Tutorium:
Diskrete Mathematik

Vorbereitung der Bonusklausur am 19.01.2023
(Teil 2)

12. Januar 2023

Steven Köhler

mathe@stevenkoehler.de

mathe.stevenkoehler.de

Kombinatorik

Additions- und Multiplikationsregel I

- *Additionsregel*: M sei eine endliche Menge und $M_1, \ldots, M_n$ seien disjunkte Teilmengen von M mit $M = M_1 \cup \ldots \cup M_n$. Dann gilt:

$$|M| = \sum_{i=1}^{n} |M_i|$$

- *Multiplikationsregel*: Seien $A_1, \ldots, A_n$ endliche Mengen. Dann gilt

$$|A_1 \times \ldots \times A_n| = |A_1| \cdot \ldots \cdot |A_n| = \prod_{i=1}^{n} |A_i|.$$

Permutationen

Unter einer *Permutation* versteht man eine bijektive Abbildung einer Menge auf sich selbst.

Fakultät und Faktorielle

- Mithilfe der *Fakultät* kann bspw. die Anzahl der *Permutationen* einer n-elementigen Menge bestimmt werden. Es gilt:

$$n! := n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1.$$

- Mithilfe der *k-ten Faktoriellen von n* kann die Anzahl der k-Tupel einer n-elementigen Menge berechnet werden, wobei kein Element doppelt vorkommen darf. Es gilt:

$$n^{\underline{k}} := \begin{cases} n \cdot (n-1) \cdot \ldots \cdot (n-k+1) & \text{, falls } k \geq 1 \\ 1 & \text{, sonst.} \end{cases}$$

Binomialkoeffizienten

Für die Binomialkoeffizienten gelten die folgenden Eigenschaften:

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} \qquad \text{(explizite Formel)}$$

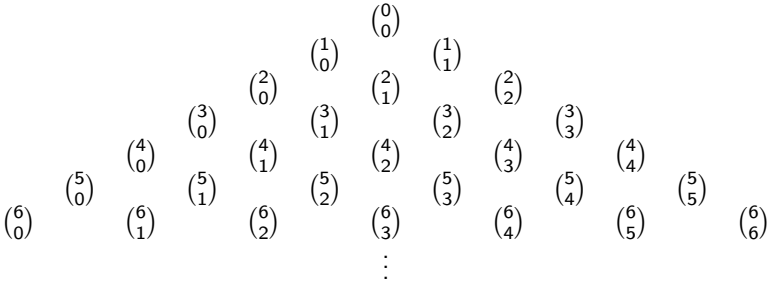
$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \qquad \text{(Rekursionsformel)}$$

$$\binom{n}{k} = \binom{n}{n-k} \qquad \text{(Symmetrie)}$$

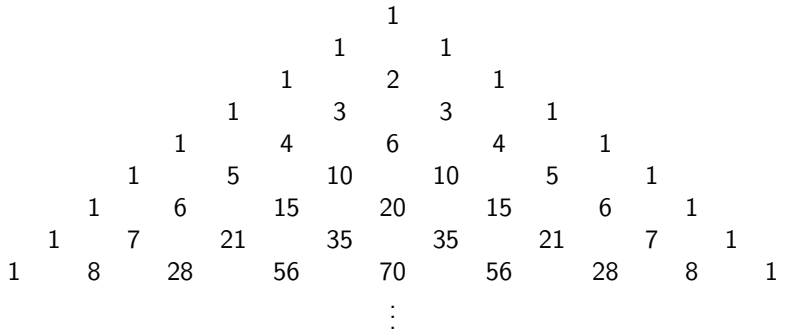
Insbesondere gilt:

$$\binom{n}{0} = \binom{n}{n} = 1$$

Pascalsches Dreieck I



Pascalsches Dreieck II



Binomischer Lehrsatz

Als Verallgemeinerung der ersten beiden binomischen Formeln ergibt sich der sogenannte *binomische Lehrsatz*:

$$\begin{aligned}(a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\ &= \binom{n}{0} a^0 b^n + \binom{n}{1} a^1 b^{n-1} + \ldots + \binom{n}{n} a^n b^0.\end{aligned}$$

