

Vorlesung Algebra 2

(Diskrete Mathematik und Algebra)

7. Körper

+	0	1	♠	♥
0	0	1	♠	♥
1	1	0	♥	♠
♠	♠	♥	0	1
♥	♥	♠	1	0

·	0	1	♠	♥
0	0	0	0	0
1	0	1	♠	♥
♠	0	♠	♥	1
♥	0	♥	1	♠

1

Körper

$(F, +, \cdot)$, eine Menge F mit Operationen

$$+ : F \times F \rightarrow F \text{ und } \cdot : F \times F \rightarrow F,$$

heisst *Körper*, falls

- (1) $(F, +)$ eine abelsche Gruppe ist (mit Neutralelement 0_F),
- (2) $(F \setminus \{0_F\})$ eine abelsche Gruppe ist (mit Neutralelement 1_F), und
- (3) das *Distributivgesetz* gilt: Für alle $a, b, c \in F$

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

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

Wir schreiben

0 für 0_F (*Nullelement*), 1 für 1_F (*Einselement*),
 $-x$ für das *additive Inverse* von $x \in F$,
 x^{-1} für das *multiplikative Inverse* von $x \in F \setminus \{0\}$,
 ab für $a \cdot b$, und $a - b$ für $a + (-b)$.

2

Beispiele

\mathbb{R}, \mathbb{Q} und \mathbb{C} sind Körper
mit üblicher Addition und Multiplikation.

Für p prim, ist \mathbb{Z}_p ein Körper
mit $\overset{+}{\text{mod } p}$ und $\overset{\times}{\text{mod } p}$.

$(\{\text{True}, \text{False}\}, \vee, \wedge)$ ist *kein* Körper.

∨	T	F
T	T	T
F	T	F

$(\{\text{True}, \text{False}\}, \overset{\oplus}{\text{xor}}, \wedge)$ ist ein Körper.

⊕	T	F
T	F	T
F	T	F

Über Körpern gibt es *Matrizen mit Addition und Multiplikation* und *Vektoren mit Skalarprodukt*.

Gibt es andere endliche Körper ausser \mathbb{Z}_p, p prim?

3

Einfache Eigenschaften

Für jeden Körper F und $x, y \in F$ gilt.

- $|F| \geq 2$.
BEWEIS Weil $F \supseteq \{0, 1\}, 0 \neq 1$.
- $xy = 0 \Leftrightarrow x = 0 \vee y = 0$.
BEWEIS (\Rightarrow) $(F \setminus \{0\}, \cdot)$ ist eine Gruppe, also gilt $x \neq 0 \wedge y \neq 0 \Rightarrow xy \neq 0$.
(\Leftarrow) $x0 + x0 = x(0 + 0) = x0 = x0 + 0$ und folglich $x0 = 0$ (man darf in $(F, +)$ kürzen).
- Falls $a \neq 0$, ist die Abbildung $F \rightarrow F$ definiert durch $x \mapsto ax$ eine Bijektion.
BEWEIS Weil $(F \setminus \{0\}, \cdot)$ eine Gruppe ist, ist die Einschränkung der Abbildung auf $F \setminus \{0\}$ eine Bijektion. Da $0 \mapsto 0$, ist sie auch auf F bijektiv.

Für $a, b \in F, a \neq 0$, hat die Gleichung $ax + b = 0$ genau eine Lösung: $x = a^{-1}(-b)$.

4

Ein Körper der Ordnung 9

Betrachte die Menge S schräg-symmetrischer 2×2 Matrizen über \mathbb{Z}_3 (beachte $|S| = 9$):

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix}, \text{ für } x, y \in \mathbb{Z}_3.$$

$(S, +)$ ist eine abelsche Gruppe, mit Nullmatrix $\underline{0}$ als Neutralelement (einfach zu zeigen).

$$\begin{aligned} \begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix} &= \\ \begin{pmatrix} x_1x_2 - y_1y_2 & x_1y_2 + x_2y_1 \\ -x_1y_2 - x_2y_1 & x_1x_2 - y_1y_2 \end{pmatrix} &= \\ \begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix} \begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix} & \end{aligned}$$

$S \setminus \{0\}$ bzgl. Multiplikation abgeschlossen und kommutativ, mit Neutralelement $\underline{1} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Addition und Mult. jeweils in \mathbb{Z}_3 , d.h. mod 3.

