

Lecture Algebra 2

(Discrete Mathematics and Algebra)

7. Fields

+	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

Fields

$(F, +, \cdot)$, where F is a set with operations

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

is called a *field*, if

- (1) $(F, +)$ is an abelian group (with identity element 0_F),
- (2) $(F \setminus \{0_F\}, \cdot)$ is an abelian group (with identity element 1_F), and

(3) *distributivity* holds: For all $a, b, c \in F$

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

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

We write

0 for 0_F (*zero-element*), 1 for 1_F (*one-element*),
 $-x$ for the *additive inverse* of $x \in F$,
 x^{-1} for the *multiplicative inverse* of $x \in F \setminus \{0\}$,
 ab for $a \cdot b$, and $a - b$ for $a + (-b)$.

2

Examples

\mathbb{R} , \mathbb{Q} and \mathbb{C} are fields
with the usual addition and multiplication

For p prime, \mathbb{Z}_p is a field
with $\text{mod } p^+$ and $\text{mod } p^\times$.

$(\{\text{Wahr, Falsch}\}, \vee, \wedge)$ is *not* a field.

∨	W	F
W	W	W
F	W	F

$(\{\text{Wahr, Falsch}\}, \underbrace{\oplus}_{\text{xor}}, \wedge)$ is a field.

⊕	W	F
W	F	W
F	W	F

Over fields the *product of matrices* can be defined. In particular the *scalar product of vectors* (over a field) makes sense.

Is there another field besides \mathbb{Z}_p , for p prime?

3

Simple properties

For every field F and $x, y \in F$ the following hold.

- $|F| \geq 2$.
PROOF Since $F \supseteq \{0, 1\}$, and $0 \neq 1$.
- $xy = 0 \Leftrightarrow x = 0 \vee y = 0$.
PROOF (\Rightarrow) $(F \setminus \{0\}, \cdot)$ is a group, so $x \neq 0 \wedge y \neq 0 \Rightarrow xy \neq 0$.
(\Leftarrow) $x0 + x0 = x(0 + 0) = x0 = x0 + 0$ which implies $x0 = 0$ (one can cancel in $(F, +)$).
- If $a \neq 0$, then the mapping $F \rightarrow F$ defined by $x \mapsto ax$ is a bijection.
PROOF Since $(F \setminus \{0\}, \cdot)$ is a group, the restriction of the mapping to $F \setminus \{0\}$ is a bijection. $0 \mapsto 0$, so the mapping on F is also bijective.

For $a, b \in F$, $a \neq 0$, the equation $ax + b = 0$ has exactly one solution: $x = a^{-1}(-b)$.

4

A field of order 9

Consider the set S of skew-symmetric 2×2 matrices over \mathbb{Z}_3 (note that $|S| = 9$):

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

$(S, +)$ is an abelian group, with the nullmatrix $\underline{0}$ as the identity element (easy to show).

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

$S \setminus \{\underline{0}\}$ is closed under multiplication and it is commutative, with identity element $\underline{1} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Addition und multiplication is in \mathbb{Z}_3 , i.e. mod 3.

So far everything (except $|S| = 9$) holds for any field F instead of \mathbb{Z}_3 .

5

Inverse

Given $(x, y) \neq (0, 0)$, we need to find a, b , such that

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

i.e. $ax - by = 1$ and $ay + bx = 0$. This holds for

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

(Check through substitution) **provided $(x^2 + y^2)^{-1}$ exists**, i.e. if $x^2 + y^2 \neq 0$.

In \mathbb{Z}_3 this holds, iff $(x, y) \neq (0, 0)$.

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

$(S \setminus \{\underline{0}\}, \cdot)$ is an abelian group, and S is a field of order 9.

$x^2 + y^2 = 0 \Leftrightarrow (x, y) = (0, 0)$ is not true in every field: for example $1^2 + 2^2 = 0$ in \mathbb{Z}_5 .

6

The characterisation of finite fields

[Évariste Galois 1811-1832]

- Every finite field is of order $q = p^r$, where p is prime.
- All fields of order q are isomorphic.
- The additive group is isomorphic to $(\mathbb{Z}_p)^r$.
- The multiplicative group is isomorphic to \mathbb{Z}_{q-1} .

"The" field of order q is denoted by \mathbb{F}_q or $GF(q)$ (Galois field).

7

Scalar product

F is a field, $n \in \mathbb{N}$.

