

Mathematik für Informatiker 3

<http://www.richiwolesch.de.vu>

WS 2006/07

Zusammenfassung

Dies ist eine Mitschrift zur Vorlesung Mathematik 3 für Informatiker von Prof. Ganter. Trotz größtmöglicher Sorgfalt kann ich keine Gewähr für die Richtigkeit geben. *Wer sich auf diese Mitschrift verlässt ist selbst Schuld!*

Die Verweise auf Folien beziehen sich auf die Vorlesungsfolien von Prof. Ganter. Die gibts hier: <http://www.math.tu-dresden.de/~ganter/inf2006/index.html>

rw

1 Die Automorphismengruppe eines Graphen

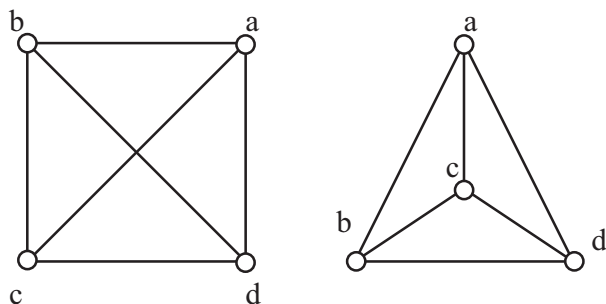


Abbildung 1: Zwei Diagramme des gleichen Graphen

Definition: Ein schlichter ungerichteter *Graph* (V, E) besteht aus einer Menge V und einer Menge E , deren Elemente zweielementige Teilmengen von V sind. Die Elemente von V nennt man *Ecken* (vertices) des Graphen (V, E) . Die Elemente von E nennt man *Kanten* (edges) des Graphen (V, E) .

In Abb. 1 ist $V = \{a, b, c, d\}$ und $E = \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}\}$

Sind die beiden Graphen in Abb. 2 *isomorph*? D.h. geben die beiden Diagramme bis auf Umbenennung den gleichen Graphen an?

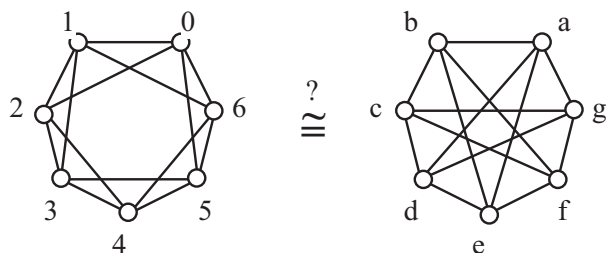


Abbildung 2: Zwei andere Graphen

Ja, es geht! Eine mögliche Zuordnung lautet:

$$\begin{pmatrix} a & b & c & d & e & f & g \\ 0 & 2 & 4 & 6 & 1 & 3 & 5 \end{pmatrix}$$

Und nochmal zur Übung (Abb. 3)...

Nein, die beiden Graphen sind nicht isomorph. (Erkennt man daran, dass der linke Graph Dreiecke enthält, z.B. $\Delta(0, 1, 2)$. Der rechte Graph enthält keine Dreiecke, egal wie man die Ecken zerzt!)

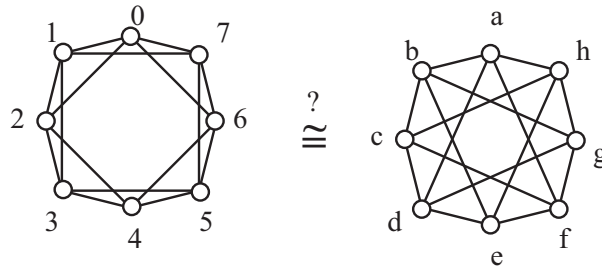


Abbildung 3: Noch zwei andere Graphen

Definition: Zwei Graphen (V_1, E_1) und (V_2, E_2) heißen (zueinander) *isomorph*, wenn es eine bijektive Abbildung

$$\varphi : V_1 \longrightarrow V_2$$

gibt, die kantenerhaltend und kantenreflektierend ist. Jede solche Abbildung wird *Isomorphismus* genannt.

Dabei heißt $\varphi : V_1 \longrightarrow V_2$ *kantenerhaltend*, falls

$$(1) \{v, w\} \in E_1 \implies \{\varphi(v), \varphi(w)\} \in E_2$$

und *kantenreflektierend*, falls

$$(2) \{v, w\} \in E_1 \iff \{\varphi(v), \varphi(w)\} \in E_2.$$

Äquivalent zu (2) ist

$$\{v, w\} \notin E_1 \implies \{\varphi(v), \varphi(w)\} \notin E_2$$

Wie stellt man fest, ob zwei gegebene Graphen isomorph sind? Gibt es dafür einen schnellen Algorithmus?

Das ist unbekannt! Das Graph Isomorphism Problem gehört zum Problemkreis $P \stackrel{?}{=} NP$.

Automorphismen („Selbst-Isomorphismen“): Für jeden Graphen ist die identische Abbildung ein Automorphismus. Die Frage die wir hier bearbeiten ist folgende: Bestimme alle Automorphismen eines beliebigen gegebenen Graphen.

Beispiel:

α, β, γ sind (verschiedene) Automorphismen:

$$\alpha := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 0 & 5 & 6 & 7 & 4 \end{pmatrix}$$

$$\beta := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 3 & 7 & 4 & 1 & 2 & 6 & 5 \end{pmatrix}$$

$$\gamma := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 0 & 3 & 2 & 5 & 4 & 7 & 6 \end{pmatrix}$$

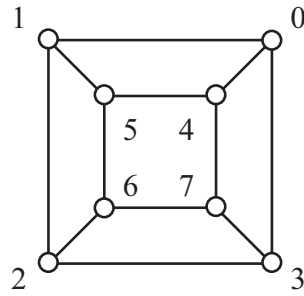


Abbildung 4: Automorphismen

Dabei ist α eine 90°-Drehung und β eine 120°-Drehung um die Diagonale (0, 6). γ ist eine Spiegelung an der Vertikalen durch die Mitte.

Bijektive Abbildungen einer Menge V auf sich nennt man *Permutation* von V . Ist V eine endliche Menge mit $n = |V|$ Elementen, dann gibt es genau $n!$ Permutationen von V .