Bislang gilt alles (ausser $|S| = 9$) für jeden Körper F statt \mathbb{Z}_3 .

5

Inverse

Gegeben $(x, y) \neq (0, 0)$, suchen wir a, b , so dass

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

d.h. $ax - by = 1$ und $ay + bx = 0$. Dies gilt für

$$a = x(x^2 + y^2)^{-1}, \quad b = -y(x^2 + y^2)^{-1}$$

(Überprüfen durch Einsetzen) falls $(x^2 + y^2)^{-1}$ existiert, d.h. falls $x^2 + y^2 \neq 0$.

In \mathbb{Z}_3 gilt dies, gdw. $(x, y) \neq (0, 0)$.

$$\begin{array}{ccccccc} x & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ y & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ x^2+y^2 & 1 & 1 & 1 & 2 & 2 & 1 & 2 & 2 \end{array}$$

$(S \setminus \{0\}, \cdot)$ ist abelsche Gruppe, und S ein Körper der Ordnung 9.

$x^2 + y^2 = 0 \Leftrightarrow (x, y) = (0, 0)$ gilt nicht in jedem Körper: z.B. $1^2 + 2^2 = 0$ in \mathbb{Z}_5 .

6

Charakterisierung endlicher Körper

[Évariste Galois 1811-1832]

- Jeder endliche Körper hat die Ordnung $q = p^r$, p prim.
- Alle Körper der Ordnung q sind isomorph.
- Die additive Gruppe ist isomorph zu $(\mathbb{Z}_p)^r$.
- Die multiplikative Gruppe ist isomorph zu \mathbb{Z}_{q-1} .

OHNE BEW.

“Der” Körper der Ordnung q wird mit \mathbb{F}_q oder $GF(q)$ (Galois field) bezeichnet.

7

Skalarprodukt

F Körper, $n \in \mathbb{N}$.

Für Vektoren $x = (x_i)_{i=1}^n$ und $y = (y_i)_{i=1}^n$ in F^n ist das *Skalarprodukt* definiert durch

$$xy := x_1y_1 + x_2y_2 + \dots + x_ny_n = \sum_{i=1}^n x_iy_i$$

Für $x, y, z \in F^n$ gilt

$$\begin{aligned} (x + y)z &= \sum_{i=1}^n (x_i + y_i)z_i \\ &= \sum_{i=1}^n x_iz_i + y_iz_i \quad (\text{weil distributiv}) \\ &= \sum_{i=1}^n x_iz_i + \sum_{i=1}^n x_iz_i \quad (\text{weil kommutativ}) \\ &= xz + yz. \end{aligned}$$

Ausserdem $xy = yx$.

x und y heissen *orthogonal* falls $xy = 0$.
Beachte, dass $(1, 2)(1, 2) = 0$ in \mathbb{Z}_5 .

8

„Gleichheitstest“

$(\mathbb{F}_2)^6$ als „Bilder“

Seien $x, y \in (\mathbb{F}_2)^n$. Betrachte die Menge

$$\text{Eq}(x, y) := \{z \in (\mathbb{F}_2)^n : zx = zy\}.$$

LEMMA $|\text{Eq}(x, y)| = 2^{n-1}$ für $x \neq y$.

BEWEIS Sei $w \in (\mathbb{F}_2)^n$ mit genau einer 1, an einer Stelle, an der sich x und y unterscheiden (also $wx \neq wy$). Dann gilt