Multinomialkoeffizienten

Gegeben seien r verschiedene Symbole $Z_1, \ldots, Z_r$ ($r \geq 1$), die in einer Zeichenfolge mit der Gesamtlänge n insgesamt $k_1, \ldots, k_r$ mal vorkommen. Es gilt also $n = \sum_{i=1}^{r} k_i$. Die Anzahl der verschiedenen Zeichenfolgen, die aus dem Symbolen $Z_1, \ldots, Z_r$ dargestellt werden können, kann mithilfe des *Multinomialkoeffizienten* berechnet werden. Es gilt

$$\binom{n}{k_1, \ldots, k_r} = \frac{n!}{k_1! \cdot \ldots \cdot k_r!}$$

Multinomialkoeffizienten können als Verallgemeinerung der Binomialkoeffizienten aufgefasst werden.

Multinomialsatz

Für $r \geq 2$ und $n \geq 0$ gilt

$$(x_1 + \ldots + x_r)^n = \sum_{k_1+\ldots+k_r=n} \binom{n}{k_1, \ldots, k_r} x_1^{k_1} \cdot \ldots \cdot x_r^{k_r},$$

wobei die Summe über alle r-Tupel $(k_1, \ldots, k_r)$ nichtnegativer ganzer Zahlen genommen wird, für die $k_1 + \ldots + k_r = n$ gilt.

Übersicht

Für das Ziehen von k Elementen aus einer n-elementigen Menge gelten die folgenden Formeln:

	mit Reihenfolge	ohne Reihenfolge
mit Zurücklegen	n^k	$\binom{k+n-1}{k}$
ohne Zurücklegen	$n^{\underline{k}}$	$\binom{n}{k}$

Aufgaben

Aufgabe 1

Es sei $L = \{a, b, c\}$, $M = \{1, 2, 3, 4, 5\}$ und $N = \{1, 2, \ldots, 15\}$. Mit $\mathcal{P}(L)$, $\mathcal{P}(M)$ und $\mathcal{P}(N)$ seien die Potenzmengen von L, M und N bezeichnet.

a) Wie viele Elemente besitzen $\mathcal{P}(M)$ und $\mathcal{P}(N)$?

b) Gib alle Elemente von $\mathcal{P}(L)$ an.

c) Wie viele 5-elementige Teilmengen besitzt N?

d) Wie viele Abbildungen $f : L \to M$ gibt es und wie viele davon sind injektiv?

e) Wie viele Abbildungen $f : L \to M$ sind surjektiv?

Aufgaben

Aufgabe 2

a) Gegeben seien zwei Mengen A und B mit $|A| = 17$ und $|B| = 5$. Wie viele Abbildungen $f : A \to B$ gibt es, für die paarweise verschiedene Elemente $a_1, a_2, a_3, a_4 \in A$ mit $f(a_1) = f(a_2) = f(a_3) = f(a_4)$ existieren?

b) Wie viele binäre Relationen, die symmetrisch und reflexiv sind, gibt es über einer 5-elementigen Menge?

c) Eine Zeile im Pascalschen Dreieck lautet:

$$1 \quad 8 \quad 28 \quad 56 \quad 70 \quad 56 \quad 28 \quad 8 \quad 1$$

Berechne die nächste Zeile!

d) Es sei $n = 10.000$. Berechne $\binom{n}{2} + \binom{n}{9.998}$.

Aufgaben

Aufgabe 3

a) Wie viele sinnvolle oder nicht sinnvolle Wörter lassen sich aus den Buchstaben von Rhabarberbarbarabarbarbarenbartbarbierbier bilden?

b) Wie lautet der Koeffizient von x^5y^8 in $(x+y)^{13}$?

c) Wie lautet der Koeffizient von $x^3y^5z^7$ in $(x+y+z)^{15}$?

d) Wie viele Möglichkeiten gibt es, im Lotto höchstens 2 richtige Gewinnzahlen anzukreuzen?

e) Wie viele Möglichkeiten gibt es, eine Getränkekiste mit 19 Flaschen zusammenzustellen, wenn 5 verschiedene Getränkesorten (in ausreichender Menge) zur Verfügung stehen, die beliebig gemixt werden können?

