Formelsammlung zur Klausur
Grundlagen der Algebra und elementaren Zahlentheorie im Modul 4b

Satz 1.2.1
Schneiden sich zwei Geraden a und b im Punkt Z unter einem Zwischenwinkel $\angle(b,a)$ mit $|\angle(b,a)| = \alpha$, dann folgt: $s_b \circ s_a = d_{Z,2\alpha}$

Definition 1.3.1

- Eine **binäre, innere Verknüpfung** $\circ$ weist jeweils zwei Elementen x und y einer Menge M ein Element z aus derselben Menge M zu:
$$x \circ y = z$$
- Eine binäre Operation kann man auch als Funktion auf der Menge $M \times M$ aller Paare (x,y) mit x und y aus M auffassen.
$$\circ : M \times M \to M, (x,y) \mapsto \circ\,(x,y)$$
- Eine Menge M zusammen mit einer Operation $\circ$ bezeichnet man auch als **algebraische Struktur** $(M,\circ)$.

Eigenschaftskatalog

- Für jede Operation kann man fragen, welche Eigenschaften sie besitzt.
- Zu den *möglichen* Eigenschaften gehören die vom Operieren mit Zahlen vertrauten Eigenschaften.

Allgemeine Eigenschaften

- Kommutativität: $\forall_{a,b\in M}\ a \circ b = b \circ a$
- Assoziativität: $\forall_{a,b,c\in M}\ (a \circ b) \circ c = a \circ (b \circ c)$

Eigenschaften spezieller Elemente

- Neutrale Elemente: $\forall_{a\in M}\ a \circ id = a$
- Involutorische Elemente: $a \circ a = id$

Vereinfachende Schreibweisen

- $a \circ b \circ c = (a \circ b) \circ c = a \circ (b \circ c)$ wenn das Assoziativgesetz gilt
- $a^n := \underbrace{a \circ a \circ \cdots \circ a}_{n \text{ mal}}$

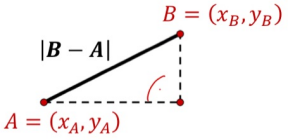
Bei mehreren Operationen

- Sind für eine Menge mehrere Operationen definiert, kann man *untersuchen, ob* diese Operationen auf bestimmte Weise miteinander verbunden sind.
- Distributivität: $\forall_{a,b,c\in M}\ (a * b) \circ c = (a \circ c) * (b \circ c)$
- Binomische Formel:
$$\forall_{a,b\in M}\ (a * b)^2 = (a * b) \circ (a * b) = a^2 * (a \circ b) * (b \circ a) * b^2$$

Definition 2.1.1

- Eine geometrische Figur F ist eine Menge von Punkten der Ebene $\mathbb{R}^2 = \{(x,y)|x,y \in \mathbb{R}\}$.
  Eine Figur F ist demnach eine Teilmenge der Ebene: $F \subseteq \mathbb{R}^2$
- Kongruenzabbildungen (Isometrien) der Ebene $\mathbb{R}^2$ auf sich, sind die Abbildungen φ, die die Abstände zwischen Punkten der Ebene und damit die Form aller Figuren nicht verändern.
  $Isom(\mathbb{R}^2) := \{\varphi: \mathbb{R}^2 \to \mathbb{R}^2 | \forall_{A,B\in\mathbb{R}^2} |\varphi(B) - \varphi(A)| = |B - A|\}$
- Eine Kongruenzabbildung φ, die eine Figur F mit sich selbst zur Deckung bringt, für die also gilt $\varphi(F) = F$, heißt **Deckabbildung** oder Symmetrieabbildung von F.
- Eine Figur heißt genau dann **symmetrisch**, wenn sie mindestens eine von der Identität verschiedene Deckabbildung besitzt.
- Die Menge $G_F = \{\varphi \in Isom(\mathbb{R}^2) | \varphi(F) = F\}$ aller Deckabbildungen einer Figur F wird als **Symmetrie der Figur F** bezeichnet.