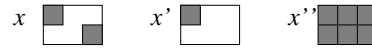
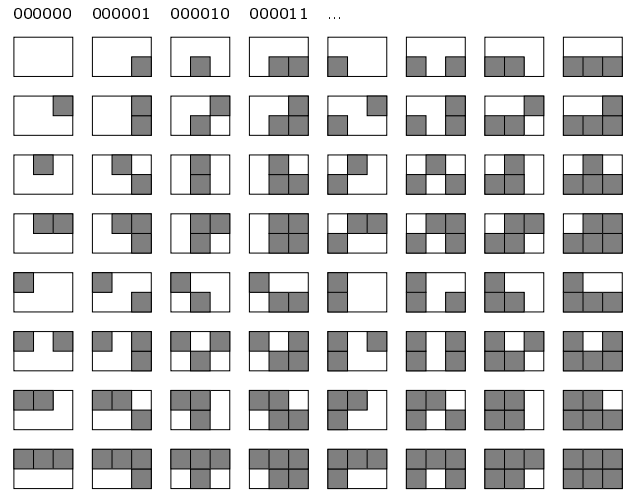
$$zx = zy \Leftrightarrow (z + w)x \neq (z + w)y.$$

$z \mapsto z + w$ ist eine Bijektion $((z + w) + w = z)$

$$\text{Eq}(x, y) \rightarrow (\mathbb{F}_2)^n \setminus \text{Eq}(x, y),$$

und $|\text{Eq}(x, y)| = |(\mathbb{F}_2)^n|/2 = 2^n/2$ ist gezeigt.

Sind x und y verschieden, so gilt $zx \neq zy$ für 50% aller $z \in (\mathbb{F}_2)^n$. Die Wahrscheinlichkeit, dass $xz = yz$ für 20 zufällige z ist $2^{-20} \approx 10^{-6}$.



Kleine zu grossen Unterschieden

Orthogonale Vektoren

Für $x \in (\mathbb{F}_q)^n \setminus \{0\}$ sei

$$\text{Orth}(x) := \{y \in (\mathbb{F}_q)^n \mid xy = 0\}.$$

LEMMA $|\text{Orth}(x)| = q^{n-1}$ für $x \in (\mathbb{F}_q)^n \setminus \{0\}$.

BEWEIS Für $z = (z_1, \dots, z_n) \in (\mathbb{F}_q)^n$, sei $z' := (z_1, \dots, z_{n-1})$. Es gilt $yz = y'z' + y_n z_n$.

Betrachte nun $x \in (\mathbb{F}_q)^n$ mit $x_n \neq 0$. Die Abbildung $\mathbb{F} \rightarrow \mathbb{F}$ def. durch $c \mapsto x_n c$ ist eine Bijektion. Für jedes $u = (u_i)_{i=1}^{n-1} \in (\mathbb{F}_q)^{n-1}$ gibt es also genau ein c mit

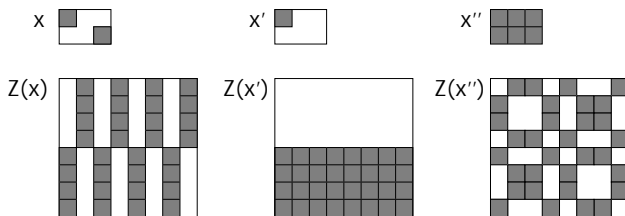
$$x(u_1, \dots, u_{n-1}, c) = x'u + x_n c = 0,$$

nämlich $c = x_n^{-1}(-x'u)$. Folglich gilt $|\text{Orth}(x)| = |(\mathbb{F}_q)^{n-1}| = q^{n-1}$.

Ist $x \in (\mathbb{F}_q)^n \setminus \{0\}$, dann gibt es ein $x_i \neq 0$, und wir können analog argumentieren. \square

Beachte, dass $\text{Eq}(x, y) = \text{Orth}(x - y)$!

$$(\mathbb{F}_2)^n \ni x \mapsto Z(x) := (xz)_{z \in (\mathbb{F}_2)^n}$$



Aber $Z(x)$ ist sehr gross!

Geraden und Punkte in der Ebene: Durch je zwei Punkte geht genau eine Gerade. Je zwei Geraden schneiden sich in genau einem Punkt – oder sind parallel (affine Ebene).

Ebenen und Geraden durch den Ursprung 0 im \mathbb{R}^3 : Je zwei Geraden spannen eine eindeutige Ebene auf. Je zwei Ebenen schneiden sich in genau einer Geraden – immer! (projektive Ebene).

