Tutorium: Diskrete Mathematik

Vorbereitung der Klausur am 17.02.2020
(Teil 1)

12. Februar 2020

Steven Köhler

mathe@stevenkoehler.de

mathe.stevenkoehler.de

Polynome

Definition I

Ein *Polynom* ist ein Ausdruck der folgenden Form:

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0.$$

Ein Polynom lässt sich mit dem Summenzeichen auch wie folgt darstellen:

$$p(x) = \sum_{k=0}^{n} a_k x^k.$$

Als *Grad des Polynoms* bezeichnet man die höchste im Polynom vorkommende Potenz n.

Definition II

Beispiele:

- $a(x) = 2x^2 + 3x - 7$
- $b(x) = -x^3 + 4$
- $c(x) = x^{10} + x^8 - x^6 + 2x^5 + 10x^4 - x + 1$
- $d(x) = 1$

Definition III

Eine *Nullstelle* eines Polynoms p ist ein Wert x_0, für den gilt:

$$p(x_0) = 0.$$

Ein Polynom vom Grad n besitzt höchstens n reelle Nullstellen (und exakt n komplexe Nullstellen) – allerdings besitzt nicht jedes Polynom reelle Nullstellen. Ein Beispiel hierfür ist das folgende *irreduzible Polynom*:

$$x^2 + 1.$$

Hat ein Polynom einen ungeraden Grad, so besitzt es stets mindestens eine reelle Nullstelle.

Addition & Subtraktion von Polynomen I

Gegeben seien zwei Polynome $a(x)$ und $b(x)$ (mit $m, n \in \mathbb{N}$):

$$a(x) = \sum_{k=0}^{n} a_k x^k$$

$$b(x) = \sum_{k=0}^{m} b_k x^k$$

Die Summe $c(x)$ dieser beiden Polynome lässt sich wie folgt berechnen (nicht vorhandene Koeffizienten a_k bzw. b_k haben per Definition den Wert 0):

$$c(x) = a(x) + b(x) = \sum_{k=0}^{\max(m,n)} (a_k + b_k)\, x^k.$$

Addition & Subtraktion von Polynomen II

Gegeben seien zwei Polynome $a(x)$ und $b(x)$ (mit $m, n \in \mathbb{N}$):

$$a(x) = \sum_{k=0}^{n} a_k x^k$$

$$b(x) = \sum_{k=0}^{m} b_k x^k$$

Die Differenz $c(x)$ dieser beiden Polynome lässt sich wie folgt berechnen (nicht vorhandene Koeffizienten a_k bzw. b_k haben per Definition den Wert 0):

$$c(x) = a(x) - b(x) = \sum_{k=0}^{\max(m,n)} (a_k - b_k)\, x^k.$$

Addition & Subtraktion von Polynomen III

Beispiel:

Gegeben seien die beiden Polynome $a(x)$ und $b(x)$.

$$a(x) = x^3 + 2x^2 - 5x + 3$$
$$b(x) = x^2 + x - 1$$

Hieraus ergibt sich:

$$\begin{aligned} a(x) + b(x) &= x^3 + (2+1)x^2 + (-5+1)x + (3-1) \\ &= x^3 + 3x^2 - 4x + 2 \\ a(x) - b(x) &= x^3 + (2-1)x^2 + (-5-1)x + (3-(-1)) \\ &= x^3 + x^2 - 6x + 4 \end{aligned}$$

Multiplikation von Polynomen I

Gegeben seien zwei Polynome $a(x)$ und $b(x)$ (mit $m, n \in \mathbb{N}$):

$$a(x) = \sum_{k=0}^{n} a_k x^k$$

$$b(x) = \sum_{k=0}^{m} b_k x^k$$

Das Produkt dieser beiden Polynome lässt sich auf die folgenden Arten berechnen:

$$a(x) \cdot b(x) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i \cdot b_j \cdot x^{i+j} \qquad \text{bzw.}$$

$$a(x) \cdot b(x) = \sum_{i=0}^{m+n} \left(x^i \cdot \sum_{k=0}^{i} (a_k \cdot b_{i-k}) \right)$$

Multiplikation von Polynomen II

Beispiel:

Gegeben seien die beiden Polynome $a(x)$ und $b(x)$.

