzahl p der einzige Körper mit p Elementen.

Beweis: Sei K ein Körper mit p Elementen. Wir zeigen zuerst, dass K dann von der Charakteristik p sein muss. Angenommen die Charakteristik von K sei $q > p$. Dann besitzt die Folge

$$0,\ 1,\ 1+1,\ 1+1+1,\ \ldots,\ \underbrace{1+1+1+\ldots+1}_{\text{q mal}},\ \ldots$$

mindestens einen sich wiederholenden Term, da wir nur p Elemente in K haben. Sei also $j_1 \cdot 1 = j_2 \cdot 1$ mit $j_1 < j_2$. Dann ist $(j_2 - j_1) \cdot 1 = 0$. Somit ist $j_1 = j_2$ und wir haben einen Widerspruch.
Wäre $1 < q < p$, dann bildet die Menge $G = \{j \cdot 1 \mid 0 < j \leq q\}$ eine Untergruppe von $(K,\ +)$, denn offensichtlich sind 0 und 1 in G und das Inverse zu $j \cdot 1$ ist $(q - j) \cdot 1$ welches ebenfalls in G ist. Nach dem Satz von Lagrange müsste q nun aber ein Teiler von p sein. Dies ist wiederum ein Widerspruch, da p eine Primzahl ist, also muss K von der Charakteristik p sein.
Aus Proposition 1.10 folgt, dass K einen Primkörper hat der zu $\mathbb{Z}/p\mathbb{Z}$ isomorph ist. Da aber $\mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen ist, muss K schon der Primkörper sein und somit isomorph zu $\mathbb{Z}/p\mathbb{Z}$.

Betrachten wir nun einen endlichen Körper K mit Primkörper $\mathbb{F}_p$. So kann man K auch als einen Vektorraum über $\mathbb{F}_p$ betrachten.

Satz 1.13
Sei K ein endlicher Körper. Dann ist K ein Körper mit p^n Elementen für ein $n \in \mathbb{N}$:

Beweis: Da K von der Charakteristik p ist, besitzt K einen Primkörper $\mathbb{F}_p$. Nehmen wir an K sei ein Vektorraum der Dimension n über dem Primkörper $\mathbb{F}_p$. Dann existiert eine Basis $\{e_1,\ e_2,\ e_3,\ \ldots,\ e_n\}$ von K über $\mathbb{F}_p$. Jedes Element $a \in K$ ist dann eindeutig in der Form $a = \sum_{i=1}^{n} \lambda_i e_i$, $\lambda_i \in \mathbb{F}_p$ darstellbar. Für jeden Koeffizienten λ_i gibt es genau p Möglichkeiten. Daraus folgt, dass K

$$\underbrace{p \cdot p \cdot \ldots \cdot p}_{n\ mal} = p^n$$

Elemente besitzt.

Korollar 1.14
Jeder endlicher Körper hat p^n Elemente, wobei p eine Primzahl und n eine natürliche Zahl ist.

Beweis: Dies folgt sofort aus Proposition 1.9, Proposition 1.10 und Satz 1.13.

2 Die Multiplikative Gruppe eines endlichen Körpers

Wir wollen nun zeigen, dass die multiplikative Gruppe eines endlichen Körpers zyklisch ist. Außerdem werden wir die Anzahl an Erzeugern dieser Gruppe bestimmen.

Definition 2.1
Eine Gruppe G ist eine zyklische Gruppe, falls es ein $g \in G$ gibt, mit der Eigenschaft

$$G = \{x \mid x = g^n,\, n \in \mathbb{Z}\}$$

Das heißt G wird vom Element g erzeugt.

Definition 2.2
Der Exponent e einer Gruppe G ist die kleinste natürliche Zahl e mit der Eigenschaft: $g^e = 1\ \forall g \in G$. Wir bemerken, dass eine endliche Gruppe immer einen endlichen Exponenten besitzt. Denn andernfalls gäbe es ein $a \in G$ mit $a^n \neq 1\ \forall n \in \mathbb{N}$. Daraus folgt, dass die Ordnung von a unendlich wäre und somit im Widerspruch zum Satz 1.1 von Lagrange stünde.

Lemma 2.3
Sei G eine kommutative Gruppe und $a \in G$ von der Ordnung m und $b \in G$ von der Ordnung n. Falls $ggT\,(m,n) = 1$ ist, dann hat $a \cdot b$ die Ordnung $n \cdot m$.

Beweis: Angenommen $a \cdot b$ hat die Ordnung d. Es gilt: $(ab)^{nm} = (a^m)^n\,(b^n)^m = 1$. Daraus folgt, dass $d|nm$. Andererseits gilt ebenfalls $(ab)^d = 1$ und somit $(ab)^{nd} = 1$ und deswegen ist $a^{nd} = 1$, da $b^{nd} = (b^n)^d = 1$ gilt. Weil aber a von der Ordnung m ist, folgt aus $m|nd$ und $ggT\,(m,n) = 1$, dass $m|d$ sein muss. Analog erhält man $n|d$ in dem man $(ab)^{md}$ betrachtet. Wir erinnern uns nun an folgende Behauptungen:

$$a,\, b \in \mathbb{N} \Rightarrow a \cdot b = ggT\,(a,\, b) \cdot kgV\,(a,\, b)$$
$$a,\, b \in \mathbb{Z}\backslash\,\{0\}\,,\, c \in \mathbb{Z} \text{ mit } a|c,\, b|c \Rightarrow kgV\,(a,\, b)\,|c$$

Daraus folgt dann, dass $mn|d$ gilt, da $ggT\,(m,n) = 1$ und $mn = kgV\,(m,n)$ sind. Somit muss auch $d = n \cdot m$ gelten.

Lemma 2.4
Sei G eine endliche und kommutative Gruppe mit Exponent e. Dann besitzt G ein Element a mit der Ordnung e.

Beweis: Sei $e = \prod_{j=1}^{n} p_j^{a_j}$ die Primfaktorzerlegung von e. Zu jedem $i \in \{1, \ldots, n\}$ gibt es ein $a \in G$ und ein m für welche gilt: $a^{mp_i^{a_i}} = 1$. Denn aus $a^e = 1 \; \forall \; a \in G$ folgt

$$\begin{aligned} 1 &= a^{\prod_{j=1}^{n} p_j^{a_j}} \\ &= \left(a^{\prod_{j=1, j\neq i}^{n} p_j^{a_j}}\right)^{p_i^{a_i}} \\ &= a^{mp_i^{a_i}} \end{aligned}$$

wobei $m = \prod_{j=1, j\neq i}^{n} p_j^{a_j}$ ist. Der Fall, dass $a^{mp_i^{b_i}} = 1$ für $b_i < a_i$ für alle $a \in G$ ist nicht möglich, denn in dem Fall wäre für

$$e' = p_i^{b_i} \cdot \prod_{\substack{j=1 \\ j\neq i}}^{n} p_j^{a_j}$$

$a^{e'} = 1 \; \forall a \in G$ und $e' < e$, was jedoch der Minimalität von e widerspricht. Sei nun $\alpha_i = a^m$, dann ist α_i von der Ordnung $p_i^{a_i}$ für jedes $i \in \{1, \ldots, n\}$. Nach Lemma 2.3 ist dann $\beta = \prod_{i=1}^{n} \alpha_i$ von der Ordnung e, denn $ggT\left(p_i^{a_i}, p_j^{a_j}\right) = 1 \; \forall i, j \in \{1, \ldots, n\}, \; i \neq j$.

Korollar 2.5
Sei G eine endliche Kommutative Gruppe mit Exponent e. Dann gilt $e | \|G\|$.

Beweis: Aus Lemma 2.4 wissen wir, dass G ein Element der Ordnung e enthält. Wegen des Satzes von Lagrange teilt die Ordnung eines Elements die Kardinalität der Gruppe. Insbesondere gilt $e | \|G\|$.

Satz 2.6
Sei $\mathbb{F}_q$ ein endlicher Körper. Dann ist die multiplikative Gruppe $\mathbb{F}_q^*$ eine zyklische Gruppe.

Beweis: Angenommen $\mathbb{F}_q^*$ hat als Exponent e. In dem Fall erfüllt jedes der $q-1$ Elemente $a \in \mathbb{F}_q^*$ die Gleichung $x^e - 1 = 0$. Da ein Polynom vom Grad d höchstens d Nullstellen hat, folgt, dass $q - 1 \leq e$ ist. Da aber wegen Korollar 2.5 $e | q-1$ gilt, muss ebenfalls $e \leq q-1$ gelten. Also erhalten wir $e = q-1$. Aus Lemma 2.4 folgt, dass $\mathbb{F}_q^*$ ein Element der Ordnung $q-1$ besitzt, welches $\mathbb{F}_q^*$ erzeugt (da die Gruppe q-1 Elemente besitzt). Insbesondere ist $\mathbb{F}_q^*$ zyklisch.

Definition 2.7
Sei $\mathbb{F}_q$ ein endlicher Körper. Wir nennen einen Erzeuger von $\mathbb{F}_q^*$ primitives Element.

Lemma 2.8
Sei g ein Erzeuger einer zyklischen Gruppe C_n bestehend aus n Elementen. Die Ordnung von g^r ist in dem Fall $\frac{n}{ggT(r,n)}$.