Allgemeines Prinzip (Abstraktion): Ein Mengensystem (P, \mathcal{L}) , P Menge, $\mathcal{L} \subseteq 2^P$, mit

$$\forall \{p, q\} \in \binom{P}{2}: \exists \ell \in \mathcal{L} : \ell \supseteq \{p, q\},$$

$$\forall \{k, \ell\} \in \binom{\mathcal{L}}{2}: |k \cap \ell| = 1, \text{ und}$$

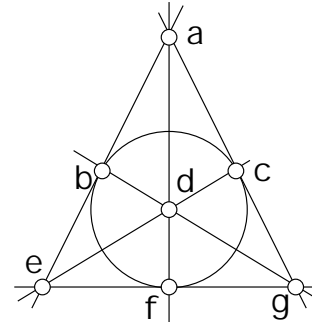
$$\exists Q \subseteq P: (|Q| = 4) \wedge (\forall \ell \in \mathcal{L} : |\ell \cap Q| \leq 2),$$

heisst **projektive Ebene**.

$$P = \{a, b, c, d, e, f, g\}$$

$$\mathcal{L} = \{\{a, c, g\}, \{a, d, f\}, \{a, b, e\}, \{b, d, g\}, \{c, d, e\}, \{e, f, g\}, \{b, c, f\}\}$$

Fano Ebene



Entspricht einem $K_{2,2}$ -freien bipartiten Graph mit 14 Knoten und 21 Kanten (wie?).

Konstruktion projektiver Ebenen

Sei F ein Körper. Für $x, y \in F^3 \setminus \{0\}$, sei

$$x \sim y \iff x = cy \text{ für ein } c \in F.$$

Für $x = (x_1, x_2, x_3) \in F^3, c \in F$, sei $cx := (cx_1, cx_2, cx_3)$.

\sim ist eine Äquivalenzrelation mit Äquivalenzklassen

$$[x] := \{y \in F^3 \setminus \{0\} : x \sim y\},$$

für $x \in F^3 \setminus \{0\}$.

$F = \mathbb{Z}_3$: $[(0, 2, 1)] = \{(0, 2, 1), (0, 1, 2)\}$.
 $F = \mathbb{R}$: $[x]$ ist die Gerade durch 0 und x (ohne 0).

Falls $|F| = n$ endlich, gilt für alle $x \in F^3 \setminus \{0\}$, dass $|[x]| = n - 1$, und es gibt folglich

$$\frac{n^3 - 1}{n - 1} = n^2 + n + 1$$

Äquivalenzklassen.

Konstruktion – Fortsetzung

Wähle für $[x]$ als Repräsentant den Vektor, dessen letzte Nichtnull eine 1 ist.

$F = \mathbb{Z}_3$: Es gibt 13 Äquivalenzklassen mit Repräsentanten

$$9 \left\{ \begin{array}{l} (0, 0, 1), (0, 1, 1), (0, 2, 1), \\ (1, 0, 1), (1, 1, 1), (1, 2, 1), \\ (2, 0, 1), (2, 1, 1), (2, 2, 1), \end{array} \right.$$

$$3 \left\{ \begin{array}{l} (0, 1, 0), (1, 1, 0), (2, 1, 0), \\ (1, 0, 0) \end{array} \right.$$

Nun sei

$$P := \{[x] : x \in F^3 \setminus \{0\}\}$$

$$\mathcal{L} := \{\ell_{[x]} : x \in F^3 \setminus \{0\}\},$$

wobei $\ell_{[x]} := \{[y] \in P : xy = 0\}$.

Beachte, dass

$$|\ell_{[x]}| = \frac{|\text{Orth}(x)| - 1}{n - 1} = \frac{n^2 - 1}{n - 1} = n + 1.$$

Punkte und Geraden sind gleichwertig/austauschbar; durch jeden Punkt gehen $n + 1$ Geraden.

OHNE BEW. (P, \mathcal{L}) bildet für jeden Körper F eine projektive Ebene. Für $|F| = n \in \mathbb{N}$ gibt es $n^2 + n + 1$ Punkte, ebensoviele Geraden, jede Gerade hat $n + 1$ Punkte, und jeder Punkt liegt in $n + 1$ Geraden. Dies gilt für jede endliche projektive Ebene!

