Codierungstheorie
endliche Körper

Reinhold Hübl

Herbst 2022 / 3. Vorlesung

Definition

Ein **Körper** ist eine nicht–leere Menge K mit zwei ausgezeichneten Elementen 0 und 1, wobei $0 \neq 1$, und mit zwei inneren Verknüpfungen (also Abbildungen) $+$ und $\cdot$

$$\begin{array}{ccccc} + & : & K \times K \longrightarrow K, & & (a,b) \longmapsto a+b \\ \cdot & : & K \times K \longrightarrow K, & & (a,b) \longmapsto a \cdot b \end{array}$$

so dass gilt

1. $(K, +)$ ist eine kommutative Gruppe mit neutralem Element 0.
2. $(K \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe mit neutralem Element 1.
3. Es gilt das Distributivgesetz, dh. für alle $a, b, c \in K$ gilt

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Beispiele

Beispiel

$\mathbb{R}$, $\mathbb{Q}$ und $\mathbb{C}$ sind Körper

Beispiel

Die Menge $\mathbb{F} = \{0, 1\}$ mit

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

ist ein Körper. Dieser Körper wird auch mit $\mathbb{F}_2$ bezeichnet.

Definition

Ein endlicher Körper K ist ein Körper $(K, +, \cdot)$ mit $|K| < \infty$.

Beispiele

Beispiel

Die Menge $\mathbb{Z}_n$ oder $\mathbb{Z}/n\mathbb{Z}$ ist der Menge der Äquivalenzklassen ganzer Zahlen modulo n. Er kann beschrieben werden durch die Repräsentanten $0, 1, \ldots, n-1$. Auf diesen Repräsentanten definieren wir eine Addition $+$ und eine Multiplikation $\cdot$ explizit wie folgt:

$$\begin{aligned} x + y &= (x+y) \mod n \\ x \cdot y &= x \cdot y \mod n \end{aligned}$$

dh. wir addieren bzw. multiplizieren die Repräsentanten zunächst in $\mathbb{Z}$, dividieren das Ergebnis mit Rest durch n und nehmen diesen Rest als Ergebnis der Addition bzw. der Multiplikation.

Dadurch wir $\mathbb{Z}/n\mathbb{Z}$ zum (kommutativen) Ring.

Beispiele

Beispiel

In $\mathbb{Z}/12\mathbb{Z}$ gilt

- $3 + 4 = 7$.
- $9 + 10 = 7$.
- $4 + 8 = 0$, dh. $8 = -4$.
- $2 \cdot 3 = 6$.
- $5 \cdot 6 = 6$.
- $3 \cdot 4 = 0$.

Folgerung

$\mathbb{Z}/12\mathbb{Z}$ ist kein Körper.

Beispiele

Beispiel

Es ist $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$ der Körper von oben mit zwei Elementen.

Übung

Ist auch $\mathbb{Z}/15\mathbb{Z}$ ein Körper?

Primkörper

Der Ring $\mathbb{Z}/n\mathbb{Z}$ kann also ein Körper sein, muss aber nicht.

Satz

Genau dann ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper, wenn n eine Primzahl ist.

Bezeichnung

Ist p eine Primzahl, so schreiben wir $\mathbb{F}_p$ für $\mathbb{Z}/p\mathbb{Z}$ und nennen $\mathbb{F}_p$ den **Primkörper** mit p Elementen.

Beispiel

$\mathbb{F}_2$, $\mathbb{F}_3$ und $\mathbb{F}_5$ sind Körper.

Arithmetik in Primkörpern

Addition, Subtraktion und Multiplikation in den Körpern $\mathbb{F}_p$ sind einfach, da wir hier zunächst in $\mathbb{Z}$, addieren, subtrahieren oder multiplizieren können und dann Restklassen mod p bilden.

Beispiel

In $\mathbb{F}_7$ gilt

$$\begin{array}{rcrcl} 5+6 & = & 11 & \mod 7 & = & 4 \\ 5-6 & = & -1 & \mod 7 & = & 6 \\ 5\cdot 6 & = & 30 & \mod 7 & = & 2 \end{array}$$

Schwieriger ist die Division bzw. die Bestimmung eines inversen Elements.

