<u>Erinnere:</u> Ein Homomorphismus von Gruppen $G \xrightarrow{f} H$ ist eine Abbildung, die die Gruppenstruktur respektiert

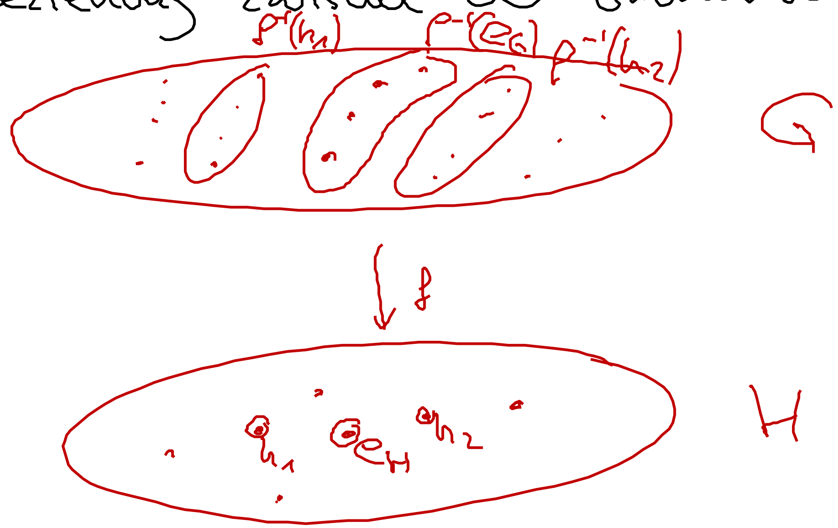
d.h.
$$\left(\begin{array}{c} f(g \circ h) = f(g) \circ f(h) \\ f(g^{-1}) = f(g)^{-1} \\ f(e_G) = e_H \end{array}\right)$$

$f: G \xrightarrow{\sim} H$ bijektiv $\Longrightarrow$ f^{-1} Homomorphismus

Die Gruppen sind isomorph, also "dieselben".

$f: G \twoheadrightarrow H$ <u>surjektiv</u>

Wie ist die Beziehung zwischen der Struktur von G und H ?



Beobachtung: Für $h \in H$ ist $f^{-1}(h)$ eine Rechts-/Linksnebenklasse von $f^{-1}(e_H) = \ker(f)$.

Begründung: $x \in f^{-1}(h)$ und $k \in \ker(f)$

$$\Rightarrow \quad f(x \cdot k) = f(x) \circ \underbrace{f(k)}_{e_G} = f(x) = h$$

$$f(k \cdot x) = f(k) \circ f(x) = f(x) = h$$

$x_1, x_2 \in f^{-1}(h)$

$$f(x_1 \circ x_2^{-1}) = f(x_1) \circ f(x_2)^{-1} = h \circ h^{-1} = e_G \quad \Rightarrow \quad k := x_1 \circ x_2^{-1} \in \ker(f)$$

$$k \cdot x_2 = x_1$$

$$f(x_2^{-1} \circ x_1) = f(x_2)^{-1} \cdot f(x_1) = h^{-1} \circ h = e_G \quad \Rightarrow \quad k := x_2^{-1} \circ x_1 \in \ker(f)$$

$$x_2 \cdot k = x_1$$

Folgerung: Abbildung f kann man wie folgt zusammensetzen

$$\begin{tikzcd} G \arrow[r, "\text{projektion}"] \arrow[rr, bend right, "f"'] & G/\ker(f) \arrow[r, "\tilde{f}"] & H \end{tikzcd}$$

Man überlegt sich, dass $\tilde{f}$ ein Gruppenisomorphismus ist (Homomorphiesatz)

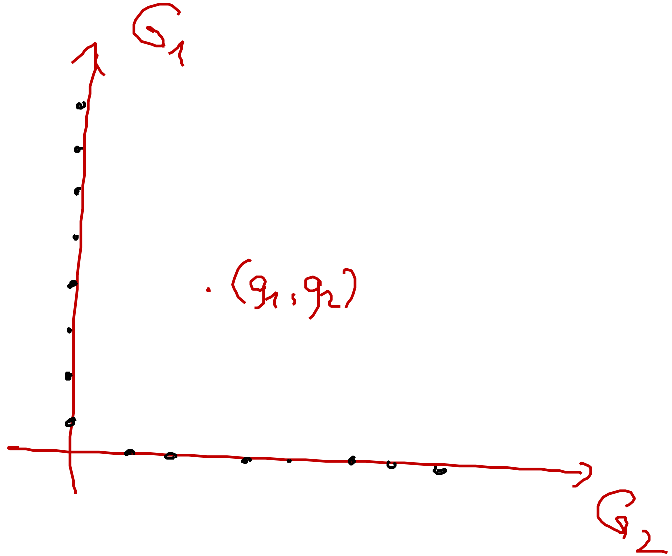
$$G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \dots \trianglerighteq \{e\}$$

G_i / G_{i+1} einfach

Produkte von Gruppen

G_1 und G_2 Gruppen

$$G_1 \times G_2 := \{ (g_1, g_2) \mid g_1 \in G_1,\ g_2 \in G_2 \}$$



Gruppenstruktur:

$$(g_1, g_2) \circ (h_1, h_2) := (g_1 \circ h_1, g_2 \circ h_2)$$

$$(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$$

(e_{G_1}, e_{G_2}) neutrales Element von $G_1 \times G_2$.

klar, dass Gruppenaxiome gelten.