$$a(x) = x^3 + 2x^2 - 5x + 3$$
$$b(x) = x^2 + x - 1$$

Hieraus ergibt sich:

$$\begin{aligned} a(x) \cdot b(x) &= x^3 \cdot x^2 + x^3 \cdot x + x^3 \cdot (-1) \\ &\quad + 2x^2 \cdot x^2 + 2x^2 \cdot x + 2x^2 \cdot (-1) \\ &\quad - 5x \cdot x^2 - 5x \cdot x - 5x \cdot (-1) \\ &\quad + 3x^2 + 3x + 3 \cdot (-1) \\ &= x^5 + 3x^4 - 4x^3 - 4x^2 + 8x - 3 \end{aligned}$$

Division von Polynomen I

Zu je zwei Polynomen $a(x)$ und $b(x)$ mit $b(x) \neq 0$ gibt es eindeutig bestimmte Polynome $q(x)$ und $r(x)$ mit $\operatorname{grad}(r(x)) < \operatorname{grad}(b(x))$ oder $r(x) = 0$, so dass

$$a(x) = q(x)b(x) + r(x)$$

gilt. Man nennt dies eine *Zerlegung mit Rest* von $a(x)$ bezüglich $b(x)$.

Division von Polynomen II

Beispiel:

Gegeben seien die beiden Polynome $a(x)$ und $b(x)$.

$$a(x) = 2x^4 + x^3 + x + 3$$
$$b(x) = x^2 + x - 1$$

Es folgt:

$$\begin{array}{rllll|l}
 & (2x^4 & +x^3 & & +x \quad +3) & : (x^2 + x - 1) = 2x^2 - x + 3 \\
- & (2x^4 & +2x^3 & -2x^2) & & \\
\hline
 & & -x^3 & +2x^2 & +x \quad +3 & \\
 & - & (-x^3 & -x^2 & +x) & \\
\hline
 & & & 3x^2 & \quad +3 & \\
 & & - & (3x^2 & +3x \quad -3) & \\
\hline
 & & & & -3x \quad +6 &
\end{array}$$

Division von Polynomen III

Als Ergebnis erhält man die folgende Zerlegung mit Rest:

$$\underbrace{2x^4 + x^3 + x + 3}_{a(x)} = \underbrace{(2x^2 - x + 3)}_{q(x)}\underbrace{(x^2 + x - 1)}_{b(x)} + \underbrace{(-3x + 6)}_{r(x)}.$$

Das Ergebnis lässt sich auch wie folgt schreiben:

$$\frac{2x^4 + x^3 + x + 3}{x^2 + x - 1} = 2x^2 - x + 3 + \frac{-3x + 6}{x^2 + x - 1}.$$

Aufgabe 1

Es seien die folgenden beiden Polynome gegeben:

$$\begin{aligned} a(x) &= x^9 + 2x^7 - 3x^6 + 2x^4 - x^3 + 5x^2 + x - 23 \\ b(x) &= x^{10} - 5x^9 + 2x^6 - 3x^5 - 4x^4 + 2x^3 - x + 42. \end{aligned}$$

a) Bestimme den Grad des Polynoms $a(x) \cdot b(x)$.

b) Welchen Koeffizienten besitzt x^{13} im Produkt $a(x) \cdot b(x)$?

Aufgabe 2

Gegeben seien die beiden folgenden Polynome aus $\mathbb{Z}_5[x]$:

$$a(x) = 2x^6 + 4x^5 + 3x^4 + 4x^3 + x^2 + 1$$
$$b(x) = 4x^2 + 4.$$

Bestimme den Quotienten $a(x) : b(x)$.

Aufgabe 3

Gegeben seien die beiden folgenden Polynome aus $\mathbb{Q}[x]$:

$$a(x) = 2x^3 + 2x^2 + x + 1$$
$$b(x) = x^2 + 2x + 1.$$

Bestimme den normierten größten gemeinsamen Teiler von $a(x)$ und $b(x)$.

RSA

Beschreibung des RSA-Verfahrens I

Zum Erzeugen des öffentlichen und des privaten Schlüssels werden die folgenden Schritte ausgeführt:

1. Auswahl von zwei verschiedenen Primzahlen p und q.
2. Bestimmen des RSA-Moduls $N = p \cdot q$.
3. Berechnen des Werts $\varphi(N) = (p-1) \cdot (q-1)$.
4. Auswahl einer zu $\varphi(N)$ teilerfremden Zahl e mit $1 < e < \varphi(N)$.
5. Berechnen des Werts d mit $1 < d < \varphi(N)$, so dass gilt:

$$e \cdot d \equiv 1 \pmod{\varphi(N)}.$$

Man erhält den *öffentlichen Schlüssel* (e, N) sowie den *privaten Schlüssel* (d, N).