Mit Permutationen kann man rechnen, denn es gibt eine natürliche Verknüpfung, die aus je zwei Permutationen von V eine neue macht: Die *Hintereinanderausführung*.

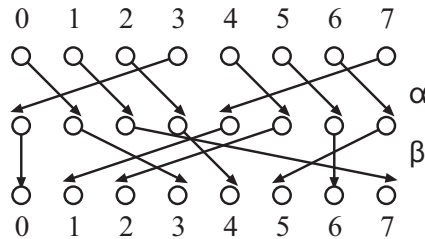


Abbildung 5: Hintereinanderausführung von α und β

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 7 & 4 & 3 & 2 & 6 & 5 & 1 \end{pmatrix} = \alpha; \beta = \beta \circ \alpha$$

Für Permutationen α und β von V definiert man $\alpha; \beta(v) = \beta \circ \alpha(v) = \beta(\alpha(v))$ für alle $v \in V$. Man spricht: $\alpha; \beta$ - Alpha vor Beta und $\beta \circ \alpha$ - Beta nach Alpha.

Hintereinanderausführung von Automorphismen ergibt Automorphismen.

→ siehe Folien „Automorphismen“

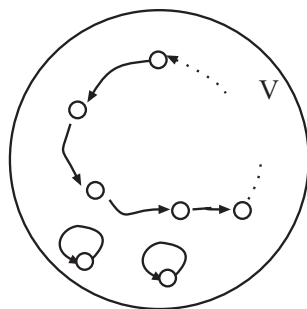


Abbildung 6: Spezielle Permutationen: Zyklus der Länge r

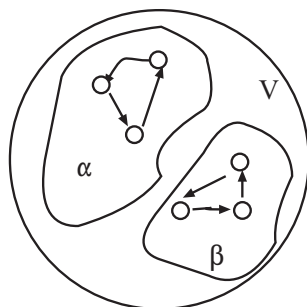


Abbildung 7: Elementfremde Permutationen α und β

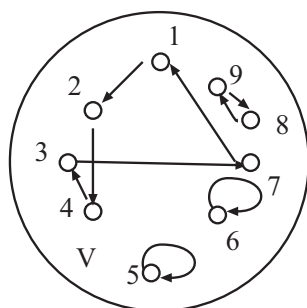


Abbildung 8: Hintereinanderausführung von Zyklen: $(12437) \circ (5) \circ (6) \circ (89)$

Man beachte, dass \circ die Hintereinanderausführung von „rechts nach links“ ist!

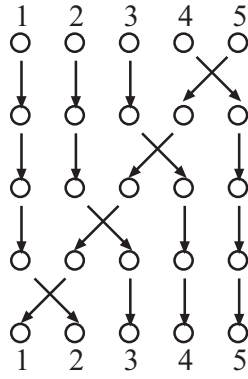


Abbildung 9: $(12345) = (12) \circ (23) \circ (34) \circ (45)$

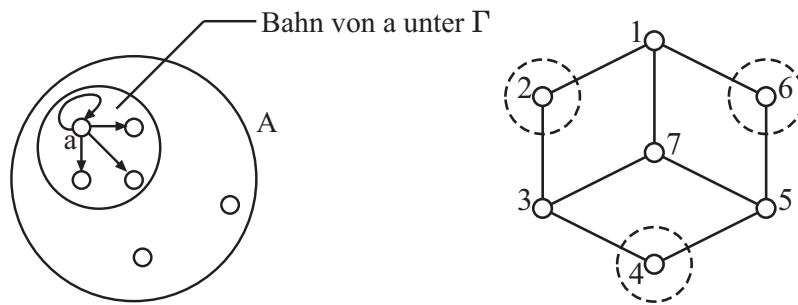


Abbildung 10: Orbits

In Abb. 10 (rechts) liegen z.B. 2, 4 und 6 in einer Bahn: $2^\Gamma = \{2, 4, 6\}$

Außerdem: $1^\Gamma = \{1, 3, 5\}$ und $7^\Gamma = \{7\}$

Finde die Bahnen (Orbits) von $\text{Aut}(V, E)$, der Automorphismengruppe dieses Graphen (Abb. 11)!

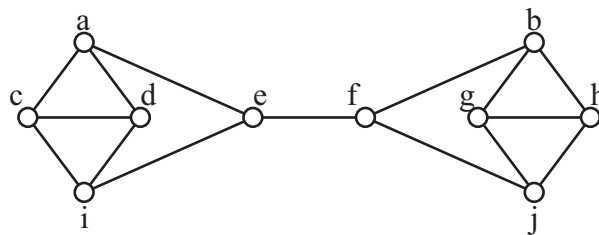


Abbildung 11: Bahnen finden...

Man zeichnet dazu einen anderen Graphen auf der gleichen Eckenmenge (Abb. 12).

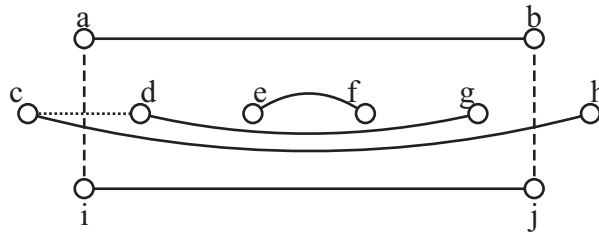


Abbildung 12: ... Schritt 1

1. Rate einige Automorphismen des Graphen, z.B.:

$$\alpha := (ab) \circ (ch) \circ (dg) \circ (ef) \circ (ij)$$

$$\beta := (ai) \circ (bj)$$

$$\gamma := (cd)$$

2. Trenne Ecken, die an unterschiedlichen Zusammenhangskomponenten liegen, durch trennende Eigenschaften.

3. Wenn dies nicht gelingt, müssen weitere Automorphismen geraten werden. Wenn je zwei Zusammenhangskomponenten getrennt werden können, dann gilt:

Die Bahnen der Automorphismengruppe sind genau die Zusammenhangskomponenten des Hilfsgraphen.

