ENDLICHE KÖRPER – EINE KURZE WIEDERHOLUNG

BENJAMIN KLOPSCH

ZUSAMMENFASSUNG. Dieser Aufsatz basiert auf zwei Vorträgen, die ich im Rahmen des Seminars "Kodierungstheorie" im Wintersemester 2001/02 gehalten habe. Vor dem Hintergrund der allgemeinen Theorie der Körpererweiterungen wird an die wichtigsten Eigenschaften endlicher Körper erinnert. Auf ausführliche Beweise wird verzichtet, stattdessen bemühe ich mich, die wesentlichen Gedanken in Kurzform darzustellen. Als Leser stelle ich mir Studierende der Mathematik vor, die bereits einmal eine Vorlesung über die Galoissche Theorie gehört haben, möglicherweise sich aber an Details kaum erinnern.

1. EINLEITUNG

Die Theorie der endlichen Körper bildet den Ausgangspunkt für die Konstruktion vieler interessanter kombinatorischer und geometrischer Objekte. Anwendungen solcher Konstruktionen finden sich zum Beispiel in der Kodierungstheorie oder der Krytographie. Dort wird—mit Hilfe von Computern—auch ganz konkret gerechnet, und zunächst völlig abstrakt definierte Objekte rücken greifbar näher. Zum besseren Verständnis der Mathematik im Alltag (Stichwörter CD-Spieler und Internetbanking) trägt heutzutage nicht zuletzt auch das Studium der endlichen Körper bei. In diesem Aufsatz sollen die grundlegenden Eigenschaften endlicher Körper kurz und übersichtlich dargestellt werden. Gedanklich entwickelt werden sie aus der allgemeineren Körpertheorie und dienen somit auch als Illustration weiterführender Begriffe und Sätze.

Historisch gesehen entwickelte sich die Theorie der endlichen Körper aus den im 17ten und 18ten Jahrhundert einsetzenden zahlentheoretischen Untersuchungen der spezielleren endlichen Primkörper. Die Namen Fermat, Euler, Lagrange und Legendre sind hier zu nennen. Allgemeinere endliche Körper wurden dann im Zuge des 19ten Jahrhunderts betrachtet, entscheidend waren dabei die Arbeiten von Gauss und Galois. Von Dickson, einem Schüler Moores, stammt die vielleicht erste systematische Darstellung der Theorie endlicher Körper in Buchform [2]; sie erschien 1901. Die zahlreichen Anwendungen außerhalb der Mathematik sind jüngeren Datums und vor allem ein Produkt der computer-technischen Entwicklung am Ende des 20ten Jahrhunderts.

Literaturhinweise. In fast jedem Algebralehrbuch findet sich eine Darstellung der allgemeinen Körpertheorie. Endliche Körper werden häufig im Rahmen der Galoisschen Theorie mitbehandelt. Besonders hinweisen möchte ich aber auf die folgenden Werke.

- *Galoissche Theorie* von E. Artin [1]. Ein klassischer Text, im Taschenbuchformat, hervorgegangen aus einer Übersetzung des englischen Titels *Galois Theory* (aus der Reihe *Notre Dame Mathematical Lectures*).

- *Introduction to Finite Fields and Their Applications* von R. Lindl und H. Niederreiter [3]. Ein sehr ausführliches Buch, eine Kurzform des Lexikonwerkes *Finite Fields* (Band 20 in der Reihe *Encyclopedia of Mathematics and Its Applications*).
- *Finite Fields for Computer Scientists and Engineers* von R.J. McEliece [4]. Eine anspruchsvolle, aber elementare Einführung.

Gliederung. In Kapitel 2 werden grundlegende Begriffe und Sätze der Körpertheorie behandelt. Im Mittelpunkt steht dabei die sogenannte Kronecker-Konstruktion. In Kapitel 3 geht es darum, aus der allgemeineren Theorie die wichtigsten speziellen Eigenschaften endlicher Körper herzuleiten. Anschließend werden in Kapitel 4 beispielhaft zwei besonders einfache endliche Körper konstruiert und kurz untersucht.

2. Grundlegende Begriffe und Sätze aus der Körpertheorie

2.1. **Körper und Körpererweiterungen.** In einem *Körper* $K = (K, +, \cdot)$ gibt es zwei Verknüpfungen, eine Addition und eine Multiplikation, die den gleichen Grundgesetzen gehorchen, wie sie von dem reellen Zahlkörper $\mathbb{R}$ her bekannt sind. Zum Beispiel gilt das sogenannte Distributivgesetz, welches die beiden Verknüpfungen verbindet: $a(b+c) = ab + ac$ für alle $a, b, c \in K$. Als besondere Elemente, nämlich als *neutrale Elemente* bezüglich Addition und Multiplikation, fungieren die *Null* 0 und die *Eins* 1. Der kleinste denkbare Körper, das ist $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$, besteht überhaupt nur aus diesen beiden Elementen!

Notation 2.1. Für die weitere Diskussion seien K, L stets Körper.

Jedes von Null verschiedene Element $a \in K$ besitzt ein multiplikativ Inverses a^{-1}. Die *multiplikative Gruppe* von K wird mit $K^\times := K \setminus \{0\}$ bezeichnet.

Eine *Körpererweiterung* $K \leq L$ liegt vor, falls K eine Teilmenge von L ist und die Verknüpfungen in K sich durch Restriktion aus den Verknüpfungen in L ergeben. Man sagt dann, K sei ein *Teil-* oder *Unterkörper* von L, beziehungsweise L sei ein *Erweiterungs-* oder *Oberkörper* von K.

Bekannte Beispiele sind die unendlichen Körper $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ der rationalen, reellen und komplexen Zahlen. Die einfachsten Beispiele für endliche Körper erhält man durch Betrachtung der ganzen Zahlen $\mathbb{Z}$ modulo einer Primzahl $p \in \mathbb{P}$, in Zeichen $\mathbb{Z}/p\mathbb{Z}$. Nicht-Beispiele sind die Ringe $\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N} \setminus \mathbb{P}$.