Beschreibung des RSA-Verfahrens II

Beim *Verschlüsseln* einer Nachricht m (mit $1 \leq m < N$) kann die verschlüsselte Nachricht c (mit $1 \leq c < N$) wie folgt berechnet werden:

$$m^e \equiv c \pmod{N}.$$

Beim *Entschlüsseln* einer verschlüsselten Nachricht c kann die ursprüngliche Nachricht m wie folgt berechnet werden:

$$c^d \equiv m \pmod{N}.$$

Aufgabe 4

Es seien der öffentliche RSA-Schlüssel $(23, 247)$ sowie die verschlüsselte Nachricht $c = 42$ gegeben. Wie lautet die unverschlüsselte Nachricht m?

Algebraische Strukturen

Algebraische Strukturen I

Eine *algebraische Struktur* (oder *Algebra*) ist ein Paar

$$\Big(A, (f_i)\Big),$$

bestehend aus einer nichtleeren Menge A, der *Trägermenge* der Algebra, und einer Familie (Menge) von (endlichstelligen) Verknüpfungen auf A, die auch *fundamentale Operationen* genannt werden.

Meistens hat eine Algebra nur endlich viele Verknüpfungen $f_1, \ldots, f_n$; man schreibt dann für die Algebra einfach nur

$$\Big(A, f_1, \ldots, f_n\Big).$$

Algebraische Strukturen II

Die Trägermenge A der Algebra ist *abgeschlossen* bezüglich der definierten Operationen, d.h., die Verknüpfung von zwei Elementen $a, b \in A$ (im Fall einer binären Verknüpfung) liefert stets ein Element $c \in A$. a, b und c müssen dabei nicht notwendigerweise verschieden sein.

Halbgruppen I

Eine *Halbgruppe* ist eine algebraische Struktur

$$\mathcal{H} = \left(H, \star\right)$$

mit der Trägermenge H und einer zweistelligen Verknüpfung $\star$.

Für die Verknüpfung $\star$ gilt das Assoziativgesetz, d.h., für alle $a, b, c \in H$ gilt stets

$$a \star (b \star c) = (a \star b) \star c.$$

Halbgruppen II

Häufig wird für die Verknüpfung $\star$ das Symbol $\cdot$ benutzt, man spricht dann von einer *multiplikativ geschriebenen Halbgruppe*. Wie auch bei der gewöhnlichen Multiplikation, kann in vielen Situationen der Malpunkt weggelassen werden.

Eine Halbgruppe lässt sich auch *additiv* notieren, indem für die Verknüpfung $\star$ das Symbol $+$ benutzt wird.

Halbgruppen III

Da das Assoziativgesetz gilt, kann eine vereinfachte, klammerfreie Notation verwendet werden:

$$a \star (b \star c) = (a \star b) \star c = a \star b \star c.$$

Monoide I

Ein *Monoid* ist eine algebraische Struktur

$$\mathcal{M} = \left(M, \star\right)$$

mit der Trägermenge M und einer zweistelligen Verknüpfung $\star$.

Ein Monoid ist eine Halbgruppe mit einem *neutralen Element* e.

Monoide II

Für Monoide gelten also die folgenden Eigenschaften:

- Für die Verknüpfung $\star$ gilt das Assoziativgesetz:

$$\forall a, b, c \in M : a \star (b \star c) = (a \star b) \star c = a \star b \star c.$$

- Es existiert ein neutrales Element e, für das gilt:

$$\forall a \in M : e \star a = a \star e = a.$$

Das Element e ist also sowohl links- als auch rechtsneutral bzgl. der definierten Operation $\star$.

Gruppen I

Eine *Gruppe* ist eine algebraische Struktur

$$\mathcal{G} = \left(G, \star\right)$$

mit der Trägermenge G und einer zweistelligen Verknüpfung $\star$.

Eine Gruppe ist ein Monoid, in dem für jedes Element $a \in G$ das zugehörige *inverse Element* a^{-1} in G enthalten ist.