→ siehe Folien „Nebenklassen“ Ist U eine Untergruppe der Gruppe G und g ein Element

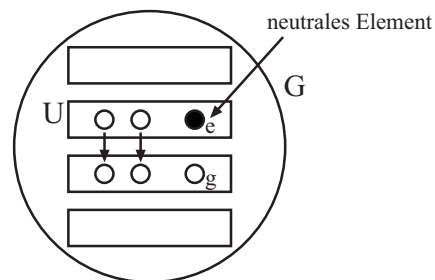


Abbildung 13: Nebenklassen

von G , dann nennt man $g \circ U := \{g \circ u \mid u \in U\}$ eine Nebenklasse von U in G . In Abb. 13 ist die Nebenklasse von U also die Klasse, die g enthält. Es gilt:

$$\left. \begin{array}{l} U \longrightarrow g \circ U \\ u \longmapsto g \circ u \end{array} \right\} \text{ ist bijektiv}$$

Aus $g \circ u_1 = g \circ u_2$
 folgt $g^{-1} \circ g \circ u_1 = g^{-1} \circ g \circ u_2$
 also $u_1 = u_2$.

Alle Nebenklassen haben kein Element gemeinsam (disjunkt) und sind gleich groß.

$[G:U]$ ist die Anzahl der Nebenklassen der Gruppe G . Sie heißt Index. G hat eine endliche Mächtigkeit: $|G|$ ist endlich.

$$\langle a \rangle = \{e, a, a^2, \dots, a^{m-1}\}$$

e ist das neutrale Element. Es wird gelegentlich auch mit 1 bezeichnet.

$$a^m = e, \quad m \mid |a| \quad (m \text{ teilt } |a|)$$

$$m \cdot n = |G| \quad n \in \mathbb{N}$$

$$a^{|G|} = a^{m \cdot n} = (a^m)^n = e$$

→ siehe Folien „Satz von Cauchy-Frobenius“

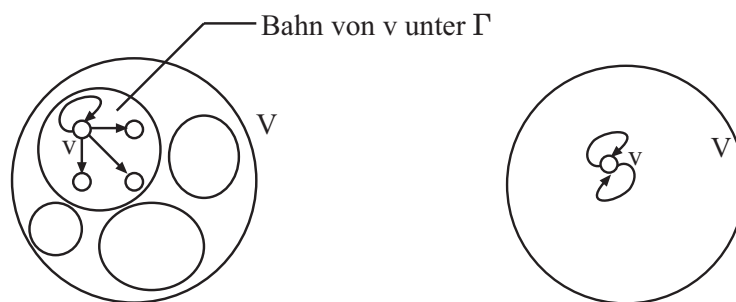


Abbildung 14: Bahn (Orbit) von v unter Γ und Stabilisator von v

Abb. 14 zeigt links die Bahn von v unter Γ mit $\Gamma < S_v$. Bahnen zerschneiden V , können aber unterschiedlich groß sein. Rechts sieht man den Stabilisator von v in Γ .

$$\Gamma_v = \{\gamma \in \Gamma \mid \gamma(v) = v\}$$

- $\alpha(v) = v = \beta(v) \implies (\alpha \circ \beta)(v) = v$
- $\alpha(v) = v \implies \alpha^{-1}(v) = v$
- $id(v) = v$

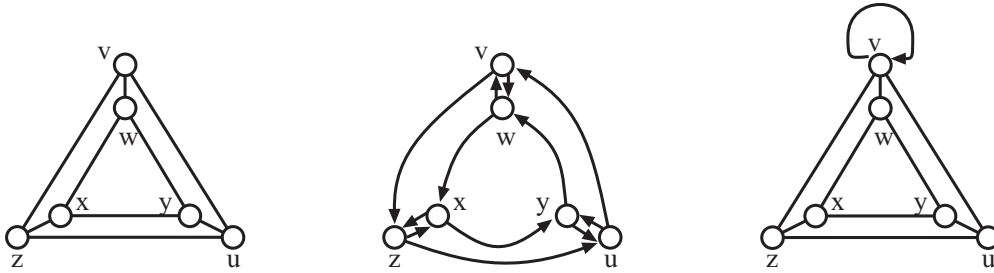


Abbildung 15: Wieviele Automorphismen hat der Graph? Berechnung mit Hilfe des Satzes von Cauchy-Frobenius. . .

Die Anzahl der Automorphismen eines Graphen ermittelt man am besten, indem man den Satz von Cauchy-Frobenius anwendet. Für den Graphen in Abb. 15 ergibt sich damit folgendes:

1. Raten einiger Automorphismen und Eintragen in den Hilfsgraphen, z.B.:
 $\alpha = (vzu)(wxy)$
 $\beta = (vw)(zx)(uy)$
 Wie in der mittleren Abbildung zu sehen ist, besteht der Hilfsgraph nur aus einer Zusammenhangskomponente. Folglich ist $\text{Aut}(G)$ transitiv und $|\Gamma| = 6$.
2. Der Stabilisator (Hilfsgraph rechts) besitzt nur zwei Elemente:
 $\gamma = (xy)(uz) \in \Gamma_v$ und die Identität id
 Folglich ist $\Gamma_v = 2$.
3. Nach Cauchy-Frobenius ist $|\Gamma| = 12$.

Der Graph hat also 12 Automorphismen.

Und weil es uns so gut gefiel, noch einmal das schöne Spiel. . .

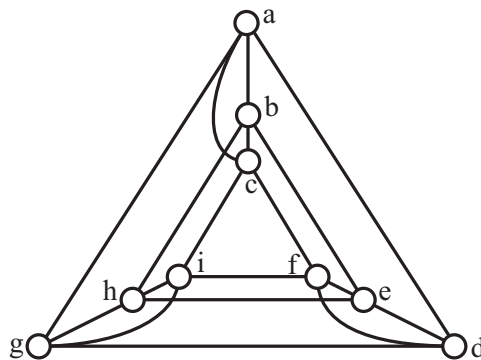


Abbildung 16: Noch einmal ist die Anzahl der Automorphismen gefragt.