Aufgaben

Aufgabe 4

Die Funktion $f : \mathbb{N} \to \mathbb{Z}$ sei gegeben durch

$$f(n) = \binom{n+5}{5} + \binom{n+5}{6} - \binom{n+6}{n}.$$

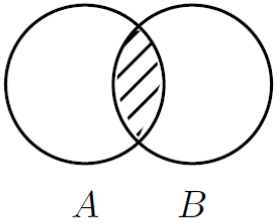
Begründe (kurz), wieso f nicht injektiv ist.

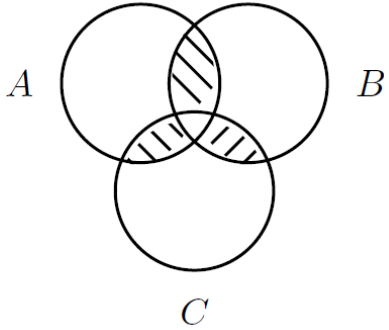
Das Prinzip der Inklusion und Exklusion (Siebformel) I

Mithilfe der *Siebformel* kann die Anzahl der Elemente

$$|A_1 \cup \ldots \cup A_n|$$

in der Vereinigung von n nicht-disjunkten Mengen $A_1, \ldots, A_n$ bestimmt werden.





Das Prinzip der Inklusion und Exklusion (Siebformel) II

Für endliche Mengen $A_1, \ldots, A_n$ gilt:

$$|A_1 \cup \ldots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{1 \leq i_1 < \ldots < i_r \leq n} |A_{i_1} \cap \ldots \cap A_{i_r}|.$$

Das Prinzip der Inklusion und Exklusion (Siebformel) III

Aufgabe 5

Bestimme mithilfe der Siebformel die Anzahl der zu 30 teilerfremden Zahlen $n \in \mathbb{N}$ mit $1 \leq n \leq 30$.

Modulare Arithmetik

Definition

Gegeben seien zwei ganze Zahlen $a, b \in \mathbb{Z}$ sowie eine natürliche Zahl $m \in \mathbb{N}$. Man nennt a und b

- *kongruent modulo* m und schreibt $a \equiv b \pmod{m}$, falls $m \mid (a - b)$ gilt;
- *inkongruent modulo* m und schreibt $a \not\equiv b \pmod{m}$, falls $m \nmid (a - b)$ gilt.

Sind a und b kongruent modulo m, so lassen a und b bei Ganzzahldivision durch m folglich denselben Rest.

Rechnen mit Kongruenzen I

Es seien $a, b \in \mathbb{Z}$ zwei ganze Zahlen, für die die folgenden Zerlegungen mit Rest gegeben sind (für $m, q_a, q_b, r_a, r_b \in \mathbb{Z}$ mit $0 \leq r_a < m$ und $0 \leq r_b < m$):

$$a = q_a \cdot m + r_a$$
$$b = q_b \cdot m + r_b.$$

Dann gilt:

$$a + b \equiv r_a + r_b \pmod{m}$$
$$a - b \equiv r_a - r_b \pmod{m}$$
$$a \cdot b \equiv r_a \cdot r_b \pmod{m}$$
$$a^n \equiv r_a^n \pmod{m}$$

Rechnen mit Kongruenzen II

Aufgabe 6

Es seien $a, b \in \mathbb{Z}$ zwei ganze Zahlen, für die die folgenden Zerlegungen mit Rest gegeben sind (für $m, q_a, q_b, r_a, r_b \in \mathbb{Z}$ mit $0 \leq r_a < m$ und $0 \leq r_b < m$):

$$a = q_a \cdot m + r_a$$
$$b = q_b \cdot m + r_b.$$

Beweise die folgende Aussage:

$$a \cdot b \equiv r_a \cdot r_b \pmod{m}.$$

Restklassenring I

Wir betrachten die Kongruenzrelation $\equiv$ modulo m. Es handelt es sich um eine Äquivalenzrelation, bei deren Äquivalenzklassen es sich um die Restklassen $[0]_m$, $[1]_m$, …, $[m-1]_m$ handelt.

