Lineare Algebra und Analytische Geometrie I*

Prof. Dr. Jürg Kramer

Mitschrift von Michael Kreikenbaum

Version vom 28. August 2006

Inhaltsverzeichnis

zur Literatur G. Fischer "Lineare Algebra" (S. 30-70) und M. Artin "Algebra" (S. 40-80) enthalten Grundlagen der Gruppentheorie. Das Standardwerk ist S. Lang "Algebra" (Springer).

Dank Danke an Fabian Müller für seine Mitschrift der Vorlesung vom 9.11.2005.
Danke an Irene Winkler für die Definitionen der Ordnung einer Gruppe und des Monoids.

0 Gruppen, Ringe, Körper

0.1 Mengentheoretische Grundlagen

0.1.1 Definition: Menge

Eine **Menge** ist eine Kollektion paarweise verschiedener Objekte, etwa Zahlen oder Buchstaben, zu einem Ganzen. [1]
Es sei A eine Menge: Die in A enthaltenen Objekte heißen **Elemente von** A. Ist a ein Element von A, so schreiben wir $a \in A$, andernfalls $a \notin A$.
Soll eine Menge B explizit angegeben werden, so schreiben wir deren Elemente in geschweiften Klammern auf, zum Beispiel

$$B = \{1, 2, 3\}$$

Die **leere Menge** bezeichnen wir mit $\emptyset$ (alternativ $\{\}$).
Die **Anzahl der Elemente von** A wird mit $|A|$ bezeichnet. (alternativ: $\#A$), man spricht auch von der **Kardinalität** oder **Mächtigkeit von** A. Hat A unendlich viele Elemente, so schreiben wir $|A| = \infty$.
Speziell:
$\mathbb{N}$ Menge der natürlichen Zahlen
$\mathbb{Z}$ Menge der ganzen Zahlen
$\mathbb{Q}$ Menge der rationalen Zahlen
$\mathbb{R}$ Menge der reellen Zahlen

Ist jedes Element von A auch Element von B, so heißt A **Teilmenge von** B oder B **Obermenge von** A; man sagt auch: A ist in B enthalten.
Wir schreiben: $A \subseteq B$.
Ist A **echte Teilmenge** von B, so schreiben wir: $A \subsetneq B$.
Man stellt fest: A ist genau dann gleich B, wenn sowohl A Teilmenge von B als auch B Teilmenge von A ist:
Kurz (Äquivalenz)

$$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$$

[1] Die Definition geht auf Georg Cantor (1845-1918) zurück:

> Eine Menge ist eine Zusammenfassung bestimmter, wohlunterschiedlicher Dinge unserer Anschauung oder unseres Denkens, welche Elemente der Menge genannt werden, zu einem Ganzen.

0.1.2 Definition: Vereinigung

$$A \cup B := \{x \mid x \in A \vee x \in B\}$$

Es gilt:
$(A \cup B) \cup C = A \cup (B \cup C)$ (Assoziativität)
$A \cup B = B \cup A$ (Kommutativität)
Wir schreiben: $A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_n = \bigcup_{j=1}^{n} A_j$

0.1.3 Definition: Durchschnitt

$$A \cap B := \{x \mid x \in A \wedge x \in B\}$$

Es gilt:
$(A \cap B) \cap C = A \cap (B \cap C)$ (Assoziativität)
$A \cap B = B \cap A$ (Kommutativität)
Wir schreiben: $A_1 \cap A_2 \cap A_3 \cap \ldots \cap A_n = \bigcap_{j=1}^{n} A_j$

0.1.4 Definition: kartesisches Produkt

Seien A, B zwei Mengen. Dann heißt die Menge

$$A \times B := \{(a, b) \mid a \in A, b \in B\}$$

der geordneten Paare (a, b) das **kartesische Produkt von A mit B.**
Generell

$$A_1 \times A_2 \times \ldots \times A_n := \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}$$

0.1.5 weitere Symbole

$\forall$ "für alle"
$\exists$ "es existiert" = "es gibt"
$\nexists$ "es existiert nicht" = "es gibt kein"
$\exists!$ "es existiert genau ein" = "es gibt genau ein"

0.1.6 Definition: Abbildung

Seien A, B Mengen. Eine Vorschrift, die jedem Element $a \in A$ genau ein Element $b \in B$ zuordnet, heißt eine **Abbildung von A nach B.**
Schreibweise:

$$f : A \longrightarrow B$$

$$a \mapsto b = f(a)$$

- Mit $\mathrm{im}(f)$ oder auch $f(A)$ bezeichnen wir die Menge aller Bilder $f(a)$ mit $a \in A$, also
$$\mathrm{im}(f) = \{f(a) \mid a \in A\} \subseteq B$$
Wir sprechen vom **Bild von A unter f.**

- Zwei Abbildungen $f_1, f_2 : A \to B$ sind einander **gleich**, in Zeichen $f_1 = f_2$, [2] falls $f_1(a) = f_2(a)$ für alle $a \in A$.

- Eine Abbildung $f : A \to B$, bei der jedes $b \in B$ als Bild eines $a \in A$ auftritt, für die also $\mathrm{im}(f) = B$ gilt, heißt **surjektiv**.

- Eine Abbildung $f : A \to B$, bei der jedes $b \in B$ *höchstens einmal* als Bild eines $a \in A$ auftritt, für die also aus $f(a_1) = f(a_2)$ immer $a_1 = a_2$ folgt, heißt **injektiv**.

- Eine injektive und surjektive Abbildung $f : A \to B$ heißt **bijektiv**.
Für eine bijektive Abbildung $f : A \to B$ gibt es zu jedem $b \in B$ genau ein $a \in A$ mit $f(a) = b$.

- Die Bezeichnung $b \mapsto a$ definiert für die bijektive Abbildung $f : A \to B$ eine Abbildung:
$$f^{-1} : B \to A$$
die sogenannte **Umkehrabbildung von f**:
$$A \overset{f}{\to} B \overset{f^{-1}}{\to} A$$
$$a \mapsto f(a) = b \mapsto f^{-1}(b) = a$$
also $(f^{-1} \circ f)(a) = f^{-1}(f(a)) = a \quad \forall a \in A$
$f^{-1} \circ f = \mathrm{id}_A$ (id_A = identische Abbildung in A: $f(x) = x$)
Ebenso gilt: $(f \circ f^{-1})(b) = f(f^{-1}(b)) = b \quad \forall b \in B$
$f \circ f^{-1} = \mathrm{id}_B$ (id_B = identische Abbildung in B)

- Seien $f : A \to B$ und $g : B \to C$ Abbildungen. Die **Komposition von f mit g** ist die durch Hintereinanderausführung von zuerst f und dann g, d.h.
$$C \ni g(f(a)) = (g \circ f)(a) \quad a \in A$$
Die Komposition von Abbildungen ist assoziativ, sind also $f : A \to B, f : B \to C$ und $h : C \to D$ Abbildungen, so gilt:
$$h \circ (g \circ f) = (h \circ g) \circ f$$

[2] = oder $\equiv$?

0.2 Halbgruppen und Gruppen

0.2.1 Definition: Verknüpfung $\circ_M$ auf M

Sei $M \neq \emptyset$ eine beliebige nicht-leere Menge. Eine **Verknüpfung $\circ_M$ auf M** ist eine Vorschrift, die jedem (geordneten) Paar $(m_1, m_2) \in M \times M$ ein weiteres Element $m_3 \in M$ zuordnet. In Zeichen:

$$M \times M \to M$$

$$(m_1, m_2) \mapsto m_3 =: m_1 \circ_M m_2$$

m_3 ist also Verknüpfung von m_1 mit m_2.
Man sagt auch: M **bildet mit $\circ_M$ eine Struktur**.

Beispiel $M = \mathbb{N}, \circ_M = + : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
$(a, b) \mapsto a + b$

0.2.2 Definition: assoziativ

Sei $M, \circ_M$ eine Menge mit Verknüpfung.
Die Verknüpfung (oder die Struktur) heißt **assoziativ**, falls

$$(m_1 \circ_M m_2) \circ_M m_3 = m_1 \circ_M (m_2 \circ_M m_3) \quad \forall m_1, m_2, m_3 \in M$$

gilt. Falls $\circ_M$ assoziativ ist, können bei mehrfacher Ausführung der Verknüpfung die Klammern weglassen, d.h. $m_1 \circ_M m_2 \circ_M \ldots \circ_M m_n$ ist wohldefiniert.

Bemerkung Ist die zugrunde liegende Menge M fixiert, so schreiben wir $\circ$ anstelle $\circ_M$.

0.2.3 Definition: Halbgruppe

Eine nicht-leere Menge H mit einer assoziativen Verknüpfung $\circ = \circ_H$ heißt eine **Halbgruppe**. Wir schreiben kurz: $(H, \circ)$ oder noch kürzer: H.

Beispiele:

1. $(H, \circ) = (\mathbb{N}, +)$ ist Halbgruppe.
2. $(H, \circ) = (\mathbb{Z}, \cdot)$ ist Halbgruppe.
3. Sei A eine Menge und $\mathrm{Abb}(A) = \{f : A \to A\} \ni \mathrm{id}_A$.
   Dann ist $(H, \circ) = (\mathrm{Abb}(A), \circ)$ ist eine Halbgruppe. Für $f, g \in \mathrm{Abb}(A)$ ist auch $g \circ f \in \mathrm{Abb}(A)$.

0.2.4 Definition: Gruppe

Eine Halbgruppe $G = (G, \circ)$ heißt **Gruppe**, falls gilt:

1. Es existiert ein $e \in G$ mit $e \circ g = g$ für alle $g \in G$. Das Element e wird **linksneutrales Element** genannt.
2. Für alle $g \in G$ existiert ein $g' \in G$ mit $g' \circ g = e$. Das Element $g' \in G$ heißt **zu** g **linksinverses Element** und wird in der Regel mit g^{-1} bezeichnet.

Bemerkung Eine Halbgruppe $G = (G, \circ)$ heißt also Gruppe, falls gilt:

1. $\exists e \in G : e \circ g = g \quad \forall g \in G$

2a. $\forall g \in G : \exists g^{-1} \in G : g^{-1} \circ g = e$
Dies ist noch nicht korrekt, da wir noch keine Eindeutigkeit für e gezeigt haben.

2b. alternativ dazu: $\forall e \in G$ linksneutral $: \forall g \in G : \exists g^{-1} \in G : g^{-1} \circ g = e$

Bemerkung Man zeigt, daß ein linksneutrales Element $e \in G$ auch rechtsneutrales Element ist, d.h $g \circ e = g \quad \forall g \in G$ erfüllt. Somit ist es erlaubt, von **einem neutralen Element** $e \in G$ zu sprechen. Dieses ist eindeutig bestimmt: siehe Aufgabe 2(a), Serie 1.

Man zeigt überdies, dass ein linksinverses $g^{-1} \in G$ auch rechtsinvers ist, also $g \circ g^{-1} = e$ erfüllt. Überdies ist g^{-1} dann eindeutig bestimmt. Man spricht von **dem Inversen** g^{-1} **von** g.

0.2.5 Definition: Gruppe (formaler)

Eine Halbgruppe $G = (G, \circ)$ heißt **Gruppe**, falls gilt:

1. $\exists! e \in G : e \circ g = g = g \circ e \quad \forall g \in G$ (e ist **das neutrale Element** von G).
2. $\forall g \in G : \exists g^{-1} \in G : g^{-1} \circ g = e = g \circ g^{-1}$ (g^{-1} ist **das Inverse zu** g).