Beweis: Angenommen die Ordnung von g^r sei d und $ggT\,(r,n) = e$. Dann folgt aus $e|n$ und $e|r$, dass $n = en'$ und $r = er'$ mit $ggT\,(r',n') = 1$, da ansonsten e nicht maximal wäre. Somit gilt

$$(g^r)^{n'} = \left(g^{er'}\right)^{n'} = \left(g^{en'}\right)^{r'} = (g^n)^{r'} = 1$$

Also folgt $d|n'$. Andererseits gilt aber auch:

$$\begin{aligned}(g^r)^d = 1 &\Rightarrow g^{rd} = 1 \\ &\Rightarrow n|rd \ \text{ (da g von der Ordnung n ist)} \\ &\Rightarrow en'|er'd \\ &\Rightarrow n'|r'd \\ &\Rightarrow n'|d \text{ da } ggT\,(r',n') = 1\end{aligned}$$

Es folgt $d = n' = \frac{n}{e} = \frac{n}{ggT(n,r)}$

Definition 2.9 (Euler ϕ Funktion)
Die eulersche ϕ Funktionen gibt zu jeder natürlichen Zahl n an, wie viele positive natürliche Zahlen $a < n$ zu ihr teilerfremd sind.

$$\phi\,(n) = \Big|\{1 \leq a \leq n \mid ggT\,(a,n) = 1\}\Big|$$

Lemma 2.10
Eine zyklische Gruppe C_n mit n Elementen, hat $\phi\,(n)$ Erzeuger. Wobei ϕ die Euler Funktion ist.

Beweis: Angenommen g ist ein Erzeuger von C_n. Es genügt die Anzahl der Elemente g^r mit $0 < r < n$ zu finden, welche ebenfalls Erzeuger von C_n sind. Die Anzahl der Elemente der Ordnung n in C_n (also die Anzahl der Erzeuger) ist wegen Lemma 2.8 gleich der Anzahl an natürlichen Zahlen r mit $0 < r < n$ welche teilerfremd zu n sind. Dies ist per Definition $\phi\,(n)$ wobei ϕ die Euler Funktion ist.

Proposition 2.11
Die Anzahl an primitiven Elementen eines endlichen Körpers $\mathbb{F}_q$ ist $\phi\,(q-1)$.

Beweis: Folgt direkt aus Satz 2.6 und Lemma 2.10.

3 Eindeutigkeit endlicher Körper

In diesem Kapitel wollen wir zeigen, dass es für jede Primzahl p und jede natürliche Zahl n höchstens einen endlichen Körper mit p^n Elementen geben kann.

Definition 3.1
Ein Polynom $f(x)$ vom Grad $d \geq 1$ ist irreduzibel über einem Körper K, falls $f(x)$ nicht als Produkt zweier Polynome von strikt niedrigerem Grad als $f(x)$ geschrieben werden kann.

Proposition 3.2
Sei K ein endlicher Körper mit Primkörper P. Jedes Element $a \in K$ ist eine Wurzel eines eindeutig bestimmten irreduzibelen und unitären Polynoms $m(x)$ mit Koeffizienten aus P. Ist K ein Körper mit p^n Elementen, dann folgt, dass $m(x)$ vom Grad $k \leq n$ ist. Für jedes Polynom $f(x)$ mit Koeffizienten aus P gilt, dass $f(a) = 0$ genau dann, wenn $m(x) | f(x)$ gilt.

Beweis: Falls K ein Körper mit p^n Elementen ist, dann ist $\dim_P K = n$. Sei nun $a \in K$, dann müssen die $n+1$ Elemente 1, a, a^2, a^3, $\ldots$, a^n linear abhängig sein, d.h. $c_0 + c_1 a + c_2 a^2 + \ldots + c_n a^n = 0$ für $c_i \in P$ (nicht alle gleichzeitig Null). In anderen Worten das Element a ist eine Nullstelle des Polynoms $g(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_n x^n$. In dem man durch c_n teilt, kann man das Polynom unitär machen. Dies beweist, dass es mindestens ein Polynom gibt für welches a eine Nullstelle ist.
Sei nun $m(x)$ das unitäre Polynom vom kleinsten Grad größer als 1, für welches $m(a) = 0$ gilt. Dann gilt $\deg m(x) \leq \deg g(x) \leq n$. Des weiteren muss das Polynom $m(x)$ irreduzibel sein, denn ansonsten wäre $m(x) = u(x) v(x)$ und $0 = m(a) = u(a) v(a)$ und somit müsste $u(a) = 0$ oder $v(a) = 0$ sein, da K ein Körper ist. Dies wäre ein Widerspruch zur Annahme, dass $m(x)$ minimal ist.
Schlussendlich angenommen $f(a) = 0$. In dem wir das Polynom $f(x)$ durch $m(x)$ teilen, erhalten wir $f(x) = m(x) q(x) + r(x)$ mit $\deg r(x) < \deg m(x)$. Dann gilt $r(a) = f(a) - m(a) q(a) = 0$. Wegen der Minimalität von $m(x)$ kann dies nur für $r(x) \equiv 0$ wahr sein. Also ist $m(x) | f(x)$.
Die umgekehrte Richtung ist trivial, denn aus $m(x) | f(x)$ folgt, dass $f(a) = m(a) q(a) = 0$ ist. Hieraus lässt sich auch die Eindeutigkeit von $m(x)$ folgern, denn angenommen es gibt 2 Polynome $m_1(x)$ und $m_2(x)$. Da $m_1(a) = 0$ und $m_2(a) = 0$ sind, muss $m_1(x) | m_2(x)$ und $m_2(x) | m_1(x)$ gelten. Also auch $m_1(x) = m_2(x)$

Satz 3.3
Sei K ein endlicher Körper mit q Elementen. Jedes Element $a \in K$ erfüllt die Gleichung $x^q - x = 0$.

Beweis: Die Kardinalität von K^* ist $q-1$ und die Ordnung eines Elements $a \in K^*$ muss nach dem Satz von Lagrange die Kardinalität von K^* teilen. Da $a^{q-1} = 1$ für alle $a \in K^*$ gelten muss, folgt durch multiplizieren mit a, dass $a^q = a$ ist. Diese Gleichung ist auch für 0 erfüllt. Also ist sie für alle $a \in K$ erfüllt.

Korollar 3.4
Sei K ein endlicher Körper mit q Elementen. Dann ist

$$x^q - x \equiv \prod_{a \in K} (x - a)$$

Beweis: Dies ist klar, da jedes Element $a \in K$ nach Satz 3.3 eine Lösung des Polynoms $x^q - x$ ist und ein Polynom vom Grad q auch nicht mehr als q Lösungen besitzen kann.

Korollar 3.5
Sei K ein endlicher Körper mit q Elementen und $p(x) \in P[x]$, wobei P der Primkörper von K ist. Dann gilt $p(x) = 0 \; \forall x \in K$ genau dann wenn $x^q - x | p(x)$ gilt.

Beweis: Angenommen es gilt $p(x) = 0 \; \forall x \in K$. Da K ein Körper mit q Elementen ist, muss nach Korollar 3.4 $p(x)$ mindestens vom Grad q sein. Da $x^q - x$ vom Grad q ist und alle Wurzeln von $x^q - x$ auch Wurzeln von $p(x)$ sind, folgt $x^q - x | p(x)$.
Umgekehrt nehmen wir nun an, dass $x^q - x | p(x)$ gilt. Da $x^q - x = 0$ für alle $x \in K$ ist, folgt sofort $p(x) = 0$ für alle $x \in K$.

Lemma 3.6
Sei $\mathbb{F}_{p^n}$ ein endlicher Körper mit p^n Elementen und von der Charakteristik p. Dann gilt für alle $a, b \in \mathbb{F}_{p^n}$ die Gleichung $(a+b)^p = a^p + b^p$.

Beweis:

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

Es gilt $p | \binom{p}{k} = \frac{p!}{k!(p-k)!}$ für alle $k \neq 0$ und $k \neq p$, denn p teilt in diesem Fall den Zähler, aber nicht den Nenner. Weil die Charakteristik p ist, müssen diese Terme alle verschwinden.

Satz 3.7 (Eindeutigkeit endlicher Körper)
Zwei endliche Körper mit der gleichen Anzahl an Elementen sind isomorph zueinander.