Man definiert die Menge $\mathbb{Z}_m$ (oder $\mathbb{Z}/m\mathbb{Z}$) als die Menge der Äquivalenzklassen der Kongruenzrelation modulo m:

$$\mathbb{Z}_m = \Big\{[0]_m, [1]_m, \ldots, [m-1]_m\Big\}.$$

Wenn klar ist, dass es sich um Elemente aus $\mathbb{Z}_m$ handelt, kann anstelle von $[0]_m$, $[1]_m$, …, $[m-1]_m$ stellvertretend auch einfach $0, 1, \ldots, m-1$ geschrieben werden.

Restklassenring II

Für alle $x, y \in \mathbb{Z}$ sind die Operationen $\oplus$ und $\odot$ wie folgt definiert:

$$[x]_m \oplus [y]_m = [x + y]_m$$
$$[x]_m \odot [y]_m = [x \cdot y]_m$$

Anstelle von $\oplus$ und $\odot$ wird oft auch nur $+$ und $\cdot$ geschrieben.

Es handelt sich bei $(\mathbb{Z}_m, \oplus, \odot)$ bzw. $(\mathbb{Z}_m, +, \cdot)$ um einen *kommutativen Ring*.

Für Primzahlen p handelt es sich bei $(\mathbb{Z}_p, \oplus, \odot)$ bzw. $(\mathbb{Z}_p, +, \cdot)$ um einen *Körper*.

Restklassenring III

Für beliebige $[a]_m, [b]_m, [c]_m \in \mathbb{Z}_m$ gilt:

(I) $[a]_m \oplus [b]_m = [b]_m \oplus [a]_m$

$[a]_m \odot [b]_m = [b]_m \odot [a]_m$

(II) $([a]_m \oplus [b]_m) \oplus [c]_m = [a]_m \oplus ([b]_m \oplus [c]_m)$

$([a]_m \odot [b]_m) \odot [c]_m = [a]_m \odot ([b]_m \odot [c]_m)$

(III) $[a]_m \oplus [0]_m = [a]_m$

$[a]_m \odot [1]_m = [a]_m$

(IV) $[a]_m \odot ([b]_m \oplus [c]_m) = ([a]_m \odot [b]_m) \oplus ([a]_m \odot [c]_m)$

(V) $[a]_m \oplus [-a]_m = [0]_m$

Restklassenring IV

Aufgabe 7

Zeige die nachfolgende Aussage mithilfe einer vollständigen Induktion!

$$[a]_m^n = [a^n]_m$$

Multiplikatives Inverses I

Es sei $[a]_m \in \mathbb{Z}_m$. Ein Element $[x]_m \in \mathbb{Z}_m$ heißt *multiplikatives Inverses* von $[a]_m$, falls gilt:

$$[a]_m \odot [x]_m = [1]_m.$$

Besitzt $[a]_m$ ein multiplikatives Inverses, so nennt man $[a]_m$ *invertierbar*.

Hinweis: Per Konvention wird für das multiplikative Inverse stets der kleinste, nichtnegative Vertreter der entsprechenden Restklasse angegeben.

Erweiterter Euklidischer Algorithmus

Zum Bestimmen des *multiplikativen Inversen* von $[a]_m$ in $\mathbb{Z}_m$ kann der *erweiterte Euklidische Algorithmus* verwendet werden.

- Bestimmen von $\mathrm{ggT}(a, m)$.
- Gilt $\mathrm{ggT}(a, m) \neq 1$, so existiert kein multiplikatives Inverses von $[a]_m$ in $\mathbb{Z}_m$.
- Gilt $\mathrm{ggT}(a, m) = 1$, so kann das multiplikatives Inverse durch *Rückwärtseinsetzen* bestimmt werden.

Square-and-Multiply-Verfahren

Das *Square-and-Multiply-Verfahren* ist eine sehr effiziente Methode zum Berechnen von natürlichen Potenzen, also von Ausdrücken der Form a^n mit natürlichen Exponenten n.