Beispiele und Nicht-Beispiele

1. $(G, \circ) = (\mathbb{N}, +)$, so ist dies keine Gruppe:
Wohl ist $e = 0 \in \mathbb{N}$ (Nullelement) neutral,
aber zum Beispiel zu $2 \in \mathbb{N} : \nexists n \in \mathbb{N} : 2 + n = 0 = n + 2$.
2. $(G, \circ) = (\mathbb{Z}, +)$. Dies ist eine Gruppe:
$0 \in \mathbb{Z}$ ist neutrales Element.
Für $n \in \mathbb{Z}$ ist $(-n) \in \mathbb{Z}$ das (additiv) Inverse zu n, da $n + (-n) = 0$.
3. $(G, \circ) = (\mathbb{Z}, \cdot)$. Dies ist keine Gruppe:
Wohl ist $e = 1 \in \mathbb{Z}$ (Einselement) neutral, aber zum Beispiel zu $2 \in \mathbb{Z}, \nexists n \in \mathbb{Z} :$
$2 \cdot n = 1 = n \cdot 2$.

4. $(G, \circ) = (\mathbb{Q}^\times, \cdot)$. $(\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\})$. ist eine Gruppe: $e = 1 \in \mathbb{Q}$ ist neutrales Element; $a \in \mathbb{Q}^\times$, dann ist $a^{-1} = \frac{1}{a} \in \mathbb{Q}^\times$.

5. Siehe Aufgabe 3 Serie 1.

0.2.6 Definition: Ordnung von G

Ist $G = (G, \circ)$ eine Gruppe, so bezeichnet $|G|$ [3] die **Ordnung von** G.

Bemerkung: Monoid Eine Halbgruppe $M = (M, \circ)$ in der es zudem ein (eindeutig bestimmtes) neutrales Element gibt, wird **Monoid** genannt.

0.2.7 Definition: abelsch

Eine Gruppe $G = (G, \circ)$ (repektive Monoid, Halbgruppe) heißt **kommutativ** oder **abelsch**, falls

$$g_1 \circ g_2 = g_2 \circ g_1 \quad \forall g_1, g_2 \in G$$

Beispiele

1. $(\mathbb{Z}, +)$ kommutative Gruppe, $|\mathbb{Z}| = \infty$
2. $(\mathbb{Q}^*, \cdot)$ kommutative Gruppe, $|\mathbb{Q}^*| = \infty$
3. D_n n-te Diedergruppe (siehe Serie 1, Aufgabe 4)
4. $S_n = \{\pi : \{1, \ldots, n\} \to \{1, \ldots, n\} \mid \pi \text{ bijektiv}\}$ ist die Menge der Permutationen der Zahlen $1, \ldots, n$. Die Struktur auf S_n ist die Verknüpfung der Abbildungen.

D_n und S_n sind nicht-kommutative Gruppen, $|S_n| = n!$.

Schreibweise Für eine beliebige Gruppe $G = (G, \circ)$ und $n \in \mathbb{N}$ führen wir die vorteilhafte Notation für n-malige Verknüpfung eines Elements $g \in G$ mit sich selbst wie folgt ein:

$$g^n := \underbrace{g \circ \ldots \circ g}_{n\text{-mal}}$$

wobei $g^0 := e, g^1 := g$.
Weiter schreiben wir für $n \in \mathbb{N}$:

$$g^{-n} := \underbrace{g^{-1} \circ \ldots \circ g^{-1}}_{n\text{-mal}}$$

Somit ist g^m für $m \in \mathbb{Z}$ definiert.

[3] die Anzahl der Elemente von G

Rechenregeln (ohne Beweis):
$g^n \circ g^m = g^{n+m}$
$(g^n)^m = g^{n \cdot m}$ $(g \in G; m, n \in \mathbb{Z})$.

0.2.8 Definition: Untergruppe

Eine **Untergruppe** U **von** G ($G = (G, \circ)$ Gruppe), in Zeichen $U \leq G$, ist Teilmenge $U \subseteq G$, die mit der von G *induzierten Struktur* (Verknüpfung) selbst eine Gruppe ist.

$G \times G \overset{\circ}{\to} G$
$(g_1, g_2) \mapsto g_1 \circ g_2$
...

Beispiele

1. Sei $G = (G, \circ)$ eine Gruppe mit neutralem Element e. Dann sind G und $U = \{e\}$ Untergruppen von G.

2. $\mathbb{Z} = (\mathbb{Z}, +)$, $2\mathbb{Z} = (2\mathbb{Z}, +)$.
   $2\mathbb{Z} \leq \mathbb{Z}$. [4]

3. $\mathbb{Q}^\times = (\mathbb{Q}^\times, \cdot), \mathbb{R}^\times = (\mathbb{R}^\times, \cdot)$
   $\mathbb{Q} \leq \mathbb{R}$

4. $S_4 = \{$alle Permutationen von vier Elementen$\}$
   $U = \{\binom{1234}{1234}, \binom{1234}{2341}, \binom{1234}{3412}, \binom{1234}{4123}\}$
   $|U| = 4$; es ist $U \leq S_4$.

0.2.9 Lemma: Untergruppenkriterium

Sei $G = (G, \circ)$ eine Gruppe und $H \subseteq G$ eine nicht-leere Teilmenge.
Dann gilt:

$$H \leq G \Leftrightarrow g \circ h^{-1} \in H \quad \forall g, h \in H$$

Beweis: $\Rightarrow$: *Voraussetzung:* $H \leq G$
Behauptung: $g \circ h^{-1} \in H \quad \forall g, h \in H$
Beweis: H ist Untergruppe, d.h. mit $h \in H$ auch $h^{-1} \in H$.
Mit $g \in H$, $h^{-1} \in H$, da $H \leq G$ ist auch $g \circ h^{-1} \in H$.
$\Leftarrow$: *Voraussetzung:* $g \circ h^{-1} \in H \quad \forall g, h \in H$
Behauptung: $H \leq G$
Beweis: Gruppenaxiome testen:

1. $H \neq \emptyset$

2. $(H, \circ)$ ist Halbgruppe

[4] Schreibweise: $H \leq G :=$ H ist Untergruppe von G

a) $H \times H \to H$ Abgeschlossenheit

b) Assoziativität

3. $\exists e \in H$
4. $\forall h \in H, \exists h^{-1} \in H$

Beweis siehe Serie 2 Aufgabe 1. □

0.2.10 Definition: zyklische Untergruppe

Sei $G = (G, \circ)$ eine Gruppe.
Eine Untergruppe $U \leq G$ heißt **zyklisch**, falls ein $g \in G$ mit

$$U = \{\ldots, g^{-2}, g^{-1}, g^0 = e, g^1 = g, g^2, \ldots\} = \{g^m \mid m \in \mathbb{Z}\} = \{g^{\mathbb{Z}}\}$$

Man schreibt auch $U = \langle g \rangle$. Man nennt g den **Erzeuger** oder **Generator von** $U = \langle g \rangle$.

Beispiel

1. $G = (\mathbb{Z}, +) = \langle 1 \rangle$.
   (denn: $\mathbb{N} \ni n = \underbrace{1 + \ldots + 1}_{\text{n-mal}}$).
2. Vgl. Serie 1, Aufg. 4:
   $D_1 \ni b$ mit $b^3 = e$
   bzw. die Drehung um $\frac{2\pi}{n}$
   $D_n \geq \langle b \rangle = \{b^0 = e, b^1 = b, b^2, \ldots, b^{n-1}\}, |\langle b \rangle| = n$
   $D_n \geq \langle a \rangle = \{a^0 = e, a^1 = a\}, |\langle a \rangle| = 2$

0.2.11 Definition: Ordnung eines Elementes

Sei $G = (G, \circ)$ eine Gruppe und $g \in G$. Die kleinste, positive, natürliche Zahl $n \in \mathbb{N}$ mit $g^n = e$ heißt die **Ordnung von** g **(in** G**)** und wird mit $\text{ord}_G(g)$ bezeichnet. Wenn klar ist, auf welche Gruppe wir uns beziehen, schreiben wir kurz $\text{ord}(g)$ anstelle von $\text{ord}_G(g)$. Gibt es kein $n \in \mathbb{N}$ mit $g^n = e$, so setzen wir

$$\text{ord}_G(g) = \text{ord}(g) := \infty$$

Beispiele

1. $1 \in (\mathbb{Z}, +) : \text{ord}_{\mathbb{Z}}(1) = \infty$
2. $D_n \ni b$ (wie oben) $\text{ord}_{D_n}(b) = n$
   $D_n \ni a$ (wie oben) $\text{ord}_{D_n}(a) = 2$

Bemerkung Sei $G = (G, \circ)$ eine Gruppe und $g \in G$ mit $\mathrm{ord}_G(g) = n < \infty$.
Betrachte $\langle g \rangle = \{e = g^0, g = g^1, g^2, \ldots, g^{n-1}\}$
Wir stellen fest:

$$| \langle g \rangle | = n = \mathrm{ord}_G(g).$$

0.2.12 Definition: Homomorphismus, Isomorphismus

Seien $G = (G, \circ_G)$ und $H = (H, \circ_H)$ zwei Gruppen.
Eine Abbildung $f : G \to H$ heißt **Homomorphismus**, falls für alle $g_1, g_2 \in G$ die Gleichheit

$$f(g_1 \circ_G g_2) = f(g_1) \circ_H f(g_2)$$

besteht. (Strukturtreue von f).
Ein bijektiver Homomorphismus heißt **Isomorphismus**.

Bemerkung Sei $f : G \to H$ ein Isomorphismus.
Wir sagen "G und H sind zueinander isomorphe Gruppen". (in Zeichen $G \cong H$), oder: die Gruppen G, H sind strukturgleich.

Beispiel $G = D_3$ (3te Diedergruppe) $= \{a^l \circ b^m \mid l \in \{0, 1\}, m \in \{0, 1, 2\}\}$,
wobei $a =$ Spiegelung eines Dreiecks an der Vertikale
und $b =$ Drehung eines Dreiecks um $360/3 = 120$ Grad
$H = S_3$ (symmetrische Gruppe mit 3 Elementen)
Behauptung: $D_3 \cong S_3$
Beweis: Definiere Abbildung

$$f : D_3 \to S_3$$

Sei $g \in D_3$. g lässt das Dreieck ABC invariant, vertauscht dabei die Ecken. Nummeriere die Ecken A=1, B=2, C=3.
Zum Beispiel $g = b : 123 \to 312 \Rightarrow \begin{pmatrix} 123 \\ 231 \end{pmatrix}$
Prüfe: f ist bijektiv. □

0.2.13 Definition: Kern, Bild

Seien $G = (G, \circ_G)$ und $H = (H, \circ_H)$ Gruppen und $f : G \to H$ ein Homomorphismus.
Dann heißt

$$\ker(f) = \{g \in G \mid f(g) = e_H\}^5$$

der **Kern von** f und

$$\mathrm{im}(f) = \{h \in H \mid \exists g \in G : f(g) = h\}$$

das **Bild von** f.

[5] e_H = neutrales Element von H

Bemerkung Sei $f : G \to H$ ein Homomorphismus.