Beweis: Angenommen K und K' sind zwei Körper mit jeweils q Elementen. Sei π ein primitives Element von K und $m(x)$ sein wie in Proposition 3.2 definiertes minimales Polynom. Es folgt ebenfalls aus Proposition 3.2, dass $m(x) | x^q - x$ ist, da π eine Wurzel von beiden Polynomen ist. Zudem folgt aus Korollar 3.4, dass

$$x^q - x = \prod_{a' \in K'} (x - a')$$

und somit $m(x)$ sich in K' vollständig in lineare Terme faktorisieren lässt. Sei also

$$m(x) = (x - a'_1)(x - a'_2) \dots (x - a'_d)$$

Wir wählen eine dieser Wurzeln. Ohne Einschränkung sei $\pi' = a'_1$. Wir definieren die Abbildung

$$\Theta : K \to K'$$
$$\pi \mapsto \pi'$$

Wir bemerken, dass π' ein primitives Element von K' ist (also von der Ordnung q-1). Denn angenommen die Ordnung von π' ist $d < q - 1$, dann erfüllt π' die Gleichung $x^d - 1 = 0$. Weil π' auch $m(x)$ erfüllt und $m(x)$ minimal ist, folgt wiederum aus Proposition 3.2, dass

$$m(x) | x^d - 1 \Rightarrow x^d - 1 = p(x) m(x) \Rightarrow \pi^d - 1 = p(\pi) m(\pi) = 0$$

und somit die Ordnung von $\pi = d < q-1$ ist. Dies wäre aber ein Widerspruch zur Tatsache, dass π ein primitives Element ist. Also ist π' ein primitives Element von K' und somit sind π und π' Erzeuger von zyklischen Gruppen C_{q-1} mit q-1 Elementen. Darum können wir folgenden Gruppenisomorphismus definieren

$$\begin{aligned} \Theta : K^* &\to K'^* \\ \pi^i &\mapsto \pi'^i \end{aligned}$$

Dieser Isomorphismus lässt sich zu einer Bijektion $\Theta : K \to K'$ zwischen K und K' erweitern in dem wir $0 \mapsto 0$ definieren. Diese Bijektion erhält sicherlich die Multiplikation, denn offensichtlich gilt für alle $a = \pi^i$ und $b = \pi^j$, dass $\Theta(ab) = \Theta\left(\pi^i\pi^j\right) = \Theta\left(\pi^{i+j}\right) = \pi'^{i+j} = \pi'^i\pi'^j = \Theta(a)\,\Theta(b)$. Es bleibt also zu zeigen, dass die Addition ebenfalls erhalten bleibt, es muss also $\Theta(a+b) = \Theta(a) + \Theta(b)$ gelten. Im Falle, dass einer der beiden Terme 0 ist, ist die Bedingung trivial erfüllt. Wir können also annehmen, dass $a,\, b \neq 0$ sind. Wir unterscheiden nun 2 Fälle. Jener wo $a + b = 0$ und jener wo $a + b \neq 0$ ist.
Betrachten wir zuerst den zweiten Fall. Sei $a = \pi^i$, $b = \pi^j$ und $a + b = \pi^k$. Also ist $\pi^i + \pi^j = \pi^k$. In anderen Worten π erfüllt die Gleichung $x^i + x^j - x^k = 0$. Es folgt also $m(x) \,|x^i + x^j - x^k$. Da π' eine Wurzel von $m(x)$ ist, muss π' die Gleichung $x^i + x^j - x^k = 0$ ebenfalls erfüllen. Somit ergibt sich, dass $\pi'^i + \pi'^j = \pi'^k$ gilt. Aus $\pi'^j = \Theta\left(\pi^j\right)$ schließen wir, dass $\Theta(a+b) = \Theta(a) + \Theta(b)$ gilt.
Betrachten wir jetzt den Fall $a + b = 0$. Ist die Charakteristik von K und somit auch jene von K' 2, dann folgt aus $a + b = 0$, dass $a = b$ und daraus

$$\begin{aligned} \Theta(a) = \Theta(b) &\Rightarrow \Theta(a) + \Theta(b) = \Theta(b) + \Theta(b) \\ &\Leftrightarrow \Theta(a) + \Theta(b) = 0 \\ &\Leftrightarrow \Theta(a) + \Theta(b) = \Theta(0) \\ &\Leftrightarrow \Theta(a) + \Theta(b) = \Theta(a+b) \end{aligned}$$

Ist die Charakteristik von K verschieden von 2, dann folgt, dass -1 das einzige Element der Ordnung 2 ist, denn das Polynom $x^2 - 1 = (x-1)(x+1)$ besitzt nur die 2 Nullstellen: 1 und -1. Da 1 von der Ordnung 1 ist, ist -1 das einzige Element von der Ordnung 2. Es gilt $-1 = \pi^{\frac{q-1}{2}}$, da das Element auf der rechten Seite sicherlich von der Ordnung 2 ist, denn $\left(\pi^{\frac{q-1}{2}}\right)^2 = \pi^{q-1} = 1$ ist. Das Gleiche gilt

natürlich auch in K', wobei $\left(\pi'^{\frac{q-1}{2}}\right)^2 = \pi'^{q-1} = 1$ ist. Sei nun ohne Einschränkung $i > j$, dann folgt

$$\begin{aligned}
\pi^i + \pi^j = 0 &\Rightarrow \pi^i\pi^{-j} + \pi^j\pi^{-j} = 0 \\
&\Rightarrow \pi^{i-j} = -1 \\
&\Rightarrow \pi^{i-j} = \pi^{\frac{q-1}{2}} \\
&\Rightarrow i - j = \frac{q-1}{2} \\
&\Rightarrow \pi'^{i-j} = \pi'^{\frac{q-1}{2}} \\
&\Rightarrow \pi'^{i-j} = -1 \\
&\Rightarrow \pi'^{i-j}\pi'^{j} = -\pi'^{j} \\
&\Rightarrow \pi'^{i} + \pi'^{j} = 0 \\
&\Rightarrow \Theta\left(\pi^i\right) + \Theta\left(\pi^j\right) = \Theta\left(\pi^i + \pi^j\right)
\end{aligned}$$

Also bleibt die Addition auch in diesem Fall erhalten. Daraus folgt, dass Θ ein Isomorphismus zwischen K und K' ist.

4 Existenz endlicher Körper

Wir haben bis jetzt bewiesen, dass es für jede Primzahl p und jede natürliche Zahl n höchstens einen endlichen Körper mit p^n Elementen gibt. Wir werden nun zeigen, dass es genau einen solchen Körper gibt.

Definition 4.1
Ein Automorphismus über einem endlichen Körper K ist ein Isomorphismus von K nach K.

Proposition 4.2
Sei K ein endlicher Körper der Charakteristik p. Die Abbildung $a \mapsto a^p$ bildet einen Automorphismus über K.

Beweis: Die Abbildung erhält offensichtlich die Multiplikation, denn $(a \cdot b)^p = a^p \cdot b^p$. Die Abbildung erhält aber auch die Addition, denn nach Lemma 3.6 ist $(a+b)^p = a^p + b^p$. Zudem ist die Abbildung injektiv, denn $a^p = 0$ ist genau dann wahr wenn $a = 0$ ist. Weil K endlich ist, ist die Abbildung auch surjektiv und somit bijektiv und deshalb ein Automorphismus über K.

Definition 4.3 (Frobenius Automorphismus)
Wir nennen den Automorphismus $a \mapsto a^p$ den Frobenius-Automorphismus von K und schreiben ihn Φ.

Satz 4.4
Sei $m(x) \in P[x]$ ein irreduzibles Polynom über dem Primkörper $P = \mathbb{F}_p$. Dann existiert ein endlicher Körper K der Charakteristik p, und ein Element $\alpha \in K$, so dass $m(x)$ das Minimalpolynom von α ist.

Beweis: Sei $K = P[x]/(m(x))$. Die Elemente aus K sind also Äquivalenzklassen in $P[x]$ mit der Äquivalenzrelation $f(x) \equiv g(x) \Leftrightarrow m(x) | f(x) - g(x)$. Es gilt nun zu zeigen, dass diese Äquivalenzklassen einen Körper bilden. Seien dazu, $\overline{f}$, $\overline{g}$, $\overline{h} \in K$. Es folgt:

$$\begin{aligned}
\overline{f} + \overline{g} &= f(x) + q_1(x)\, m(x) + g(x) + q_2(x)\, m(x) \\
&= \overline{f+g} \\
\left(\overline{f} + \overline{g}\right) + \overline{h} &= (f(x) + q_1(x)\, m(x) + g(x) + q_2(x)\, m(x)) + h(x) + q_3(x)\, m(x) \\
&= \overline{f} + \left(\overline{g} + \overline{h}\right) \\
\overline{f} + \overline{0} &= f(x) + q_1(x)\, m(x) + 0 + q_4(x)\, m(x) \\
&= \overline{f} \\
\overline{f} + \overline{-f} &= f(x) + q_1(x)\, m(x) + (-f)(x) + q_5(x)\, m(x) \\
&= \overline{0} \\
\overline{f} + \overline{g} &= f(x) + q_1(x)\, m(x) + g(x) + q_2(x)\, m(x) \\
&= \overline{g} + \overline{f}
\end{aligned}$$

Damit ist $(K,+)$ eine kommutative Gruppe. Man sieht sehr leicht, dass die Addition unabhängig vom Repräsentanten der Klasse ist. Man überprüft für $(K\setminus\{0\},\cdot)$ auf identische Weise, dass die Assoziativität und die Kommutativität gelten und, dass $\overline{1} = 1 + m(x)$ das neutrale Element für die Multiplikation ist. Für die Existenz eines inversen Elements geht man wie folgt vor. Sei $0 \neq \overline{f} \in K$, das heißt $m(x) \nmid f(x)$. Es folgt, dass $ggT(m(x), f(x)) = 1$ ist, da $m(x)$ irreduzibel ist. Der euklidische Algorithmus erlaubt es uns $a(x), b(x) \in P[x]$ zu finden, für welche gilt $a(x) f(x) + b(x) m(x) = 1$. Daraus folgt: $m(x) \mid a(x) f(x) - 1$ und damit $\overline{af} = 1$. Also besitzt $\overline{f}$ ein inverses Element. $(K\setminus\{0\},\cdot)$ ist damit eine kommutative Gruppe. Auch hier hängt die Multiplikation offensichtlich nicht von der Wahl des Repräsentanten ab. Das Distributivgesetz ist ebenfalls durch aus-multiplizieren sofort ersichtlich. Somit ist K ein Körper.
Betrachten wir nun das Polynom $i(x) = x$ und sein entsprechendes Element $\overline{i} \in K$. Es folgt $\overline{i}^2 = \overline{x^2}$, $\overline{i}^3 = \overline{x^3} \ldots$. Insbesondere gilt $m(\overline{i}) = \overline{m(x)} = \overline{0}$. Also besitzt $m(x)$ eine Lösung im Körper K, nämlich das Element $\overline{i}$.