2.2. **Primkörper und Charakteristik.** Ein *Primkörper* ist ein Körper, der keine echten Teilkörper besitzt, also in gewisser Weise minimal ist. Gibt es Primkörper? Wie sehen sie aus? Wir beobachten zwei wichtige Tatsachen. Erstens, für jede Menge $\mathcal{C}$, bestehend aus Teilkörpern von K, ist der Schnitt $\bigcap \mathcal{C}$ wiederum ein Teilkörper von K. Zweitens, der von 1 in K erzeugte Unterring ist entweder isomorph zu $\mathbb{Z}$ oder zu $\mathbb{Z}/n\mathbb{Z}$ für geeignetes $n \in \mathbb{N}$. Daraus folgt

Satz 2.2. *Jeder Körper enthält genau einen Primkörper. Bis auf Isomorphie sind die Primkörper genau die Körper $\mathbb{Q}$ und $\mathbb{Z}/p\mathbb{Z}$ für $p \in \mathbb{P}$.*

Die *Charakteristik* von K ist definiert als

$$\operatorname{char}(K) := \begin{cases} 0 & \text{falls der Primkörper von } K \text{ isomorph zu } \mathbb{Q} \text{ ist,} \\ p & \text{falls der Primkörper von } K \text{ isomorph zu } \mathbb{Z}/p\mathbb{Z} \text{ ist.} \end{cases}$$

Notwendigerweise hat jeder endliche Körper K Charakteristik $\mathrm{char}(K) > 0$. Der Körper $\mathbb{F}_2(t)$ der rationalen Funktionen über dem Körper $\mathbb{F}_2$ mit zwei Elementen hat Charakteristik zwei, ist aber dennoch unendlich.

Aufgrund unserer Überlegungen können wir noch an eine weitere Notation erinnern. Ist $K \leq L$ eine Körpererweiterung und $b \in L$, so bezeichnet $K(b)$ den kleinsten Teilkörper von L, der sowohl K als auch b enthält.

2.3. **Grad einer Erweiterung.** Sei $K \leq L$ eine Körpererweiterung. Wie läßt sich der Größenunterschied zwischen L und K quantitativ beschreiben? Für endliche Körper geschieht dies natürlich durch Abzählen und anschließende Quotientenbildung: $\#L/\#K$. Im allgemeinen Fall bemerken wir, daß L eine natürliche Vektorraumstruktur über K trägt—wir "vergessen" einfach die Multiplikation in L. Der *Grad* von L über K ist definiert als

$$[L : K] := \dim_K(L).$$

Die Erweiterung $K \leq L$ heißt *endlich*, falls sie endlichen Grad hat. Jede Erweiterung endlicher Körper ist endlich.

Als Beispiele halten wir fest:

$$\begin{aligned}
[\mathbb{C} : \mathbb{R}] &= 2, \text{ in der Tat ist } (1, i) \text{ eine Basis von } \mathbb{C} \text{ über } \mathbb{R};\\
[\mathbb{R} : \mathbb{Q}] &= \infty, \text{ denn } \mathbb{Q} \text{ ist abzählbar und } \mathbb{R} \text{ überabzählbar}\\
&\qquad \text{(Cantor läßt grüßen)};\\
[\mathbb{Q}(\pi) : \mathbb{Q}] &= \infty \text{ besagt, daß } \pi \text{ über } \mathbb{Q} \text{ transzendent ist.}
\end{aligned}$$

2.4. **Körpererweiterungen ins "Nichts".** Ausgehend von einem Körper K können wir Erweiterungen nach unten, das heißt Teilkörper, oder aber Erweiterungen nach oben, also Oberkörper, studieren. Für Erweiterungen nach unten ist der Rahmen automatisch gegeben: Alles spielt sich innerhald von K ab. Für Erweiterungen nach oben gibt es zunächst gar keinen Rahmen: Ein "Nichts" tut sich auf, das es zu füllen gilt.

Aus solch einer Situation sind zum Beispiel—mit einigen Geburtswehen—die komplexen Zahlen entwickelt worden. Konkret ging es darum, gewisse Lücken zu schließen, die das Lösen algebraischer Gleichungen über $\mathbb{R}$ verhinderten. So besitzt das Polynom $X^2 + 1$ keine Nullstellen in $\mathbb{R}$. Für das Polynom $X^{100} - 2$ finden sich in $\mathbb{R}$ nur zwei Lösungen. All diese Merkwürdigkeiten werden durch die Erweiterung des Zahlbereiches von $\mathbb{R}$ nach $\mathbb{C}$ beseitigt. Erstaunlicherweise reicht es dazu aus, einfach "formal" eine Lösung i der Gleichung $X^2 + 1 = 0$ zu $\mathbb{R}$ zu adjungieren.

Dieser Prozeß des Adjungierens von Polynomnullstellen läßt sich allgemein begrifflich fassen und ist unter dem Namen "Kronecker-Konstruktion" bekannt.

2.5. **Polynome.** Ein *Polynom* über K ist ein Ausdruck der Form

$$f = f_0 + f_1 X + f_2 X^2 + \ldots + f_n X^n \tag{2.1}$$

mit Koeffizienten $f_i \in K$ und $n \in \mathbb{N}_0$. Die Polynome über K lassen sich wie üblich addieren und multiplizieren; sie bilden einen kommutativen Ring $K[X]$ mit 1. In $K[X]$ besitzen nur die konstanten Polynome ungleich Null ein multiplikativ Inverses, sie bilden die *Einheitengruppe* $K[X]^\times = K^\times$. Insbesondere handelt es sich bei $K[X]$

nicht um einen Körper. (Jedoch erhält man durch Hinzufügen der fehlenden Inversen leicht den sogenannten Körper $K(X)$ der rationalen Funktionen über K.)

Sei $f \in K[X] \setminus \{0\}$ von der Gestalt (2.1) mit $f_n \neq 0$. Dann hat f den *Grad* $\operatorname{grad}(f) := n$. (Zweckmäßigerweise definiert man zusätzlich $\operatorname{grad}(0) := -\infty$.) Eine wichtige Eigenschaft der Gradabbildung beschreibt die Gleichung

$$\operatorname{grad}(gh) = \operatorname{grad}(g) + \operatorname{grad}(h) \qquad \text{für alle } g, h \in K[X].$$

Zum Beispiel folgt daraus unmittelbar, daß $K[X]$ nullteilerfrei und daher ein Integritätsbereich ist.

Das Polynom f heißt *normiert*, falls $f_n = 1$ ist. Bezüglich der symmetrisierten Teilbarkeitsrelation,

$$g \sim h \text{ in } K[X] \qquad \text{genau dann wenn } g \mid h \text{ und } h \mid g,$$

zerfällt $K[X] \setminus \{0\}$ in Äquivalenzklassen. Wegen $K[X]^\times = K^\times$ besitzt jede dieser Klassen genau einen normierten Vertreter.