Bsp.: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \not\cong \mathbb{Z}/4\mathbb{Z}$

$\circ$	$\binom{0}{0}$	$\binom{1}{0}$	$\binom{0}{1}$	$\binom{1}{1}$
$\binom{0}{0}$	$\binom{0}{0}$	$\binom{1}{0}$	$\binom{0}{1}$	$\binom{1}{1}$
$\binom{1}{0}$	$\binom{1}{0}$	$\binom{0}{0}$	$\binom{1}{1}$	$\binom{0}{1}$
$\binom{0}{1}$	$\binom{0}{1}$	$\binom{1}{1}$	$\binom{0}{0}$	$\binom{1}{0}$
$\binom{1}{1}$	$\binom{1}{1}$	$\binom{0}{1}$	$\binom{1}{0}$	$\binom{0}{0}$

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

<u>Behauptung:</u> G zyklisch $\Rightarrow$ $G \simeq \mathbb{Z}/6\mathbb{Z}$

Berechne Ordnung von $(1,1)$

$$\begin{aligned} 1\cdot(1,1) &= (1,1) \\ 2\cdot(1,1) &= (2,0) \\ 3\cdot(1,1) &= (0,1) \\ 4\cdot(1,1) &= (1,0) \\ 5\cdot(1,1) &= (2,1) \\ 6\cdot(1,1) &= (0,0) \end{aligned}$$

<u>Fakt:</u> $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ist zyklisch $\Leftrightarrow$ $\mathrm{ggT}(m,n) = 1$. (Übung)

<u>Ringe</u> <u>2 Operation</u> $+$ und $\cdot$

$+$ kommutativ

$\cdot$ nicht unbedingt kommutativ.

$\mathbb{Z}$ ganze Zahlen

$\mathbb{R}$ reelle Zahlen

$\mathbb{C}$ komplexe Zahlen (allgemeiner: jeder Körper)

$\mathbb{R}[X]$ $\{a_n X^n + a_{n-1} X^{n-1} + \dots + a_0 \mid a_i \in \mathbb{R}\}$ Polynome über $\mathbb{R}$.

— alle kommutativ —

$$M_{n\times n}(\mathbb{R}) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{n1} \\ \vdots & & \vdots \\ a_{1n} & \cdots & a_{nn} \end{pmatrix} \;\middle|\; a_{ij} \in \mathbb{R} \right\}$$

Ring bzgl. Matrixmultiplikation.

Bsp.: $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ $\quad$ $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ $\quad$ nicht kommutativ

Definition: Ein (unitärer) Ring besteht aus einer nicht-leeren Menge R mit zwei zweistelligen Operationen $+, \cdot : R^2 \longrightarrow R$ mit folgenden Eigenschaften:

- $R, +$ ist eine kommutative Gruppe
- $\cdot$ ist assoziativ und hat ein neutrales Element 1
- Es gelten die Distributivgesetze

$$(r_1 + r_2) \cdot s = r_1 \cdot s + r_2 \cdot s$$
$$s \cdot (r_1 + r_2) = s \cdot r_1 + s \cdot r_2$$

Bemerkungen:
- Kommutativität von $+$ folgt aus dem Distributivitätsgesetz.
- Es gilt $a \cdot 0 = 0 \quad \forall a \in R$
- Es muss nicht unbedingt $1 \neq 0$ gelten, aber falls $1 = 0$ folgt
  $a = a \cdot 1 = a \cdot 0 = 0 \quad \Rightarrow R = \{0\}$ sog. Nullring
- R heißt kommutativ, falls $\cdot$ kommutativ ist.

- alle vorigen Beispiele erfüllen diese Eigenschaft
- Ein (Schief-)körper unterscheidet sich von einem Ring nur durch die Existenz des Inversen bzgl. $\cdot$.

Daraus folgt insbesondere:

$$a \cdot b = 0 \Rightarrow a = 0 \text{ oder } b = 0$$

Nullteilerfreiheit

Dies muss in einem allg. Ring nicht gelten!

z.B. $R = M_{2\times 2}(\mathbb{R})$ $\quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

(aber nicht invertierbar)

z.B. $\mathbb{Z}/6\mathbb{Z}$ $\quad \bar{2} \cdot \bar{3} = \bar{0}$

Ringhomorphismen: Eine Abbildung $R_1 \xrightarrow{f} R_2$ heißt Ringhom, falls sie die Ringstruktur respektiert.