Was sonst? Wozu?

Jede endliche projektive Ebene hat $n^2 + n + 1$ Punkte und Geraden, für ein $n \in \mathbb{N}$. n nennt man die *Ordnung* der Ebene (d.h. falls $|F| = n$, so erzeugt F eine endliche projektive Ebene der Ordnung n).

Die Fano Ebene, von \mathbb{Z}_2 erzeugt, ist die kleinste projektive Ebene. Nach der Charakterisierung endlicher Körper existieren endliche projektive Ebenen auf jeden Fall für alle $n = p^r$, p prim; also $n = 2, 3, 4, 5, 7, 8, 9, 11, 13, \dots$. Ob dies auch für andere n möglich ist, ist unbekannt. Bereits Euler versuchte zu zeigen, dass $n = 6$ unmöglich ist, was allerdings erst um 1900 Tarry gelang. Für $n = 10$ war es erst Ende des letzten Jahrhunderts (20.) unter enormen Einsatz von Computern möglich zu zeigen, dass dies nicht die Ordnung einer projektiven Ebenen sein kann. Der Fall $n = 12$ ist offen.

Endliche projektive Ebenen galten – wie so viel in der Mathematik – lange Zeit als (für einige Mathematiker) faszinierende Objekte ohne Anwendung. Heute spielen sie eine grosse Rolle wegen der Theorie elliptischer Kurven, die in endlichen projektiven Ebenen ‘leben.’ Diese ‘Kurven’ sind in der modernen Kryptographie relevant.

Der Inzidenzgraph zwischen Punkten und Geraden einer endlichen projektiven Ebene der Ordnung n hat $N = 2(n^2 + n + 1)$ Knoten, hat $(n^2 + n + 1)(n + 1) > (N/2)^{3/2} \approx 0.35N^{3/2}$ Kanten und ist $K_{2,2}$ -frei. Wir zeigten, dass ein $K_{2,2}$ -freier Graph mit N Knoten höchstens $\frac{1}{2}(N^{3/2} + N)$ Kanten haben kann.

17

Polynome

Sei F ein Körper. $F[x]$ bezeichnet die Menge der Polynome in der Unbekannten x mit Koeffizienten in F .

$$F[x] := \left\{ \sum_{i=0}^{\infty} a_i x^i : a_i \in F, \text{ nur endl. viele } \neq 0 \right\}$$

$$\mathbb{Z}_2[x] = \{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1, \dots\}$$

Polynome kann man **addieren**,

$$(\sum_i a_i x^i) + (\sum_i b_i x^i) := \sum_i (a_i + b_i) x^i$$

multiplizieren

$$(\sum_i a_i x^i) \cdot (\sum_i b_i x^i) := \sum_i c_i x^i$$

wobei $c_i := \sum_{j=0}^i a_j b_{i-j}$.

und an einer ‘Stelle’ $s \in F$ **auswerten**:

$$\sum_{i=0}^n a_i s^i \in F, \quad n := \max(\{i : a_i \neq 0\} \cup \{0\})$$

n heisst *Grad* des Polynoms.

$F[x]$ ist also einerseits eine Menge von Vektoren über F mit Operationen $+$ und \cdot , andererseits eine Menge von Funktionen $F \rightarrow F$. In $\mathbb{Z}_2[x]$ sind x^2 und x gleich als Funktionen $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$, aber nicht als Vektoren: $(0, 0, 1, 0, \dots) \neq (0, 1, 0, 0, \dots)$. (Es gibt nur 4 Funktionen $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$.)

$(F[x], +)$ ist eine Gruppe. $(F[x], +, \cdot)$ ist ein Ring.

18

Ringe

$(R, +, \cdot)$, eine Menge R mit Operationen

$$+ : R \times R \rightarrow R \quad \text{und} \quad \cdot : R \times R \rightarrow R,$$

heisst *Ring*, falls

- (1) $(R, +)$ eine abelsche Gruppe ist,
- (2) \cdot assoziativ ist und es ein Neutralelement gibt,
- (3) und das *Distributivgesetz* gilt:
Für alle $a, b, c \in R$

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (a + b) \cdot c &= (a \cdot c) + (b \cdot c). \end{aligned}$$

$(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, \overset{+}{\text{mod } m}, \text{mod } m)$, $n \geq 2$, sind Ringe.