1. f ist surjektiv $\Leftrightarrow \text{im}(f) = H$
2. f ist injektiv $\Leftrightarrow \ker(f) = \{e_G\}$[6]

Beweis

1. Verwende die Definition von Surjektivität.
2. (Beachte Serie 2, Aufgabe 3).
   $\underline{\Rightarrow}$ Gemäß Aufg. 3 gilt: $f(e_G) = e_H$, also $e_G \in \ker(f)$, $\{e_G\} \subseteq \ker(f)$.
   Wenn $\{e_G\} \subsetneq \ker(f)$, dann $\exists g \neq e_G \in \ker(f)$.
   Dann hätten wir $f(e_G) = f(g) = e_H$. Das widerspricht der Injektivität von f.
   Somit kann $\{e_G\} \subsetneq \ker(f)$ nicht gelten.
   Also gilt die Gleichheit: $\ker(f) = \{e_G\}$.
   $\underline{\Leftarrow}$ Sei aber $\ker(f) = \{e_G\}$.
   Wir müssen zeigen: f ist injektiv.
   Seien $g_1, g_2 \in G$ mit $f(g_1) = f(g_2)$, Zeige: $g_1 = g_2$
   Wir haben $f(g_1) = f(g_2)$ — multipliziere von links mit $f(g_2)^{-1}$
   $\Rightarrow f(g_2)^{-1} \circ_H f(g_1) = f(g_2)^{-1} \circ_H f(g_2) = e_H$
   Aus Übungsaufgabe 3b) folgt: $f(g_2)^{-1} = f(g_2^{-1})$
   $\Rightarrow f(g_2^{-1}) \circ_H f(g_1) = e_H$
   $\underset{f \text{ Hom.}}{\Rightarrow} f(g_2^{-1} \circ_G g_1) = e_H$
   $\underset{\text{Def.}}{\Rightarrow} g_2^{-1} \circ_G g_1 \in \ker(f) = \{e_G\}$
   $\Rightarrow g_2^{-1} \circ_G g_1 = e_G$ — multipliziere von links mit g_2
   $\Rightarrow (g_2 \circ_G (g_2^{-1}) \circ g_1) = g_2 \circ_G e_g = g_2$
   $g_1 = e_G \circ_G g_1 = g_2 \Rightarrow g_1 = g_2$.
   f ist also injektiv. □

0.2.14 Lemma: $\ker(f)$ ist Untergruppe von G, $\text{im}(f)$ ist Untergruppe von H

Seien $G = (G, \circ_G)$ und $H = (H, \circ_H)$ Gruppen und $f : G \to H$ ein Homomorphismus. Dann gilt

1. $\ker(f)$ ist Untergruppe von G, d.h. $\ker(f) \leq G$.
2. $\text{im}(f)$ ist Untergruppe von H, d.h. $\text{im}(f) \leq H$

Beweis Siehe Serie 2, Aufgabe 3, insbesondere 3c), 3d)

[6] e_G = neutrales Element von G

Beispiel Sei $n \in \mathbb{N}, n > 0$. Sei

$$\mathcal{R}_n = \{0, 1, \ldots, n-1\} \neq \emptyset$$

Abbildung $\oplus$ auf $\mathcal{R}_n$:
Seien $a, b \in \mathcal{R}_n$ $a \oplus b :=$ $\underbrace{R_n(a+b)}_{\text{Rest der Summe nach Division durch n}}$
Damit

$$\mathcal{R}_n \times \mathcal{R}_n \to \mathcal{R}_n$$
$$(a, b) \mapsto a \oplus b$$

Diese Struktur ist assoziativ: $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
$R_n(R_n(a+b)+c) = R_n(a+R_n(b+c))$
0 ist neutrales Element.
Jedes Element besitzt ein Inverses.
$\Rightarrow (\mathcal{R}_n, \oplus)$ ist eine abelsche Gruppe.

Beispiel $(G, \circ_G) = (\mathbb{Z}, +), (H, \circ_H) = (\mathcal{R}_n, \oplus)$
Definiere $f : \mathbb{Z} \to \mathcal{R}_n$
$a \mapsto R_n(a)$
Behauptung: f ist Homomorphismus, d.h.
$f(a+b) = f(a) \oplus f(b)$, d.h.
$R_n(a+b) = R_n(R_n(a) + R_n(b))$
$\text{im}(f) = \mathcal{R}_n$, d.h. f ist surjektiv
$\ker(f) = \{a \in \mathbb{Z} \mid a = k \cdot n, k \in \mathbb{Z}\} = n\mathbb{Z}$
d.h. f ist nicht injektiv.

0.2.15 Definition: Äquivalenzrelation

Sei G eine Menge. Eine (binäre) Relation $\sim$ auf G heißt **Äquivalenzrelation**, falls gilt:

1. $g \sim g \quad \forall g \in G$ (Reflexivität)
2. $g_1 \sim g_2 \Rightarrow g_2 \sim g_1 \quad \forall g_1, g_2 \in G$ (Symmetrie)
3. $g_1 \sim g_2, g_2 \sim g_3 \Rightarrow g_1 \sim g_3 \quad \forall g_1, g_2, g_3 \in G$ (Transitivität)

Beispiel Die Gleichheit "=" von Elementen der Menge G ist eine Äquivalenzrelation.

0.2.16 Definition Äquivalenzklasse, Repräsentant

Sei G eine Menge mit einer Äquivalenzrelation $\sim$. Ist $g \in G$, so nennen wir die Menge $M_g = \{h \in G \mid h \sim g\}$ die **Äquivalenzklasse zu** g.
Jedes $h \in M_g$ nennen wir **Repräsentant von** M_g; speziell ist g Repräsentant von M_g.

0.2.17 Lemma: disjunkte Zerlegung in Äquivalenzklassen

Sei G eine Menge mit einer Äquivalenzrelation $\sim$. Dann gilt:

1. Zwei Äquivalenzklassen sind entweder identisch oder disjunkt.
2. Die Äquivalenzrelation $\sim$ induziert eine disjunkte Zerlegung von G in Äquivalenzklassen.

Beweis

1. Seien $g_1, g_2 \in G$ und $M_{g_1} \cap M_{g_2} \neq \emptyset$.
   Zu zeigen: $M_{g_1} = M_{g_2}$
   $M_{g_1} \cap M_{g_2} \neq \emptyset \Rightarrow \exists g \in M_{g_1} \cap M_{g_2} \underset{\text{Sym.}}{\Rightarrow} g \sim g_1, g \sim g_2 \Rightarrow g_1 \underset{\text{Transitivität}}{\Rightarrow} g_1 \sim g_2$.
   Sei $h \in M_{g_1} : h \sim g_1$.
   Wegen $g_1 \sim g_2$ folgt mit Transitivität: $h \sim g_2 \Rightarrow h \in M_{g_2} \Rightarrow M_{g_1} \subseteq M_{g_2}$.
   Symmetrisch dazu: $M_{g_2} \subseteq M_{g_1} \Rightarrow M_{g_1} = M_{g_2}$.
2. Sei $g_1 \in G$ und M_{g_1} die zugehörige Äquivalenzklasse. Dann gilt:
   Entweder $G = M_{g_1}$
   Oder $G \neq M_{g_1}$, d.h. $G \setminus M_{g_1} \neq \emptyset$.
   Im ersten Fall sind wir fertig.
   Im zweiten Fall: Sei $g_2 \in G \setminus M_{g_1}$. Dann gilt:
   Entweder $G = M_{g_1} \cup M_{g_2}$ (disjunkt nach (1))
   Oder $G \neq M_{g_1} \cup M_{g_2}$, d.h. $G \setminus M_{g_1} \cup M_{g_2} \neq \emptyset$.
   Im ersten Fall sind wir fertig.
   Im zweiten Fall: Sei $g_3 \in G \setminus M_{g_1} \cup M_{g_2}$. Dann gilt:
   Entweder $G = M_{g_1} \cup M_{g_2} \cup M_{g_3}$ (disjunkt nach (1))
   Oder eben nicht.
   Im letzteren Fall fahre entsprechend fort. □

Beispiel konkrete Anwendung in der Gruppentheorie
Sei $G = (G, \circ)$ Gruppe und $H \leq G$ eine Untergruppe.
Definiere

$$g_1 \sim g_2 \overset{\text{Def.}}{\Leftrightarrow} g_1^{-1} \circ g_2 \in H$$

Behauptung: Dies definiert eine Äquivalenzrelation auf G.

Beispiel: Seien $G = \mathbb{Z}, n \in \mathbb{N}, n > 0$. $a \sim b :\Leftrightarrow n \mid (a - b) \quad a, b \in \mathbb{Z}$ [7]

- reflexiv: $n|(a - a)$, da $n|(a - a) = 0$
- symmetrisch: $n|(a - b) \Rightarrow \exists k \in \mathbb{Z} : a - b = nk \Rightarrow b - a = n \cdot (-k) \Rightarrow n|(b - a)$

[7] (n teilt $(a - b)$), $n|(a - b)$, d.h. $\exists k \in \mathbb{Z} : a \cdot b = n \cdot k$, siehe 0.3.9

- transitiv: $n|(a-b) \wedge n|(b-c)$
  $\Rightarrow \exists k_1, k_2 \in \mathbb{Z} : a-b = nk_1 \wedge b-c = nk_2$
  $\Rightarrow (a-b)+(b-c) = a-c = n(k_1+k_2)$
  $\Rightarrow a \sim c$

Äquivalenzklassen Für $0 \in \mathbb{Z}$ ist $M_0 = \{a \in \mathbb{Z} \mid a \sim 0\}$
$= \{a \in \mathbb{Z} \mid n|a\}$
$= \{a \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : a = nk\}$
$= \{a \in \mathbb{Z} \mid a = n\text{-faches}\}$
$= n\mathbb{Z}$

$n = 1$ $M_0 = \mathbb{Z}$

$n > 1$ $M_0 = n\mathbb{Z} \subsetneq \mathbb{Z}$
$\mathbb{Z} \setminus M_0 = \mathbb{Z} \setminus n\mathbb{Z} \neq \emptyset$
$M_1 = \{a \in \mathbb{Z} \mid a \sim 1\}$
$= \{a \in \mathbb{Z} \mid n|(a-1)\}$
$= \{a \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : a-1 = nk\}$
$= \{a \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : a = nk+1\}$
$= \{a \in \mathbb{Z} \mid R_n(a) = 1\}$ [8] $\mathbb{Z} = \underbrace{M_0}_{R_n(a)=0} \cup \underbrace{M_1}_{R_n(a)=1} \cup \dot{\vdots}$.

$n = 2$ $\mathbb{Z} = \underset{\text{“gerade”}}{M_0} \dot\cup \underset{\text{“ungerade”}}{M_1}$

$n > 2$ Bild mit Zahlengerade und Zahlen in M_0 und M_1. Fehlende Zahlen.
$M_2 = \{a \in \mathbb{Z} \mid a \sim 2\} = \{A \in \mathbb{Z} \mid R_n(a) = 2\}$

$n = 3$ $\mathbb{Z} = M_1 \dot\cup M_2 \dot\cup M_3$

Allgemein $\mathbb{Z} = M_1 \dot\cup M_2 \dot\cup \ldots \dot\cup M_{n-1}$

zurück zu den Gruppen

0.2.18 Definition: Relation $\sim$

Seien $G = (G, \circ)$ eine Gruppe und $H \leq G$ eine Untergruppe. Definiere

$$g_1 \sim g_2 :\Leftrightarrow g_1^{-1} \circ g_2 \in H \quad \forall g_1, g_2 \in G$$

0.2.19 Lemma: $\sim$ ist Äquivalenzrelation

Die Relation $\sim$ der vorhergehenden Definition ist eine Äquivalenzrelation.

[8] $R_n(a) :=$ Rest von a nach Division durch $n = \{0, \ldots, n-1\}$

Beweis

- Reflexivität:
  Zu zeigen: $g \in H \Rightarrow g \sim g$.
  Wir haben: $\underbrace{g^{-1} \circ g}_{e_G} \in H$.
  Wegen $e_G \in H$, folgt $g^{-1} \circ g \in H$, also $g \sim g$.

- Symmetrie:
  Zu zeigen: $g_1, g_2 \in G$ mit $g_1^{-1} \circ g_2 \in H \Rightarrow g_2^{-1} \circ g_1 \in H$
  Wir haben: $g_1^{-1} \circ g_2 \in H$
  $\underset{H \leq G}{\Rightarrow} (g_1^{-1} \circ g_2)^{-1} \in H \underset{\text{Serie 1}}{\Rightarrow} g_2^{-1} \circ (g_1^{-1})^{-1} \in H \Rightarrow g_2 \sim g_1$.