Es gilt

$$a^n = \begin{cases} \left(a^{\frac{n}{2}}\right)^2 & \text{, für gerade } n \\ a^{n-1} \cdot a & \text{, für ungerade } n. \end{cases}$$

Kleiner Satz von Fermat

Es sei p eine Primzahl und a sei eine ganze Zahl, für die $\text{ggT}(a, p) = 1$ gilt; a und p sind also teilerfremd. Dann gilt:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Eulersche φ-Funktion

Die *eulersche φ-Funktion* ist eine Funktion, die zu einer natürlichen Zahl n angibt, wie viele zu n teilerfremde natürliche Zahlen es gibt, die kleiner gleich n sind.

$$\varphi(n) = \left|\left\{a \in \mathbb{N} : 1 \leq a \leq n \wedge \mathrm{ggT}(a, n) = 1\right\}\right|$$

Berechnung der eulerschen φ-Funktion I

Da eine Primzahl p nur durch 1 und sich selbst teilbar ist, ist sie zu den Zahlen 1 bis $p-1$ teilerfremd. Da $p \geq 2$ gilt und somit p niemals zu sich selbst teilerfremd ist, gilt stets

$$\varphi(p) = p - 1.$$

Berechnung der eulerschen φ-Funktion II

Sind m und n zwei teilerfremde ganze Zahlen, so gilt:

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

Berechnung der eulerschen φ-Funktion III

Eine Potenz p^k einer Primzahl p besitzt als einzigen Primfaktor die Zahl p. Daher hat p^k nur mit Vielfachen von p einen von 1 verschiedenen gemeinsamen Teiler. Im Bereich $1, \ldots, p^k$ sind dies die Zahlen

$$1 \cdot p, 2 \cdot p, \ldots, p^{k-1} \cdot p.$$

Es gibt also insgesamt p^{k-1} Zahlen, die nicht teilerfremd zu p^k sind. Für die eulersche φ-Funktion gilt folglich:

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1} \cdot (p-1) = p^k \cdot \left(1 - \frac{1}{p}\right).$$

Berechnung der eulerschen φ-Funktion IV

Der Wert der eulerschen φ-Funktion lässt sich für jede natürliche Zahl n aus deren Primfaktorzerlegung berechnen. Hierbei sei

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}.$$

Dann gilt

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k}).$$

Berechnung der eulerschen φ-Funktion V

Aufgabe 4

Berechne den Wert $\varphi(30)$.

Satz von Euler

Es seien a und n zwei natürliche Zahlen mit $\text{ggT}(a, n) = 1$. Dann gilt

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Dieser Satz ist auch als *Satz von Euler-Fermat* bekannt.

Chinesischer Restsatz I

Gegeben sei das folgende System aus zwei Kongruenzen mit teilerfremden natürlichen Moduln m_1, m_2 und beliebigen ganzen Zahlen a_1, a_2.

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

Aufgrund der Teilerfremdheit der Werte m_1 und m_2 können ganze Zahlen s_1 und s_2 gefunden werden, sodass

$$s_1 \cdot m_1 + s_2 \cdot m_2 = 1$$

gilt; diese können beispielsweise mit dem erweiterten euklidischen Algorithmus berechnet werden. Mithilfe der Werte s_1 und s_2 kann die gesuchte Lösung der simultanen Kongruenz nun direkt berechnet werden; es gilt:

$$x = a_1 \cdot s_2 \cdot m_2 + a_2 \cdot s_1 \cdot m_1.$$

Chinesischer Restsatz II

In der abstrakten Algebra kann der chinesische Restsatz nun wie folgt formuliert werden: Für teilerfremde natürliche Zahlen $m_1, \ldots, m_n$ sowie die Zahl $M = m_1 \cdot \ldots \cdot m_n$ handelt es sich bei der Abbildung

$$\mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$$

$$[x]_M \mapsto \left([x]_{m_1}, \ldots, [x]_{m_n}\right)$$

des Restklassenrings $\mathbb{Z}_M$ auf den Ring $\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$ (das kartesische Produkt der Restklassenringe $\mathbb{Z}_{m_1}, \ldots, \mathbb{Z}_{m_n}$) um einen Ringisomorphismus, d. h. um eine strukturerhaltende, bijektive Abbildung zwischen den beiden Ringen.