Die Matrizen $(\mathbb{Z}^{2 \times 2}, +, \cdot)$ bilden einen Ring, in dem die Multiplikation nicht kommutativ ist.

Für jeden Körper F , bilden die Polynome $(F[x], +, \cdot)$ einen Ring (als Vektoren und als Funktionen).

19

Verschicken von Nachrichten

Gegeben sei eine Folge $(a_i)_{i=0}^{m-1}$ von m Nachrichten mit $a_i \in \mathbb{N}_0$. Wähle $q = p^r$, p prim, so dass $q \geq m$ und $q \geq \max_i a_i$, und fasse die a_i als Elemente von \mathbb{F}_q auf.

Betrachte nun das Polynom

$$p(x) := \sum_{i=0}^{m-1} a_i x^i \in \mathbb{F}_q[x].$$

Wir verschicken $n \geq m$ ‘Pakete’ $(s, p(s))$, $s \in \mathbb{F}_q$. Aus je m dieser Paare (Stützstellen) lassen sich die Koeffizienten des Polynoms vom Grad $\leq m-1$ rekonstruieren, und damit die ursprünglichen Nachrichten.

Was für beliebige Körper zu beweisen wäre!

20

Beispiel

Nachrichten:

$$(4, 3, 2)$$

Wir wählen

$$p(x) := 4 + 3x + 2x^2 \in \mathbb{Z}_7[x]$$

$$p(0) = 4, p(1) = 2, p(2) = 4, p(3) = 3, p(4) = 6$$

$$p(5) = (4 + 3 \cdot 5 + 2 \cdot 25) \bmod 7 = (4 + 1 + 1) \bmod 7 = 6$$

Verschickt werden die Pakete

$$(0, 4), (1, 2), (2, 4), (3, 3), (4, 6), (5, 6).$$

Kommen nur drei Pakete an, z.B. $(1, 2)$, $(3, 3)$ und $(4, 6)$ so kann man immer noch das Polynom $p(x)$ und damit die Folge der Koeffizienten $(4, 3, 2)$ rekonstruieren.

21

Filterpolynome

Für jedes $a \in \mathbb{F}_q$, sei

$$f_a(x) := \prod_{\xi \in \mathbb{F}_q \setminus \{a\}} (x - \xi) \cdot \prod_{\xi \in \mathbb{F}_q \setminus \{a\}} (a - \xi)^{-1} \in \mathbb{F}_q[x],$$

ein Polynom vom Grad $\leq q - 1$. Für $a, b \in \mathbb{F}_q$ gilt

$$f_a(b) = \begin{cases} 1 & \text{falls } a = b, \text{ und} \\ 0 & \text{sonst.} \end{cases}$$

LEMMA Für jede Funktion $g: \mathbb{F}_q \rightarrow \mathbb{F}_q$ gibt es genau ein Polynom $p(x) \in \mathbb{F}_q[x]$ vom Grad $\leq q - 1$ mit

$$\forall a \in \mathbb{F}_q : p(a) = g(a).$$

BEWEIS Setze

$$p(x) := \sum_{a \in \mathbb{F}_q} g(a) f_a(x).$$

Eindeutigkeit folgt, weil es q^q Funktionen $\mathbb{F}_q \rightarrow \mathbb{F}_q$, und ebensoviele Polynome vom Grad $\leq q - 1$ in $\mathbb{F}_q[x]$ gibt. \square

22

Beispiel

$$\mathbb{F}_q \cong \mathbb{Z}_3 = \{0, 1, 2\}:$$

$$\begin{aligned} f_0(x) &= (x + \overbrace{2}^{-1})(x + \overbrace{1}^{-2})(0 + 2)^{-1}(0 + 1)^{-1} \\ &= (x^2 + \overbrace{2x + x}^{0x} + 2) \cdot 2 \cdot 1 = 2x^2 + 2 \cdot 2 \\ &= 2x^2 + 1 \end{aligned}$$

$$\begin{aligned} f_1(x) &= (x + 0)(x + 1)(1 + 0)^{-1}(1 + 1)^{-1} \\ &= 2x^2 + 2x \end{aligned}$$

$$\begin{aligned} f_2(x) &= (x + 0)(x + 2)(2 + 0)^{-1}(2 + 2)^{-1} \\ &= 2x^2 + x \end{aligned}$$