- Transitivität:
  Zu zeigen: Für $g_1, g_2, g_3 \in G$ mit $g_1 \sim g_2, g_2 \sim g_3$, also $g_1^{-1} \circ g_2 \in H$
  muss gelten: $g_2^{-1} \circ g_3 \in H \Rightarrow g_1 \sim g_3$, also $g_1^{-1} \circ g_3 \in H$.
  Wir haben: $g_1^{-1} \circ g_2 \in H, g_2^{-1} \circ g_3 \in H$
  $\underset{\text{verknüpft}}{\Rightarrow} (g_1^{-1} \circ g_2) \circ (g_2^{-1} \circ g_3) \in H$
  $\underset{\text{Assoz.}}{\Rightarrow} g_1^{-1} \circ (g_2 \circ g_2^{-1}) \circ g_3 \in H$
  $\Rightarrow g_1^{-1} \circ g_3 \in H$. □

0.2.20 Definition: Linksnebenklassen

Beobachte die Äquivalenzrelation zu $g \in G$.
$M_g = \{h' \in G \mid h' \sim g\}$
$= \{h' \in G \mid g \sim h'\}$
$= \{h' \in G \mid g^{-1} \circ h' \in H\}$
$= \{h' \in G \mid g^{-1} \circ h' = h \in H\}$
$= \{h' \in G \mid h' = g \circ h \in H\}$
$= g \circ H$

Die Äquivalenzklassen M_g in dieser speziellen Schreibweise sind von der Form:

$$M_g = g \circ H \quad (g \in G)$$

und heißen **Linksnebenklassen von H zu g.** [9]
Nach dem Vorhergehenden zerfällt G disjunkt in Linksnebenklassen von H.

$$G = \dot{\bigcup_{g \in I}} (g \circ H)$$

wobei $I \subseteq G$ ein *vollständiges Repräsentantensystem* der Linksnebenklassen von G nach H ist.

[9] Der Begriff hat sich einmal von rechts nach links vertauscht: siehe
Algebra-Buch von v.d.Waerden: "Moderne Algebra"(1920)
und von Lang: "Algebra"(aktuell)

Beispiel $(G, \circ) = (\mathbb{Z}, +), (H, \circ) = (n\mathbb{Z}, +)$
Was bedeutet $g_1^{-1} \circ g_2 \in H, (g_1, g_2 \in \mathbb{Z})$?
Es bedeutet: $-g_1 + g_2 \in n\mathbb{Z} \Leftrightarrow n \mid (g_2 - g_1)$
$\mathbb{Z} = \dot{\bigcup}_{g \in I} (g + n\mathbb{Z})$
Es ist $I = \mathcal{R}_n = \{0, \dots n-1\}$ und $\mathbb{Z} = \dot{\bigcup}_{i=0}^{n-1} (j + n\mathbb{Z}) \underset{\text{kommutativ}}{=} \dot{\bigcup}_{i=0}^{n-1} (n\mathbb{Z} + j)$. [10]

0.2.21 Definition/Schreibweise: Menge der Linksnebenklassen

Seien $G = (G, \circ)$ eine Gruppe und $H \leq G$ eine Untergruppe von G.
Wir bezeichnen die Menge der Linksnebenklassen $g \circ H, (g \in I)$ mit G/H. In Formeln:

$$G/H := \{g \circ H \mid g \in I\}$$

Beispiel "Menge der Linksnebenklasssen zu H"
$\mathbb{Z}/n\mathbb{Z} = \{(j + n\mathbb{Z}) \mid j \in \{0, \dots, n-1\}\} \overset{\text{bijektiv}}{\to} \mathcal{R}_n = \{0, \dots, n-1\}$

0.2.22 Lemma: Gleiche Mächtigkeit der Nebenklassen

Sei $G = (G, \circ)$ eine Gruppe und $H \leq G$ eine Untergruppe. Dann besitzen alle Linksnebenklassen $g \circ H \in G/H$ die gleiche Mächtigkeit, sie haben also gleichviele Elemente und stehen somit alle in Bijektion zueinander.

Beweis Seien $g_1 \circ H, g_2 \circ H \in G/H$.
Zu zeigen: Es gibt eine Bijektion von $g_1 \circ H$ auf $g_2 \circ H$.
Definiere $\varphi : g_1 \circ H \to g_2 \circ H$ durch die Zuordnung:

$$g_1 \circ h \mapsto g_2 \circ h, (h \in H)$$

Zeige: φ ist bijektiv.

- φ surjektiv: Sei $g_2 \circ h \in g_2 \circ H$ gegeben.
  Gesucht: $h' \in g_1 \circ H$ mit $\varphi(h') = g_2 \circ h$.
  Wähle $h' = g_1 \circ h$; dann folgt:
  $\varphi(h') = \varphi(g_1 \circ h) = g_2 \circ h$
- φ injektiv: Seien $g_1 \circ h, g_1 \circ \overline{h} \in g_1 \circ H, (h, \overline{h} \in H)$ mit
  $\varphi(g_1 \circ h) = \varphi(g_1 \circ \overline{h})$
  $\Rightarrow g_2 \circ h = g_2 \circ \overline{h} \Rightarrow (g_2^{-1} \circ (g_2) \circ h) = (g_2^{-1} \circ (g_2) \circ \overline{h}) \Rightarrow h = \overline{h} \Rightarrow g_1 \circ h = g_1 \circ \overline{h}$

□

[10] $n\mathbb{Z} + j = \{a \in \mathbb{Z} \mid R_n(a) = j\}$

0.2.23 Lemma: (Satz von Lagrange)

Seien $G = (G, \circ)$ eine *endliche* Gruppe (d.h. $|G| < \infty$) und $H \leq G$ eine Untergruppe. Dann gilt: Die Ordnung $|H|$ von H ist ein Teiler der Gruppenordnung $|G|$ von G; in Zeichen

$$|H| \mid |G|$$

Beweis Zerlege G in Linksnebenklassen nach H

$$G = \dot{\bigcup_{g \in I}} (g \circ H)$$

Es ist $|I| < \infty$, also zum Beispiel $I = \{g_1, \ldots, g_n\}$

$$G = g_1 \circ H \,\dot\cup\, g_2 \circ H \,\dot\cup \ldots \dot\cup\, g_n \circ H$$

$\Rightarrow |G| = |g_1 \circ H| + |g_2 \circ H| + \ldots + |g_n \circ H| = \sum_{j=1}^{n} |g_j \circ H|$
Nach dem vorigen Lemma gilt:

$$|g_i \circ H| = |g_j \circ H| \quad \forall i, j \in \{1, \ldots, n\}$$

$\Rightarrow |G| = n \cdot |g_1 \circ H|$
Ohne Einschränkung können wir annehmen, dass $g_1 = e$ unser erster Repräsentant ist.
$\Rightarrow n \cdot |H| \Rightarrow |H| \mid |G|$ □

0.2.24 Definition: Index von H in G

Sei $G = (G, \circ)$ eine Gruppe und $H \leq G$ eine Untergruppe.
Die Ordnung von G/H (die Anzahl der Linksnebenklassen von H) wird als **Index von H in G** bezeichnet. Man schreibt dafür $(G : H)$.
In Formeln:

$$|G| = (G : H) \cdot |H|$$

Beispiel $(G, \circ) = (\mathbb{Z}, +)$
$H = n\mathbb{Z}$
$(\mathbb{Z} : n\mathbb{Z}) = n$

Bemerkung ("Rechtsnebenklassen")
Sei $G = (G, \circ)$ unsere Gruppe, $H \leq G$
eine Untergruppe. Betrachte

$$g_1 \overset{R}{\sim} g_2 \Leftrightarrow g_2 \circ g_1^{-1} \in H (g_1, g_2 \in G)$$

Dies definiert eine Äquivalenzrelation.
Äquivalenzklasse von $g \in G$ ist $H \circ g = \{h \circ g \mid h \in H\}$.

$H \circ g$ heißt **Rechtsnebenklasse von H zu g.**

$$H\backslash G = \{H \circ g \mid H \circ g = \text{Rechtsnebenklasse zu } H\}$$

$$G = \bigcup_{g \in H\backslash G} H \circ g \ ^{11}$$

Bemerkung Ist $G = (G, \circ)$ kommutativ,
so stimmen natürlich Links- und Rechtsnebenklassen von H zu g überein:

$$g \circ H = \{g \circ h \mid h \in H\} = \{h \circ g \mid h \in H\} = H \circ g$$

Bemerkung Es besteht eine Bijektion

$$\psi : G/H \to H\backslash G$$

gegeben durch die Zuordnung

$$g \circ H \mapsto H \circ g$$

(prüfe zum Beispiel Injektivität & Surjektivität von ψ, oder beachte, dass eine Umkehrabbildung von ψ durch die Zuordnung $H \circ g \mapsto g \circ H$ gegeben ist)

$$\Rightarrow |G/H| = |G : H| = |H\backslash G|$$

0.2.25 Definition: Normalteiler

Sei $G = (G, \circ)$ eine Gruppe. Eine Untergruppe $N \leq G$ heißt **Normalteiler**, falls für alle $g \in G$ die Gleichheit

$$g \circ N = N \circ g$$

besteht, d.h.

$$g \circ N = \{g \circ n \mid n \in N\} = N \circ g = \{n \circ g \mid n \in N\}^{12}$$

Bemerkung $g \circ N = N \circ g \quad \forall g \in G$
$\Leftrightarrow g \circ N \circ g^{-1} = N \quad \forall g \in G$
$\Leftrightarrow g \circ N \circ g^{-1} \subseteq N \wedge\ g \circ N \circ g^{-1} \supseteq N \quad \forall g \in G$
$\Leftrightarrow g \circ n \circ g^{-1} \in N, n \in g \circ N \circ g^{-1} \quad \forall g \in G \quad \forall n \in N$
Voraussetzung $g \circ n \circ g^{-1} \in N \quad \forall g \in G \quad \forall n \in N$
Behauptung: $n \in g \circ N \circ g^{-1} \quad \forall g \in G$
Beweis: Wenn ich mit g die ganze Gruppe G durchlaufe, so durchläuft g^{-1} auch ganz G, d.h. die Inversenabbildung

$$G \to G, g \mapsto g^{-1}$$

ist bijektiv.

[11] g durchläuft ein vollständiges Repräsentantensystem der Rechtsnebenklassen von H.
[12] Dies gilt für Mengen und *nicht* für jedes einzelne Element.

Damit kann die Voraussetzung wie folgt reformuliert werden:

$$g^{-1} \circ n \circ g \in N \quad \forall g \in G, \forall n \in N$$

d.h. $\forall g \in G, \forall n \in N$ gilt:
$g^{-1} \circ n' \circ g = n \in N \quad \forall g \in G, \forall n \in N$ — multipliziere links mit g^{-1} und rechts mit g
$n' = g \circ g^{-1} \circ n' \circ g \circ g^{-1} = g \circ n \circ g^{-1} \in g \circ N \circ g^{-1} \quad \forall g \in G$

Die Definition ist äquivalent damit, zu zeigen:

$$g \circ n \circ g^{-1} \in N \quad \forall g \in G, \forall n \in N$$

Beispiel $S_3 = \left\{ \underbrace{\begin{pmatrix}123\\123\end{pmatrix}}_{\pi_1}, \underbrace{\begin{pmatrix}123\\231\end{pmatrix}}_{\pi_2}, \underbrace{\begin{pmatrix}123\\312\end{pmatrix}}_{\pi_3}, \underbrace{\begin{pmatrix}123\\132\end{pmatrix}}_{\pi_4}, \underbrace{\begin{pmatrix}123\\321\end{pmatrix}}_{\pi_5}, \underbrace{\begin{pmatrix}123\\213\end{pmatrix}}_{\pi_6}, \right\}$
$A_3 = \{\pi_1, \pi_2, \pi_3\} = \langle \pi_2 \rangle$
(nebenbei $|S_3| = 6, |A_3| = 3, (S_3 : A_3) = \frac{6}{3} = 2$).