Gruppen II

Für Gruppen gelten also die folgenden Eigenschaften:

- Für die Verknüpfung $\star$ gilt das Assoziativgesetz:

$$\forall a, b, c \in G : a \star (b \star c) = (a \star b) \star c = a \star b \star c.$$

- Es existiert ein neutrales Element e, für das gilt:

$$\forall a \in G : e \star a = a \star e = a.$$

- Existenz inverser Elemente:

$$\forall a \in G : \exists a^{-1} \in G \text{ mit } a \star a^{-1} = a^{-1} \star a = e.$$

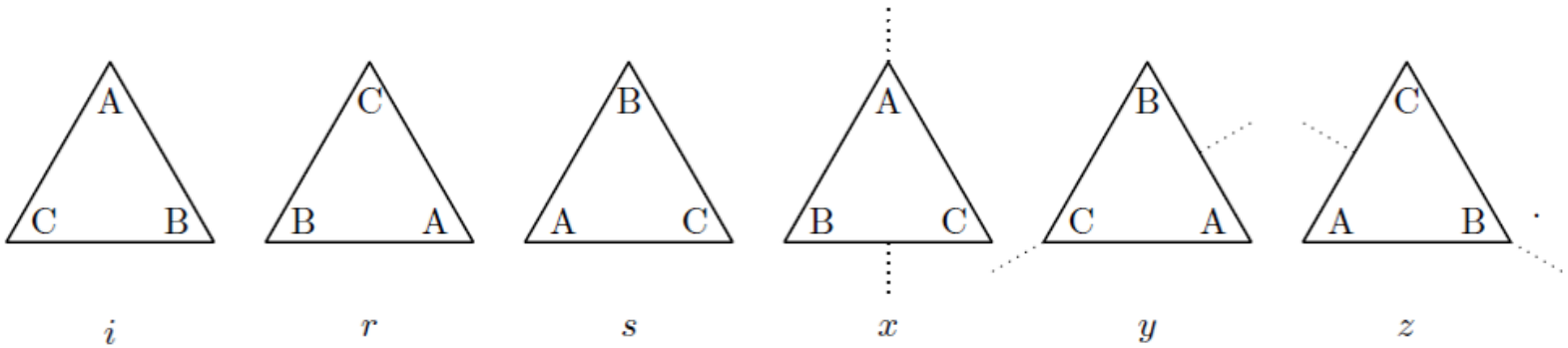
Gruppen III

Beispiele für Gruppen

- $\left(\mathbb{Z}, +\right)$
- $\left(\mathbb{Q} \setminus \{0\}, \cdot\right)$
- $\left(\mathbb{R}, +\right)$
- Kleinsche Vierergruppe
- Dreiecksgruppe

Die Dreiecksgruppe I

Die Dreiecksgruppe G_Δ ist eine Gruppe, die die folgenden Elemente enthält:



i, r und s sind dabei Drehungen um $0°$, $120°$ bzw. $240°$. x, y und z sind Spiegelungen an den Winkelhalbierenden des Dreiecks.

Die Dreiecksgruppe II

Diese Gruppe besitzt die folgende *Gruppentafel*, in der die Ergebnisse der Veknüpfung der Elemente tabellarisch notiert sind:

$\circ$	i	r	s	x	y	z
i	i	r	s	x	y	z
r	r	s	i	y	z	x
s	s	i	r	z	x	y
x	x	z	y	i	s	r
y	y	x	z	r	i	s
z	z	y	x	s	r	i

Die Ordnung einer Gruppe

Die Mächtigkeit (Kardinalität) $|G|$ der Trägermenge der Gruppe nennt man die *Ordnung der Gruppe* oder auch die *Gruppenordnung*.

Für endliche Mengen G ist dies einfach die Anzahl der Elemente in G.

Die Ordnung eines Gruppenelements

Unter der *Ordnung eines Elements* $a \in G$ einer Gruppe $\mathcal{G} = (G, \star)$ versteht man die kleinste natürliche Zahl $m > 0$, für die $a^m = e$ gilt; e ist dabei das neutrale Element der Gruppe.

Gibt es keine derartige Zahl m, so hat a *unendliche Ordnung*.

Man definiert die Potenzen eines Gruppenelements wie folgt:

$$a^0 := e$$
$$a^{n+1} := a^n \star a.$$

Untergruppen I

Ist U eine Teilmenge der Trägermenge G einer Gruppe $\mathcal{G} = (G, \star)$ (also $U \subseteq G$) und ist $\mathcal{U} = (U, \star)$ selbst eine Gruppe, so nennt man $\mathcal{U}$ eine Untergruppe von $\mathcal{G}$.