Definition 4.5 (Endliche Körpererweiterung)
Seien K und L zwei Körper. Falls K ein Unterkörper von L ist, so nennt man L einen Erweiterungskörper oder eine Körpererweiterung von K. Eine Körpererweiterung ist endlich, falls $\dim_K L < \infty$ ist.

Proposition 4.6
Seien K und $\mathbb{F}$ zwei endliche Körper mit $\alpha \in K \supseteq \mathbb{F}$, $m(x)$ das Minimalpolynom von α über $\mathbb{F}$ und $\deg m = n$. Dann gilt:

(1) $\mathbb{F}(\alpha) \cong \mathbb{F}[x]/m(x)$

(2) $\dim_{\mathbb{F}} \mathbb{F}(\alpha) = n$. Eine Basis von $\mathbb{F}(\alpha)$ ist $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.

Wobei $\mathbb{F}(\alpha)$ der kleinste Erweiterungskörper von $\mathbb{F}$ ist, welcher α enthält.

Beweis: (1) Jeder Körper ist offensichtlich auch ein Ring und die Abbildung

$$\tau : \mathbb{F}[x] \to \mathbb{F}(\alpha), \ f \mapsto f(\alpha)$$

ist ein Ringhomomorphismus, denn

$$\begin{aligned} \tau(f+g) &= (f+g)(\alpha) = f(\alpha) + g(\alpha) = \tau(f) + \tau(g) \\ \tau(f \cdot g) &= (f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha) = \tau(f) \cdot \tau(g) \\ \tau\left(1_{\mathbb{F}[x]}\right) &= 1_{\mathbb{F}[x]}(\alpha) = 1 \end{aligned}$$

und aus Proposition 3.2 folgt $\ker\tau := \{h(x) \in \mathbb{F}[x] \mid h(\alpha) = 0\} = \langle m \rangle$ wobei $\langle m \rangle$ das von m erzeugte Ideal ist. Nun ist also $\mathbb{F}[x]/\ker\tau = \mathbb{F}[x]/m(x) \cong \operatorname{Im}\tau$. Aus dem Beweis von Satz 4.4 folgt, dass $\operatorname{Im}\tau$ ein Körper ist, da m ein irreduzibles Polynom ist. Zudem ist $\tau(x) = \alpha$ und $\operatorname{Im}\tau$ ein Unterkörper von $\mathbb{F}(\alpha)$. Also muss $\mathbb{F}(\alpha) = \operatorname{Im}\tau$ sein. Somit ist $\mathbb{F}(\alpha) = \operatorname{Im}\tau \cong \mathbb{F}[x]/m(x)$

(2) Nach (1) ist $\theta \in \mathbb{F}(\alpha)$ darstellbar als $f(\alpha)$ für $f \in \mathbb{F}[x]$. Da modulo m reduziert wird, reicht $\deg f < n$ aus, also ist θ eine Linearkombination von $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ mit Koeffizienten aus $\mathbb{F}$. Die Elemente $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ müssen linear unabhängig sein, denn sonst ist $\sum_{i=1}^{n-1} a_i \alpha^i = 0$ und nicht alle $a_i = 0$. Dann hätte das Polynome $h(x) = \sum_{i=1}^{n-1} a_i x^i$ in α eine Nullstelle und wäre vom Grad kleiner als das Minimalpolynom.

Definition 4.7
Sei $f \in K[x]$ ein nicht konstantes Polynom. Die Körpererweiterung L von K heißt Zerfällungskörper von f, wenn alle Nullstellen von f in L liegen und L diesbezüglich minimal ist.

Satz 4.8
Jedes Polynom f besitzt über jedem beliebigen Körper K einen Zerfällungskörper, d.h es existiert eine endliche Körpererweiterung von K in welcher das Polynom f in lineare Terme zerfällt.

Beweis: Wir beweisen die Existenz mittels Induktion über $n = \deg f$.

Induktionsanfang: Ist $n = 1$, dann ist $f(x) = ax + b$ mit $a, b \in K$. Da K ein Körper ist, ist $a^{-1} \cdot (-b)$ ebenfalls in K und die Lösung von f. Der Zerfällungskörper ist somit K selbst.

Induktionsvoraussetzung: Angenommen $n \geq 2$ und die Behauptung ist wahr für alle Polynome vom Grad $d < n$.

Induktionsschritt: Sei $f(x)$ vom Grad n. Sei h ein irreduzibler Faktor von f und $K_1 = K[x]/(h)$. Sei $\varepsilon := \overline{x} \in K_1$ (die Klasse des Polynoms x) wegen Satz 4.4 eine Wurzel von h also auch von f. K_1 ist offensichtlich eine endliche Erweiterung von K. Damit lässt sich f über K_1 wie folgt beschreiben: $f = (x - \varepsilon)\, g$, wobei $g \in K_1[x]$ ein Polynom vom Grad n-1 ist. Nach Induktionsvoraussetzung existiert eine endliche Körpererweiterung E von K_1 für welche g in lineare Terme zerfällt. Somit zerfällt f in E vollständig in lineare Terme und E ist eine endliche Körpererweiterung von K.

Proposition 4.9
Sei P ein nicht konstantes Polynom. Wenn P und seine Ableitung P' keinen gemeinsamen Teiler haben, dann besitzt P keine Wurzel mit Vielfachheit strikt größer als 1.

Beweis: Angenommen P hat eine Wurzel der Vielfachheit $k > 1$. Dann lässt sich P als folgendes Produkt $P = (x - \alpha)^k Q$ schreiben. Und damit folgt:

$$P' = k \cdot (x - \alpha)^{k-1} Q + (x - \alpha)^k Q'$$
$$P' = \cdot (x - \alpha)^{k-1} \cdot R$$

Damit haben P und P' einen gemeinsamen Teiler. Daraus folgt unsere Behauptung. Haben also P und P' keine gemeinsamen Wurzeln und ist P vom Grad k, dann hat P in seinem Zerfällungskörper k verschiedene Lösungen.

Satz 4.10 (Existenz endlicher Körper)
Sei p eine Primzahl, $n \geq 1$ und $q = p^n$. Sei K der Zerfällungskörper des Polynoms $x^q - x$ über $\mathbb{F}_p$. In dem Fall gibt es $q = p^n$ Elemente in K.

Beweis: Sei K der Zerfällungskörper des Polynoms $Q := x^q - x$ über $\mathbb{F}_p$. Die Ableitung von Q ist das konstante Polynom $Q' = -1$ und hat somit keine gemeinsamen Lösungen mit Q. Es folgt aus Proposition 4.9, dass es q verschiedene Lösungen von Q in K gibt. Dies sind genau die Lösungen der Gleichung $x^q = x$, also jene welche den Endomorphismus Φ^n invariant lassen. Zudem bilden diese Lösungen einen Unterkörper K_1 von K mit q Elementen, denn offensichtlich sind $0 \in K_1$ und $1 \in K_1$,

da beide die Gleichung trivial erfüllen.

$$\begin{aligned} x, y \in K_1 &\Rightarrow \Phi^n x = x,\, \Phi^n y = y \\ &\Rightarrow \Phi^n(x+y) = (x+y)^{p^n} = x^{p^n} + y^{p^n} = \Phi^n(x) + \Phi^n(y) = x + y \\ &\text{und } \Phi^n(xy) = (xy)^{p^n} = x^{p^n} y^{p^n} = \Phi^n(x) \cdot \Phi^n(y) = xy \\ &\Rightarrow x + y,\, xy \in K_1 \end{aligned}$$

Sei nun $a \in K_1$, dann gilt

$$\begin{aligned} \Phi^n(0) = 0 &\Rightarrow \Phi^n(a-a) = a - a \\ &\Rightarrow \Phi^n(a) + \Phi^n(-a) = a - a \\ &\Rightarrow \Phi^n(-a) = -a \end{aligned}$$

Da $\Phi^n(a) = a$ gilt. Also ist $-a \in K_1$. Ist zusätzlich $a \neq 0$, dann gilt

$$\begin{aligned} \Phi^n(1) = 1 &\Rightarrow \Phi^n\left(a \cdot a^{-1}\right) = a \cdot a^{-1} \\ &\Rightarrow \Phi^n(a) \cdot \Phi^n\left(a^{-1}\right) = a \cdot a^{-1} \\ &\Rightarrow \Phi^n\left(a^{-1}\right) = a^{-1} \end{aligned}$$

wiederum da $\Phi^n(a) = a$ gilt. Also ist $a^{-1} \in K_1$. Somit ist K_1 ein Unterkörper von K in dem Q in lineare Terme zerfällt. Nach Voraussetzung ist K minimal, also muss $K = K_1$ gelten.

Proposition 4.11
Sei f ein irreduzibles Polynom vom Grad n über $\mathbb{F}_p$. Dann ist

$$K = \mathbb{F}_p[x]/f$$

ein Körper mit p^n Elementen.