Behauptung: A_3 ist Normalteiler von S_3.
Beweis: Zu zeigen: $\pi_j \circ A_3 = A_3 \circ \pi_j, (j = 1, \ldots, 6)$
zum Beispiel $j = 1, 2, 3$ gilt: $\pi_j \circ A_3 = A_3 = A_3 \circ \pi_j$
$\pi_4 \circ A_3 = \{\pi_4 \circ \pi_1, \pi_4 \circ \pi_2, \pi_4 \circ \pi_3\} = \{\pi_4, \pi_5, \pi_6\}$
$A_3 \circ \pi_4 = \{\pi_1 \circ \pi_4, \pi_2 \circ \pi_4, \pi_3 \circ \pi_4\} = \{\pi_4, \pi_6, \pi_5\}$
$\Rightarrow \pi_4 \circ A_3 = A_3 \circ \pi_4 \neq A_3$
Ebenso: $\pi_5 \circ A_3 = A_3 \circ \pi_5$ und $\pi_6 \circ A_3 = A_3 \circ \pi_6$
$\Rightarrow A_3$ ist Normalteiler in S_3.

$$S_3/A_3 = \{A_3,\ \pi_4 \circ A_3\}$$

Schreibweise Ist N Normalteiler in G, so schreiben wir dafür kurz

$$N \trianglelefteq G$$

Bemerkung Sei $G = (G, \circ)$ Gruppe und
$N \trianglelefteq G$ Normalteiler. Dann gilt

$$G/N = N \backslash G$$

$$g \circ N = N \circ g$$

0.2.26 Bemerkug/Definition: Faktorgruppe

Seien $G = (G, \circ)$ eine Gruppe und $N \trianglelefteq G$ ein Normalteiler. Dann wird durch

$$(g_1 \circ N) \bullet (g_2 \circ N) := (g_1 \circ g_2) \circ N, (g_1, g_2 \in G)$$

eine Verknüpfung definiert.
Behauptung:

1. $\bullet$ ist wohldefiniert, also unabhängig von der Wahl der Repräsentanten g_1, g_2 der (Links-) Nebenklassen.
2. $(G/N, \bullet)$ ist eine Gruppe.

Beweis

1. Seien g_1, g_1' bzw. g_2, g_2' Vertreter der Linksnebenklasse $g_1 \circ N$ bzw. $g_2 \circ N$.
   D.h. $g_1' \in g_1 \circ N \Leftrightarrow g_1' = g_1 \circ n_1, (n_1 \in N)$
   $g_2' \in g_2 \circ N \Leftrightarrow g_2' = g_2 \circ n_2, (n_2 \in N)$ [13]
   Zu zeigen $(g_1 \circ g_2) \circ N = (g_1' \circ g_2') \circ N$
   Berechne:
   $(g_1' \circ g_2') \circ N$
   $= ((g_1 \circ n_1) \circ (g_2 \circ n_2)) \circ N$
   $= ((g_1 \circ n_1 \circ g_2) \circ n_2) \circ N$
   $= \{(g_1 \circ n_1 \circ g_2) \circ (n_2 \circ n) \mid n \in N\}$ [14]
   $(g_1 \circ n_1 \circ g_2) \circ N$ [15]
   $= (g_1 \circ (g_2 \circ n_1') \circ N)$
   $= g_1 \circ g_2 \circ (n_1' \circ N)$
   $= g_1 \circ g_2 \circ N$
2. Die Verknüpfung $\bullet$ ist assoziativ:
   $((g_1 \circ N) \bullet (g_2 \circ N)) \bullet (g_3 \circ N) = ((g_1 \circ g_2) \circ N) \bullet (g_3 \circ N) = ((g_1 \circ g_2) \circ g_3) \circ N = (g_1 \circ (g_2 \circ g_3)) \circ N = (g_1 \circ N) \bullet ((g_2 \circ g_3) \circ N) = (g_1 \circ N) \bullet ((g_2 \circ N) \bullet (g_3 \circ N))$
   $N = e \circ N$ ist neutrales Element in $G/N \neq \emptyset$:
   $N \bullet (g \circ N) = (e \circ g) \circ N = g \circ N$
   Zu jedem $g \circ N \in G/N$ gibt es ein Inverses $g^{-1} \circ N$:
   $(g \circ N) \bullet (g^{-1} \circ N) = (g \circ g^{-1}) \circ N = e \circ N = N$
   Damit ist $(G/N, \bullet)$ eine Gruppe. $\square$

Die Gruppe $(G/N, \bullet)$ heißt **Faktorgruppe von** G/N.

0.2.27 Lemma: kanonische Projektion

Sei $G = (G, \circ)$ eine Gruppe und $N \trianglelefteq G$ ein Normalteiler in G. Dann wird durch die Zuordnung $\pi : G \to G/N$ mit $\pi(g) := g \circ N \quad \forall g \in G$ ein surjektiver Homomorphismus definiert. π heißt **natürliche** oder **kanonische Projektion**.

[13] $g_1 \sim g_1' \Leftrightarrow g_1^{-1} \circ g_1' = n_1 \in N$
[14] Unterbehauptung: $\{n_2 \circ n \mid n \in N\} = N$
Zu zeigen: durchläuft n ganz N, so durchläuft $n_2 \circ n$ ganz N
Zu zeigen: $N \to N, n \mapsto n_2 \circ n$ ist bijektiv
Injektiv: $n_2 \circ n = n_2 \circ n' \Rightarrow n' = n$ — Kürzen von n_2
Surjektiv: Sei $n' \in N$ beliebig; mit $n = n_2^{-1} \circ n' \in N$ folgt $n_2 \circ n = n_2 \circ (n_2^{-1} \circ n') = n'$.
[15] $N \trianglelefteq G : g_2 \circ N = N \circ g_2 \Leftrightarrow g_2 \circ n \circ g_2^{-1} \in N \quad \forall n \in N \Leftrightarrow g_2^{-1} \circ n \circ g_2 \in N \quad \forall n \in N$
Speziell für $n = n_1$: $g_2^{-1} \circ n_1 \circ g_2 = n_1' \in N \Rightarrow n_1 \circ g_2 = g_2 \circ n_1'$

Beweis $\pi(g_1 \circ g_2) = (g_1 \circ g_2) \circ N = (g_1 \circ N) \bullet (g_2 \circ N) = \pi(g_1) \bullet \pi(g_2)$. Die Surjektivität folgt, weil es zu jedem $g \circ N \in G/N$ ein $g \in G$ mit $\pi(g) = g \circ N$ gibt. □

Bemerkung Für die kanonische Projektion $\pi : G \to G/N$ gilt

$$\ker(\pi) = \{g \in G \mid \pi(g) = N\} = \{g \in G \mid g \circ N = N\} = N$$

0.2.28 Lemma: $\ker(f) \trianglelefteq G$

Seien G, H Gruppen und $f : G \to H$ ein Homomorphismus. Dann gilt:

$$\ker(f) \trianglelefteq G$$

Beweis siehe Serie 3, Aufgabe 3b)

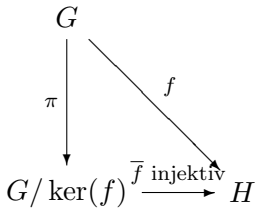
Beispiele

1. $G = (\mathbb{Z}, +), N = (n\mathbb{Z}, +), (n \in N, n \geq 1)$: $N \trianglelefteq G$ und es ist $G/N = \mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, n\mathbb{Z} + 1, \ldots, n\mathbb{Z} + (n-1)\}$ und
   $(n\mathbb{Z} + a) \bullet (n\mathbb{Z} + b) = n\mathbb{Z} + (a + b) = n\mathbb{Z} + \mathcal{R}_n(a + b)$
2. $G = S_3, N = A_3 = \langle(123)\rangle$: $A_3 \trianglelefteq S_3$, $(S_3 : A_3) = 2$ und es ist
   $S_3/A_3 = \{A_3, (23)A_3\} = \langle(23)A_3\rangle \cong \mathbb{Z}/2\mathbb{Z}$

0.2.29 Homomorphiesatz für Gruppen

Seien G, H Gruppen und $f : G \to H$ ein Homomorphismus.
Dann gibt es einen injektiven Homomorphismus $\overline{f} : G/\ker(f) \to H$ mit der Eigenschaft

$$\overline{f} \circ \pi = f$$



Beweis

1. Definition von $\overline{f} : G/\ker(f) \to H$: Die Abbildung

   $$\overline{f}(g \circ \ker(f)) := f(g) \quad \forall g \in G$$

   besitzt automatisch die obige Eigenschaft. Sie ist unabhängig von der Wahl des Repräsentanten der Nebenklasse und damit wohldefiniert, denn zu jedem $g' \in g \circ \ker(f)$ gibt es $n \in \ker(f)$ mit $g' = g \circ n$ und es folgt

   $$\overline{f}(g' \circ \ker(f)) = f(g') = f(g \circ n) = f(g) \circ f(n) = f(g) \circ e = f(g)$$

2. $\overline{f}$ ist Homomorphismus: Für $g_1, g_2 \in G$ gilt:
   $\overline{f}((g_1 \circ \ker(f)) \bullet (g_2 \circ \ker(f)))$
   $= \overline{f}((g_1 \circ g_2) \circ \ker(f))$
   $= f(g_1 \circ g_2)$
   $= f(g_1) \circ f(g_2)$
   $= \overline{f}(g_1 \circ \ker(f)) \circ \overline{f}(g_2 \circ \ker(f))$

3. $\overline{f}$ ist injektiv: Für $g_1, g_2 \in G$ sind äquivalent:
   $\overline{f}(g_1 \circ \ker(f)) = \overline{f}(g_2 \circ \ker(f))$
   $\Leftrightarrow f(g_1) = f(g_2)$
   $\Leftrightarrow e = f(g_1)^{-1} \circ f(g_2) = f(g_1^{-1} \circ g_2)$
   $\Leftrightarrow g_1^{-1} \circ g_2 \in \ker(f)$
   $\Leftrightarrow g_2 \in g_1 \circ \ker(f)$
   $\Leftrightarrow g_1 \circ \ker(f) = g_2 \circ \ker(f)$

□

Zusatz: Ist überdies f surjektiv, so ist $\overline{f}$ ein Isomorphismus, d.h.

$$G/\ker(f) \cong H$$

Beweis davon $\overline{f}$ ist bereits als injektiver Homomorphismus nachgewiesen, es bleibt die Surjektivität zu zeigen
Zu zeigen: Sei $h \in H$, dann gibt es ein $g \circ \ker(f) \in G/\ker(f)$ mit

$$\overline{f}(g \circ \ker(f)) = h$$

Da f surjektiv ist, gibt es ein $g \in G$ mit $f(g) = h$. Mit $g \circ \ker(f) \in G/\ker(f)$ berechnen wir: $\overline{f}(g \circ \ker(f)) = f(g) = h$. Dies beweist die Surjektivität. □

Beispiel Seien $G = (\mathbb{Z}, +), H = (\mathcal{R}, \oplus)$.

$$f : \mathbb{Z} \to \mathcal{R}_n$$

$$a \mapsto \mathcal{R}_n(a)$$

Das ist ein surjektiver Homomorphismus.
Wir zeigen:

$$\ker(f) = \{a \in \mathbb{Z} \mid \mathcal{R}_n(a) = 0\} = n\mathbb{Z}$$

Aus dem Homomorphiesatz folgt: $\mathbb{Z}/n\mathbb{Z} \cong \mathcal{R}_n$.

0.3 Ringe und Körper

0.3.1 Definition: Ring

Eine nicht-leere Menge R mit einer additiven Verknüpfung $+$ und einer multiplikativen Verknüpfung $\cdot$ heißt ein **Ring**, falls folgende Eigenschaften erfüllt sind:

1. $(R, +)$ ist eine kommutative Gruppe (wir bezeichnen das neutrale Element bzgl $+$ durch 0 und nennen es **Nullelement**).

2. $(R, \cdot)$ ist eine Halbgruppe, (also ist $(R, +, \cdot)$ im allgemeinen weder kommutativ, noch besitzt es ein neutrales Element bezüglich $\cdot$)

3. Für $a, b, c \in R$ gelten die Distributivgesetze:

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

   Da $\cdot$ stärker bindet als $+$, schreiben wir auch:

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

Beispiele

1. $R = (R, +, \cdot)$ gegeben durch
   $\mathbb{Z} = (\mathbb{Z}, +, \cdot)$ ist ein Ring, da $(\mathbb{Z}, +)$ abelsche Gruppe und $(\mathbb{Z}, \cdot)$ Halbgruppe ist. Bekanntlich gelten die Distributivgesetze.