1. Auch der Graph in Abb. 16 ist transitiv. Deshalb ist $|a^\Gamma| = 9$.

2. Wir versuchen deshalb den Stabilisator eines Elements zu bestimmen, z.B. Γ_a .
Dann raten wir Elemente von Γ_a , z.B.:

$$\alpha = (if)(he)(gd)$$

$$\beta = (bc)(ef)(hi)$$

(Dazu zeichnet man am besten wieder einen Hilfsgraphen.)

3. Bestimme die Bahn eines Elements, z.B. e unter Γ_a . Da e bei festem a weder auf c noch auf d abgebildet werden kann, sondern nur auf f , h und i ergibt sich $|e^{\Gamma_a}| = 4 = |\{e, f, h, i\}|$.
4. Bestimme $|\Gamma_{a,e}|$! Dazu muss man alle Automorphismen finden, bei denen die Ecken a und e fest bleiben. Das gilt nur für die identische Abbildung id und für die Abbildung

$$\gamma := (bd)(cg)(fh).$$

Damit ist $\Gamma_{a,e} = \{id, \gamma\}$ und $|\Gamma_{a,e}| = 2$.

5. $|\Gamma| = |a^\Gamma| \cdot |\Gamma_a| = 9 \cdot |e^{\Gamma_a}| \cdot |\Gamma_{a,e}| = 9 \cdot 4 \cdot 2 = 72$
Damit gibt es 72 Automorphismen für diesen Graph.

2 Körper

→ siehe Folien „Klassifikation der endlichen abelschen Gruppen“

Wann ist $\mathbb{Z}_m \times \mathbb{Z}_n$ zyklisch?

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{m \cdot n} \Leftrightarrow \text{ggT}(m, n) = 1$$

Für $(i, j) \in \mathbb{Z}_m \times \mathbb{Z}_n$ bilde die Vielfachen $(i, j), (i, j) + (i, j), 3(i, j), \dots$

Dabei ist $a(i, j) = ((a \cdot i) \bmod m, (a \cdot j) \bmod n)$. Die Ordnung von (i, j) ist die kleinste natürliche Zahl a mit $a \cdot (i, j) = (0, 0)$, also die kleinste Zahl a mit $\left\{ \begin{array}{l} a \cdot i \bmod m = 0 \text{ und} \\ a \cdot j \bmod n = 0 \end{array} \right\}$.

Wenn $a = \text{kgV}(m, n)$ ist, ist diese Bedingung sicher erfüllt. Die Ordnung ist also bestimmt $\leq \text{kgV}(m, n)$, für $i = j = 1$ ist sie sogar gleich dem $\text{kgV}(m, n)$.

Die Gruppe $\mathbb{Z}_m \times \mathbb{Z}_n$ enthält also genau dann ein Element der Ordnung $m \cdot n$, wenn $m \cdot n = \text{kgV}(m, n)$ ist.

Also: $\mathbb{Z}_m \times \mathbb{Z}_n$ ist genau dann zyklisch, wenn m und n teilerfremd sind.

Noch eine Motivation zum Thema Automorphismengruppen:

Die *Polya-Theorie* dient dazu, die Anzahl nicht isomorpher Lösungen bestimmter Probleme zu finden.

Beispiel: Wieviele Möglichkeiten gibt es einen Würfel mit zwei Farben einzufärben?

| Anzahl in einer Farbe gefärbter Flächen | Anordnung der Flächen | Möglichkeiten |
|---|------------------------|---------------|
| 0 bzw. 6 | alle | 2 |
| 1 | | 2 |
| 2 | aneinandergrenzend | 2 |
| 2 | gegenüberliegend | 2 |
| 3 | u-förmig | 1 |
| 3 | an einer Ecke zusammen | 1 |
| | | $\Sigma = 10$ |

Es gibt 10 Möglichkeiten, die zueinander nicht isomorph sind.

→ siehe Folien „Nullteiler und Einheiten in Ringen“

Potenzen von Einheiten sind keine Nullteiler

Beweis: Angenommen a, a^2, a^3, \dots, a^n ($a \neq 0$) sind alle nicht Nullteiler. Beachte $a^{(n+1)}$. Wäre diese ein Nullteiler, gäbe es ein $b \neq 0$ mit $a^{(n+1)} \cdot b = 0$. Aus $a^{(n+1)} \cdot b = 0$ folgt

$$a \cdot (a^n \cdot b) = 0,$$

woraus, weil a kein Nullteiler ist,

$$a^n \cdot b = 0$$

folgt. Dann wäre a^n ein Nullteiler. \implies Widerspruch!

Einheiten modulo 24

Anzahl der Einheiten in \mathbb{Z}_{24} :

$$\varphi(24) = 24 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 24 \cdot \frac{1}{2} \cdot \frac{2}{3} = 8$$

Es gibt 8 Einheiten in \mathbb{Z}_{24} .

Die Menge $\mathbb{Z}_{24}^* = \{1, 5, 7, 11, 13, 17, 19, 23\}$ der Einheiten und mod 24 bilden mit der Multiplikation mod 24 eine abelsche Gruppe.

Welche? $\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2$ oder $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Die Einheitengruppe \mathbb{Z}_{24}^* ist isomorph zu $(\mathbb{Z}_2)^3$.

Zur Erinnerung noch eine wichtige Konsequenz: Einheiten mod n sind genau die Elemente von \mathbb{Z}_n , die zu n teilerfremd sind. Wenn n eine Primzahl ist (und nur dann), dann ist jedes Element $\neq 0$ eine Einheit, d.h. für p prim ist \mathbb{Z}_p ein Körper.

→ siehe Folien „Schieberegister und Polynomdivision“

Sensation: Körper mit 4 Elementen entdeckt!

Beachte: Der Körper kann nicht zu \mathbb{Z}_4 isomorph sein, denn \mathbb{Z}_4 enthält einen Nullteiler und ist folglich kein Körper!