Beweis: Wir haben in Satz 4.4 gezeigt, dass K ein Körper ist, und aus Proposition 4.6 folgt, dass $\dim_{\mathbb{F}_p} K = n$ ist. Da $\mathbb{F}_p$ ein Körper mit p Elementen ist, folgt aus Satz 1.13, dass K ein Körper mit p^n Elementen sein muss.

5 Galoistheorie endlicher Körper

In diesem Kapitel wollen wir die Galoisgruppen endlicher Körper finden. Wir werden zeigen, dass diese zyklisch sind und einen Erzeuger suchen. Außerdem werden wir die Galoiskorrespondenz zwischen den Unterkörpern eines endlichen Körpers und den Untergruppen seiner Galoisgruppe aufstellen. Wir werden keinen Beweis zum Hauptsatz der Galoistheorie angeben. Ein ausführlicher Beweis befindet sich zum Beispiel in [4].

Definition 5.1 (Galoisgruppe)
Sei L ein Körper und K ein Unterkörper von L. Sei außerdem $\dim_K L < \infty$. Wir definieren

$$GAL\,(L/K) = \{\sigma : L \to L \mid \sigma \text{ Automorphismus und } \sigma\,(x) = x \;\forall\; x \in K\}$$

und nennen diese Gruppe, die Galoisgruppe Gruppe von L über K.

Lemma 5.2
Der Frobenius-Automorphismus Φ über $\mathbb{F}_{p^n}$ hat die Ordnung n.

Beweis: Wir wissen, dass $a^{p^n} = a$ für alle $a \in \mathbb{F}_{p^n}$. Dies ist äquivalent zu $\Phi^n\,(a) = a$ für alle $a \in \mathbb{F}_{p^n}$. Das heißt Φ^n ist die Identität. Angenommen Φ^m ist schon die Identität für ein $m < n$. Daraus folgt $a^{p^m} = a$ für alle $a \in \mathbb{F}_{p^n}$ Diese Gleichung der Ordnung p^m besitzt $p^n > p^m$ Lösungen. Dies ist ein Widerspruch. Also hat Φ die Ordnung n.

Lemma 5.3
Jeder Automorphismus über einem endlichen Körper lässt die Elemente seines Primkörpers P unverändert.

Beweis: Der Primkörper eines endlichen Körpers ist nach Proposition 1.10 $\mathbb{Z}/p\mathbb{Z}$. Jedes Element $c \in \mathbb{Z}/p\mathbb{Z}$ lässt sich schreiben als $c = 1 + 1 + \ldots + 1$. Daraus folgt:

$$\Phi\,(c) = \Phi\,(1 + 1 + \ldots + 1) = \Phi\,(1) + \ldots + \Phi\,(1) = 1 + \ldots + 1 = c$$

Lemma 5.4
Die einzigen Elemente die der Frobenius-Automorphismus unverändert lässt, sind die Elemente des Primkörpers P eines endlichen Körpers.

Beweis: Aus Lemma 5.3 folgt, dass die p Elemente $a \in P$ alles Lösungen von $x^p - x = 0$ sind. Diese Gleichung ist vom Grad p und kann deshalb auch nicht mehr als p Lösungen besitzen.

Lemma 5.5
Sei π ein primitives Element eines endlichen Körpers K. Jeder Automorphismus über K ist vollständig durch das Verhalten von π definiert. Falls Θ' und Θ zwei Automorphismen sind mit $\Theta'\,(\pi) = \Theta\,(\pi)$, dann muss $\Theta' = \Theta$ gelten.

Beweis: Da jedes Element $a \neq 0$ in K von der Form $a = \pi^i$ ist, folgt sofort

$$\Theta'(\pi) = \Theta(\pi) \Rightarrow \Theta'\left(\pi^i\right) = \Theta\left(\pi^i\right) \ \forall\, i \Rightarrow \Theta' = \Theta$$

Satz 5.6
Sei f ein irreduzibles Polynom vom Grad m in $\mathbb{F}_p[x]$. Dann besitzt f eine Lösung in $\mathbb{F}_{p^m}$

Beweis: Wir wissen aus Satz 4.4, dass f eine Lösung in $\mathbb{F}_p[x]/(f)$ besitzt. Nach Proposition 4.11 ist $\mathbb{F}_p[x]/(f)$ ein Körper mit p^m Elementen. Also besitzt f eine Lösung in $\mathbb{F}_{p^m}$

Satz 5.7
Jedes irreduzibele Polynom vom Grad m in $\mathbb{F}_p[x]$ besitzt m verschiedene Lösungen in $\mathbb{F}_{p^m}$. Wenn α eine Lösung ist, so lauten die anderen Lösungen α, α^p, α^{p^2}, $\ldots$, $\alpha^{p^{m-1}}$

Beweis: Sei $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_0$ ein irreduzibles Polynom vom Grad m in $\mathbb{F}_p[x]$. Aus Satz 5.6 wissen wir, dass f eine Lösung α in $\mathbb{F}_{p^m}$ besitzt. In dem wir den Frobenius-Automorphismus auf f anwenden, erhalten wir

$$\begin{aligned}
\Phi \circ f(x) &= \Phi\left(a_m x^m + a_{m-1}x^{m-1} + \ldots + a_0\right) \\
&= \Phi(a_m)\,\Phi(x^m) + \Phi(a_{m-1})\,\Phi\left(x^{m-1}\right) + \ldots + \Phi(a_0) \\
&= a_m \Phi(x^m) + a_{m-1}\Phi\left(x^{m-1}\right) + \ldots + a_0 \\
&= f(\Phi(x))
\end{aligned}$$

Und damit

$$\begin{aligned}
f(\alpha) = 0 &\Rightarrow \Phi \circ f(\alpha) = 0 \\
&\Rightarrow f(\Phi(\alpha)) = 0 \\
&\Rightarrow f(\alpha^p) = 0
\end{aligned}$$

Also ist α^p ebenfalls eine Lösung. In dem man nun dieselbe Rechnung auf α^p anwendet sieht man, dass α^{p^2} auch eine Lösung ist. Also sind α, α^p, α^{p^2}, $\ldots$, $\alpha^{p^{m-1}}$ alles Lösungen von f. Da der Frobenius-Automorphismus wegen Lemma 5.2 die Ordnung m hat, sind unsere m Lösungen alle verschieden. Weil f auch nicht mehr als m Lösungen besitzen kann, sind alle Lösungen von f in $\mathbb{F}_{p^m}$

Satz 5.8
Die Galoisgruppe $GAL(\mathbb{F}_{p^m}/\mathbb{F}_p)$ ist eine zyklische Gruppe der Ordnung m und wird vom Frobenius-Automorphismus erzeugt.

Beweis: Wir wissen, dass der Frobenius-Automorphismus von der Ordnung m ist. Sei α ein primitives Element von $\mathbb{F}_{p^m}$. Wegen Proposition 3.2 besitzt α ein Minimalpolynom welches vom Grad kleiner oder gleich als m ist. Sei also $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_0$ dieses Minimalpolynom. Nehmen wir außerdem an, dass $\zeta \in GAL(\mathbb{F}_{p^m}/\mathbb{F}_p)$ ist. Es folgt

$$\begin{aligned}
\zeta \circ f(x) &= \zeta\left(a_m x^m + a_{m-1}x^{m-1} + \ldots + a_0\right) \\
&= \zeta(a_m)\,\zeta(x^m) + \zeta(a_{m-1})\,\zeta\left(x^{m-1}\right) + \ldots + \zeta(a_0) \\
&= a_m \zeta(x^m) + a_{m-1}\zeta\left(x^{m-1}\right) + \ldots + a_0 \\
&= f(\zeta(x))
\end{aligned}$$

Und somit ist $\zeta(\alpha)$ eine Lösung des Minimalpolynoms. Da aber alle Lösungen wegen Satz 5.7 von der Form α^{p^j} sind, muss auch $\zeta(\alpha) = \alpha^{p^j} = \Phi^j(\alpha)$ sein. Aus Lemma 5.5 folgt $\zeta = \Phi^j$. Somit erzeugt der Frobenius-Automorphismus die Galoisgruppe $GAL(\mathbb{F}_{p^m}/\mathbb{F}_p)$.

Definition 5.9 (Normale Körpererweiterung)
Sei L ein Körper mit Unterkörper K. L heißt normale Erweiterung von K, wenn alle Minimalpolynome von Elementen aus L in L vollständig in Linearfaktore zerfallen. Ist a in L und f sein Minimalpolynom, dann heißen die Nullstellen von f in L die Konjugierten von a.

Proposition 5.10
$\mathbb{F}_{p^n}$ ist für alle $n \in \mathbb{N}$ eine normale Körpererweiterung von $\mathbb{F}_p$.

Beweis: Sei α ein Element von $\mathbb{F}_{p^n}$. Dann ist α schon ein Element von $\mathbb{F}_p(\alpha)$. Wobei $\mathbb{F}_p(\alpha)$ der kleinste Erweiterungskörper von $\mathbb{F}_p$ ist, welcher α enthält. Außerdem ist $\mathbb{F}_p(\alpha)$ ein Unterkörper von $\mathbb{F}_{p^n}$. Sei m_α das Minimalpolynom von α mit $\deg m_\alpha = k \leq n$. Aus Proposition 4.6 folgt, dass der Körper $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^k}$ ist. Da α eine Lösung von m_α in $\mathbb{F}_{p^k}$ ist, folgt aus Satz 5.7, dass m_α alle seine Lösungen in $\mathbb{F}_{p^k}$ hat und m_α in diesem Körper somit in lineare Terme zerfällt. Also zerfällt m_α in $\mathbb{F}_{p^n}$ ebenfalls in lineare Terme.