Um zu zeigen, dass $\mathcal{U}$ eine Untergruppe von $\mathcal{G}$ ist, genügt es zu zeigen, dass Folgendes gilt:

- $U \neq \emptyset$
- $a, b \in U \Rightarrow a \star b, b \star a \in U$;
- $a \in U \Rightarrow a^{-1} \in U$.

Untergruppen II

Jedes Element $a \in G$ einer endlichen Gruppe $\mathcal{G}$ erzeugt eine Untergruppe $\mathcal{H}$.

Die durch $a \in G$ erzeugte Untergruppe wird mit $< a >$ bezeichnet.

Aufgabe 5

Gegeben seien die beiden Gruppen $\mathcal{G} = (G, \star)$ und $\mathcal{H} = (H, \star)$. Zeige, dass $(G \cap H, \star)$ sowohl eine Untergruppe von $\mathcal{G}$ als auch von $\mathcal{H}$ ist.

Der Satz von Lagrange

Der *Satz von Lagrange* wurde nach dem italienischen Mathematiker Joseph-Louis Lagrange benannt.

Der Satz besagt, dass die Mächtigkeit (oder Ordnung) einer Untergruppe stets die Mächtigkeit der Gruppe teilt.

Es sei $\mathcal{G}$ eine endliche Gruppe:

- Ist $\mathcal{H}$ eine Untergruppe von $\mathcal{G}$, so ist die Mächtigkeit $|H|$ ein Teiler von $|G|$.
- Insbesondere teilt die Ordnung eines Elements $a \in G$ die Mächtigkeit $|G|$ von G.

Aufgabe 6

Gegeben seien die beiden Gruppen $\mathcal{G} = (G, \star)$ und $\mathcal{H} = (H, \star)$. Es gelte $|G| = 48$ und $|H| = 56$. Zudem gelte $|G \cap H| \geq 2$. Zeige, dass in $(G \cap H, \star)$ stets ein Element der Ordnung 2 existiert.

Die symmetrische Gruppe

Als *symmetrische Gruppe* bezeichnet man die Gruppe S_n aller möglichen Permutationen über n Elementen.

Die Operation der Gruppe ist die Nacheinanderausführung $\circ$ von Permutationen.

Da es $n!$ verschiedene Permutationen über n Elementen gibt, gilt

$$|S_n| = n!$$

Permutationsgruppen

Als *Permutationsgruppe* bezeichnet man eine Untergruppe einer symmetrischen Gruppe S_n.

Isomorphie von Gruppen

Zwei Gruppen heißen *isomorph* oder *strukturgleich*, wenn es zwischen ihren Elementen eine strukturerhaltende, bijektive Abbildung gibt, d.h., wenn ihre Gruppentafeln bis auf die Bezeichnungen der Elemente übereinstimmen.

Eine wichtige Voraussetzung für Isomorphie ist, dass die Gruppen gleich viele Elemente einer jeweiligen Ordnung besitzen.

Zyklische Gruppen derselben Ordnung sind stets isomorph.

Aufgabe 7

Zeige, dass die folgenden beiden Gruppen der Ordnung 4 isomorph sind:

$(G, \star)$:

	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

$(H, \circ)$:

	1	$\diamondsuit$	$\square$	$\triangle$
1	1	$\diamondsuit$	$\square$	$\triangle$
$\diamondsuit$	$\diamondsuit$	$\triangle$	1	$\square$
$\square$	$\square$	1	$\triangle$	$\diamondsuit$
$\triangle$	$\triangle$	$\square$	$\diamondsuit$	1

Zyklische Gruppen

Eine Gruppe $\mathcal{G} = (G, \star)$ heißt *zyklisch*, wenn sie mindestens ein Element enthält, aus dem sämtliche Elemente der Gruppe erzeugt werden können.

Mit anderen Worten: In G muss mindestens ein Element der Ordnung $|G|$ existieren.

Zyklische Gruppen sind stets kommutativ; kommutative Gruppen aber nicht stets zyklisch.