→ siehe Folien „endliche Körper“

Rechnen in $GF(16) = GF(2)[X]/p(X)$, $p(x) = X^4 + X + 1$

Weil das Polynom $p(x)$ primitiv ist, sind die von 0 verschiedenen Elemente von $GF(2)[X]/p(X)$ genau die Elemente $X, X^2, X^3, \dots, X^{q-1} \text{ mod } p(X)$

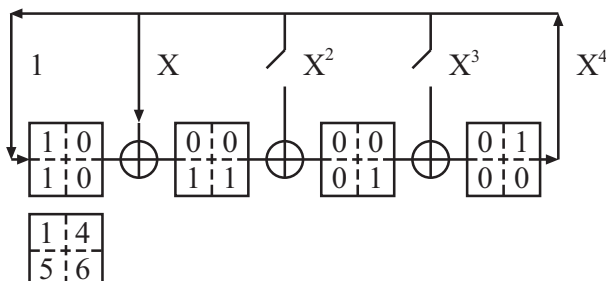


Abbildung 17: Rückkopplungspolynom $p(X)$; Schieberegister - dargestellt sind die Zustände 1, 4, 5 und 6

Berechnung der Potenzen von X , wie in Abb. 17: $1, X, X^2, X^3, 1 + X, X + X^2, X^2 + X^3, 1 + X + X^3, 1 + X^2, X + X^3, 1 + X + X^2, X + X^2 + X^3, 1 + X + X^2 + X^3, 1 + X^2 + X^3, 1 + X^3, (1)$

Als Tabelle:

| Potenz | Tupel | Körperelement | Log. | Potenz | Tupel | Körperelement | Log. |
|--------|-------|---------------|-----------|--------------|-------|---------------------|------|
| 0 | 0000 | 0 | $-\infty$ | X^7 | 1101 | $1 + X + X^3$ | 7 |
| 1 | 1000 | 1 | 0 | X^8 | 1010 | $1 + X^2$ | 8 |
| X | 0100 | X | 1 | X^9 | 0101 | $X + X^3$ | 9 |
| X^2 | 0010 | X^2 | 2 | X^{10} | 1110 | $1 + X + X^2$ | 10 |
| X^3 | 0001 | X^3 | 3 | X^{11} | 0111 | $X + X^2 + X^3$ | 11 |
| X^4 | 1100 | $1 + X$ | 4 | X^{12} | 1111 | $1 + X + X^2 + X^3$ | 12 |
| X^5 | 0110 | $X + X^2$ | 5 | X^{13} | 1011 | $1 + X^2 + X^3$ | 13 |
| X^6 | 0011 | $X^2 + X^3$ | 6 | X^{14} | 1001 | $1 + X^3$ | 14 |
| | | | | $X^{15} = 1$ | 1000 | 1 | 0 |

- Addition: Addition der Koeffiziententupel (mod 2)
- Multiplikation: Addition der Logarithmen (mod 15)

Beispiel: $\frac{X+X^2}{1+X^3}(1 + X + X^3)$

Laut Tabelle gilt:

$$\log(X + X^2) = 5$$

$$\begin{aligned} \log(1 + X^3) &= 14 \\ \log(1 + X + X^3) &= 7 \end{aligned}$$

und damit

$$\log\left(\frac{X + X^2}{1 + X^3}(1 + X + X^3)\right) = 5 - 14 + 7 = 13 \pmod{15} = \log(1 + X^2 + X^3)$$

also

$$\frac{X + X^2}{1 + X^3}(1 + X + X^3) = 1 + X^2 + X^3 \text{ in } GF(16)$$

→ siehe Folien „Kryptosysteme und zyklische Codes“

n-te Einheitswurzeln in GF(64)

α sei ein primitives Element in GF(64). Wegen $63 = 3 \cdot 3 \cdot 7$ gibt es in GF(64) also 3-te, 7-te, 9-te und 21-te Einheitswurzeln.

α^3 ist eine 21. Einheitswurzel, denn $(\alpha^3)^{21} = \alpha^{63} = 1$.

β^3 ist eine 21. Einheitswurzel, für $\beta \neq 0$.

In GF(64) zerfällt das Polynom X^{21} in Linearfaktoren.

→ siehe Folien „???“

Charakteristik eines Körpers

$$\underbrace{1 + 1 + \dots + 1}_n = \underbrace{1 + 1 + 1 + \dots + 1}_m \quad n < m$$

ergibt

$$0 = \underbrace{1 + 1 + \dots + 1}_{m-n>0}$$

Die *Charakteristik* eines Körpers \mathbb{K} ist entweder 0 oder eine Primzahl p . Wenn

$$\underbrace{(1 + 1 + \dots + 1)}_n \cdot \underbrace{(1 + 1 + \dots + 1)}_m = 0$$

also

$$n \cdot 1 = 0 \text{ oder } m \cdot 1 = 0$$

$GF(p^n)$ hat Charakteristik p .

In einem Körper der Charakteristik p gilt für jedes Element a :

$$\underbrace{a + a + \dots + a}_{p\text{-mal}} = 0 = a \cdot \underbrace{1 + 1 + \dots + 1}_{p\text{-mal}}$$

Beispiel zur Faktorisierungsstrategie

X^{17} soll in $GF(2^s)$ in Linearfaktoren zerlegt werden. Wie ist s zu wählen?

Antwort: So, dass 17 ein Teiler von $2^s - 1$ ist. Man nimmt *also* $s = 8$. Man ermittelt s , indem man die Potenzen von $p (=2)$ modulo 17 bildet, bis 1 herauskommt:

$$\begin{array}{cccccccc} 2, & 4, & 8, & 16, & 15, & 13, & 9, & 1, \dots \\ 2^1 & 2^2 & 2^3 & 2^4 & 2^5 & 2^6 & 2^7 & 2^8 \end{array}$$

Folglich ist $2^8 - 1$ durch 17 teilbar. Also $s = 8$.

In $GF(2^8) = GF(2)[X]/X^8 + X^4 + X^3 + X^2 + 1$ ist das Polynom X ein primitives Element und

$$\beta := X^{15} \text{ mod } X^8 + X^4 + X^3 + X^2 + 1$$

eine primitive 17. Einheitswurzel, denn

$$\beta^{17} \equiv (X^{15})^{17} = X^{15 \cdot 17} \equiv 2^{255} \equiv 1 \text{ mod } X^8 + X^4 + X^3 + X^2 + 1$$

und $\beta^i, 1 \leq i \leq 17$ ist ebenfalls 17. Einheitswurzel.