For vectors $x = (x_i)_{i=1}^n$ and $y = (y_i)_{i=1}^n$ in F^n the *scalar product* is defined as

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

For $x, y, z \in F^n$

$$\begin{aligned} (x + y)z &= \sum_{i=1}^n (x_i + y_i)z_i \\ &= \sum_{i=1}^n x_iz_i + y_iz_i \quad (\text{because of distributivity}) \\ &= \sum_{i=1}^n x_iz_i + \sum_{i=1}^n y_iz_i \quad (+ \text{ is commutative}) \\ &= xz + yz. \end{aligned}$$

Moreover $xy = yx$.

x and y is called *orthogonal* when $xy = 0$. Note, that $(1, 2)(1, 2) = 0$ in \mathbb{Z}_5 .

8

"Equality test"

Let $x, y \in (\mathbb{F}_2)^n$. Consider the set

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

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

PROOF Let $w \in (\mathbb{F}_2)^n$ with exactly one 1, at some coordinate where x and y differ (so $wx \neq wy$). Then we have

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

$z \mapsto z + w$ is a bijection $((z + w) + w = z)$

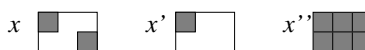
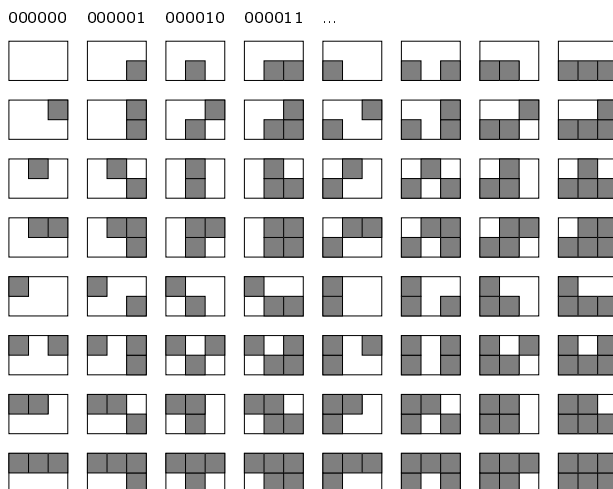
$$\text{Eq}(x, y) \rightarrow (\mathbb{F}_2)^n \setminus \text{Eq}(x, y),$$

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

When x and y differ, $zx \neq zy$ holds for 50% of all $z \in (\mathbb{F}_2)^n$. The probability, that $xz = yz$ for 20 randomly chosen z is $2^{-20} \approx 10^{-6}$.

9

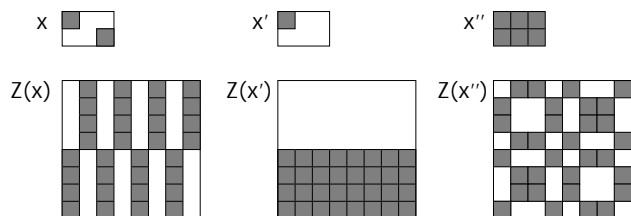
$(\mathbb{F}_2)^6$ as "pictures"



10

From small to large differences

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



But $Z(x)$ is very big!

11

Orthogonal vectors

For $x \in (\mathbb{F}_q)^n \setminus \{0\}$ let

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

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

PROOF For $z = (z_1, \dots, z_n) \in (\mathbb{F}_q)^n$, let $z' := (z_1, \dots, z_{n-1})$. We have $yz = y'z' + y_n z_n$.

Consider an $x \in (\mathbb{F}_q)^n$ with $x_n \neq 0$. The mapping $\mathbb{F} \rightarrow \mathbb{F}$ defined by $c \mapsto x_n c$ is a bijection. Thus for every $u = (u_i)_{i=1}^{n-1} \in (\mathbb{F}_q)^{n-1}$ there is exactly one c with

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

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

If $x \in (\mathbb{F}_q)^n \setminus \{0\}$, then there is an $x_i \neq 0$, and we can argue similarly. \square

Observe, that $\text{Eq}(x, y) = \text{Orth}(x - y)$!

12

Lines and points in the plane: There is exactly one line through any two points. Every two lines intersect in exactly one point – or they are parallel (*affine plane*).

Planes and lines through the origin 0 in \mathbb{R}^3 : Any two lines span a unique plane. Any two planes intersect in exactly one line – always! (*projective plane*).

General principle (Abstraction): Let P be a set and $\mathcal{L} \subseteq 2^P$. The set system (P, \mathcal{L}) with the following properties:

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

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

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

is called a *projective plane*.