Abelsche Gruppen

Eine Gruppe $\mathcal{G} = (G, \star)$ heißt *abelsch* oder *kommutativ*, wenn zusätzlich zu den bisher genannten Gruppeneigenschaften das Kommutativgesetz gilt, d.h.:

$$\forall a, b \in G : a \star b = b \star a.$$

Nebenklassen

Es sei $\mathcal{H}$ eine Untergruppe einer Gruppe $\mathcal{G}$ und a sei ein Element von G. Mithilfe von a und $\mathcal{H}$ definieren wir eine Teilmenge von $\mathcal{G}$ wie folgt:

$$a\mathcal{H} := \Big\{ g \in G : \text{ Es gibt ein } h \in H \text{ mit } g = a \star h \Big\}.$$

Man nennt eine solche Teilmenge $a\mathcal{H}$ eine *Linksnebenklasse* von $\mathcal{H}$ in $\mathcal{G}$.

Analog werden die *Rechtsnebenklassen* $\mathcal{H}a$ definiert.

Aufgabe 8

Es sei $\mathcal{G}$ die symmetrische Gruppe S_3 und $\mathcal{H}$ die durch den Zyklus (123) erzeugte Untergruppe von $\mathcal{G}$. Bestimme die Links- und die Rechtsnebenklassen von $\mathcal{H}$.

Ringe I

Ein *Ring* ist eine algebraische Struktur

$$\mathcal{R} = \left(R, +, \cdot\right)$$

mit der Trägermenge R und zwei zweistelligen Verknüpfungen $+$ und $\cdot$.

Ringe II

In einem Ring gelten die folgenden Eigenschaften:

- Bezüglich der Operation $+$ bildet $(R, +)$ eine kommutative Gruppe.
- Bezüglich der Operation $\cdot$ bildet $(R, \cdot)$ ein Monoid.
- Es gelten die Distributivgesetze:

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

Die Einheitengruppe

Als *Einheitengruppe* $E(\mathcal{R})$ eines Rings $\mathcal{R}$ bezeichnet man die Menge derjenigen Elemente, die im Ring $\mathcal{R}$ ein multiplikatives Inverses besitzen.

Aufgabe 9

a) Berechne die Ordnung der Einheitengruppe $E(\mathbb{Z}_{42})$ des Rings $(\mathbb{Z}_{42}, +, \cdot)$ mithilfe der Siebformel.

b) Berechne die Ordnung der Einheitengruppe $E(\mathbb{Z}_{42})$ des Rings $(\mathbb{Z}_{42}, +, \cdot)$ mithilfe der Eulersche φ-Funktion.

c) Gib die Elemente von $E(\mathbb{Z}_{42})$ an.

d) Ist $E(\mathbb{Z}_{42})$ zyklisch?

Körper I

Ein *Körper* ist eine algebraische Struktur

$$\mathcal{K} = \left(K, +, \cdot\right)$$

mit der Trägermenge K und zwei zweistelligen Verknüpfungen $+$ und $\cdot$.

Körper II

In einem Körper gelten die folgenden Eigenschaften:

- Bezüglich der Operation $+$ bildet $(K, +)$ eine kommutative Gruppe.
- Bezüglich der Operation $\cdot$ bildet $(K \setminus \{e_+\}, \cdot)$ eine kommutative Gruppe.
- Es gelten die Distributivgesetze:

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

Körper III

Beispiele für Körper

- $(\mathbb{Q}, +, \cdot)$
- $(\mathbb{R}, +, \cdot)$
- $(\mathbb{C}, +, \cdot)$
- der *Galoiskörper* GF_2 (oder auch $\mathbb{F}_2$)

Permutationen

Aufgabe 10a-d

Eine Permutation $\pi \in S_9$ sei wie folgt definiert:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & 5 & 7 & 4 & 6 & 9 & 8 \end{pmatrix}.$$

a) Gib π in Zyklenschreibweise an.

b) Gib π als Nacheinanderausführung von Transpositionen an.

c) Ist π eine gerade oder eine ungerade Permutation?

d) Bestimme $\operatorname{sign} \pi$.

Aufgabe 10e-f

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & 5 & 7 & 4 & 6 & 9 & 8 \end{pmatrix}$$

e) Entscheide, ob durch die folgende Permutation $\rho \in S_9$ dieselbe Permutation wie durch π beschrieben wird:

$$\rho = (12)(23)(13)(42)(98)(46)(12)(16)(21)(25)(83)(39)(98).$$

f) Entscheide, ob durch π und φ dieselbe Permutation beschrieben ist:

$$\pi = (12)(34)(13)(24)(14)(23)$$
$$\varphi = (13)(24)(12)(24)(13)(23).$$