Definition 5.11 (Separabele Körpererweiterung)
Eine Körpererweiterung L eines Körpers K heißt separabele Körpererweiterung wenn jedes Element aus L die Wurzel eines separablen Polynoms ist.
Ein Polynom $f \in K[x]$ vom Grad n ist separabel über K wenn es n verschiedene Wurzeln in einem Zerfällungskörper L besitzt.

Proposition 5.12
$\mathbb{F}_{p^n}$ ist für alle $n \in \mathbb{N}$ eine separable Körpererweiterung von $\mathbb{F}_p$.

Beweis: $\mathbb{F}_{p^n}$ ist der Zerfällungskörper von $x^{p^n} - x$. Da $\left(x^{p^n} - x\right)' = -1$ ist, besitzt $x^{p^n} - x$ nur einfache Nullstellen. Da nach Satz 3.3 die p^n Elemente von $\mathbb{F}_{p^n}$ alles Nullstellen sind, muss $\mathbb{F}_{p^n}$ separabel sein.

Satz 5.13
Die Unterkörper von $\mathbb{F}_{p^n}$ sind $\mathbb{F}_{p^k}$ mit $k|n$.

Beweis: Der Hauptsatz der Galoistheorie sagt, dass wenn L eine normale und separable Körpererweiterung von K ist, dann sind die beiden Abbildungen Ψ und Ξ Bijektionen und $\Psi \circ \Xi = id$. Es gilt folgende Korrespondenz:

$$\begin{aligned} \{\text{Untergruppen von } GAL(L/K)\} &\longrightarrow \{\text{Zwischenkörper}\} \\ H &\overset{\Psi}{\longmapsto} L^H \\ GAL(L/M) &\overset{\Xi}{\longleftarrow\!\shortmid} M \end{aligned}$$

wobei $L^H := \{\alpha \in L | \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$. Außerdem gilt dann:

$$\dim_K Z = \frac{|GAL(L/K)|}{|GAL(L/Z)|}$$

Wie wir soeben gesehen haben, sind endliche Körper normale und separable Erweiterungen ihrer Primkörper. Wir können also den Hauptsatz der Galoistheorie anwenden. Da $GAL(\mathbb{F}_{p^n}/\mathbb{F}_p)$ zyklisch

ist, können wir seine Untergruppen berechnen. Nach dem Satz von Lagrange muss die Ordnung der Untergruppe, die Ordnung von $GAL\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)$ teilen. Wir erhalten somit eine Untergruppe G_k für jedes k mit $k|n$. Aus $n = k \cdot d$ folgt:

$$G_k = \left\{I, \Phi^k, \Phi^{2k}, \ldots, \Phi^{(d-1)k}\right\} = GAL\left(\mathbb{F}_{p^n}/K_k\right)$$

Jeder dieser Gruppen entspricht ein Unterkörper K_k von $\mathbb{F}_{p^n}$. Es gilt

$$\dim_{\mathbb{F}_p} K_k = \frac{\left|GAL\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)\right|}{\left|GAL\left(\mathbb{F}_{p^n}/K_k\right)\right|} = \frac{n}{d} = k$$

Also ist $K_k = \mathbb{F}_{p^k}$. Somit haben wir alle Unterkörper von $\mathbb{F}_{p^n}$ bestimmt. Es sind alle $\mathbb{F}_{p^k}$ mit $k|n$.

6 Das Polynom $x^{p^n} - x$

Das Polynom $x^{p^n} - x$ ist für endliche Körper von großer Bedeutung, da sich durch dieses Polynom unter anderem die Existenz dieser Körper beweisen lässt. Wir werden in diesem Kapitel einige weitere Eigenschaften dieses Polynoms sehen.

Proposition 6.1
Sei F ein Körper und k, l natürliche Zahlen. Das Polynom $x^k - 1$ teilt das Polynom $x^l - 1$ in $F[x]$ genau dann, wenn k ein Teiler von l ist.

Beweis: Sei $l = kq + r$ mit $0 \leq r < k$. Es gilt $x^l \equiv x^{kq+r} \equiv x^r \mod \left(x^k - 1\right)$, denn offensichtlich gilt $x^{kq+r} = \left(x^k - 1\right)\left(\sum_{i=0}^{q-1} x^{ki+r}\right) + x^r$. Des weiteren ist $x^k - 1$ ein Teiler von $x^l - 1$ genau dann, wenn $x^l - 1 = \left(x^k - 1\right) \cdot P$ gilt, wobei P ein beliebiges Polynom aus $F[x]$ ist. Dies gilt aber genau dann, wenn $x^l \equiv 1 \mod \left(x^k - 1\right)$ ist. Da aber $r < k$ ist, gilt $x^r \equiv 1 \mod \left(x^k - 1\right)$ genau dann, wenn $r = 0$ gilt. Das ist genau dann der Fall, wenn k ein Teiler von l ist.

Proposition 6.2
Seien $a \geq 2$, k und l natürliche Zahlen. $a^k - 1$ ist genau dann ein Teiler von $a^l - 1$, wenn k ein Teiler von l ist.

Beweis: Der Beweis ist nahezu identisch zum Beweis von Proposition 6.1.

Satz 6.3
Seien $a \geq 2$, k und l natürliche Zahlen und F ein Körper. Dann ist das Polynom $x^{a^k} - x$ ein Teiler von $x^{a^l} - x$ in $F[x]$ genau dann, wenn k ein Teiler von l ist.

Beweis: Das Polynom $x^{a^k} - x$ ist ein Teiler von $x^{a^l} - x$ genau dann, wenn $x^{a^k - 1} - 1$ ein Teiler von $x^{a^l - 1} - 1$ ist. Nach Proposition 6.1 ist dies genau dann der Fall wenn $a^k - 1$ ein Teiler von $a^l - 1$ ist. Dies wiederum ist wegen Proposition 6.2 genau dann wahr wenn k ein Teiler von l ist.

Satz 6.4
Sei I die Menge der irreduzibelen unitären Polynome aus $\mathbb{F}_p[x]$. Dann gilt

$$x^{p^n} - x = \prod_{\substack{P \in I \\ \deg P | n}} P(x)$$

Beweis: Wir bemerken sofort, dass das Polynom $x^{p^n} - x$ keine Faktoren mit Vielfachheit verschieden von 1 besitzen kann. Ansonsten müsste $x^{p^n} - x$ eine Nullstelle mit einer Vielfachheit besitzen, welche von 1 verschieden ist. Dies wäre aber im Widerspruch zu Proposition 4.9, da $\left(x^{p^n} - x\right)' = -1$ keine Nullstellen besitzt. Es genügt also zu zeigen, dass wenn f ein unitäres und irreduzibeles Polynom vom Grad k ist, dann teilt f das Polynom $x^{p^n} - x$ genau dann, wenn k ein Teiler von n ist.

Sei also f ein unitäres und irreduzibeles Polynom vom Grad k. Sei $E = \mathbb{F}_p[x]/f = F(\alpha)$ wobei α eine Wurzel von f in E ist. Da f vom Grad k ist, ist $E = \mathbb{F}_{p^k}$. Sei Φ der Frobenius Automorphismus von E über $\mathbb{F}_p$.
Wir behaupten f ist ein Faktor von $x^{p^n} - x$ genau dann, wenn $\Phi^n(\alpha) = \alpha$. In der Tat ist f das Minimalpolynom von α und somit ein Teiler von $x^{p^n} - x$ genau dann, wenn α eine Nullstelle von $x^{p^n} - x$ ist. Also genau dann, wenn $\alpha^{p^n} = \alpha$ gilt. Dies ist gleichbedeutend zu $\Phi^n(\alpha) = \alpha$.
Des weiteren behaupten wir, dass $\Phi^n(\alpha) = \alpha$ genau dann gilt, wenn $\Phi^n(\zeta) = \zeta$ für alle $\zeta \in E$ gilt. Es ist offensichtlich, dass wenn die Behauptung für alle $\zeta \in E$ gilt, dass sie dann auch für α gelten muss. Sei also nun $\Phi^n(\alpha) = \alpha$. Da $\left\{\alpha, \ \ldots, \ \alpha^k\right\}$ eine Basis von E bildet, kann man jedes $\zeta \in E$ als $\zeta = g(\alpha)$ schreiben, wobei g ein Polynom aus $\mathbb{F}_p[x]$ ist. Daraus folgt analog zur den Rechnungen im Beweis von Satz 5.8, dass $\Phi^n(\zeta) = \Phi^n(g(\alpha)) = g(\Phi^n(\alpha)) = g(\alpha) = \zeta$ ist. Schlussendlich ist $\Phi^n(\zeta) = \zeta$ für alle ζ in E genau dann, wenn Φ^n die Identität ist. Da der Frobenius Automorphismus von E über $\mathbb{F}_p$ von der Ordnung k ist, gilt dies genau dann, wenn $k|n$ gilt.