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:

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

Aufgaben

Aufgabe 6

Gegeben seien die beiden Primzahlen $p = 13$ und $q = 5$. Bestimme den öffentlichen Schlüssel (e, N) sowie den privaten Schlüssel (d, N). Es gelte $e = 35$.

Aufgaben

Aufgabe 7

Es seien der private RSA-Schlüssel $(115, 161)$ sowie die verschlüsselte Nachricht $c = 28$ gegeben. Es sei bekannt, dass $161 = 7 \cdot 23$ gilt. Wie lautet die unverschlüsselte Nachricht m?

a) Berechne die unverschlüsselte Nachricht durch modulares Potenzieren.

b) Berechne die unverschlüsselte Nachricht mithilfe des chinesischen Restsatzes.

Aufgaben

Aufgabe 8

Seien (e, N) und (d, N) ein öffentlicher und der dazugehörige private RSA-Schlüssel. Zeige, dass es sich bei $m' \equiv c^d \pmod{N}$ tatsächlich um die unverschlüsselte Nachricht m handelt, wenn für die verschlüsselte Nachricht $c \equiv m^e \pmod{N}$ gilt.

Permutationen

Permutationen I

Aufgabe 9

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 $\operatorname{sign} \pi$.

e) Bestimme die Ordnung der Permutation π in S_9.

Permutationen II

Aufgabe 10

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:

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

Algebraische Strukturen

Aufgaben I

Aufgabe 11

Es seien a, b, c, d Elemente einer Gruppe $\mathcal{G}$.

a) Vereinfache den folgenden Ausdruck:

$$a\left(bdc^{-1}\right)^{-1}bd^{-1}a\left(b^{-1}d^{-1}a\right)^{-1}a^{-1}b^{-1}$$

b) Können weitere Vereinfachungen vorgenommen werden, wenn zusätzlich vorausgesetzt wird, dass $\mathcal{G}$ kommutativ ist?

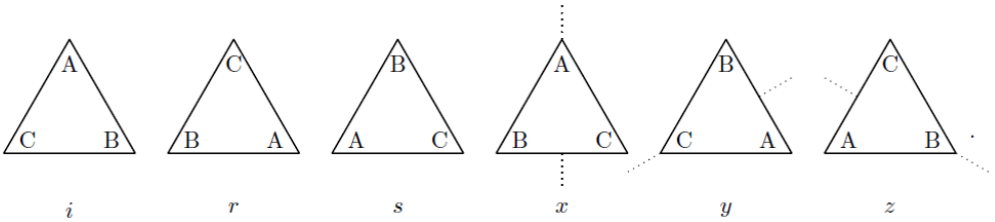
Aufgaben II

Aufgabe 12

Gegeben seien eine Gruppe $(G, \star)$ sowie zwei Untergruppen U_1 und U_2 von G. Zeige, dass es sich bei $U_1 \cap U_2$ ebenfalls um eine Untergruppe von G handelt.

Die Dreiecksgruppe

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.

Aufgaben III

Aufgabe 13

Entscheide, ob die Dreiecksgruppe isomorph zur symmetrischen Gruppe S_3 ist.

$\circ$	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

$\circ$	id	(12)	(13)	(23)	(123)	(132)
id	id	(12)	(13)	(23)	(123)	(132)
(12)	(12)	id	(132)	(123)	(23)	(13)
(13)	(13)	(123)	id	(132)	(12)	(23)
(23)	(23)	(132)	(123)	id	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	id
(132)	(132)	(23)	(12)	(13)	id	(123)

Aufgaben IV

Aufgabe 14

a) Berechne die Ordnung der Einheitengruppe $E(\mathbb{Z}_{30})$ des Rings $(\mathbb{Z}_{30}, +, \cdot)$ mithilfe der Siebformel.

b) Berechne die Ordnung der Einheitengruppe $E(\mathbb{Z}_{30})$ des Rings $(\mathbb{Z}_{30}, +, \cdot)$ mithilfe der Eulerschen φ-Funktion.

c) Gib die Elemente von $E(\mathbb{Z}_{30})$ an.

d) Ist $E(\mathbb{Z}_{30})$ zyklisch?