Der euklidische Algorithmus

- **Vorbereitungsschritt:** Ordne m und n so, dass $m \geq n$. (Vertausche m und n, falls nötig, denn $\mathrm{ggT}(m, n) = \mathrm{ggT}(n, m)$). Setzen $i = 0$ und $r_0 = m$, $r_1 = n$.
- **Verarbeitungsschritt:** Wir dividieren r_i durch r_{i+1} mit Rest:

$$r_i = a \cdot r_{i+1} + b$$

  mit einer natürlichen Zahl a und einem Rest $b \in \{0, 1, \ldots, r_{i+1} - 1\}$.
  - Falls $b = 0$ (d.h. die Division geht ohne Rest auf) $\longrightarrow$ **STOPP**.
  - Falls $b \neq 0$ setze $r_{i+2} = b$ und $i = i + 1$. Wiederhole den Verarbeitungsschritt.
- **Ergebnisschritt:** Nach endlich vielen Verarbeitungsschritten (höchstens m vielen) geht die Division erstmals ohne Rest auf, d.h. $r_i = a \cdot r_{i+1} + 0$ mit $r_{i+1} \neq 0$, Das STOPP–Kriterium wird also immer erreicht und r_{i+1} ist der größte gemeinsame Teiler von m und n, $r_{i+1} = \mathrm{ggT}(m, n)$.

Der euklidische Algorithmus

Beispiel

Wir betrachten die Zahlen $m = 222$ und $n = 156$. Hier gilt bereits $m \geq n$, und wir setzen $r_0 = 222$ und $r_1 = 156$.

- $i = 0$: $222 = 1 \cdot 156 + 66$. Wir setzen $r_2 = 66$.
- $i = 1$: $156 = 2 \cdot 66 + 24$. Wir setzen $r_3 = 24$.
- $i = 2$: $66 = 2 \cdot 24 + 18$. Wir setzen $r_4 = 18$.
- $i = 3$: $24 = 1 \cdot 18 + 6$. Wir setzen $r_5 = 6$.
- $i = 4$: $18 = 3 \cdot 6 + 0$. $\longrightarrow$ **STOPP**.

Ergebnis: $\mathrm{ggT}(222, 156) = 6$.

Der euklidische Algorithmus

Übung

Bestimmen Sie den größten gemeinsamen Teiler von $m = 239$ und $n = 144$.

Der erweiterte euklidische Algorithmus

Satz

Sind $m, n \in \mathbb{N} \setminus \{0\}$ *mit* $\mathrm{ggT}(m, n) = g$, *so gibt es ganze Zahlen* a, b *mit*

$$a \cdot m + b \cdot n = g$$

Das erhält man durch Rückwärtsrechnen aus dem euklidischen Algorithmus.

Der erweiterte euklidische Algorithmus

Beispiel

Wir wollen 6 mit 156 und 222 darstellen.

1. Aus Schritt $i = 3$ erhalte: $6 = 24 - 1 \cdot 18$.
2. Aus Schritt $i = 2$ erhaltet $18 = 66 - 2 \cdot 24$. Eingesetzt in (1):
$$6 = 24 - 1 \cdot (66 - 2 \cdot 24) = 3 \cdot 24 - 1 \cdot 66$$
3. Aus Schritt $i = 1$ erhalte zunächst $24 = 156 - 2 \cdot 66$. Eingesetzt in (2):
$$6 = 3 \cdot (156 - 2 \cdot 66) - 1 \cdot 66 = 3 \cdot 156 - 7 \cdot 66$$
4. aus Schritt $i = 0$ erhalte zunächst $66 = 222 - 1 \cdot 156$. Eingesetzt in (3):
$$6 = 3 \cdot 156 - 7 \cdot (222 - 1 \cdot 156) = 10 \cdot 156 - 7 \cdot 222$$

Damit haben wir eine gewünschte Darstellung $6 = 10 \cdot 156 + (-7) \cdot 222$.

Der erweiterte euklidische Algorithmus

Übung

Schreiben Sie $1 = \mathrm{ggT}(239, 144)$ in der Form

$$1 = a \cdot 239 + b \cdot 144$$

mit ganzen Zahlen a und b.

Division in Primkörpern

Der erweiterte euklidische Algorithmus kann benutzt werden, um die Division in einem endlichen Körper $\mathbb{F}_p$ durchzuführen. ist notwendig

$$\mathrm{ggT}(n, p) = 1$$

da p eine Primzahl.
Der erweiterte euklidische Algorithmus liefert dann ganze Zahlen a, b mit

$$1 = a \cdot n + b \cdot p$$

Rechnen wir dann modulo p, so gilt

$$1 = (a \cdot n + b \cdot p) \bmod p = a \cdot n \bmod p$$

und damit gilt (in $\mathbb{F}_p$)

$$\frac{1}{n} = a, \qquad \frac{1}{a} = n$$

Division in Primkörpern

Beispiel

Die Zahl $p = 239$ ist prim, und es gilt

$$1 = 47 \cdot 239 + (-78) \cdot 144$$

Damit gilt:

$$1 = (-78) \cdot 144 \mod 239 = 161 \cdot 144 \mod 239$$

also in $\mathbb{F}_{239}$:

$$\frac{1}{144} = 161$$

Damit gilt dann auch

$$\frac{67}{144} = 67 \cdot 161 = 32$$

Division in Primkörpern

Übung

Berechnen Sie die Elemente

$$a = \frac{1}{87}, \quad b = \frac{127}{90}$$

in $\mathbb{F}_{179}$.