Korollar 6.5
Sei $I_p(n)$ die Anzahl der irreduzibelen unitären Polynome vom Grad n aus $\mathbb{F}_p[x]$. Dann gilt:

$$p^n = \sum_{d|n} d \cdot I_p(d)$$

Beweis: Wir wissen aus Satz 6.4, dass

$$x^{p^n} - x = \prod_{\substack{P \in I \\ \deg P | n}} P(x)$$

Und daraus folgt:

$$\begin{aligned} p^n = \deg\left(x^{p^n} - x\right) &= \deg \prod_{\substack{P \in I \\ \deg P | n}} P(x) \\ &= \sum_{\deg P | n} \deg P(x) \, I_p(\deg P(x)) \\ &= \sum_{d|n} d \cdot I_p(d) \end{aligned}$$

Definition 6.6 (Möbius Funktion)
Die Möbius Funktion μ ist wie folgt definiert: sei $n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ die Primfaktorzerlegung von n, dann ist

$$\mu(n) = \begin{cases} 0 & \text{falls } e_i > 1 \text{ für irgend ein } i \in \{1, \ \ldots, \ r\}. \\ (-1)^r & \text{sonst. (wobei r die Anzahl der verschiedenen Primteiler ist)} \end{cases}$$

Proposition 6.7
Seien $n, m \in \mathbb{N}$ und μ die Möbius Funktion. Dann ist $\mu(m \cdot n) = \mu(m) \cdot \mu(n)$, falls $ggT(m, \ n) = 1$. Weiterhin ist $\mu(1) = 1$. Zudem gilt:

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{falls } n = 1. \\ 0 & \text{sonst.} \end{cases}$$

Beweis: Seien $n, m \in \mathbb{N}$, $ggT(m,\ n) = 1$ und die Primfaktorzerlegungen $n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ sowie $m = q_1^{f_1} q_2^{f_2} \cdot \ldots \cdot q_k^{f_k}$, wobei alle p_i und q_j paarweise verschieden sein müssen. Ist ein $e_i > 1$ oder $f_j > 1$, dann ist $\mu(m \cdot n) = 0 = \mu(m) \cdot \mu(n)$ und die Behauptung stimmt. Sind nun alle $e_i = 1$ und alle $f_j = 1$, dann ist $\mu(m \cdot n) = (-1)^{r+k} = (-1)^r (-1)^k = \mu(m) \cdot \mu(n)$. Außerdem ist $\mu(1) = (-1)^0 = 1$. Damit können wir nun die letzte Aussage mittels Induktion über r, die Anzahl der verschiedenen Primteiler von n, beweisen.

Induktionsanfang: Sei $r = 1$, dann ist $n = p_1^{e_1} > 1$. Daraus folgt:

$$\sum_{d|n} \mu(d) = \underbrace{\mu(1)}_{=1} + \underbrace{\mu(p_1)}_{=-1} + \underbrace{\mu\left(p_1^2\right) + \ldots + \mu\left(p_1^{e_1}\right)}_{=0} = 0$$

Induktionsvoraussetzung: Nehmen wir an die Behauptung ist wahr für alle $r < l$.

Induktionsschritt: Sei l die Anzahl der verschiedenen Primteiler von n, dann ist $n = n' \cdot p_l^{e_l} > 1$ mit

$$ggT\left(n',\ p_l^{e_l}\right) = 1,\ n' > 1,\ e_l \geq 1$$

Dann sind alle Teiler von n von der Form $d = d' p_l^t$, wobei $d' | n'$ und $0 \leq t \leq e_l$ und somit:

$$\sum_{d|n} \mu(d) = \sum_{\substack{d'|n' \\ 0 \leq t \leq e_l}} \mu\left(d' p_l^t\right) = \sum_{\substack{d'|n' \\ 0 \leq t \leq e_l}} \mu(d')\, \mu\left(p_l^t\right) = \underbrace{\left(\sum_{d'|n'} \mu(d')\right)}_{\substack{=0 \\ \text{(Induktionsvoraussetzung)}}} \underbrace{\left(\sum_{0 \leq t \leq e_l} \mu\left(p_l^t\right)\right)}_{\substack{=0 \\ \text{(Induktionsanfang)}}} = 0$$

Satz 6.8 (Inversionsformel von Möbius)
Seien f, g zwei Funktionen von $\mathbb{N}$ nach $\mathbb{Z}$. Sei g definiert als $g(n) = \sum_{d|n} f(d)$. Dann gilt für alle $n \in \mathbb{N}^*$, dass $f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$ sein muss, wobei μ die Möbius Funktion ist.

Beweis:

$$\begin{aligned}
\sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) &= \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{c|d} f(c) \\
&= \sum_{c|n} \Bigg(\sum_{\substack{d \in \mathbb{N} \\ c|d \text{ und} \\ d|n}} \mu\left(\frac{n}{d}\right) \Bigg) f(c) \\
&= f(n)
\end{aligned}$$

Der letzte Schritt folgt mit $d' = \frac{n}{d} \Leftrightarrow d = \frac{n}{d'}$ und

$$\sum_{\substack{d \in \mathbb{N} \\ c|d \text{ und} \\ d|n}} \mu\left(\frac{n}{d}\right) = \sum_{\substack{d \in \mathbb{N} \\ d = k_1 \cdot c \text{ und} \\ n = k_2 \cdot d}} \mu\left(\frac{n}{d}\right) = \sum_{\substack{d' \in \mathbb{N} \\ \frac{n}{d'} = k_1 \cdot c \text{ und} \\ n = k_2 \cdot \frac{n}{d'}}} \mu(d') = \sum_{\substack{d' \in \mathbb{N} \\ \frac{n}{c} = k_1 \cdot d' \text{ und} \\ d' \cdot n = k_2 \cdot n}} \mu(d') = \sum_{d' | \frac{n}{c}} \mu(d') = \begin{cases} 1 & \text{wenn } \frac{n}{c} = 1 \\ 0 & \text{sonst} \end{cases}$$

Korollar 6.9
Die Anzahl an irreduzibelen und unitären Polynomen vom Grad n über $\mathbb{F}_p$ (p eine Primzahl) ist

$$I_p(n) = \frac{1}{n} \sum_{d|n} p^d \mu\left(\frac{n}{d}\right)$$

Des weiteren ist $I_p(n)$ für alle $n \in \mathbb{N}$ strikt größer als 0. Es gibt also über jedem endlichen Körper $\mathbb{F}_p$ mindestens ein irreduzibeles Polynome von jedem Grad.

Beweis: Wir wissen aus Korollar 6.5, dass $f(d) = d \cdot I_p(d)$ und $g(n) = p^n$ die Voraussetzungen für Satz 6.8 erfüllen. In dem wir Satz 6.8 anwenden, erhalten wir $n \cdot I_p(n) = \sum_{d|n} p^d \mu\left(\frac{n}{d}\right)$ und damit unsere erste Behauptung. Wir bemerken zudem, dass $\sum_{d|n} p^d \mu\left(\frac{n}{d}\right)$ ein Vielfaches von n ist. Außerdem gilt

$$\sum_{d|n} p^d \mu\left(\frac{n}{d}\right) = p^n + \sum_{\substack{d|n \\ d<n}} p^d \mu\left(\frac{n}{d}\right) \geq p^n - \sum_{d=1}^{n-1} p^d = p^n - \frac{1-p^n}{1-p} > 0$$

Da $\sum_{d|n} p^d \mu\left(\frac{n}{d}\right)$ ein Vielfaches von n ist, ist der kleinste mögliche Wert den diese Summe annehmen kann n. Somit ist $I_p(n)$ immer strikt größer als 0.

Bemerkung 6.10
Aus Satz 6.4 kann man einen Algorithmus erstellen der Polynome auf ihre Irreduzibilität testet. Sei f ein unitäres Polynom vom Grad l. Das Polynom $x^{p^k} - x$ ist das Produkt aller irreduzibeler unitärer Polynome deren Grad ein Teiler von k ist. Also ist $ggT(x^p - x, f)$ das Produkt aller Linearfaktoren von f. Besitzt f keine Linearfaktoren, dann ist $ggT\left(x^{p^2} - x, f\right)$ das Produkt aller irreduzibelen Faktoren vom Grad 2. Ist f nicht irreduzibel, dann ist f durch ein unitäres irreduzibeles Polynom, dessen Grad höchstens $\frac{l}{2}$ ist, teilbar. Ist also g ein irreduzibeler Faktor von f vom Grad k, dann ist $ggT\left(x^{p^k} - x, f\right) \neq 1$.
Ist f irreduzibel, dann ist $ggT\left(x^{p^k} - x, f\right) = 1$ für alle $0 < k < \frac{l}{2}$. Um herauszufinden ob f irreduzibel ist, genügt es also zu untersuchen ob $ggT\left(x^{p^k} - x, f\right) = 1$ für alle $0 < k \leq \frac{l}{2}$. Ist dies der Fall, so ist f irreduzibel, andernfalls ist f nicht irreduzibel.