Abstand
Abstand $|B - A|$ der Punkte A und B:
$|B - A| = \sqrt{(x_B - x_A)^2 + (y_B - y_A)^2}$



Definition 2.1.2: Gruppe

Eine Menge G zusammen mit einer binären Operation $\circ$ heißt **Gruppe** $(G,\circ)$, wenn die binäre Operation folgende Eigenschaften aufweist:

(G0)	$\forall_{a,b\in G}\ a \circ b \in G$	(Abgeschlossenheit)
(G1)	$\forall_{a,b,c\in G}\ a \circ (b \circ c) = (a \circ b) \circ c$	(Assoziativität)
(G2)	$\exists_{e\in G}\ \forall_{a\in G}\ a \circ e = e \circ a = a$	(Existenz eines neutralen Elements)
(G3)	$\forall_{a\in G}\ \exists_{a^{-1}\in G}\ a \circ a^{-1} = a^{-1} \circ a = e$	(Existenz inverser Elemente)

- **Bemerkung:** Bei regulären n-Ecken mit
  - geradzahligem n treten zwei Arten von Symmetrieachsen auf:
    - $\frac{n}{2}$ Symmetrieachsen durch gegenüberliegende Eckpunkte,
    - $\frac{n}{2}$ Symmetrieachsen durch gegenüberliegende Seitenmitten.
  - ungeradzahligem n gibt es nur eine Art von Symmetrieachsen:
    - Alle n Symmetrieachsen verlaufen durch einen Eckpunkt und die gegenüberliegende Seitenmitte.

Satz 2.1.1: Deckabbildungen des regulären n-Ecks mit Mittelpunkt M

Jedes reguläre n-Eck ist n-fach drehsymmetrisch und n-fach achsensymmetrisch. Es gibt genau n Deckdrehungen um M mit den Drehwinkeln $k \cdot \alpha = \frac{k}{n} \cdot 360°$, wobei $0 \leq k < n$ ist und genau n Deckspiegelungen, wobei der Schnittwinkel zwischen zwei Symmetrieachsen ein Vielfaches von $\frac{1}{n} \cdot 180°$ ist.

Satz 2.1.2: Verkettung von Drehungen um dasselbe Zentrum

Die Verkettung zweier Drehungen $d_{Z,\alpha}$ und $d_{Z,\beta}$ um dasselbe Zentrum Z ist eine Drehung um Z mit dem Drehwinkel $\alpha + \beta$.

Kurz: $d_{Z,\beta} \circ d_{Z,\alpha} = d_{Z,\alpha+\beta}$

Satz 2.1.3: Gruppe der Drehungen um ein festes Zentrum

Die Menge der Drehungen um ein festes Zentrum Z bildet bezüglich der Verkettung eine kommutative Gruppe.

Satz 2.1.4: Gruppe der Drehungen und Spiegelungen

Die Menge der Drehungen um ein festes Zentrum Z und aller Spiegelungen an Geraden durch Z bildet bezüglich der Verkettung eine *nicht*-kommutative Gruppe.

Definition 2.1.3

- Die Gruppe der Deckabbildungen eines regulären n-Ecks heißt Diedergruppe $\boldsymbol{D_n}$.
- Die zyklische Gruppe der Deckdrehungen eines regulären n-Ecks heißt zyklische Drehgruppe $\boldsymbol{Z_n}$.

Satz 2.1.5

- Die Diedergruppe D_n enthält $2n$ Elemente:
  - n Drehungen um Vielfache von $\frac{360°}{n}$ um den Mittelpunkt M des regulären n-Ecks, die man als $id, d, d^2, \dots, d^{n-1}$ schreiben kann.
  - n Spiegelungen $s_1, \dots, s_n$.
- Für Drehungen gilt: $d^i \circ d^k = d^{i+k}$ (bzw. $d^i \circ d^k = d^{i+k-n}$, falls $i + k \geq n$)
- Für Spiegelungen gilt: $(s_i)^2 = s_i \circ s_i = id$
- Die Diedergruppe D_n ist für $n \geq 3$ *nicht* kommutativ, denn $s_i \circ d \neq d \circ s_i$.

Satz 2.1.6: Symmetrische Figuren

Jede Figur mit endlichen vielen Symmetrien hat als Symmetriegruppe entweder eine zyklische Drehgruppe Z_n oder eine Diedergruppe D_n.