Für die ganzen Zahlen gilt analog: $\mathbb{Z}^\times = \{1, -1\}$, und jede Äquivalenzklasse der symmetrisierten Teilbarkeitsrelation in $\mathbb{Z} \setminus \{0\}$ besitzt genau einen positiven Vertreter; zum Beispiel vertritt 24 die Klasse $\{24, -24\}$.

In $\mathbb{Z}$ spielen die Primzahlen eine wichtige Rolle. Sie fungieren als Elementarbausteine bezüglich der Multiplikation, da sie nicht weiter zerlegt werden können. In $K[X]$ wird diese Rolle von den irreduziblen Polynomen übernommen. Ein Polynom $f \in K[X]$ heißt *irreduzibel in* $K[X]$, falls

(i) f keine Einheit in $K[X]$ ist, und
(ii) f sich in $K[X]$ nur auf triviale Weise faktorisieren läßt, also für jede Zerlegung $f = gh$ mit $g, h \in K[X]$ gilt: entweder g oder h ist eine Einheit in $K[X]$.

Ohne weitere Ausführungen erinnern wir daran, daß sich in $K[X]$ die Division mit Rest (Rest von kleinerem Grade als der Divisor!) effektiv durchführen läßt. Der damit in Verbindung stehende Euklidische Algorithmus liefert effektiv den größten gemeinsamen Teiler zweier Polynome. Es folgt, daß $K[X]$ ein Hauptidealring ist und eine eindeutige Primfaktorzerlegung zuläßt. All dies funktioniert ganz ähnlich wie in dem bekannten Ring $\mathbb{Z}$, dessen Ideale bekanntlich von der Form $n\mathbb{Z}$, $n \in \mathbb{N}_0$, sind.

Wir erwähnen nun noch zwei direkte Anwendungen der Division mit Rest. Für alle $f \in K[X]$ und $a \in K$ gilt: $f(a) = 0$ genau dann wenn $(X - a) \mid f$ in $K[X]$. Per Induktion folgt daraus

Satz 2.3. *Ein Polynom vom Grad $n \geq 0$ über K besitzt höchstens n verschiedene Nullstellen in K.*

Sei $K \leq L$ eine endliche Körpererweiterung und $b \in L$. Dann gibt es genau ein normiertes irreduzibles Polynom $f \in K[X]$ mit $f(b) = 0$, dieses wird als *Minimalpolynom* von b über K bezeichnet. Wie im nächsten Abschnitt erläutert, gilt dann $K(b) \cong K[X]/(f)$.

2.6. **Kronecker-Konstruktion.** Gegeben sei ein nicht-konstantes Polynom $f \in K[X]$. Gesucht ist ein Oberkörper L von K, in dem f eine Nullstelle besitzt. Zum besseren Verständnis der folgenden Überlegungen machen wir schon jetzt eine Übersichtsskizze.

$$\begin{array}{ccccc} L = K(b) & \xrightarrow[\cong]{\widehat{\eta}} & L_0 = K_0(b_0) & \big(\cong K[X]/(f)\big) \\ \vert & & \vert & \\ K & \xrightarrow[\cong]{\eta} & K_0 & \\ & & & \\ f \in K[X] & \xmapsto[\cong]{\tilde{\eta}} & f_0 \in K_0[X] & \end{array}$$

Wir dürfen o.B.d.A. annehmen, daß f irreduzibel über K ist. Dann ist $(f) = f \cdot K[X]$ ein maximales Ideal von $K[X]$, und daher $L_0 := K[X]/(f)$ ein Körper. Die Elemente von L_0 sind gegeben durch die Restklassen $\overline{g} := g + (f)$, $g \in K[X]$. Addition und Multiplikation werden mit Hilfe von Representanten durchgeführt, Gleicheit ergibt sich aus der Kongruenz von Representanten modulo (f).

Wir behaupten, daß L_0 bis auf Isomorphie schon der gesuchte Körper ist. Dazu bemerken wir, daß die Abbildung $\eta : K \to L_0$, $a \mapsto \overline{a}$ eine Einbettung von K in L_0 liefert. Wir bezeichnen das Bild von K in L_0 mit K_0. Die Abbildung η induziert auf natürliche Weise einen Isomorphismus $\tilde{\eta} : K[X] \to K_0[X]$, sei f_0 das Bild von f unter $\tilde{\eta}$. Wir zeigen nun, daß f_0 in L_0 die Nullstelle $b_0 := \overline{X}$ besitzt. In der Tat gilt in $L_0 = K[X]/(f)$:

$$f_0(b_0) = f_0(\overline{X}) = \overline{f(X)} = f + (f) = 0 + (f) = 0.$$

Bilden wir also über K einen zu L_0 isomorphen Oberkörper L, so daß sich der Isomorphismus $\eta : K \to K_0$ fortsetzt zu einem Isomorphismus $\widehat{\eta} : L \to L_0$, und wählen wir $b \in L$ mit $\widehat{\eta}(b) = b_0$, so haben wir das ursprüngliche Problem gelöst: $K \leq L$ und $f(b) = 0$.

Bei dieser Konstruktion ist zu beachten, daß der Oberkörper L in gewisser Hinsicht so klein wie möglich ausfällt. Es gilt nämlich $L = K(b)$. Was ist nun der Grad der Körpererweiterung $K \leq L$? Sei $d := \operatorname{grad}(f)$. Es ist leicht zu prüfen, daß $(1, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{d-1})$ eine Basis von $L_0 = K[X]/(f)$ über K_0 bildet. Also ist $(1, b, b^2, \ldots, b^{d-1})$ eine Basis von L über K, und $[L : K] = d = \operatorname{grad}(f)$.

Gibt es vielleicht noch ganz andere Oberkörper von K, in denen f eine Nullstelle besitzt? Im Grunde genommen nicht. Es gilt nämlich

Theorem 2.4 (Kronecker)**.** *Sei $f \in K[X]$ irreduzibel. Dann liefert die voranstehende Konstruktion einen Oberkörper $L = K(b)$ von K mit $f(b) = 0$. Dieser ist bis auf Isomorphie eindeutig bestimmt, in folgendem Sinne.*

Sei $\eta : K \to K_0$ ein Körperisomorphismus, und bezeichne mit f_0 das Bild von f unter dem induzierten Ringisomorphismus $\tilde{\eta} : K[X] \to K_0[X]$. Sei $L_0 = K_0(b_0)$ ein Oberkörper von K_0 mit $f_0(b_0) = 0$. Dann läßt sich η fortsetzen zu einem Körperisomorphismus $\widehat{\eta} : L \to L_0$ mit $\widehat{\eta}(b) = b_0$.