Ergebnis: In $GF(2^8)[X]$ ist

$$X^{17} - 1 = (X - \beta)(X - \beta^2) \cdots (X - \beta^{14}), \beta \text{ primitive 17. Einheitswurzel}$$

Wenn $f(X)$ ein Teiler von $X^{17} - 1$ ist, dessen Koeffizienten aus $GF(2)$ sind, und wenn β eine Nullstelle von $f(X)$ ist, dann auch $\beta^2, \beta^4, \beta^8, \dots$

Also auch β^i , wobei $i \in 1, 2, 4, 8, 16, 15, 13, 9$.

$$f(x) = (X - \beta)(X - \beta^2)(X - \beta^4)(X - \beta^8)(X - \beta^{16})(X - \beta^{15})(X - \beta^{13})(X - \beta^9)$$

ist dafür die kleinste Möglichkeit.

Dieses Polynom $f(x)$ hat Koeffizienten in $GF(2)$.

Erledigt: Wie findet man alle Teiler von $X^n - 1$, n ungerade in $GF(2)[X]$?

Wichtigstes Hilfsmittel: Die zyklotomen Klassen $\text{mod } n$. Zu jeder solchen Klasse gehört ein irreduzibler Teiler.

BCH-Codes

→ siehe Folien „BCH-Codes“

Konstruiert werden soll (als Beispiel) ein 2 Fehler korrigierender Binär-BCH-Code der Länge 15.

Eine primitive 15. Einheitswurzel über $GF(2)$ findet man in $GF(2^4)$. Um in $GF(16)$ rechnen zu können, schlagen wir ein primitives Polynom vom Grad 4 über $GF(2)$ nach und finden $X^4 + X + 1$, bzw. $\alpha^4 + \alpha + 1$.

| | | | |
|----|---------------|------------------------------------|------|
| 0 | α^0 | 1 | 1000 |
| 1 | α^1 | α | 0100 |
| 2 | α^2 | α^2 | 0010 |
| 3 | α^3 | α^3 | 0001 |
| 4 | α^4 | $1 + \alpha$ | 1100 |
| 5 | α^5 | $\alpha + \alpha^2$ | 0110 |
| 6 | α^6 | $\alpha^2 + \alpha^3$ | 0011 |
| 7 | α^7 | $1 + \alpha + \alpha^3$ | 1101 |
| 8 | α^8 | $1 + \alpha^2$ | 1010 |
| 9 | α^9 | $\alpha + \alpha^3$ | 0101 |
| 10 | α^{10} | $1 + \alpha + \alpha^2$ | 1110 |
| 11 | α^{11} | $\alpha + \alpha^2 + \alpha^3$ | 0111 |
| 12 | α^{12} | $1 + \alpha + \alpha^2 + \alpha^3$ | 1111 |
| 13 | α^{13} | $1 + \alpha^2 + \alpha^3$ | 1011 |
| 14 | α^{14} | $1 + \alpha^3$ | 1001 |
| 15 | α^{15} | 1 | 1000 |

Womit gezeigt wäre, dass die 15. Einheitswurzel in $GF(2)[X]/X^4 + X + 1$ existiert.

Die Teiler von $X^{15} - 1$ findet man mit Hilfe der zyklotomen Klassen mod 15.

| | | |
|---------------------|---|---|
| $\{0\}$ | $X - \alpha^0 = X - 1$ | |
| $\{1, 2, 4, 8\}$ | $(X - \alpha^1)(X - \alpha^2)(X - \alpha^4)(X - \alpha^8) = X^4 + X + 1$ | * |
| $\{3, 6, 12, 9\}$ | $(X - \alpha^3)(X - \alpha^6)(X - \alpha^{12})(X - \alpha^9) = X^4 + X^3 + X^2 + X + 1$ | * |
| $\{5, 10\}$ | $(X - \alpha^5)(X - \alpha^{10})$ | |
| $\{7, 14, 13, 11\}$ | $(X - \alpha^7)(X - \alpha^{14})(X - \alpha^{13})(X - \alpha^{11})$ | |

Beispielrechnung für $(X - \alpha^3)(X - \alpha^6)(X - \alpha^{12})(X - \alpha^9)$:

$$\begin{aligned}
 & (X - \alpha^3)(X - \alpha^6)(X - \alpha^{12})(X - \alpha^9) \\
 &= (X^2 - (\alpha^3 + \alpha^6)X + \alpha^9)(X - \alpha^{12})(X - \alpha^9) \\
 &= (X^2 - \alpha^2 X + \alpha^9)(X^2 - (\alpha^{12} + \alpha^9)X + \alpha^{21}) \\
 &= (X^2 - \alpha^2 X + \alpha^9)(X^2 - \alpha^8 X + \alpha^6) \\
 &= X^4 + (-\alpha^2 - \alpha^8)X^3 + (\alpha^6 + \alpha^{10} + \alpha^9)X^2 + (-\alpha^8 - \alpha^7)X + \alpha^{15} \\
 &= X^4 + X^3 + X^2 + X + 1
 \end{aligned}$$

* Das Produkt dieser beiden Polynome ist Generatorpolynom eines BCH-Codes mit $n = 15$ und $d \geq 5$.

$$g(X) = (X^4 + X^3 + X^2 + X + 1)(X^4 + X + 1) = X^8 + X^7 + X^6 + X^4 + 1$$

Es ist nun der Code C gegeben durch

$$C = \{m(X) \cdot g(X) \mid m(X) \in GF(2)[X], \text{grad}(m(X)) < 7\}$$

also $|C| = 2^7$ und $d = 5$.

Beispiele für Elemente des Codes C :

$$\begin{aligned}
 g(X) &\hat{=} (000000111010001) \\
 X^3 \cdot g(X) &\hat{=} (000111010001000) \\
 (1 + X^3) \cdot g(X) &\hat{=} (000111101011001)
 \end{aligned}$$

Schluß mit diesem Thema.