Bemerkung: Es gilt:

- $d^k s = s d^{n-k}$ $(*)$
- $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ $(**)$

Definition 2.2.1: Untergruppe

- Sei $(G,\circ)$ eine Gruppe. Wenn eine Teilmenge U der Menge G $(U \subseteq G)$ zusammen mit der Verknüpfung $\circ$ der Gruppe $(G,\circ)$ wieder eine Gruppe $(U,\circ)$ bildet, dann nennt man U eine **Untergruppe** von G und schreibt: $U \leq G$
- Das „$\leq$“-Zeichen statt des „$\subseteq$“ bedeutet, dass nicht nur die Mengen ineinander liegen, son-dern mit derselben Verknüpfung $\circ$ auch die Gruppenkriterien Abgeschlossenheit, Assoziati-vität, Existenz eines neutralen Elements und Existenz von inversen Elementen erfüllt sind.
- Die triviale Gruppe $E = \{id\}$ und die Gruppe G selbst, sind immer Untergruppen von G.
- Die Schnittmenge von zwei Untergruppe H und I einer Gruppe G ist Untergruppe beider Gruppen: $H \leq G \wedge I \leq G \Rightarrow H \cap I \leq H \wedge H \cap I \leq I$

Satz 2.2.1: Untergruppenkriterium

Ist U eine nichtleere Teilmenge der Gruppe $(G,\circ)$, gilt also $U \subseteq G$ und $U \neq \{\}$, dann ist U genau dann eine Untergruppe von G $(U \leq G)$, wenn gilt:

(UG1) $\forall_{a,b \in U}\ a \circ b \in U$ (Abgeschlossenheit)

(UG2) $\forall_{a \in U}\ a^{-1} \in U$ (Inverse in U enthalten)

Definition 2.2.2: Erzeugendensystem und erzeugte Untergruppe

- Zu einer Teilmenge $A \subseteq G$ einer *endlichen* Gruppe $(G,\circ)$ entstehen durch Bildung von Inversen und Verknüpfung von Elementen neue Mengen.
- $A_0 = A$, man geht also von der ursprünglichen Teilmenge $A \subseteq G$ aus.
- Im n-ten Schritt bildet man alle Inversen und Verknüpfungen der Elemente aus A_{n-1} und erhält

$$A_n = A_{n-1} \cup (A_{n-1})^{-1} \cup A_{n-1} \circ A_{n-1}$$
$$= A_{n-1} \cup \{a^{-1} | a \in A_{n-1}\} \cup \{a \circ b | a, b \in A_{n-1}\}.$$

- Der Prozess endet, wenn in einem Schritt m keine neuen Elemente hinzukommen, also gilt $A_m = A_{m-1}$.
- Die Menge $\langle A \rangle = A_m$ heißt die vom **Erzeugendensystem A erzeugte Untergruppe** $(\langle A \rangle,\circ)$.

Definition 3.1.0: Kongruenzrelation

- Seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}\backslash\{0\}$ und $r \in \mathbb{N}$ mit $0 \leq r < m$.
- Wenn a und b bei Division durch m denselben Rest r lassen, dann ist ***a* kongruent *b* modulo *m***.
- Man schreibt dann: $a \equiv b \bmod m$
- Hinweis: a und b lassen bei Division durch m genau dann denselben Rest r, wenn es Zahlen $p, q \in \mathbb{Z}$ gibt, für die gilt $a = p \cdot m + r$ und $b = q \cdot m + r$.

Satz 3.1.1: Kongruenzrelation

- Seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}\backslash\{0\}$.
- Es gilt $a \equiv b \bmod m$ genau dann, wenn $m|(a-b)$, also m Teiler von $a - b$ ist.

Definition 3.1.1: Restklassen von $\mathbb{Z}$ modulo n

- Die Menge der ganzen Zahlen $\mathbb{Z}$ lässt sich für ein gegebenes $n \in \mathbb{N}$ in disjunkte Klassen (also Mengen ohne gemeinsame Schnittmengen), sogenannte **Restklassen**, unterteilen:

$$\mathbb{Z} = n\mathbb{Z} \cup (1 + n\mathbb{Z}) \cup \cdots \cup \big((n-1) + n\mathbb{Z}\big)$$

- Diese **Restklassen** (es handelt sich um Mengen) kann man als neue Objekte $[a]_n := a + n\mathbb{Z}$ eines Zahlenraums auffassen:

$$\mathbb{Z}_n := \{[0]_n, [1]_n, \ldots, [n-1]_n\}$$

- Auf diesem Zahlenraum wird eine Addition und eine Multiplikation wie folgt definiert:

$$[a]_n + [b]_n := [a+b]_n, \quad \text{d. h.} \quad (a + n\mathbb{Z}) + (b + n\mathbb{Z}) := (a+b) + n\mathbb{Z}$$

$$[a]_n \cdot [b]_n := [a \cdot b]_n, \quad \text{d. h.} \quad (a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) := (a \cdot b) + n\mathbb{Z}$$