2. $\mathcal{R}_n = \{0, 1, \ldots, n-1\}$.
   $\oplus$ Addition auf $\mathcal{R}_n$: $(\mathcal{R}_n, \oplus)$ ist abelsche Gruppe.
   $\odot$ Multiplikation auf $\mathcal{R}_n$ definiert durch: $a \odot b = R_n(a \cdot b) \in \mathcal{R}_n, (a, b \in \mathcal{R}_n)$. Diese Multiplikation ist assoziativ.
   $\Rightarrow (\mathcal{R}_n, \oplus, \odot)$ ist ein Ring. (prüfe noch Distributivität!)

3. $R = (2\mathbb{Z}, +, \cdot) \not\ni 1$ ist ein (kommutativer) Ring ohne Einselement.

Bemerkungen

1. Ein Ring $R = (R, +, \cdot)$ heißt **kommutativ**, falls für alle $a, b \in R$ gilt

   $$a \cdot b = b \cdot a$$

   d.h. die Halbgruppe $(R, \cdot)$ ist kommutativ.

2. Falls ein neutrales Element bzgl. $\cdot$ in $R = (R, +, \cdot)$ existiert, so nennen wir dieses **Einselement** und bezeichnen es durch 1.

Nebenbemerkung In dieser Vorlesung soll jeweils $0 \neq 1$ gelten, d.h. ein Ring $R = (R, +, \cdot)$ mit Einselement besitzt mindestens zwei Elemente.

Bezeichnungsweisen Sei $R = (R, +, \cdot)$ ein Ring.

1. Wenn $a \in R$, so bedeutet $-a \in R$ das **additiv Inverse**, d.h. $a + (-a) = 0$.
2. Wenn $a \in R$ und ein **multiplikativ Inverses** besitzt, [16] so schreiben wir dieses als a^{-1} oder $\frac{1}{a}$. Also gilt $a^{-1} \cdot a = a \cdot a^{-1} = 1$.
3. Seien $a, b \in R$, so heißt
$$a - b := a + (-b)$$
die **Differenz** von a und b.

0.3.2 Lemma: Rechenregeln in Ringen

Es sei $R = (R, +, \cdot)$ ein beliebiger Ring.
Dann gelten für a, b, c folgende Rechenregeln:

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b) = -a \cdot b$
3. $(-a) \cdot (-b) = a \cdot b$
4. $a \cdot (b - c) = a \cdot b - a \cdot c$
5. $(b - c) \cdot a = b \cdot a - c \cdot a$

Beweis Serie 4, Aufgabe 3

0.3.3 Definition: rechter/linker Nullteiler

Ein Element $a \neq 0$ eines Ringes $R = (R, +, \cdot)$ heißt **linker Nullteiler von** R, wenn ein $b \in R, b \neq 0$, existiert, so dass $a \cdot b = 0$ ist.
Entsprechend definiert man **rechte Nullteiler**.
Wenn a sowohl rechter als auch linker Nullteiler ist, so nennt man a **Nullteiler von** R.
Ein Ring $R = (R, +, \cdot)$ ohne Nullteiler heißt **nullteilerfrei**.

Beispiele

1. Der Ring $(\mathbb{Z}, +, \cdot)$ ist nullteilerfrei.
2. $R = \mathcal{R}_6 = \{0, 1, \ldots, 5\} \ni 2, 3 \neq 0$.
$2 \odot 3 = 0$. d.h. $2, 3$ sind Nullteiler in $\mathcal{R}_6$.

0.3.4 Definition: Integritätsbereich

Ein *kommutativer, nullteilerfreier* Ring $R = (R, +, \cdot)$ heißt **Integritätsbereich**.

[16] Vorausgesetzt: Ring mit Einselement

Beispiele

1. $R = \mathbb{Z}$ ist Integritätsbereich.
2. $R = (\mathbb{Q}, +, \cdot)$, $R = (\mathbb{R}, +, \cdot)$, $R = (\mathbb{C}, +, \cdot)$ sind alles Integritätsbereiche.
   [17] $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

0.3.5 Definition: (Rechts-/Links-)Inverses

Sei $R = (R, +, \cdot)$ ein Ring mit Einselement 1. Sei weiter $a \in R$. Ein $b \in R$ heißt **Rechtsinverses von** a, falls $a \cdot b = 1$. Entsprechend wird **Linksinverses** definiert.
Ist das Rechtsinverse gleich dem Linksinversen, so spricht man vom **Inversen**.

0.3.6 Definition: Einheit

Ist $a \in R$ und besitzt a ein Inverses (in R), so heißt a eine **Einheit in** R.

Bezeichnung Ist $R = (R, +, \cdot)$ ein Ring mit 1, so wird mit $R^\times$ die Menge der Einheiten bezeichnet.

Beispiel

1. $R = \mathbb{Z} : \mathbb{Z}^\times = \{+1, -1\}$
2. $R = \mathbb{Q} : \mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$
   $R = \mathbb{R} : \mathbb{R}^\times = \mathbb{R} \setminus \{0\}$
   $R = \mathbb{C} : \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$
3. $R = \mathcal{R}_6 : \mathcal{R}_6^\times = \{1, 5\}$

0.3.7 Bemerkung / Definition: Einheitengruppe

Die Menge der Einheiten $R^\times$ eines Rings $R = (R, +, \cdot)$ mit Einselement 1 ist eine (multiplikative) Gruppe.
Sie wird die **Einheitengruppe von** R genannt. [18]

0.3.8 Definition: Schiefkörper, Körper

Sei $R = (R, +, \cdot)$ ein Ring mit Einselement.
Falls $R^\times = R \setminus \{0\}$ gilt, d.h. alle $a \in R, a \neq 0$, besitzen ein multiplikativ Inverses, dann wird $R = (R, +, \cdot)$ ein **Schiefkörper** genannt. Ein kommutativer Schiefkörper heißt **Körper**.

[17] Hier stand vorher statt $\mathbb{C}$ noch einmal $\mathbb{Z}$. Nachprüfen.
[18] zu Aufgabe 5: $\mathbb{Z}/m\mathbb{Z} \leftrightarrow \mathcal{R}_m$ und $(\mathbb{Z}/m\mathbb{Z})^\times \leftrightarrow \mathcal{R}_m^\times$

Beispiele

1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper.
2. $\mathcal{R}_2 = \{0, 1\}$ mit

$\oplus$	0	1
0	0	1
1	1	0

$\odot$	0	1
0	0	0
1	0	1

ist ein Körper.

Einschub Körper mit endlich vielen Elementen !?
Wir kennen die Körper $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Vorbemerkung Kandidaten sind $\mathcal{R}_n$ für gewisse $n \in \mathbb{N}, n > 0$. zum Beispiel

- $\mathcal{R}_2$ ist ein Körper
- $\mathcal{R}_6$ ist kein Körper

"Falls ein Ring Nullteiler hat, so kann er kein Körper sein:"
$2, 3$ sind Nullteiler von $\mathcal{R}_6 \Rightarrow 2 \odot 3 = 0 \quad (*)$
Wäre $\mathcal{R}_6$ ein Körper, so besäße insbesondere 2 ein multiplikativ Inverses $a (= 2^{-1})$ in $\mathcal{R}_6$, d.h. $a \odot 2 = 1$.
Multipliziere (*) von links mit a:
$(a \odot 2) \odot 3 = a \odot 0 \Rightarrow 3 = 0$
Das ist ein Widerspruch zur Eindeutigkeit des Nullelements, $\mathcal{R}_6$ ist also kein Körper.

0.3.9 Definition: Teilbarkeit in $\mathbb{Z}$, (größter) gemeinsamer Teiler

1. Seien $a, b \in \mathbb{Z}, b \neq 0$
   b **teilt** a, in Zeichen $(b|a) :\Leftrightarrow \exists c \in \mathbb{Z} : a = b \cdot c$
2. Für $a, b \in \mathbb{Z}, d \neq 0$
   d heißt **gemeinsamer Teiler von** $a, b :\Leftrightarrow d|a$ und $d|b$
3. Seien $a, b \in \mathbb{Z}$ nicht beide Null
   $d \in \mathbb{N}$ heißt **größter gemeinsamer Teiler von** $a, b :\Leftrightarrow$
   - d ist gemeinsamer Teiler von a, b
   - $\forall n \in \mathbb{N} : n|a, n|b \Rightarrow n|d$

Schreibweise $(a, b) = \mathrm{ggT}(a, b) =$ größter gemeinsamer Teiler von a, b.

0.3.10 Berechnung des ggT über Primfaktorzerlegung:

$a \in \mathbb{Z}, (a \neq 0) : a = \prod\limits_{p \in \mathbb{P}} p^{\alpha_p}$
wobei $\alpha_p \in \mathbb{N}$, für fast alle p ist $\alpha_p = 0$.

$a = 44 : a = +2^2 \cdot 11^1$
$b = 16 : b = 2^4 \cdot 11^0$
$\Rightarrow (a, b) = 2^2 = 4$

Allgemein: $a = \pm \prod\limits_{p \in \mathbb{P}} p^{\alpha_p}$, $b = \pm \prod\limits_{p \in \mathbb{P}} p^{\beta_p}$, $(a, b) = + \prod\limits_{p \in \mathbb{P}} p^{\min\{\alpha_p, \beta_p\}}$

0.3.11 Euklidischer Algorithmus

Seien $a, b \in \mathbb{Z}, b \neq 0$. Fortgesetzte Division mit Rest führt zu folgendem Schema:

(-1). $a = q_1 b + r_1 \quad 0 \leq r_1 < |b|$

0. $b = q_2 r_1 + r_2 \quad 0 \leq r_2 < r_1$

1. $r_1 = q_3 r_2 + r_3 \quad 0 \leq r_3 < r_2$

2. $r_2 = q_4 r_3 + r_4 \quad 0 \leq r_4 < r_3$
$\vdots$

(n-2). $r_{n-2} = q_n r_{n-1} + r_n \quad 0 \leq r_n < r_{n-1}$

(n-1). $r_{n-1} = q_{n+1} r_n + 0$ (r_n ist der letzte, von Null verschiedene Rest.)

Dann gilt:

$$r_n = (a, b)$$

Dann finden sich $x, y \in \mathbb{Z}$, so dass:

$$(a, b) = r_n = x \cdot a + y \cdot b$$

Achtung: x, y sind dabei nicht eindeutig bestimmt.

Beispiel $a = 44, b = 15$
$44 = 2 \cdot 16 + 12$
$16 = 1 \cdot 12 + 4$
$12 = 3 \cdot \boxed{4} + 0$
$n = 2, r_2 = (44, 16) = 4$

Berechnung von x und y:
$4 = 16 - 1 \cdot 12 = 16 - 1 \cdot (44 - 2 \cdot 16) = (-1) \cdot 44 + 3 \cdot 16$

Beweis Zu zeigen: $r_n = (a, b)$, d.h. r_n ist gemeinsamer Teiler und r_n ist maximal damit.

I(n-1). $r_n | r_{n-1}$

(n-2). $r_n | r_{n-2}$ [19]

$\vdots$

2. $r_n | r_2$

1. $r_n | r_1$

0. $r_n | b$

-1. $r_n | a$

II. Sei t ein beliebiger gemeinsamer Teiler von a, b.
zz: $t | r_n$

-1. $t | r_1$ [20]

0. $t | r_2$

1. $t | r_3$

$\vdots$

n-3. $t | r_{n-1}$

n-2. $t | r_n$

zurück zum Ausgangsproblem

1. Betrachte $\mathcal{R}_n = (\mathcal{R}_n, \oplus, \odot)$ für $n \notin \mathbb{P}$, d.h. $n = n_1 n_2$, wobei $n_i \neq 1, (i = 1, 2)$.
   Behauptung: $\mathcal{R}_n$ ist kein Körper.
   Beweis: n_1 ist Nullteiler von $\mathcal{R}_n$, denn $n_1 \odot n_2 = 0$ (in $\mathcal{R}_n$).