Gleichungssysteme über Primkörpern

Beispiel

Betrachte über $\mathbb{F}_5$ das lineare Gleichungssystem

$$\begin{array}{rcrcrcr} 2x & + & 3y & + & 2z & = & 1 \\ 3x & + & y & + & z & = & 2 \\ x & + & 2y & + & 3z & = & 3 \end{array}$$

Augmentierte Matrix und Normalform:

$$\left(\begin{array}{ccc|c} 2 & 3 & 2 & 1 \\ 3 & 1 & 1 & 2 \\ 1 & 2 & 3 & 3 \end{array}\right), \qquad \left(\begin{array}{ccc|c} 1 & 4 & 1 & 3 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 4 \end{array}\right)$$

Lösung: $x = 3,\ y = 4,\ z = 4.$

Gleichungssysteme über Primkörpern

Übung

Betrachte über $\mathbb{F}_3$ das lineare Gleichungssystem

$$\begin{array}{rcrcrcl} x & + & 2y & + & z & = & 0 \\ 2x & + & 2y & + & z & = & 0 \end{array}$$

Untersuchen Sie, ob das Gleichungssystem Lösungen hat und bestimmen Sie diese gegebenenfalls.

Endliche Körper

Beispiel

Betrachte $M = \{0, 1, \alpha, \alpha + 1\}$ mit

$+$	0	1	α	$\alpha+1$	$\cdot$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$	0	0	0	0	0
1	1	0	$\alpha+1$	α	1	0	1	α	$\alpha+1$
α	α	$\alpha+1$	0	1	α	0	α	$\alpha+1$	1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha+1$	0	$\alpha+1$	1	α

Dann ist $(M, +, \cdot)$ ein Körper.

Dabei ist $M \neq \mathbb{Z}/4\mathbb{Z}$, und es gilt auch nicht $M = \mathbb{F}_p$ für eine Primzahl p.

Dieser Körper wird mit $\mathbb{F}_4$ bezeichnet.

Endliche Körper

Es gibt also offensichtlich endliche Körper K, die **nicht** von der Form $K = \mathbb{F}_p$ sind.
Damit stellt sich die Frage, für welche $n \in \mathbb{N}$ es einen Körper mit n Elementen gibt und wie solche Körper aussehen.

endliche Körper

Ist K ein Körper, so schreiben wir kurz

$$n = n \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{n\text{–mal}}$$

und für $a \in K$ beliebig

$$n \cdot a = \underbrace{a + a + \cdots + a}_{n\text{–mal}}$$

Bemerkung

Ist K ein endlicher Körper, so gibt es immer eine Zahl $n \in \mathbb{N}$, $n > 0$ mit

$$n = 0 \qquad \text{in } K$$

Definition

Ist K ein endlicher Körper, so heißt die kleinste Zahl $n > 0$ mit $n \cdot 1 = 0$ in K die **Charakteristik** von K, geschrieben $\mathrm{char}(K)$.

endliche Körper

Beispiel

Für jede Primzahl p gilt $\mathrm{char}(\mathbb{F}_p) = p$.
Der Körper mit p Elementen hat also Charakteristik p.

Satz

Ist K ein endlicher Körper, so ist $\mathrm{char}(K) = p$ eine Primzahl und $\mathbb{F}_p \subseteq K$ als Unterkörper.

Beispiel

Der Körper $\mathbb{F}_4$ hat die Charakteristik 2 und $\mathbb{F}_2 \subseteq \mathbb{F}_4$

Satz (Frobenius–Formel)

Ist $p = \mathrm{char}(K)$, so gilt

$$(a+b)^p = a^p + b^p \qquad \text{für alle } a, b \in K$$

endliche Körper

Satz

Ist K ein endlicher Körper der Charakteristik p mit q Elementen, so ist $q = p^l$ für ein $l \in \mathbb{N}$ und es gibt ein $\alpha \in K$, sodass $1, \alpha, \alpha^2, \ldots, \alpha^{l-1}$ eine Basis von K als $\mathbb{F}_p$–Vektorraum ist. Insbesondere haben wir also eine Relation

$$\alpha^l = r_{l-1} \cdot \alpha^{l-1} + r_{l-2} \cdot \alpha^{l-2} + \cdots + r_1 \cdot \alpha + r_0$$

Es gibt für jede Primzahl p und jedes $l \in \mathbb{N}$ genau einen Körper mit $q = p^l$ Elementen.

Definition

Eine solche Relation

$$\alpha^l = r_{l-1} \cdot \alpha^{l-1} + r_{l-2} \cdot \alpha^{l-2} + \cdots + r_1 \cdot \alpha + r_0$$

heißt definierende Relation des Körpers K.

endliche Körper

Bezeichnung

Der Körper K mit $q = p^l$ Elementen wir mit $\mathbb{F}_q$ bezeichnet.