Zum Nachweis der Eindeutigkeitsaussage vergewissert man sich, daß die einzig denkbare Abbildung $\widehat{\eta}$ tatsächlich einen Isomorphismus liefert.

2.7. **Beispiele zur Kronecker-Konstruktion.** Wir betracheten drei Beispiele.
Beispiel 1. Für $K = \mathbb{R}$ und $f = X^2 + 1$ erhalten wir $\mathbb{C} = \mathbb{R}(i) \cong \mathbb{R}[X]/(X^2 + 1)$. Addition und Multiplikation von komplexen Zahlen ergeben sich wie vertraut.

Beispiel 2. Sei $K = \mathbb{Q}$ und $f = X^2 - 5$. Da f den Grad zwei hat und keine rationale Nullstelle besitzt, ist f irreduzibel über $\mathbb{Q}$. Wir tun so, als ob wir den Körper $\mathbb{R}$ nicht zur Verfügung hätten, und folgen der Kronecker-Konstruktion: $L = \mathbb{Q}(b)$, wobei $L \cong \mathbb{Q}[X]/(X^2 - 5)$ und $b \mapsto \overline{X}$. Suggestiv und zweckmäßig ist die Schreibweise $\sqrt{5} := b$; damit ist aber keineswegs die positive reelle Wurzel von 5 gemeint.

Eine Basis von L über $\mathbb{Q}$ ist gegeben durch $(1, \sqrt{5})$; jedes Element $a \in L$ läßt sich schreiben als $a = x + y\sqrt{5}$ mit $x, y \in \mathbb{Q}$. Addition und Multiplikation in L lassen sich auf die bekannten Verknüpfungen in $\mathbb{Q}$ wie folgt zurückführen:

$$(x + y\sqrt{5}) + (\tilde{x} + \tilde{y}\sqrt{5}) = (x + \tilde{x}) + (y + \tilde{y})\sqrt{5},$$
$$(x + y\sqrt{5}) \cdot (\tilde{x} + \tilde{y}\sqrt{5}) = (x\tilde{x} + 5y\tilde{y}) + (x\tilde{y} + y\tilde{x})\sqrt{5}.$$

Wie sieht das multiplikativ Inverse von $x + y\sqrt{5} \in L \setminus \{0\}$ aus? Durch Brucherweiterung ergibt sich

$$\frac{1}{x + y\sqrt{5}} = \frac{x - y\sqrt{5}}{x^2 - 5y^2} = \frac{x}{x^2 - 5y^2} - \frac{y}{x^2 - 5y^2}\sqrt{5}.$$

Beispiel 3. Jetzt wollen wir den einfachsten endlichen Körper konstruieren, der nicht von der Form $\mathbb{Z}/p\mathbb{Z}$, $p \in \mathbb{P}$, ist. Achte auf die Ähnlichkeit zu den vorherigen zwei Beispielen.

Sei $K = \mathbb{F}_2 = \mathbb{Z}/\mathbb{Z}_2$ und $f = X^2 + X + 1$. Da f den Grad zwei hat und keine Nullstelle in $\mathbb{F}_2$ besitzt, ist f irreduzibel über $\mathbb{F}_2$. Wir folgen der Kronecker-Konstruktion und bilden $L = \mathbb{F}_2(b)$, wobei $L \cong \mathbb{F}_2[X]/(X^2 + X + 1)$ und $b \mapsto \overline{X}$. Jetzt bietet sich keine suggestivere Schreibweise für b an.

Eine Basis von L über $\mathbb{F}_2$ ist gegeben durch $(1, b)$; jedes Element $a \in L$ läßt sich schreiben als $a = x + yb$ mit $x, y \in \mathbb{F}_2$. Also besteht L aus den vier Elementen 0, 1, b und $1 + b$. Addition und Multiplikation in L lassen sich in diesem Falle natürlich tabellarisch festhalten. Es ist jedoch lehrreich, sie wie zuvor formal auf die bekannten Verknüpfungen in $\mathbb{F}_2$ zurückzuführen:

$$(x + yb) + (\tilde{x} + \tilde{y}b) = (x + \tilde{x}) + (y + \tilde{y})b,$$
$$(x + yb) \cdot (\tilde{x} + \tilde{y}b) = (x\tilde{x} + y\tilde{y}) + (x\tilde{y} + y\tilde{x} + y\tilde{y})b.$$

Was läßt sich zur Inversenbildung sagen?

2.8. **Zerfällungskörper.** Die Konstruktion von Kronecker läßt sich offenbar wiederholt durchführen. Dieser Vorgang soll nun begrifflich gefestigt werden.

Sei $f \in K[X]$. Ein Oberkörper L von K heißt *Zerfällungskörper für f über K*, falls

(i) das Polynom f über L in Linearfaktoren zerfällt,
(ii) aber f über keinem Zwischenkörper Z mit $K \leq Z \lneqq L$ in Linearfaktoren zerfällt.

Zum Beispiel zerfällt jedes Polynom $f \in \mathbb{C}[X]$ über $\mathbb{C}$ selbst in Linearfaktoren. (Dies ist gerade die Aussage, daß $\mathbb{C}$ algebraisch abgeschlossen ist.) Der Körper $\mathbb{Q}(\sqrt{5})$ ist ein Zerfällungskörper für $X^2 - 5$ über $\mathbb{Q}$, aber nicht für $X^2 - 3$ oder $X^2 - 1$.

Aus Theorem 2.4 ergibt sich per Induktion

Theorem 2.5. *Sei $f \in K[X]$. Dann existiert bis auf Isomorphie genau ein Zerfällungskörper für f über K.*

2.9. **Irreduzible Polynome.** Um Erweiterungskörper von K effektiv zu konstruieren, ist es notwendig, Kriterien zu entwickeln, mit deren Hilfe irreduzible Polynome gefunden oder als solche erkannt werden können. Im nächsten Abschnitt werden wir auf dieses Problem speziell für endliche Grundkörper K zurückkommen. An dieser Stelle wollen wir drei bekannte Methoden auflisten: das Eisenstein Kriterium, das Gauss Lemma und die Tatsache, daß ein reduzibles Polynom $f \in K[X]$ vom Grad kleinergleich drei notwendigerweise eine Nullstelle in K besitzt.