2. *Satz:* Sei $p \in \mathbb{P}$. Dann ist der Ring $\mathcal{R}_p = (\mathcal{R}_p, \oplus, \odot)$ ein Körper.
   Beweis: $\mathcal{R}_p^\times = \mathcal{R}_p \setminus \{0\}$
   $\Leftrightarrow$ jedes von Null verschiedene $a \in \mathcal{R}_p$ besitzt ein multiplikativ Inverses in $\mathcal{R}_p$.
   $a \in \{1, 2, \ldots, p-1\} = \mathcal{R}_p \setminus \{0\} \Rightarrow (a, p) = 1$
   Nach dem vorhergehenden Satz folgt (mit $b = p$): $\exists x, y \in \mathbb{Z} : x \cdot a + y \cdot p = 1$
   $\Rightarrow R_p(1) = R_p(x \cdot a + y \cdot p) = R_p(x \cdot a) = R_p(x) \odot a$
   $\Rightarrow R_p(x) \odot a = 1$
   $\Rightarrow \mathcal{R}_p$ ist ein Körper. $\square$

[19] $r_{n-2} = q_n r_{n-1} + r_n = q_n q_{n+1} r_n + r_n = r_n(1 + q_n q_{n+1})$

[20] $t | a \Rightarrow a = a' \cdot t$
$t | b \Rightarrow b = b' \cdot t$
$a = q_1 b + r_1 \Rightarrow$
$r_1 = a q_1 + b = t(q' - q_1 b')$

Beispiel $p = 7$.
$\mathcal{R}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
$1, 2, 3, 4, 5, 6$ besitzen ein multiplikativ Inverses in $\mathcal{R}_7$ (bzgl. $\odot$).

Euklidischer Algorithmus:
Beachte zum Beispiel $2 \in \mathcal{R}_7$, $(2, 7) = 1$
$\Rightarrow \exists x, y \in \mathbb{Z} : 2x + 7y = 1$
zum Beispiel wähle $x = 4, y = -1 : 2 \cdot 4 + 7 \cdot (-1) = 1$
$\Rightarrow 2 \odot 4 = 1$
$\Rightarrow 4 \in \mathcal{R}_7$ ist multiplikativ Inverses von $w \in \mathcal{R}_7$

0.3.12 Definition: Unterring

Sei $(R, +, \cdot)$ ein beliebiger Ring.
Eine Teilmenge $U \subseteq R$ heißt **Unterring von** R, falls U mit den von R induzierten Strukturen (Addition, Multiplikation) selbst wieder ein Ring ist. In Zeichen

$$U \leq R$$

Bemerkung $U \leq R \Leftrightarrow (U, +|_U, \cdot|_U)$ ist ein Ring, d.h.

1. $(U, +|_U)$ ist abelsche Gruppe: $(U, +|_U)$ ist Untergruppe von $(R, +)$
2. $(U, \cdot|_U)$ ist Halbgruppe.
3. (ergibt sich schon aus R) Es gelten die Distributivgesetze.

Beispiel

1. $R = (\mathbb{Z}, +, \cdot)$
   $U = (3\mathbb{Z}, +, \cdot)$
   U ist Unterring von R
2. $R = (\mathbb{Q}, +, \cdot)$
   $U = (\mathbb{Z}, +, \cdot)$
   $U \leq R$

0.3.13 Definition: (Ring-) Homomorphismus

Seien $R = (R, +_R, \cdot_R)$ und $S = (S, +_S, \cdot_S)$ Ringe.
Eine Abbildung $f : R \to S$ heißt **Ringhomomorphismus von** R **nach** S, falls für $r_1, r_2 \in R$ gilt:

$$f(r_1 +_R r_2) = f(r_1) +_S f(r_2) \text{ (Strukturtreue bzgl. Addition)}$$

$$f(r_1 \cdot_R r_2) = f(r_1) \cdot_S f(r_2) \text{ (Strukturtreue bzgl. Multiplikation)}$$

Ist f bijektiv, so heißt f **Ringisomorphismus**. In Zeichen: $R \cong S$ [21]

[21] Bei Ringen mit Einselement 1 ist zusätzlich wichtig, dass $f(1) = 1$.

0.3.14 Definition: Kern, Bild

Seien $R = (R, +_R, \cdot_R)$ und $S = (S, +_S, \cdot_S)$ Ringe und $f : R \to S$ ein Ringhomomorphismus.
Dann heißt die Menge

$$\ker(f) = \{r \in R \mid f(r) = 0_S\}^{22}$$

der **Kern von** f ($\ker(f) \subseteq R$).

Weiter heißt die Menge

$$\mathrm{im}(f) = \{s \in S \mid \exists r \in R : f(r) = s\}$$

das **Bild von** f ($\mathrm{im}(f) \subseteq S$).

Beispiele

1. $R = \mathbb{Z}, S = \mathbb{Q}$, $f : \mathbb{Z} \to \mathbb{Q}$, gegeben durch $a \mapsto \frac{a}{1}$
   f ist Ringhomomorphismus, da:
   $a, b, \in \mathbb{Z} : f(a + b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b)$
   $a, b, \in \mathbb{Z} : f(a \cdot b) = \frac{a \cdot b}{1} = \frac{a}{1} \cdot \frac{b}{1} = f(a) \cdot f(b)$
   $\ker(f) = \{a \in \mathbb{Z} \mid f(a) = 0\} = \{a \in \mathbb{Z} \mid \frac{a}{1} = 0\} = \{0\}$. ($\Rightarrow f$ injektiv)
   $\mathrm{im}(f) \cong \mathbb{Z}$ [23] $\qquad \mathbb{Z} \xrightarrow{f} \mathrm{im}(f) \leq \mathbb{Q}$

2. $R = (\mathbb{Z}, +, \cdot)$, $S = (\mathcal{R}_n, \oplus, \odot)$, $f : \mathbb{Z} \to \mathcal{R}_n$, gegeben durch $a \mapsto R_n(a)$.
   Schon erkannt: $f(a + b) = f(a) \oplus f(b)$ für $a, b \in \mathbb{Z}$
   $R_n(a + b) = R_n(R_n(a) + R_n(b))$.
   Ebenso verifiziert man: $f(a \cdot b) = f(a) \cdot f(b)$ für $a, b \in \mathbb{Z}$.
   (d.h. $R_n(a \cdot b) = R_n(R_n(a) \cdot R_n(b))$).
   $\Rightarrow f$ ist Ringhomomorphismus.

   $\mathrm{im}(f) = \mathcal{R}_n$, d.h. f ist surjektiv.
   $\ker(f) = n\mathbb{Z}$

0.3.15 Lemma: $\ker(f)$ ist Unterring von R, $\mathrm{im}(f)$ ist Unterring von S

Seien R, S Ringe und $f : R \to S$ ein Ringhomomorphismus.
Dann ist $\ker(f)$ ein Unterring von R und $\mathrm{im}(f)$ ein Unterring von S.

Beweis (Skizze) Wir zeigen: $\ker(f)$ ist Unterring von R.

1. Zunächst ist per Definitionem: $\ker(f) \subseteq R$.

2. $(\ker(f), +_{\ker(f)}) \leq (R, +)$, d.h. ist Untergruppe.
   Dies wissen wir bereits aus der Gruppentheorie! (Übungsaufgabe).

[22] 0_S = Nullelement in S
[23] wir können das auch "identifizieren" und sagen $\mathrm{im}(f) = \mathbb{Z}$

3. $(\ker(f), \cdot_{\ker(f)})$ ist Halbgruppe:
   zz: die Abgeschlossenheit, d.h.
   $r_1, r_2 \in \ker(f) \Rightarrow r_1 \cdot r_2 \in \ker(f)$.
   Dazu beachten wir: $f(r_1) = 0 = f(r_2)$
   $\Rightarrow f(r_1 \cdot_R r_2) = f(r_1) \cdot_S f(r_2) = 0_S \cdot_S 0_S = 0_S$.
   $\Rightarrow r_1 \cdot r_2 \in \ker(f) \Rightarrow$ Abgeschlossenheit

4. Distributivität wird von R geerbt.

Ab jetzt: Seien die betrachteten Ringe immer kommutativ.

0.3.16 Definition: Ideal

Seien $R = (R, +, \cdot)$ ein kommutativer Ring und $\mathfrak{a} \subseteq R$ eine Teilmenge.

Die Teilmenge $\mathfrak{a}$ heißt **Ideal von** R, falls gilt:

1. $(\mathfrak{a}, +) \leq (R, +)$, d.h. $\mathfrak{a}$ ist eine Untergruppe von R.

2. $R \cdot \mathfrak{a} = \mathfrak{a} = \mathfrak{a} \cdot R$, d.h.
   $r \cdot a \in \mathfrak{a} \quad \forall r \in R, \forall a \in \mathfrak{a} \quad$ und $\quad a \cdot r \in \mathfrak{a} \quad \forall r \in R, \forall a \in \mathfrak{a}$

Bemerkung Ein Ideal $\mathfrak{a}$ in R ist insbesondere ein Unterring in R.

Beispiel

1. $R = \mathbb{Z}, \mathfrak{a} = n\mathbb{Z}$ ist Ideal.
   Es ist $(n\mathbb{Z}, +) \leq (\mathbb{Z}, +)$ Untergruppe, weiter zu zeigen: $r \in \mathbb{Z}, a \in n\mathbb{Z} \Rightarrow r \cdot a \in n\mathbb{Z}$.
   Beweis:: $r \in \mathbb{Z}, a \in n \cdot \mathbb{Z} \Rightarrow r \cdot a \in n\mathbb{Z}$.
   $a \cdot r = r \cdot a = r(n \cdot v) \in n \cdot \mathbb{Z} \Rightarrow n \cdot \mathbb{Z}$ ist Ideal von $\mathbb{Z} \in \mathbb{Z}$

2. Sei $R = (R, +, \cdot)$ beliebiger kommutativer Ring.
   Für alle $r_0 \in R$ sei $\mathfrak{a} = r_0 \cdot R = \{r_0 \cdot r \mid r \in R\}$
   Behauptung: $\mathfrak{a}$ ist Ideal in R
   Beweis:

   a) $(\mathfrak{a}, +) \leq (R, +)$ Untergruppenkriterium
      $r_1, r_2 \in R, r_i = r_0 r_i', r_i' \in R$
      $r_1 - r_2 = r_0 \cdot r_1' - r_0 \cdot r_2' = r_0 \cdot (r_1' - r_2') \in \mathfrak{a}$
   b) $a = r_0 \cdot r' (a \in \mathfrak{a}), r \in R$
      $\Rightarrow a \cdot r = r_0 \cdot r' \cdot r = r_0(r \cdot r') \in \mathfrak{a}$

Bemerkung

1. $R = (R, +, \cdot)$ kommutativer Ring und $\mathfrak{a} = r_0 \cdot R, (r_0 \in R, \text{ fixiert})$
   Ideale dieser Form heißen **Hauptideale**. Man schreibt sie auch in der Form

   $$\mathfrak{a} = (r_0)$$

2. Sei $R = \mathbb{Z}$, zunächst

   $$b|a :\Leftrightarrow (b) \supseteq (a)$$

   Sei R beliebiger kommutativer Ring; und $\mathfrak{a}, \mathfrak{b} \subseteq R$ Ideale.
   Definiere $\mathfrak{b}|\mathfrak{a} :\Leftrightarrow \mathfrak{b} \supseteq \mathfrak{a} \Rightarrow$ algebraische Zahlentheorie.

3. Seien $f : R \to S$ ein Homomorphismus von Ringen.
   Behauptung: $\ker(f)$ ist ein Ideal in R.
   Beweis:

   a) $(\ker(f), +) \leq (R, +)$ ist eine Untergruppe (s. Gruppentheorie)

   b) zu zeigen:
   $r \in R; t \in \ker(f)$
   $\Rightarrow r \cdot t = t \cdot r \in \ker(f)$
   Dies ist richtig, da:
   $t \in \ker(f) \Rightarrow f(t) = 0_S$.
   Somit folgt:
   $f(r \cdot_R t) = f(r) \cdot_S f(t) = f(r) \cdot_S 0_S = 0_S$
   $\Rightarrow r \cdot t = t \cdot r \in \ker(f)$
   $\Rightarrow \ker(f)$ ist Ideal in R.