- Damit entstehen Zahlenräume $\mathbb{Z}_n$, die – wie bei den ganzen Zahlen $\mathbb{Z}$ – *zwei* Operationen erlauben, nämlich die Addition $+$ und die Multiplikation $\cdot$. Die zugehörige algebraische Struktur $(\mathbb{Z}_n, +, \cdot)$ auf dem jeweiligen Zahlenraum $\mathbb{Z}_n$ heißt **Restklassenring**.

Definition 3.2.2: Nullteiler

$(R, +, \cdot)$ ist ein Ring und 0 ist das neutrale Element der Addition in diesem Ring.

Wenn für zwei Elemente $a, b \in R$ gilt $a \cdot b = 0$ sowie $a \neq 0$ und $b \neq 0$, dann heißen a und b **Nullteiler.**

Satz 3.2.2: $\forall_{p \in \mathbb{P}} \left(\mathbb{Z}_p \setminus \{[0]_p\}, \cdot\right)$ ist eine Gruppe.

Satz 3.2.3: Wenn eine Zahl m mit $0 < m < n$ einen gemeinsamen Teiler mit n besitzt $(\mathrm{ggT}(m,n) > 1)$, dann ist $[m]_n$ ein Nullteiler in $\mathbb{Z}_n$.

Satz 3.2.4: Wenn man aus $\mathbb{Z}_n$ die $[0]_n$ und alle Nullteiler entfernt, bleiben nur invertierbare Elemente übrig. Die so entstehende Restmenge ist zusammen mit der Multiplikation $\cdot$ eine Gruppe.

Satz 3.2.5: Das Produkt $a \cdot b$ von invertierbaren Elementen a und b ist selbst invertierbar und es gilt: $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

Definition 3.2.3: Invertierbare Elemente

Seit $(M,\cdot)$ eine Menge mit einer Multiplikation $\cdot$, die eine 1, also ein neutrales Element bezüglich $\cdot$ enthält. Dann heißt $a \in M$ **invertierbar** in M, falls es ein $b \in M$ gibt mit $a \cdot b = 1 = b \cdot a$.

b heißt dann **invers** zu a bzw. **Inverses** von a.

Definition 3.2.4: Teilmenge der invertierbaren Elemente in $\mathbb{Z}_n$

- Die Teilmenge $\mathbb{Z}_n^*$ der invertierbaren Elemente in $\mathbb{Z}_n$ bildet eine multiplikative Gruppe, die mit $(\mathbb{Z}_n^*,\cdot)$ bezeichnet wird.
- $\mathbb{Z}_n^*$ besteht aus allen Elementen $[m]_n$ mit $m < n$ für die m und n teilerfremd sind:

$$\mathbb{Z}_n^* := \{a \in \mathbb{Z}_n | a \text{ invertierbar}\}$$
$$= \{[m]_n | \mathrm{m} < \mathrm{n} \wedge \mathrm{ggT}(m,n) = 1\}$$

Definition 3.3.1: Produktgruppe

- Zu zwei Gruppen $(G,\circ)$ und $(H,\circ)$ kann man eine Produktgruppe $(G \times H, \circ)$ mit elementweiser Verknüpfung von Paaren bilden:
  - $G \times H := \{(g,h) | g \in G, h \in H\}$
  - $(g_1,h_1) \circ (g_2,h_2) := (g_1 \circ g_2, h_1 \circ h_2)$
- Die Operationen können in jedem Faktor verschieden sein.
- Die Definition kann auf mehr als zwei Faktoren erweitert werden.
- Bei n gleichen Faktoren schreibt man auch:

$$G^n := \underbrace{G \times \cdots \times G}_{n \text{ Faktoren}}$$

Definition 3.3.2: Zahlenringe

- Durch Produktbildung mit $\mathbb{Z}$ und $\mathbb{Z}_n$ erhält man unendliche Zahlengitter

$$\mathbb{Z}^n := \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n \text{ Faktoren}}$$

- und endliche Restklassengitter, z. B.

$$\mathbb{Z}_k \times \mathbb{Z}_l \times \mathbb{Z}_m \text{ oder } (\mathbb{Z}_k)^n := \underbrace{\mathbb{Z}_k \times \cdots \times \mathbb{Z}_k}_{n \text{ Faktoren}}$$

- In diesen Mengen addiert und multipliziert man komponentenweise:
  - $(a,b) + (c,d) := (a + c, b + d)$
  - $(a,b) \cdot (c,d) := (a \cdot c, b \cdot d)$
- Beide Operationen sind assoziativ und kommutativ. Die Addition führt zu einer Gruppe, die Multiplikation hat ein neutrales Element.
- Man nennt diese Strukturen **Zahlenringe**.