Von der Irreduzibilität eines Polynoms $f \in K[X]$ kann offenbar nur dann sinnvoll die Rede sein, wenn diese an den Körper K gebunden ist: Über einem geeigneten Erweiterungskörper L von K wird f immer in Linearfaktoren zerfallen. Trotzdem bleiben gewisse Aussagen durch den Übergang von $K[X]$ zu $L[X]$ unberührt. Zum Beispiel spielt es keine Rolle ob wir den Euklidischen Algorithmus für Polynome $f, g \in K[X]$ über K selbst oder über einem Erweiterungskörper anwenden. Es gilt

Lemma 2.6. *Sei $K \leq L$, und seien $f, g, h \in K[X]$. Dann ist* $\mathrm{ggT}(f,g) = h$ *in $K[X]$ genau dann wenn* $\mathrm{ggT}(f,g) = h$ *in $L[X]$. Insbesondere gilt $f \mid g$ in $K[X]$ genau dann wenn $f \mid g$ in $L[X]$.*

2.10. **Mehrfache und Einfache Nullstellen.** Sei $f \in K[X]$. Die Menge der Nullstellen von f in K bezeichnen wir mit $\mathrm{Nullst}(f, K)$. Sei nun $f \neq 0$, und $a \in \mathrm{Nullst}(f, K)$. Aufgrund von Lemma 2.6 dürfen wir die folgende Sprechweise einführen: a ist eine *Nullstelle von f der Vielfachheit n*, falls $(X-a)^n \mid f$ aber $(X-a)^{n+1} \nmid f$. Eine Nullstelle der Vielfachheit eins heißt *einfache Nullstelle*, eine der Vielfachheit größergleich zwei *mehrfache Nullstelle*.

In der elementaren Analysis wird für (hinreichend glatte) reelle Funktionen ein Zusammenhang zwischen der Vielfachheit einer Nullstelle und den lokalen Ableitungen hergestellt. Diese Überlegungen lassen sich für Polynome über beliebigen Körpern ganz formal anstellen. Die *Ableitung* von $f = \sum_{i=0}^{n} f_i X^i \in K[X]$ ist definiert als $f' := \sum_{i=1}^{n} i f_i X^{i-1}$. Es gelten die üblichen Rechenregeln, und man zeigt: f hat eine mehrfache Nullstelle genau dann wenn $\mathrm{ggT}(f, f') \neq 1$. Hieraus folgt schon die erste Hälfte des folgenden Satzes.

Satz 2.7. *Gilt entweder* $\mathrm{char}(K) = 0$ *oder ist K ein endlicher Körper, so hat jedes irreduzible Polynom $f \in K[X]$ nur einfache Nullstellen.*

Für den Beweis der zweiten Hälfte verwendet man die folgende Überlegung. Sei K ein Körper mit $p = \mathrm{char}(K) > 0$. Dann gilt für alle $a, b \in K$:

$$(a \cdot b)^p = a^p \cdot b^p,$$

$$(a+b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} + b^p = a^p + b^p.$$

Somit liefert das Potenzieren mit p einen Monomorphismus $F : K \to K$, der unter dem Namen *Frobenius-Monomorphismus* bekannt ist. Im allgemeinen ist F nicht surjektiv auf K, aber falls K endlich ist, so liefert F tatsächlichen einen Körperautomorphismus.

Beweis von Satz 2.7, zweite Hälfte. Sei also K endlich und $f \in K[X]$ irreduzibel. Für einen Widerspruch sei angenommen, f besitze mehrfachen Nullstellen. Aus $\mathrm{ggT}(f, f') \neq 1$ und $\mathrm{grad}(f) > \mathrm{grad}(f')$ folgt dann $f' = 0$, also $f = g(X^p)$ für

geeignetes $g \in K[X]$. Koeffizientenweise läßt sich nun der Automorphismus F^{-1} auf g anwenden: Wir finden $h \in K[X]$, so daß $f = g(X^p) = (h(X))^p = h^p$ gilt. Dies widerspricht der Irreduzibilität von f. □

2.11. **Flashback: Galoissche Theorie.** Sei $K \leq L$ eine endliche Körpererweiterung. Unter gewissen Zusatzvorraussetzungen liefert die Galoissche Theorie eine Beschreibung des Zwischenkörperverbandes von $K \leq L$ anhand der Untergruppenstruktur der Automorphismengruppe $\mathrm{Aut}_K(L)$. Daran soll durch eine kleine Skizze erinnert werden.

Die Automorphismen von L, welche einen gegebenen Zwischenkörper Z von $K \leq L$ elementweise festhalten, bilden eine Untergruppe von $\mathrm{Aut}(L)$,

$$\mathrm{Aut}_Z(L) := \{\sigma \in \mathrm{Aut}(L) \mid \forall a \in Z : \sigma(a) = a\}.$$

Umgekehrt, erhält man zu jeder Untergruppe $U \leq \mathrm{Aut}_K(L)$ einen Zwischenkörper von $K \leq L$, nämlich den Fixkörper

$$\mathrm{Fix}_L(U) := \{a \in L \mid \forall \sigma \in U : \sigma(a) = a\}.$$

Für jeden Zwischenkörper Z von $K \leq L$ gilt $Z \subseteq \mathrm{Fix}_L(\mathrm{Aut}_Z(L))$, und für jede Untergruppe U von $\mathrm{Aut}_K(L)$ gilt $U \subseteq \mathrm{Aut}_{\mathrm{Fix}_L(U)}(L)$.

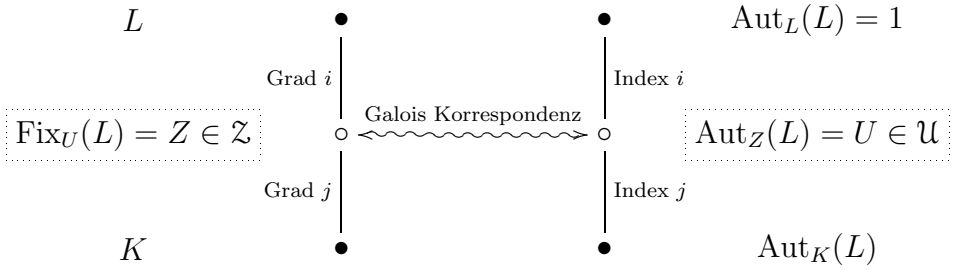
Die Erweiterung $K \leq L$ heißt *galoissch*, falls $K = \mathrm{Fix}_L(\mathrm{Aut}_K(L))$. In diesem Falle liefern die Abbildungen $Z \mapsto \mathrm{Aut}_Z(L)$ und $U \mapsto \mathrm{Fix}_L(U)$ einen Antiisomorphismus zwischen

$$\mathfrak{Z} := \{Z \mid K \leq Z \leq L\}, \quad \text{dem Verband aller Zwischenkörper von } K \leq L,$$

und

$$\mathfrak{U} := \{U \mid U \leq \mathrm{Aut}_K(L)\}, \quad \text{dem Verband aller Untergruppen von } \mathrm{Aut}_K(L),$$

mit weiteren Detaileigenschaften, auf die wir hier nicht weiter eingehen.