Beispiel

Der Körper $\mathbb{F}_4$ ist der (eindeutige) Körper mit 4 Elementen.
Er wird definiert durch die Relation

$$\alpha^2 = \alpha + 1$$

Beispiel

Der Körper $\mathbb{F}_8$ mit 8 Elementen wird definiert durch die Relation

$$\alpha^3 = \alpha + 1$$

Er wird aber auch definiert durch die Relation

$$\alpha^3 = \alpha^2 + 1$$

endliche Körper

Bemerkung

Ist $\mathbb{F}_q$ der Körper mit $q = p^l$ Elementen und ist

$$\alpha^l = r_{l-1} \cdot \alpha^{l-1} + r_{l-2} \cdot \alpha^{l-2} + \cdots + r_1 \cdot \alpha + r_0$$

eine definierende Relation von $\mathbb{F}_q$, so sind dadurch Addition und Multiplikation schon eindeutig festgelegt.
Für $a = a_{l-1} \cdot \alpha^{l-1} + \cdots + a_1 \cdot \alpha + a_0$ und
$b = b_{l-1} \cdot \alpha^{l-1} + \cdots + b_1 \cdot \alpha + b_0$ (mit $a_i, b_i \in \mathbb{F}_p$) ist

$$a + b = (a_{l-1} + b_{l-1}) \cdot \alpha^{l-1} + (a_{l-2} + b_{l-2} \cdot \alpha^{l-2} + \cdots + (a_1 + b_1) \cdot \alpha + a_0 + b_0$$

Die Multiplikation ist gegeben durch die Formel $\alpha^i \cdot \alpha^j = \alpha^{i+j}$ und die Relation.

endliche Körper

Beispiel

Im Körper $\mathbb{F}_8$ mit 8 Elementen, gegeben durch die Relation $\alpha^3 = \alpha + 1$ gelten die folgenden Beziehungen

- $(\alpha + 1) + (\alpha^2 + 1) = \alpha^2 + \alpha + 1 + 1 = \alpha^2 + \alpha.$
- $(\alpha^2 + 1) + (\alpha^2 + \alpha + 1) = 2\alpha^2 + \alpha + 2 = \alpha.$
- $\alpha \cdot (\alpha + 1) = \alpha \cdot \alpha + \alpha \cdot 1 = \alpha^2 + \alpha.$
- $\alpha^2 \cdot \alpha = \alpha^3 = \alpha + 1.$
- $\alpha^2 \cdot \alpha^2 = \alpha^4 = \alpha \cdot \alpha^3 = \alpha \cdot (\alpha + 1) = \alpha^2 + \alpha.$
- $\alpha^2 \cdot (\alpha^2 + \alpha) = \alpha^2 \cdot \alpha^2 + \alpha^2 \cdot \alpha = (\alpha^2 + \alpha) + (\alpha + 1) = \alpha^2 + 1.$

endliche Körper

Übung

Der Körper $\mathbb{F}_8$ kann auch durch die Relation $\alpha^3 = \alpha^2 + 1$ beschrieben werden.
Berechnen Sie bei dieser definierenden Relation das Element

$$x = \alpha^2 \cdot (\alpha^2 + \alpha)$$

endliche Körper

Es kann mehrere Relationen geben, die den Körper $\mathbb{F}_q$ beschreiben, aber nicht jede Relation

$$\alpha^l = r_{l-1} \cdot \alpha^{l-1} + r_{l-2} \cdot \alpha^{l-2} + \cdots + r_1 \cdot \alpha + r_0$$

ist eine definierende Relation.

Beispiel

Die Relation $\alpha^3 = \alpha^2 + \alpha + 1$ beschreibt den Körper $\mathbb{F}_8$ nicht.

endliche Körper

Definition

Ist $\alpha^l = r_{l-1} \cdot \alpha^{l-1} + r_{l-2} \cdot \alpha^{l-2} + \cdots + r_1 \cdot \alpha + r_0$ eine definierende Relation von $\mathbb{F}_q$, so heißt

$$F(X) = X^l - r_{l-1} \cdot X^{l-1} - r_{l-2} \cdot X^{l-2} - \cdots - r_1 \cdot X - r_0 \in \mathbb{F}_p[X]$$

Minimalpolynom von $\mathbb{F}_q$.

Satz

Ein Polynom $F(X) = X^l + r_{l-1} \cdot X^{l-1} + \cdots + r_1 \cdot X + r_0 \in \mathbb{F}_p[X]$ ist genau dann ein Minimalpolyonom von $\mathbb{F}_q$ (mit $q = p^l$) wenn es **keine** *Polynome $h(X)$ und $g(X)$ vom Grad mindestens 1 gibt, sodass*

$$F(X) = g(X) \cdot h(X)$$