3 Verbände

→ siehe Folien „Vollständige Verbände und boolesche Algebren“

Ein freier distributiver Verband mit 3 Erzeugenden...

$$x, y, z, x \wedge y, x \vee y, x \wedge z, x \vee z, y \wedge z, y \vee z, x \wedge y \wedge z, x \vee y \vee z, x \wedge (y \vee z), \dots$$

\vee ... Supremum

\wedge ... Infimum

Insgesamt hat der Verband 18 Elemente. (siehe Folie 12)

Fügt man noch die Elemente *true* (\top) und *false* (\perp) hinzu, so erhält man den Verband aller monotonen booleschen Funktionen in den Variablen x, y, z . (Abb. 18)

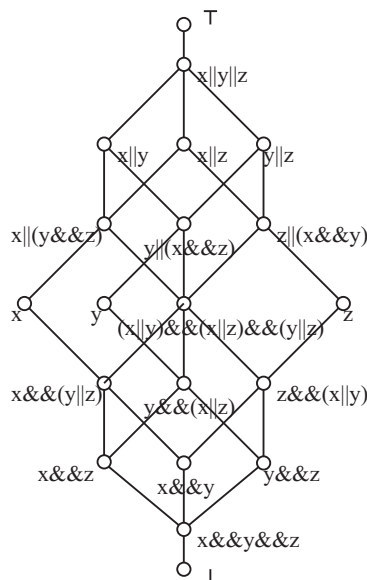


Abbildung 18: Verband aller monotonen booleschen Funktionen in den Variablen x, y, z

Die freie boolesche Algebra erzeugt von x, y kann durch den vierdimensionalen Würfel dargestellt werden. (Abb. 19)

Wiederholung: Eigenwerte, Eigenvektoren

Wir betrachten quadratische Matrizen über einem Körper \mathbb{K} , d.h. $\mathcal{A} \in \mathfrak{M}(n \times n, \mathbb{K})$.

Die Aufgabe ist, alle Eigenwerte und Eigenvektoren von \mathcal{A} zu bestimmen, d.h. alle Lösungen $\lambda \in \mathbb{K}, v \in \mathbb{K}^n$ der Gleichung

$$\mathcal{A}v = \lambda v$$

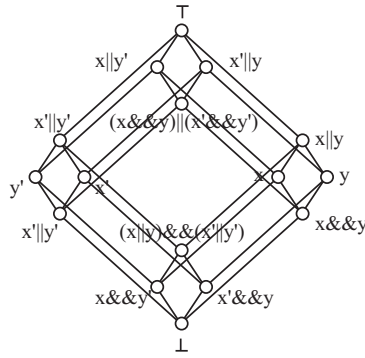


Abbildung 19: Freie Boolesche Algebra mit zwei Erzeugenden.

Ist (λ, v) eine Lösung mit $v \neq 0$, dann ist λ ein Eigenwert von \mathcal{A} und v ein Eigenvektor von \mathcal{A} zum Eigenwert λ .

Der Weg zur Bestimmung aller Eigenwerte von \mathcal{A} führt über das *charakteristische Polynom* von \mathcal{A} . Dazu formt man das Problem $\mathcal{A}v = \lambda v$ um zu $(\lambda E - \mathcal{A})v = 0$

Man muss also diejenigen Zahlen λ finden, für die $\lambda E - \mathcal{A}$ nicht regulär ist, also mit

$$\det(\lambda E - \mathcal{A}) = 0.$$

→ siehe Folien „Eigenwerte“

Diagonalisierung einer Matrix A

$$A = \begin{pmatrix} 2 & 2 & 1 \\ 1 & 3 & 1 \\ 1 & 2 & 2 \end{pmatrix}$$

Vorgehensweise:

1. Zur Bestimmung der Eigenwerte von A untersucht man das *charakteristische Polynom* $\det(\lambda E - A)$ auf Nullstellen.

$$\begin{aligned} \det \left(\lambda \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - \begin{pmatrix} 2 & 2 & 1 \\ 1 & 3 & 1 \\ 1 & 2 & 2 \end{pmatrix} \right) &= \det \begin{pmatrix} \lambda - 2 & -2 & 1 \\ -1 & \lambda - 3 & -1 \\ -1 & -2 & \lambda - 2 \end{pmatrix} \\ &= \lambda^3 - 7\lambda^2 + 11\lambda - 5 = P_\lambda(A) \end{aligned}$$

Das charakteristische Polynom $P_\lambda(A)$ wird auch mit $P_A(\lambda)$ bezeichnet.

Wegen $\lambda^3 - 7\lambda^2 + 11\lambda - 5 = (\lambda - 5)(\lambda - 1)^2$ gilt:

Die Eigenwerte von A sind also 5 (mit der Vielfachheit 1) und 1 (mit der algebraischen Vielfachheit 2).

2. Bestimmung des Eigenraumes zum Eigenwert 5.

Der Eigenraum zum Eigenwert λ besteht aus den Lösungen des homogenen Gleichungssystems $(\lambda E - A)v = \underline{0}$.

$$\lambda = 5 : \lambda E - A = \begin{pmatrix} 3 & -2 & -1 \\ -1 & 2 & -1 \\ -1 & -2 & 3 \end{pmatrix}$$

Zu lösen ist damit:

$$\begin{pmatrix} 3 & -2 & -1 \\ -1 & 2 & -1 \\ -1 & -2 & 3 \end{pmatrix} v = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Der Lösungsraum ist eindimensional (d.h. die geometrische Vielfachheit ist 1). Ein Lösungsvektor ist $(1 \ 1 \ 1)^T$, der Lösungsraum besteht also aus allen Vielfachen von

$(1 \ 1 \ 1)^T$. $(1 \ 1 \ 1)^T$ ist ein Eigenvektor der Matrix $A = \begin{pmatrix} 2 & 2 & 1 \\ 1 & 3 & 1 \\ 1 & 2 & 2 \end{pmatrix}$ zum Eigenwert 5.

Anmerkung des Autors:

Die algebraische Vielfachheit ist die Anzahl der Nullstellen des charakteristischen Polynoms für gegebenes λ .

Die Geometrische Vielfachheit ist die maximale Anzahl linear unabhängiger Eigenvektoren zu einem Eigenwert. Sie ist also größer oder gleich Eins und kleiner oder gleich der algebraischen Vielfachheit.