3. Die Spezielle Struktur Endlicher Körper

Die einfachsten endlichen Körper sind die Primkörper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $p \in \mathbb{P}$. Wir haben aber schon gesehen, daß es auch kompliziertere endliche Körper gibt. So liefert Beispiel 3 in Abschnitt 2.7 einen Körper mit vier Elementen. Gerade für spätere Anwendungen ist es wichtig, sich auch über diese komplizierteren endlichen Körper einen guten Überblick zu verschaffen.

3.1. **Zur Existenz und Eindeutigkeit Endlicher Körper.**

Satz 3.1. *Sei K ein endlicher Körper. Dann ist $\#K = p^n$, wobei $p = \mathrm{char}(K) \in \mathbb{P}$ und n den Grad von K über seinem Primkörper bezeichnet.*

Beweis. Der Primkörper κ von K ist endlich, also nicht isomorph zu $\mathbb{Q}$. Es gilt $p = \mathrm{char}(K) > 0$ und $\kappa \cong \mathbb{F}_p$. Weiterhin ist K ein endlicher κ-Vektorraum der Dimension n. Es gilt $(K, +) \cong \kappa^n$, also $\#K = (\#\kappa)^n = p^n$. □

Notation 3.2. Fürs folgende sei $p \in \mathbb{P}$.

Als nächstes geht es darum, zu klären, für welche $n \in \mathbb{N}$ es Körper mit genau p^n Elementen gibt, und wieviele.

Lemma 3.3. *Sei K ein endlicher Körper mit $\mathrm{char}(K) = p$. Sei κ der Primkörper von K, und sei $n \in \mathbb{N}$. Dann sind äquivalent:*

(i) *K besteht aus genau p^n Elementen.*
(ii) *K ist ein Zerfällungskörper für $X^{p^n} - X$ über κ.*

Beweis. Wir schreiben $q := p^n$ und $f := X^q - X$.
"(i) → (ii)". Sei $\#K = q$. Dann ist $K^\times$ eine Gruppe der Ordnung $q - 1$, also gilt nach Lagrange $x^{q-1} - 1 = 0$ für alle $x \in K^\times$. Wir erhalten $f(x) = x^q - x = 0$ für alle $x \in K$. Aus $\mathrm{grad}(f) = q$ folgt, daß $K = \mathrm{Nullst}(f, K)$ ein Zerfällungskörper von f über κ ist.
"(ii) → (i)". Sei K ein Zerfällungskörper von f über κ. Offenbar ist $\mathrm{ggT}(f, f') = \mathrm{ggT}(f, -1) = 1$, also hat f nur einfache Nullstellen und $\#\,\mathrm{Nullst}(f, K) = q$. Die n-te Potenz des Frobenius-Automorphismus $F^n : K \to K$, $x \mapsto x^q$ ist ein Automorphismus von K. Daher ist $Z := \mathrm{Nullst}(f, K) = \mathrm{Fix}_K(\langle F^n \rangle)$ ein Zwischenkörper von $\kappa \leq K$, über dem f in Linearfaktoren zerfällt. Es folgt $K = Z$, und damit $\#K = \#\,\mathrm{Nullst}(f, K) = q$. □

Aus der Existenz und Eindeutigkeit von Zerfällungskörpern (Theorem 2.5) folgt

Theorem und Definition 3.4. *Sei $n \in \mathbb{N}$. Dann gibt es bis auf Isomorphie genau einen Körper mit genau p^n Elementen. Ein Vertreter dieser Isomorphieklasse wird üblicherweise mit $\mathbb{F}_{p^n}$ bezeichnet.*

Korollar 3.5. *Sei $n \in \mathbb{N}$. Dann ist $\mathbb{F}_{p^n}$ ein Zerfällungskörper für $X^{p^n-1} - 1$ über seinem Primkörper.*

Das Korollar unterstreicht die eigentlich triviale Erkenntnis, daß es sich bei den endlichen Körpern gerade um die Kreisteilungskörper in positiver Charakteristik handelt.

3.2. **Ordnung und Exponent einer Endlichen Gruppe.** Sei G eine endliche Gruppe. Für jedes $g \in G$ ist $I_g = \{k \in \mathbb{Z} \mid g^k = 1\}$ ein nicht-triviales Ideal von $\mathbb{Z}$, und die *Ordnung* von g ist definiert als der positive Erzeuger dieses Ideales; in anderen Worten $\mathrm{ord}(g) := \min\{n \in \mathbb{N} \mid g^n = 1\}$. Offenbar ist auch $\{k \in \mathbb{Z} \mid \forall g \in G : g^k = 1\} = \bigcap\{I_g \mid g \in G\}$ ein nicht-triviales Ideal von $\mathbb{Z}$, dessen positiver Erzeuger $e(G) := \min\{n \in \mathbb{N} \mid \forall g \in G : g^n = 1\}$ der *Exponent* von G genannt wird. Es gilt $e(G) = \mathrm{kgV}\{\mathrm{ord}(g) \mid g \in G\}$. Nach dem Satz von Lagrange ist $e(G)$ stets ein Teiler der *Ordnung* $|G| := \#G$ von G.

3.3. **Die Multiplikative Gruppe eines Endlichen Körpers.**

Satz 3.6. *Sei K ein Körper, und sei G eine endliche Untergruppe von $K^\times$. Dann ist G zyklisch.*

Beweis. Es genügt zu zeigen, daß $e(G) = |G|$ ist. Nach Lagrange gilt sicherlich $e(G) \leq |G|$. Andererseits ist $G \subseteq \mathrm{Nullst}(X^{e(G)} - 1, K)$, also $|G| \leq e(G)$. □

Korollar und Definition 3.7. *Sei K ein endlicher Körper. Dann ist $K^\times$ zyklisch. Ein Erzeuger der Gruppe $K^\times$ heißt* primitives Element *von K.*

Durch Auswahl eines primitiven Elementes a in einem endlichen Körper K läßt sich die Multiplikation in K besonders übersichtlich durchführen. Dazu werden die diskrete Exponential- und Logarithmusfunktion zur Basis a definiert; vergleiche mit den Beispielen in Kapitel 4.