7 Der Körper mit 4 Elementen

Wir wissen aus Proposition 4.11, dass man mit einem irreduziblen Polynom vom Grad 2 über $\mathbb{F}_2$ einen Körper mit 4 Elementen erstellen kann. Wir wollen also nun versuchen ein solches Polynom zu finden. Sei $f(t) = c_0 + c_1 t + c_2 t^2$. c_2 muss verschieden von 0 sein, somit ist $c_2 = 1$. Ebenso muss c_0 verschieden von 0 sein, sonst ist 0 eine Nullstelle. Ist $c_1 = 0$, dann ist 1 eine Nullstelle, da $\mathbb{F}_2$ von der Charakteristik 2 ist. Daraus folgt, dass $f(t) = t^2 + t + 1$ über $\mathbb{F}_2$ ein irreduzibeles Polynom vom Grad 2 ist. Aus Korollar 6.9 folgt leicht, dass es sogar das einzige irreduzibele und unitäre Polynom ist. Der Körper $\mathbb{F}_4 \cong \mathbb{F}_2[t]/f(t)$ kann als die Menge $\{0, 1, t, t+1\}$ beschrieben werden, da dies die einzigen möglichen Reste vom Grad $n < 2$ sind die bei der Division eines Polynoms durch $f(t)$ entstehen können. Für die Addition ergeben sich folgende Resultate sofort, falls man beachtet, dass die Charakteristik des Körpers 2 ist:

$+$	0	1	t	$t+1$
0	0	1	t	$t+1$
1	1	0	$t+1$	t
t	t	$t+1$	0	1
$t+1$	$t+1$	t	1	0

Da $t^2 + t + 1 = 0$ lautet, ergibt sich sofort in dem man auf beiden Seiten $t + 1$ addiert, dass

$$t^2 = t + 1$$

Die Multiplikationstabelle lautet deshalb:

$\cdot$	0	1	t	$t+1$
0	0	0	0	0
1	0	1	t	$t+1$
t	0	t	$t+1$	1
$t+1$	0	$t+1$	1	t

8 Der Körper mit 8 Elementen

Wir wissen aus Proposition 4.11, dass man mit einem irreduziblen Polynom vom Grad 3 über $\mathbb{F}_2$ einen Körper mit 8 Elementen erstellen kann. Wir wollen also nun versuchen ein solches Polynom zu finden. Sei $f(t) = c_0 + c_1 t + c_2 t^2 + c_3 t^3$. c_3 muss verschieden von 0 sein, somit ist $c_3 = 1$. Ebenso muss c_0 verschieden von 0 sein, sonst ist 0 eine Nullstelle. c_1 und c_2 können nicht beide gleichzeitig 0 sein, ansonsten ist 1 eine Lösung des Polynoms, da $\mathbb{F}_2$ von der Charakteristik 2 ist. Aus dem selben Grund können sie auch nicht beide gleichzeitig 1 sein. Somit bleiben nur noch 2 Polynome übrig, welche offensichtlich irreduzibel sind: $f(x) = t^3 + t + 1$ und $g(t) = t^3 + t^2 + 1$. Aus Korollar 6.9 folgt leicht, dass es sogar die einzigen irreduzibelen und unitären Polynome sind. Da es nur einen Körper mit 8 Elementen gibt, ist es unerheblich welches der beiden Polynome wir wählen. Wir entscheiden uns für $f(t) = t^3 + t + 1$. Der Körper $\mathbb{F}_8 \cong \mathbb{F}_2[t]/f(t)$ kann als die Menge $\{0, 1, t, t+1, t^2, t^2+1, t^2+t, t^2+t+1\}$ beschrieben werden, da dies die einzig möglichen Reste vom Grad $n < 3$ sind die bei der Division eines Polynoms durch $f(t)$ entstehen können. Für die Addition ergeben sich sofort folgende Resultate:

$+$	0	1	t	$t+1$	t^2	t^2+1	t^2+t	t^2+t+1
0	0	1	t	$t+1$	t^2	t^2+1	t^2+t	t^2+t+1
1	1	0	$t+1$	t	t^2+1	t^2	t^2+t+1	t^2+t
t	t	$t+1$	0	1	t^2+t	t^2+t+1	t^2	t^2+1
$t+1$	$t+1$	t	1	0	t^2+t+1	t^2+t	t^2+1	t^2
t^2	t^2	t^2+1	t^2+t	t^2+t+1	0	1	t	$t+1$
t^2+1	t^2+1	t^2	t^2+t+1	t^2+t	1	0	$t+1$	t
t^2+t	t^2+t	t^2+t+1	t^2	t^2+1	t	$t+1$	0	1
t^2+t+1	t^2+t+1	t^2+t	t^2+1	t^2	$t+1$	t	1	0

Für die Multiplikation ergeben sich die folgenden Resultate:

$\cdot$	0	1	t	$t+1$	t^2	t^2+1	t^2+t	t^2+t+1
0	0	0	0	0	0	0	0	0
1	0	1	t	$t+1$	t^2	t^2+1	t^2+t	t^2+t+1
t	0	t	t^2	t^2+t	?	?	?	?
$t+1$	0	$t+1$	t^2+t	t^2+1	?	?	?	?
t^2	0	t^2	?	?	?	?	?	?
t^2+1	0	t^2+1	?	?	?	?	?	?
t^2+t	0	t^2+t	?	?	?	?	?	?
t^2+t+1	0	t^2+t+1	?	?	?	?	?	?

Aus $t^3 + t + 1 = 0$ folgt sofort $t^3 = t + 1$ und damit:

$$t \cdot \left(t^2 + 1\right) = t^3 + t = t + 1 + t = 1$$
$$t \cdot \left(t^2 + t\right) = t^3 + t^2 = t + 1 + t^2 = t^2 + t + 1$$
$$t \cdot \left(t^2 + t + 1\right) = t^3 + t^2 + t = t + 1 + t^2 + t = t^2 + 1$$
$$(t + 1) \cdot t^2 = t + 1 + t^2 = t^2 + t + 1$$
$$(t + 1) \cdot \left(t^2 + 1\right) = t + 1 + t + t^2 + 1 = t^2$$
$$(t + 1) \cdot \left(t^2 + t\right) = t + 1 + t^2 + t^2 + t = 1$$
$$(t + 1) \cdot \left(t^2 + t + 1\right) = t + 1 + t^2 + t^2 + t + t + 1 = t$$

Da $t^4 = t \cdot t^3 = t\,(t + 1) = t^2 + t$ folgt,

$$t^2 \cdot \left(t^2 + 1\right) = t^2 + t + t^2 = t$$
$$t^2 \cdot \left(t^2 + t\right) = t^2 + t + t + 1 = t^2 + 1$$
$$t^2 \cdot \left(t^2 + t + 1\right) = t^2 + t + t + 1 + t^2$$
$$\left(t^2 + 1\right) \cdot \left(t^2 + 1\right) = t^2 + t + t^2 + t^2 + 1 = t^2 + t + 1$$
$$\left(t^2 + 1\right) \cdot \left(t^2 + t\right) = t^2 + t + t + 1 + t^2 + t = t + 1$$
$$\left(t^2 + 1\right) \cdot \left(t^2 + t + 1\right) = t^2 + t + t + 1 + t^2 + t^2 + t + 1 = t^2 + t$$
$$\left(t^2 + t\right) \cdot \left(t^2 + t\right) = t^2 + t + t + 1 + t + 1 + t^2 = t$$
$$\left(t^2 + t\right) \cdot \left(t^2 + t + 1\right) = t^2 + t + t + 1 + t^2 + t + 1 + t^2 + t = t^2$$
$$\left(t^2 + t + 1\right) \cdot \left(t^2 + t + 1\right) = t^2 + t + t + 1 + t^2 + t + 1 + t^2 + t + t^2 + t + 1 = t + 1$$

$\cdot$	0	1	t	$t+1$	t^2	t^2+1	t^2+t	t^2+t+1
0	0	0	0	0	0	0	0	0
1	0	1	t	$t+1$	t^2	t^2+1	t^2+t	t^2+t+1
t	0	t	t^2	t^2+t	$t+1$	1	t^2+t+1	t^2+1
$t+1$	0	$t+1$	t^2+t	t^2+1	t^2+t+1	t^2	1	t
t^2	0	t^2	$t+1$	t^2+t+1	t^2+t	t	t^2+1	1
t^2+1	0	t^2+1	1	t^2	t	t^2+t+1	$t+1$	t^2+t
t^2+t	0	t^2+t	t^2+t+1	1	t^2+1	$t+1$	t	t^2
t^2+t+1	0	t^2+t+1	t^2+1	t	1	t^2+t	t^2	$t+1$

Literaturverzeichnis

Alle im Literaturverzeichnis aufgelisteten Webseiten waren im Mai 2008 abrufbar.

[1] Avanzi, Roberto: *Endliche Körper und ihre Anwendungen*. http://caccioppoli.mac.rub.de/website/teachingmaterial/ek-ss07/ek-skript.pdf. Version: 2005. – Vorlesungsskript Ruhr Universität Bochum

[2] Holz, Michael: *Repetitorium der Algebra*. Binomi Verlag, 2005

[3] Kurzweil, Hans: *Endliche Körper*. Springer, 2000 (Springer Lehrbuch)

[4] Lang, Serge: *Algebra*. Springer, 2002

[5] Lorenz, Falko: *Algebra, Fields and Galois Theory*. Springer, 2005

[6] Murphy, Timothy: *Finite Fields*. http://www.maths.tcd.ie/pub/Maths/Courseware/. – Vorlesungsskript University of Dublin, Trinity College, School of Mathematics,

[7] Muthsam, Herbert J.: *Lineare Algebra und ihre Anwendungen*. Spektrum Akademischer Verlag, 2006

[8] Planetmath: *Finite Field*. http://planetmath.org. Version: 2007

[9] Shoup, Victor: *A computational introduction to number theory and algebra*. Cambridge University Press, 2008 http://shoup.net

[10] Wikipedia: *Corps fini*. http://fr.wikipedia.org. Version: 2007

[11] Wikipedia: *Endliche Körper*. http://de.wikipedia.org/. Version: 2007

[12] Wikipedia: *Finite field*. http://en.wikipedia.org. Version: 2008