▷ $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

ist gleichbedeutend mit $1 \to 2 \to 3$ und 4

ist gleichbedeutend mit $(123)(4)$

ist gleichbedeutend mit (123)

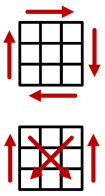
▷ Entstehung von Vierzykeln:

$(12) \circ (23) \circ (34) = (1234)$

$(13) \circ (23) \circ (24) = (1324)$

$= (12) \circ (23) \circ (12) \circ (23)$

$\circ (34) \circ (23) \circ (34)$



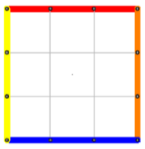
Definition 4.2.1: (Endliche) Symmetrische Gruppe $(S_n, \circ)$

Eine bijektive (also in beide Richtungen eindeutige) Abbildung zwischen einer Menge und sich selbst stellt eine „Umordnung" der Elemente dar und wird **Permutation** genannt. Die Menge aller Permutationen zur Zahlenmenge $\{1, 2, \dots, n\}$, nennt man auch **(endliche) Symmetrische Gruppe**.

$$S_n = \{\sigma: \{1, 2, \dots, n\} \to \{1, 2, \dots, n\} \mid \sigma \text{ bijektiv}\}$$

- Jede Symmetrische Gruppe bildet mit der Verkettung als Verknüpfung eine Gruppe $(S_n, \circ)$, die für $n > 2$ nicht kommutativ ist und $n!$ Elemente besitzt:
  $$|S_n| = n! := n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1$$
- Für das neutrale Element schreibt man (1).
- Zum schnelleren Vergleich legt man fest, dass jeder Zykel $(a_1 a_2 \dots a_n)$ stets mit der kleinsten Zahl beginnt.
- Das inverse Element zu $(a_1 a_2 \dots a_n)$ ist $(a_1 a_n \dots a_2)$.
- Die Permutation $(a_1 a_2)$ von genau zwei Elementen nennt man eine Transposition.

Bemerkung: Das Spiel aus Abschnitt 4.1 erzeugt die Symmetrische Gruppe S_4 mit



$S_4 = \{(1), (12), (13), (14), (23), (24), (34), (123), (124), (132), (134), (142), (143), (234), (243), (1234), (1243), (1324), (1342), (1423), (1432), (12)(34), (13)(24), (14)(23)\}$

Definition 4.2.2: Gerade und ungerade Permutationen

- In den Symmetrischen Gruppen kann man jede Permutation aus Transpositionen zusammensetzen, z.B. $(1234) = (12) \circ (23) \circ (34)$.
- Es gibt ggf. mehrere und unterschiedlich lange Möglichkeiten, eine Permutation durch eine Verkettung aus Transpositionen zu erzeugen.
- Unabhängig von der konkreten Zusammensetzung aus Transpositionen gehört jede Permutation zu einem der beiden folgenden Typen:
  - **Gerade Permutation**
    - Jede Darstellung ergibt sich aus einer **geraden Anzahl** von **Transpositionen**.
    - Zykeln mit einer ungeraden Anzahl von Elementen, z. B. (123).
  - **Ungerade Permutation**
    - Jede Darstellung ergibt sich aus einer **ungeraden Anzahl** von **Transpositionen**.
    - Zykeln mit einer geraden Anzahl von Elementen, z. B. (1234).
- Da die Verkettung zweier gerader Permutationen gerade ist, bilden die geraden Permutationen eine Untergruppe der symmetrischen Gruppe S_n, die sogenannte **Alternierende Gruppe A_n**.
  $$A_n = \{\sigma \in S_n \mid \sigma \text{ ist eine gerade Permutation}\}$$
- Die Alternierende Gruppe A_n enthält die Hälfte der Elemente der Symmetrischen Gruppe S_n.