3.4. **Der Unterkörperverband eines Endlichen Körpers.** Wir benötigen

Lemma 3.8. *Sei K ein Körper, und seien $m, n \in \mathbb{N}$.*
(1) *Es gilt $(X^m - 1) \mid (X^n - 1)$ in $K[X]$ genau dann wenn $m \mid n$ in $\mathbb{Z}$.*
(2) *Es gilt $(p^m - 1) \mid (p^n - 1)$ in $\mathbb{Z}$ genau dann wenn $m \mid n$ in $\mathbb{Z}$.*

Beweis. Wir beweisen (1), dann folgt (2) ganz ähnlich. Division mit Rest liefert $n = sm + t$ mit $s, t \in \mathbb{N}_0$ und $0 \leq t < m$, sowie

$$X^n - 1 = X^t \underbrace{\sum_{i=0}^{s-1} X^{im} (X^m - 1)}_{= X^{sm} - 1} + (X^t - 1).$$

Es gilt $t = 0$ genau dann wenn $X^t - 1 = 0$. □

Der folgende Satz zeigt das der Unterkörperverband eines endlichen Körpers $\mathbb{F}_{p^n}$ isomorph ist zum Teilerverband der natürlichen Zahl n.

Satz 3.9. *Seien $m, n \in \mathbb{N}$, und $L \cong \mathbb{F}_{p^n}$. Dann besitzt L einen Unterkörper $K \cong \mathbb{F}_{p^m}$ genau dann wenn $m \mid n$ in $\mathbb{Z}$.*

Beweis. Angenommen L besitzt einen Unterkörper $K \cong \mathbb{F}_{p^m}$. Setzte $k := [L : K]$. Dann gilt $p^n = \#L = (\#K)^k = p^{km}$, also $m \mid n$.

Gelte nun umgekehrt $m \mid n$. Bezeichne mit κ den Primkörper von L. Nach Lemma 3.8 erhalten wir $(p^m - 1) \mid (p^n - 1)$ und $(X^{p^m - 1} - 1) \mid (X^{p^n - 1} - 1)$. Nun ist L ein Zerfällungskörper für $X^{p^n - 1} - 1$ über κ. Also enthält L einen Zerfällungskörper K für $X^{p^m - 1} - 1$ über κ, und offenbar gilt $K \cong \mathbb{F}_{p^m}$. □

3.5. **Die Automorphismen eines Endlichen Körpers.** Als Beispiel haben wir in Abschnitt 2.10 bereits den Frobenius-Automorphismus kennengelernt. Es gilt sogar

Satz 3.10. *Sei $n \in \mathbb{N}$ und $L \cong \mathbb{F}_{p^n}$. Dann ist* $\mathrm{Aut}(L)$ *zyklisch der Ordnung n und wird erzeugt von dem Frobenius-Automorphismus $F : L \to L$, $x \mapsto x^p$. Für jeden natürlichen Teiler $m \mid n$ ist* $\mathrm{Fix}_L(\langle F^m \rangle) \cong \mathbb{F}_{p^m}$.

Beweis. Sei a ein primitives Element von L, und bezeichne mit κ den Primkörper von L. Insbesondere ist dann $L = \kappa(a)$. Also hat das Minimalpolynom f von a über κ den Grad n. Jeder Automorphismus σ von L fixiert die Elemente des Primkörpers und

ist eindeutig bestimmt durch das Bild a^σ von a. Weiterhin gilt $f(a^\sigma) = (f(a))^\sigma = 0$. Da f höchstens n Nullstellen hat, ergibt sich $\#\operatorname{Aut}(L) \leq n$.

Sei nun $m \in \mathbb{N}$ mit $m \mid n$. Dann ist $K := \operatorname{Fix}_L(\langle F^m \rangle)$ ein Zerfällungskörper von $X^{p^m} - X$, besitzt also genau p^m Elemente. Schließlich folgt daraus, daß der Frobenius-Automorphismus F die Ordnung n hat. Also ist $\operatorname{Aut}(L) = \langle F \rangle$ zyklisch der Ordnung n. □

3.6. **Die Galoissche Theorie Endlicher Körper.** Sei $L \cong \mathbb{F}_{p^n}$. Die Sätze 3.9 und 3.10 lassen sich als Spezialfälle der allgemeinen Galoisschen Theorie deuten. Sie besagen, daß zwischen dem Teilkörperverband $\mathfrak{Z}$ eines endlichen Körpers L und dem Untergruppenverband $\mathfrak{U}$ der Automorphismengruppe $\operatorname{Aut}(L)$ ein Antiisomorphismus besteht. Der Verband $\mathfrak{Z}$ ist nach Satz 3.9 zudem isomorph zum Teilerverband der natürlichen Zahl n.

4. Explizite Konstruktion Endlicher Körper

Im voranstehenden Kapitel wurden die grundlegenden strukturellen Eigenschaften endlicher Körper dargestellt. Jeder endliche Körper läßt sich mittels der Kronecker-Konstruktion aus einem endlichen Primkörper $\mathbb{F}_p$ und einem irreduziblen Polynom $f \in \mathbb{F}_p[X]$ herstellen. Wegen Theorem 3.4 gilt

Korollar 4.1. *Sei $p \in \mathbb{P}$. Dann gibt es zu jedem $n \in \mathbb{N}$ wenigstens ein irreduzibles Polynom $f \in \mathbb{F}_p[X]$ mit* $\operatorname{grad}(f) = n$.

Für die Konstruktion eines endlichen Körpers mit 5^{27} Elementen benötigen wir zum Beispiel ein irreduzibles Polynom $f \in \mathbb{F}_5[X]$ vom Grad 27. Es ist nicht offensichtlich, wie sich am geschicktesten ein solches Polynom bestimmen läßt.

Das Auffinden irreduzibler Polynome, das Testen eines gegebenen Polynoms auf Irreduzibilität oder das Faktorisieren einenes gegeben Polynoms in Primfaktoren sind alles wichtige Probleme, die hier nicht allgemein diskutiert werden können. Stattdessen betrachten wir abschließend zwei besonders einfache Beispiele.