Problem: Dieses Lösungsverfahren funktioniert nicht, wenn

- (1) das charakteristische Polynom nicht in Linearfaktoren zerfällt oder
- (2) die geometrische Vielfachheit ungleich der algebraischen Vielfachheit ist.

$$\lambda = 1 : \lambda E - A = \begin{pmatrix} -1 & -2 & -1 \\ -1 & -2 & -1 \\ -1 & -2 & -1 \end{pmatrix}$$

Zu lösen ist damit:

$$\begin{pmatrix} -1 & -2 & -1 \\ -1 & -2 & -1 \\ -1 & -2 & -1 \end{pmatrix} v = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Der Lösungsraum ist zweidimensional, die geometrische Vielfachheit des Eigenwerts 1 ist 2. Zwei linear unabhängige Lösungen (und damit eine Basis des Eigenraumes) sind $(1 \ 0 \ 1)^T$ und $(2 \ -1 \ 0)^T$

$$\underbrace{\begin{pmatrix} \frac{1}{4} & \frac{1}{2} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{2} & -\frac{3}{4} \\ \frac{1}{4} & -\frac{1}{2} & \frac{1}{4} \end{pmatrix}}_{P^{-1}} \underbrace{\begin{pmatrix} 2 & 2 & 1 \\ 1 & 3 & 1 \\ 1 & 2 & 2 \end{pmatrix}}_A \underbrace{\begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & -1 \\ 1 & -1 & 0 \end{pmatrix}}_P \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 5 \\ 0 \\ 0 \end{pmatrix}$$

$$P^{-1}AP \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

$$P^{-1}AP \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

also $P^{-1}AP = \begin{pmatrix} 5 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ ist Diagonalmatrix

Nutzen der Diagonalisierung, z.B.:

$$A^{60} = (PDP^{-1})^{60} = PD \underbrace{P^{-1} \cdot P}_{{=E}} D \underbrace{P^{-1} \cdot P}_{{=E}} DP^{-1} \dots = PD^{60}P^{-1}$$

→ siehe Folien „(Systeme von) Differentialgleichungen“

Skalarprodukt

→ siehe Folien „Skalarprodukt“

Das Skalarprodukt zweier Vektoren v und w schreibt man als $\langle v, w \rangle = v \circ w$. Wenn beide Vektoren gleich sind gilt:

$$u \circ u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \circ \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = u_1u_1 + \dots + u_nu_n = \sum_{i=1}^n u_i^2 \geq 0$$

Im Spezialfall $u = \underline{0}$ ist $\sum_{i=1}^n u_i^2 = 0$.

Die Länge eines Vektors wird auch als *Norm* bezeichnet. Ein Vektor der Norm 1 ist ein Einheitsvektor. Die Norm eines Vektors u schreibt man $\|u\|$.

In Abb.20 ist d die Projektion von u in die x,y -Ebene. Die Projektion $d = \begin{pmatrix} u_1 \\ u_2 \\ 0 \end{pmatrix}$ hat

die Länge $d = \sqrt{u_1^2 + u_2^2}$. Damit ergibt sich die Norm von u wie folgt:

$$\|u\| = \sqrt{d^2 + u_3^2} = \sqrt{u_1^2 + u_2^2 + u_3^2}$$

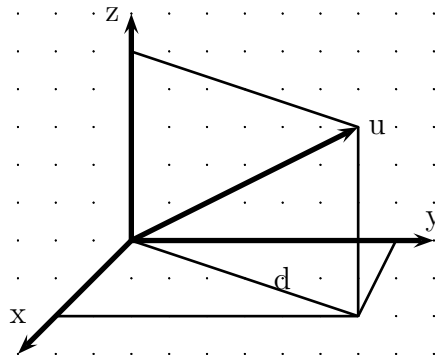


Abbildung 20: Norm eines Vektors u

Für einen beliebigen realen Faktor λ gilt: $\|\lambda u\| = |\lambda| \cdot \|u\|$

Denn:

$$\begin{aligned} \|\lambda u\| &= \sqrt{(\lambda u_1)^2 + \dots + (\lambda u_n)^2} = \sqrt{\lambda^2 \cdot (u_1^2 + \dots + u_n^2)} \\ &= \sqrt{\lambda^2} \cdot \sqrt{u_1^2 + \dots + u_n^2} = |\lambda| \cdot \|u\| \end{aligned}$$

Mit Hilfe des Abstands zweier Vektoren ist ihre Ähnlichkeit definiert. Der Abstand eines Vektors v zu einem Vektor w ist $-w + v = v - w$.

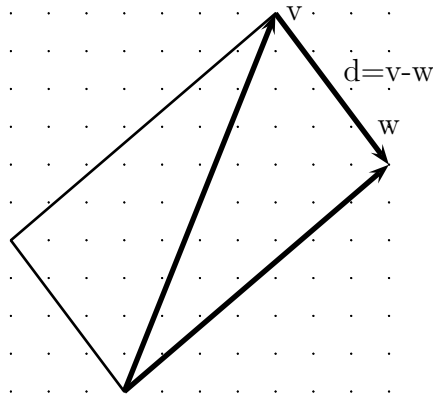


Abbildung 21: Abstand d zweier Vektoren

Tschüß!

Index

- Abstand, 22
- algebraische Vielfachheit, 20
- Automorphismen, 3

- Bahnen, 6
- BCH-Codes, 16

- Charakteristik eines Körpers, 14
- charakteristisches Polynom, 19

- Diagonalisierung, 19
- Diagonalmatrix, 21
- disjunkt, 8

- Ecken, 2
- Eigenvektoren, 18
- Eigenwerte, 18
- Einheit, 12
- Einheitswurzel, 14

- geometrische Vielfachheit, 20
- GF = Galois-Feld, 13
- Graph, 2

- Hintereinanderausführung, 4

- Index, 8
- Infimum, 18
- isomorph, 2, 3
- Isomorphismus, 3

- Körper, 11
- Kanten, 2
- kantenerhaltend, 3
- kantenreflektierend, 3
- Klassen
 - zyklotome, 15

- Norm, 21

- Orbits, 6

- Permutation, 4
- Polya-Theorie, 11

- Schieberegister, 13

- Supremum, 18

- Verbände, 18
- Vielfachheit
 - algebraische, 20
 - geometrische, 20
- vierdimensionaler Würfel, 18

- zyklotome Klassen, 15