Für $g: 0 \mapsto 2, 1 \mapsto 1, 2 \mapsto 0$ erhalten wir

$$\begin{aligned} p(x) &= 2(2x^2 + 1) + 1(2x^2 + 2x) + 0(2x^2 + x) \\ &= (2 \cdot 2 + 1 \cdot 2 + 0 \cdot 2)x^2 + (1 \cdot 2 + 0 \cdot 1)x + 2 \cdot 1 \\ &= 0x^2 + 2x + 2 = 2x + 2 \end{aligned}$$

23

Die Polynome $f_a(x)$ einfacher

Für $a \in \mathbb{F}_q$ gilt

$$a^{q-1} = \begin{cases} 0, & \text{falls } a = 0, \text{ und} \\ 1, & \text{sonst,} \end{cases}$$

weil $q - 1$ die Ordnung der multiplikativen Gruppe $(\mathbb{F}_q \setminus \{0\}, \cdot)$ ist. Folglich gilt

$$f_a(x) = 1 - (x - a)^{q-1}.$$

In \mathbb{Z}_3 erhalten wir also

$$\begin{aligned} f_0(x) &= 1 - x^2 = 2x^2 + 1 \\ f_1(x) &= 1 - (x - 1)^2 = 2x^2 + 2x \\ f_2(x) &= 1 - (x - 2)^2 = 2x^2 + x \end{aligned}$$

24

Für $a \in A \subseteq \mathbb{F}_q$, sei

$$f_a^{(A)} := \prod_{\xi \in A \setminus \{a\}} (x - \xi) \cdot \prod_{\xi \in A \setminus \{a\}} (a - \xi)^{-1} \in \mathbb{F}_q[x],$$

ein Polynom vom Grad $\leq |A| - 1$. Für $a, b \in A$ gilt

$$f_a^{(A)}(b) = \begin{cases} 1 & \text{falls } a = b, \text{ und} \\ 0 & \text{sonst.} \end{cases}$$

LEMMA $A \subseteq \mathbb{F}_q$, $k := |A|$. Für jedes $g: A \rightarrow \mathbb{F}_q$ gibt es genau ein $p(x) \in \mathbb{F}_q[x]$ vom Grad $\leq k - 1$ mit

$$\forall a \in A : p(a) = g(a).$$

BEWEIS Setze

$$p(x) := \sum_{b \in A} g(b) f_b^{(A)}(x).$$

Eindeutigkeit folgt, weil es q^k Funktionen $A \rightarrow \mathbb{F}_q$, und gleichviele Polynome vom Grad $\leq k - 1$ in $\mathbb{F}_q[x]$ gibt. \square

F ein Körper, $p(x) \in F[x]$.

$a \in \mathbb{F}_q$ heisst Nullstelle von p , falls $p(a) = 0$.

SATZ Ein Polynom $0 \neq p(x) \in \mathbb{F}_q[x]$ mit k Nullstellen hat Grad mindestens k .

BEWEIS Sei N die Menge der Nullstellen von $p(x)$, also $k = |N|$. Es gibt genau ein Polynom vom Grad $\leq k - 1$ welches alle $a \in N$ auf 0 abbildet, also ist dieses Polynom gleich 0. Da $p(x) \neq 0$, ist sein Grad $\geq k$. \square

FOLGERUNG $k \in \mathbb{N}$. Zwei Polynome in $\mathbb{F}_q[x]$ vom Grad $k - 1$, die an k Stellen übereinstimmen, sind gleich.

BEWEIS Stimmen zwei Polynome $p(x)$ und $p'(x)$ vom Grad $k - 1$ an k Stellen überein, so ist $p(x) - p'(x)$ vom Grad $\leq k - 1$ und hat k Nullstellen, und folglich $p(x) - p'(x) = 0$. \square