Beispiel 1. Wir konstruieren einen Körper $\mathbb{F}_9$ über $\mathbb{F}_3 = \{0, 1, -1\}$ und bestimmen dessen primitive Elemente.

Zunächst benötigen wir ein irreduzibles Polynom $f \in \mathbb{F}_3[X]$ vom Grad zwei, und es genügt offenbar, die Suche auf normierte Polynome zu beschränken. Es gibt genau neun normierte Polynome vom Grad zwei über $\mathbb{F}_3$. Die reduziblen lassen sich leicht berechnen:

$$\begin{aligned}
(X-0)(X-0) &= X^2,\\
(X-1)(X-0) &= X^2 - X,\\
(X+1)(X-0) &= X^2 + X,\\
(X-1)(X-1) &= X^2 + X + 1,\\
(X-1)(X+1) &= X^2 - 1,\\
(X+1)(X+1) &= X^2 - X + 1.
\end{aligned}$$

Gleichzeitig erkennen wir $f_1 := X^2 + 1$, $f_2 := X^2 + X - 1$ und $f_3 := X^2 - X - 1$ als irreduzibel über $\mathbb{F}_3$. Die Kronecker-Konstruktion kann nun mit jedem dieser Polynome durchgeführt werden, um einen Körper $\mathbb{F}_9$ zu erhalten. Zweckmäßig ist es jedoch, für die Konstruktion entweder f_2 oder f_3 zu wählen. Denn nur die Nullstellen

dieser beiden Polynome liefern automatisch primitive Elemente von $\mathbb{F}_9$. Dies sieht man wie folgt ein.

Sei $a \in \mathbb{F}_9$ mit $f_1(a) = a^2 + 1 = 0$. Dann ist $a^2 = -1$, also $a^4 = 1$. Da die multiplikative Gruppe $\mathbb{F}_9{}^\times$ zyklisch von der Ordnung acht ist, wird sie nicht von a erzeugt. Also ist a kein primitives Element von $\mathbb{F}_9$.

Sei andererseits $b \in \mathbb{F}_9$ mit $f_2(b) = b^2 + b - 1 = 0$. Wir bemerken, daß dann $b \neq 0$ und $f_3(b^{-1}) = b^{-2} - b^{-1} - 1 = -b^{-2} f_2(b) = 0$ ist. Also ist f_3 das Minimalpolynom von b^{-1} über $\mathbb{F}_3$. Die Polynome f_2 und f_3 sind "assoziiert" mittels der Gleichung $f_3(X) = -X^2 f_2(X^{-1})$. Nun ist b ein primitives Element von $\mathbb{F}_9$ genau dann wenn b^{-1} ein primitives Element von $\mathbb{F}_9$ ist. Aufgrund der vorangehenden Überlegung erkennen wir b und b^{-1} tatsächlich als primitive Elemente von $\mathbb{F}_9$.

Die Potenzen von b lassen sich natürlich auch ganz konkret berechnen:

$$\begin{aligned} b^0 &= 1, & b^1 &= b, \\ b^2 &= -b + 1, & b^3 &= -b^2 + b = -b - 1, \\ b^4 &= -b^2 - b = -1, & b^5 &= -b, \\ b^6 &= -b^2 = b - 1, & b^7 &= -b^3 = b + 1. \end{aligned}$$

Mit Hilfe dieser Tabelle lassen sich Addition und Multiplikation in $\mathbb{F}_9$ effizient durchführen. Zum Beispiel berechnet man leicht

$$\begin{aligned} \frac{b}{b^7 - b^3} &= \frac{b}{(b+1) - (-b-1)} = \frac{b}{-b-1} \\ &= bb^{-3} = b^{-2} = \begin{cases} b^6 & \text{in multiplikativer Schreibweise,} \\ b - 1 & \text{in additiver Schreibweise.} \end{cases} \end{aligned}$$

Beispiel 2. Wir konstruieren einen Körper $\mathbb{F}_8$ über $\mathbb{F}_2$ und bestimmen dessen primitive Elemente.

Wir benötigen ein irreduzibles Polynom $f \in \mathbb{F}_2[X]$ vom Grad drei. Es genügt, normierte Polynome zu betrachten, die nicht schon durch X teilbar sind. Unter den vier Kandidaten erweisen sich $X^3 + 1$ und $X^3 + X^2 + X + 1$ als reduzibel, da sie jeweils die Nullstelle 1 besitzen. Die Polynome $f_1 = X^3 + X + 1$ und $f_2 = X^3 + X^2 + 1$ erkennen wir als irreduzibel über $\mathbb{F}_2$.

Die Kronecker-Konstruktion kann mit f_1 oder f_2 durchgeführt werden. Da $\mathbb{F}_8{}^\times$ die Ordnung sieben hat, liefert jedes $a \in \mathbb{F}_8{}^\times$ ein primitives Element. Ähnlich wie zuvor bemerken wir, daß die beiden Polynome durch die Gleichung $f_2(X) = X^3 f_1(X^{-1})$ verbunden sind: Die drei Nullstellen von f_1 gehen durch Inversenbildung in die Nullstellen von f_2 über.

Sei $a \in \mathbb{F}_8$ mit $f_1(a) = 0$. Die Potenzen von a berechnen sich wie folgt:

$$\begin{aligned} a^0 &= 1, & a^1 &= a, \\ a^2 &= a^2, & a^3 &= a + 1, \\ a^4 &= a^2 + a, & a^5 &= a^3 + a^2 = a^2 + a + 1, \\ a^6 &= a^3 + a^2 + a = a^2 + 1. \end{aligned}$$

Wieder lassen sich Addition und Multiplikation konkret ausführen.

Literatur

[1] E. Artin, *Galoissche Theorie* (Verlag Harri Deutsch, Zürich, 1973).

[2] L.E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory* (Teubner, Leipzig, 1901; Dover, New York, 1958).

[3] R. Lindl und H. Niederreiter, *Introduction to Finite Fields and Their Applications* (Cambridge University Press, Cambridge, 1986).

[4] R.J. McEliece, *Finite Fields for Computer Scientists and Engineers* (Kluwer Academic Publishers, Boston, 1987).

Mathematisches Institut,
Heinrich-Heine-Universität,
40225 Düsseldorf, Germany.

E-mail address: klopsch@math.uni-duesseldorf.de