Construction of projective planes

Let F be a field. For $x, y \in F^3 \setminus \{0\}$, let

$$x \sim y \iff x = cy \text{ for some } c \in F.$$

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

\sim is an equivalence relation with equivalence classes

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

for $x \in F^3 \setminus \{0\}$.

$F = \mathbb{Z}_3: [(0, 2, 1)] = \{(0, 2, 1), (0, 1, 2)\}$.
 $F = \mathbb{R}: [x]$ is the line through 0 and x (without 0).

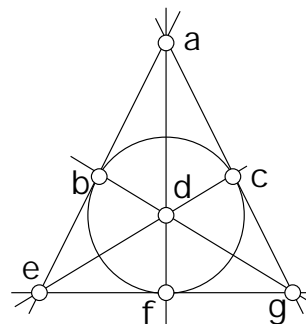
If $|F| = n$ is finite, then for all $x \in F^3 \setminus \{0\}$ we have $|[x]| = n - 1$, and consequently there are

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

equivalence classes.

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

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



Fano plane

There is a $K_{2,2}$ -free bipartite graph with 14 vertices and 21 edges corresponding to the Fano plane (how?).

Construction – continued

For each $[x]$ choose the vector, whose last nonzero coordinate is 1 as a representative.

$F = \mathbb{Z}_3$: There are 13 equivalence classes with representatives

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

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

Now let

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

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

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

Observe that

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

points and lines are interchangeable; through each point there are $n + 1$ lines.

PROOF OMITTED. For each F , (P, \mathcal{L}) forms a projective plane. For $|F| = n \in \mathbb{N}$ there are $n^2 + n + 1$ points, the same number of lines, every line has $n + 1$ points, and every point lies on $n + 1$ lines. *This holds for every finite projective plane!*

What else? Why?

Every finite projective plane has $n^2 + n + 1$ points and lines, for some $n \in \mathbb{N}$. n is then called the *order* of the plane (i.e. if $|F| = n$, then F creates a projective plane of order n).

The Fano plane, created by the field \mathbb{Z}_2 , is the smallest projective plane. According to the characterization of finite fields there exist finite projective planes for all $n = p^r$, p prime; i.e. for example when $n = 2, 3, 4, 5, 7, 8, 9, 11, 13, \dots$. Whether this is possible for other n is not known. Already Euler wanted to show that $n = 6$ is not possible; this only was achieved around 1900 by Tarry. Only by the end of the last century it became feasible to show with an enormous use of computer power that $n = 10$ cannot be the order of a projective plane. The case $n = 12$ is still open.

For a long time finite projective planes – like so many other things in mathematics – were just considered fascinating objects (for some mathematicians) without any applications. Today they play an important role because of the theory of elliptic curves, which ‘exist’ in projective planes. These ‘curves’ are relevant in modern cryptography.

The incidence graph (between points and lines) of a projective plane of order n has $N = 2(n^2 + n + 1)$ vertices, $(n^2 + n + 1)(n + 1) > (N/2)^{3/2} \approx 0.35N^{3/2}$ edges and it is $K_{2,2}$ -free. We showed that a $K_{2,2}$ -free graph with N vertices can have at most $\frac{1}{2}(N^{3/2} + N)$ edges.

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

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

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

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

Mehr Filterpolynome

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

25

Nullstellen

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

26

Polynome und \mathbb{F}_4

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

Für $a(x), b(x) \in \mathbb{Z}_2[x]$, definiere $a(x) \sim b(x)$ falls

$$a(x) - b(x) = (x^2 + x + 1)c(x)$$

für ein $c(x) \in \mathbb{Z}_2[x]$. $x^2 + x + 1$ teilt $a(x) - b(x)$

$$\begin{aligned} x^2 &\sim x + 1, & x^2 + 1 &\sim x, \\ x^2 + x &\sim 1, & x^2 + x + 1 &\sim 0, \dots \end{aligned}$$

\sim ist eine Äquivalenzrelation (zu beweisen) mit Äquivalenzklassen

$$[a(x)] := \{b(x) \in \mathbb{Z}_2[x] : b(x) \sim a(x)\}$$

Definiere

$$\begin{aligned} [a(x)] + [b(x)] &:= [a(x) + b(x)] \\ [a(x)] \cdot [b(x)] &:= [a(x) \cdot b(x)]. \end{aligned}$$

27