0.3.17 Definition: Faktorgruppe $(R/\mathfrak{a}, +)$

Seien $R = (R, +, \cdot)$ ein kommutativer Ring und $\mathfrak{a} \subseteq R$ ein Ideal.
Insbesondere wissen wir nach Definition, dass $(\mathfrak{a}, +) \leq (R, +)$, also—da abelsche Gruppen vorliegen—ist $(\mathfrak{a}, +) \trianglelefteq (R, +)$.
Wir können nun—bzgl $+$—die Faktorgruppe

$$(R/\mathfrak{a}, +)$$

bilden. Die additive Struktur $+$ auf $R/\mathfrak{a}$ ist dabei wie folgt gegeben:

$$(r_1 + \mathfrak{a}) + (r_2 + \mathfrak{a}) = (r_1 + r_2) + \mathfrak{a}, (r_1, r_2 \in R)$$

0.3.18 Definition einer multiplikativen Stuktur auf $(R/\mathfrak{a}, +)$

$$(r_1 + \mathfrak{a}) \cdot (r_2 + \mathfrak{a}) := (r_1 \cdot r_2) + \mathfrak{a}, (r_1, r_2 \in R)$$

Beweis

1. Wohldefiniertheit, d.h. Unabhängigkeit von der Wahl der Repräsentanten $r_1, r_2 \in R$, über welche das Produkt definiert wurde (vgl. Serie 5, Aufgabe 3).

2. Ist $(R/\mathfrak{a}, +, \cdot)$ ein Ring?

Beachte G kommutative Gruppe, $U \leq G$ Untergruppe $\Rightarrow U \trianglelefteq G$
$g \circ u \circ g^{-1} \in U \quad \forall g \in G, \forall u \in U \Leftrightarrow g \circ g^{-1} \circ u = u \in U$
Wir haben (aufgrund der Kommutativität der Addition), dass $(\mathfrak{a}, +) \trianglelefteq (R, +)$.
Betrachte die Faktorgruppe [24]

$$(R/\mathfrak{a}, +)$$

Die Addition + auf $R/\mathfrak{a}$ ist gegeben durch

$$(r_1 + \mathfrak{a}) + (r_2 + \mathfrak{a}) := (r_1 + r_2) + \mathfrak{a} \quad (r_1, r_2 \in R)$$

Damit wird $(R/\mathfrak{a}, +)$ zu einer abelschen Gruppe.

Wunsch: Führe auf $R/\mathfrak{a}$ noch eine Multiplikation ein!

Kandidat für Multiplikation $(r_1 + \mathfrak{a}) \cdot (r_2 + \mathfrak{a}) := (r_1 \cdot r_2) + \mathfrak{a} = r_1 \cdot r_2 + \mathfrak{a} \quad (r_1, r_2 \in R)$

Vorsicht Diese Definition hängt von der Wahl der Repräsentanten r_1, r_2 der Nebenklassen $r_1 \circ \mathfrak{a}, r_2 \circ \mathfrak{a}$ ab. Zur Wohldefiniertheit ist also die Unabhängigkeit von der Wahl der Repräsentanten zu prüfen, dazu wird wesentlich die Idealeigenschaft (2) gebraucht (siehe Aufgabe 3, Serie 5).
$(R/\mathfrak{a}, +, \cdot)$ hat folgende Eigenschaften:

1. $(R/\mathfrak{a}, +)$ ist eine abelsche Gruppe (mit neutralem Element $0 + \mathfrak{a} = 0$).

2. $(R/\mathfrak{a}, \cdot)$ ist eine abelsche Halbgruppe. [25]

3. Es gelten die Distributivgesetze.
   Zum Beispiel seien $r_1, r_2, r_3 \in R$
   $$\begin{aligned}
   &(r_1 + \mathfrak{a}) \cdot ((r_2 + \mathfrak{a}) + (r_3 + \mathfrak{a})) \\
   &\underset{\text{Def.}+}{=} (r_1 + \mathfrak{a}) \cdot ((r_2 + r_3) + \mathfrak{a}) \\
   &\underset{\text{Def.}\cdot}{=} (r_1 \cdot (r_2 + r_3)) + \mathfrak{a} \\
   &\underset{\text{Distrib.}R}{=} (r_1 \cdot r_2 + r_1 \cdot r_3) + \mathfrak{a} \\
   &\underset{\text{Def.}+}{=} ((r_1 \cdot r_2) + \mathfrak{a}) + ((r_1 \cdot r_3) + \mathfrak{a}) \\
   &\underset{\text{Def.}\cdot}{=} (r_1 + \mathfrak{a}) \cdot (r_2 + \mathfrak{a}) + (r_1 + \mathfrak{a}) \cdot (r_3 + \mathfrak{a})
   \end{aligned}$$
   Ebenso beweist man Rechtsdistributivität.

[24] bei $G = (G, \circ)$ ist $G/U = (G/U, \bullet)$ def

[25] Die Assoziativität und Kommutativität der Multiplikation auf $R/\mathfrak{a}$ wird von der Multiplikation auf R geerbt.

0.3.19 Definition: Faktorring $(R/\mathfrak{a}, +, \cdot)$

Seien $R = (R, +, \cdot)$ ein kommutativer Ring und $\mathfrak{a} \subseteq R$ ein Ideal.
Dann nennen wir

$$(R/\mathfrak{a}, +, \cdot)$$

den **Faktorring von R nach (dem Ideal) $\mathfrak{a}$**, kurz R **modulo $\mathfrak{a}$**.

Beispiel $R = \mathbb{Z}, \mathfrak{a} = n\mathbb{Z} = (n), (n \in \mathbb{N}, n > 0)$
Wir haben den Faktorring

$$R/\mathfrak{a} = \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

$\overline{0} = n\mathbb{Z}$
$\overline{1} = 1 + n\mathbb{Z}$
Seien $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$,
$\overline{a} + \overline{b} = \overline{a + b} = \overline{R_n(a + b)}$
$\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{R_n(a \cdot b)}$

Bemerkung: Kanonischer Ringhomomorphismus $R = (R, +, \cdot)$ kommutativer Ring, $\mathfrak{a} \subseteq R$ Ideal. Definiere folgende Abbildung:

$$\pi : R \to R/\mathfrak{a}$$

$$r \mapsto r + \mathfrak{a}$$

Behauptung: π ist Ringhomomorphismus, also

1. $\pi(r_1 + r_2) = \pi(r_1) + \pi(r_2)$
2. $\pi(r_1 \cdot r_2) = \pi(r_1) \cdot \pi(r_2)$

Beweis:

1. $\pi(r_1 + r_2) \underset{\text{Def. } \pi}{=} (r_1 + r_2) + \mathfrak{a} \underset{\text{Def. + in } R/\mathfrak{a}}{=} (r_1 + \mathfrak{a}) + (r_2 + \mathfrak{a}) \underset{\text{Def. rückwärts}}{=} \pi(r_1) + \pi(r_2)$
2. $\pi(r_1 \cdot r_2) \underset{\text{Def. } \pi}{=} (r_1 \cdot r_2) + \mathfrak{a} \underset{\text{Def. } \cdot \text{ in } R/\mathfrak{a}}{=} (r_1 + \mathfrak{a}) \cdot (r_2 + \mathfrak{a}) \underset{\text{Def. rückwärts}}{=} \pi(r_1) \cdot \pi(r_2)$ $\square$

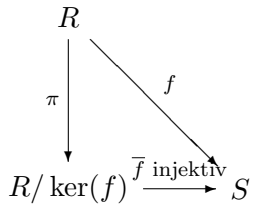
0.3.20 Homomorphiesatz für Ringe

Seien R, S kommutative Ringe und $f : R \to S$ ein Ringhomomorphismus.
Dann existiert ein injektiver Ringhomomorphismus

$$\overline{f} : R/\ker(f) \to S$$

mit der Eigenschaft

$$\overline{f}(r + \ker(f)) = f(r) \quad \forall r \in R$$



Beweis Vergessen Sie zunächst die multiplikative Struktur.

Dann besteht nach dem Homomorphiesatz für Gruppen (nämlich $(R,+),(S,+),f : (R,+) \to (S,+)$) ein injektiver Gruppenhomomorphismus:

$$\overline{f} : (R/\ker(f),+) \to (S,+)$$

Das einzige, was zu prüfen bleibt, ist die Multiplikativität von $\overline{f}$, d.h.

$$\overline{f}((r_1+\ker(f))\cdot(r_2+\ker(f))) \stackrel{?}{=} \overline{f}(r_1+\ker(f))\cdot\overline{f}(r_2+\ker(f))$$

$\overline{f}((r_1+\ker(f))\cdot(r_2+\ker(f))) = \overline{f}(r_1\cdot r_2+\ker(f)) \underset{\text{Def. von } \overline{f}}{=} f(r_1\cdot r_2) \underset{\text{Multiplikativität von } f}{=}$
$f(r_1)\cdot f(r_2) \underset{\text{Def. von } \overline{f}}{=} \overline{f}(r_1+\ker(f))\cdot\overline{f}(r_2+\ker(f))$ □

Zusatz Seien R,S kommutative Ringe und $f : R \to S$ ein *surjektiver* Ringhomomorphismus, dann ist

$$\overline{f} : R/\ker(f) \to S$$

ein Ringisomorphismus, in Zeichen

$$R/\ker(f) \cong S$$

Beispiel

1. $R=\mathbb{Z}, S=\mathcal{R}_n$, $f : \mathbb{Z} \to \mathcal{R}_n$, gegeben durch $a \mapsto R_n(a)$ ist Ringhomomorphismus, surjektiv.
   $\ker(f) = n\mathbb{Z}$.
   Homomorphiesatz für Ringe (Zusatz):

   $$\mathbb{Z}/n\mathbb{Z} \cong \mathcal{R}_n$$

   Speziell: $n = p$ = Primzahl: $\mathcal{R}_p$ ist Körper.
   $\Rightarrow \mathbb{Z}/p\mathbb{Z}$ ist Körper.
   Bemerkung: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ist Körper mit p Elementen. [26]

[26] $\mathbb{F}_p$, da Körper = field

2. Sei K Körper.
   $K[X] = \{\sum_{j=0}^{n} a_j X^j = a_n X^n + a_{n-1} X^{n-1} + \dots a_1 X + a_0 \mid a_n, \dots, a_0 \in K, a_n \neq 0, n \in \mathbb{N}\} \cup \{0\}$ Polynome n-ten Grades.
   $f \in K[X]$: $\deg(f)$ = Grad von f

   Beispiel: $f(X) = a_3 X^3 + a_2 X^2 + a_1 X + a_0$
   $g(X) = b_2 X^2 + b_1 X + b_0$
   $(f+g)(X) = a_3 X^3 + (a_2 + b_2) X^2 + (a_1 + b_1) X + (a_0 + b_0)$
   $f(X) = \sum_{j=0}^{m} a_j X^j$, $g(X) = \sum_{k=0}^{n} b_k X^k$
   $(f \cdot g)(X) = \sum_{l=0}^{m+n} (\sum_{i=0}^{l} a_i \cdot b_{l-i}) X^l$
   siehe Serie 5, Aufgabe 1: $(K[X], +, \cdot)$ Ring, kommutativ, mit 1.

   Homomorphiesatz:
   $R = K[X], S = K$, $f : K[X] \to K$, gegeben durch $\sum_{i=0}^{n} a_i X^i \mapsto a_0$ surjektiv.
   $\ker(f) = \{f \in K[X] \mid f(X) = X \cdot g(X), g \in K[X]\} = X \cdot K[X] = (X)$

Hier endet das nullte Kapitel der Vorlesung.