1. $f(r+s) = f(r) + f(s)$
2. $f(-r) = -f(r)$
3. $f(0) = 0$
4. $f(r \cdot s) = f(r) \cdot f(s)$
5. $f(1) = 1$

Bemerkung: 2. und 3. folgen aus 1. 5. folgt nicht (bis in Körpern)

Erinnerung: 1) Kerne von Gruppenhom's sind genau die Normalteiler.

2) $f: G \longrightarrow H$ surjektiver Gruppenhom. $\Rightarrow$ $H \simeq G/\ker(f)$

Was gilt für Ringe?

1. Beobachtung: f ist insbesondere ein Gruppenhom. von $(R,+)$, daher ist $\ker f$ eine Untergruppe der Gruppe $(R,+)$

2. Beobachtung: $x \in \ker(f)$ $y \in R$ $\Rightarrow$ $x \cdot y \in \ker(f)$
$y \cdot x \in \ker(f)$.

Begründung: $f(x \cdot y) \overset{4.}{=} f(x) \cdot f(y) = 0 \cdot f(y) = 0$

Definition: Eine Untergruppe I von $(R,+)$ heisst
a) Rechts- b) Links- c) beidseitiges Ideal, falls

a) $x \in I \quad y \in R \Rightarrow x \cdot y \in I$

b) $x \in I \quad y \in R \Rightarrow y \cdot x \in I$

c) — " — $\Rightarrow x \cdot y \in I$ und $y \cdot x \in I$

Zusammenfassung: Der <u>Kern</u> eines Ringhom's ist ein beidseitiges Ideal.

Beispiele: $R = \mathbb{Z}$

Untergruppen von $R,+$ sind von der Form

$$m \cdot \mathbb{Z} = \{ \dots, -2m, -m, 0, m, 2m, \dots \}$$

Begründung: Nimm $d \in U$ so dass $|d|$ minimal. $x \in U$ ein anderes beliebiges Element

$\Rightarrow ggT(d,x) = n \cdot x + m \cdot d \in U$

$\Rightarrow ggT(d,x) = d \Rightarrow d \mid x$

Diese sind offensichtlich auch Ideale.

<u>Verallgemeinerung:</u> R komm. Ring $\quad M \in R$

$\Rightarrow \quad M \cdot R = \{M \cdot r \mid r \in R\}$ Menge der Vielfachen von M heißt <u>Hauptideal</u>.

Ein Ring (wie z.B. $\mathbb{Z}$) in dem <u>jedes Ideal</u> ein Hauptideal, heisst Hauptidealring.

({0} und R sind die einzigen Ideale)

<u>Beispiele:</u> Körper, $\mathbb{Z}$, $R[X]$

<u>Gegenbeispiel:</u> $\mathbb{R}[X,Y]$ (Übung)

<u>Homomorphiesatz:</u> Analog wie für Gruppen gilt:

$f: R \twoheadrightarrow S$ surjektive Ringhom. $\Rightarrow$

f ist die Zusammensetzung

$$\begin{tikzcd} R \arrow[r, "\text{projektion}"] \arrow[rr, bend right, "f"'] & R/\ker(f) \arrow[r, "\tilde{f}"] & S \end{tikzcd}$$

Menge der (additiven) Nebenklassen

R Ring $I \subseteq R$ Ideal (beidseitig)

Warum ist R/I ein Ring?

Seien $a+I$, $b+I$ Nebenklassen

$$(a+I)\cdot(b+I) = (a\cdot b + I)$$

$a' = a + i \qquad i \in I$

$b' = b + j \qquad j \in I$

$$a' \cdot b' = (a+i)(b+j) = ab + \underset{\substack{\cap \\ I}}{ib} + \underset{\substack{\cap \\ I}}{aj} + \underset{\substack{\cap \\ I}}{ij}$$

Genauso wie für $\mathbb{Z}$ und $I = n\cdot\mathbb{Z}$ zeigt man:

- Assoziativität
- Distributivität
- Eins $(1+I)$

<u>Fazit:</u> Interessante Möglichkeit neue Ringe (sogar Körper) zu konstruieren.

$$\varphi: \mathbb{R}[X] \longrightarrow \mathbb{C} \qquad (\mathbb{R} \subset \mathbb{C})$$

$$a_n X^n + \dots + a_0 \longmapsto a_n i^n + a_{n-1} i^{n-1} + \dots + a_0$$

$$X \longmapsto i$$

$$\begin{array}{c} \mathbb{F}_p[X] \\ \cap \\ \mathbb{Z}/p\mathbb{Z}[X] \end{array} \longrightarrow \mathbb{F}_{p^n}$$

$$\mathrm{Kern}(\varphi) = (X^2+1)\mathbb{R}[X] \xRightarrow{\text{Homomorphiesatz}} \mathbb{R}[X] / (X^2+1)\mathbb{R}[X] \simeq \mathbb{C}$$

ψ

$\sigma \quad x^2+1$