Beweis: Zunächst ist $\ker f$ in der Tat ein Ideal:

Sei $a \in \ker f \iff f(a) = 0$

Sei $b \in R$ beliebig, $\Rightarrow f(a\cdot b) \underset{\text{Homo}}{\overset{\uparrow}{=}} f(a)\cdot f(b) = 0 \cdot f(b) = 0$

$\Rightarrow \forall a \in \ker f \ \ \forall b \in R$ ist $a \cdot b \in \ker f$.

$\Rightarrow R/\ker f$ ist ein Ring mit Einselement in Bezug auf $+$ und $\cdot$.

$R, \ker f$ sind mit $+$ komm. Gruppen $\Rightarrow R/\ker f \underset{\text{Gruppen}}{\cong} \operatorname{Im} f$

Man hat einen bijektiven Gruppenhomomorphismus, der zusätzlich verträglich ist mit $\cdot$.

(Wähle entsprechenden Ringhomo. Dieser ist auch Gruppenisom.)

Teilbarkeit in kommutativen Ringen

Gewisse Rechenregeln, die wir Körpern kennen, gelten in Ringen nicht mehr.

z.B. die Kürzungsregel: $ab = ac \Rightarrow b = c$ ↯

ggT und kgV sind nicht eindeutig etc. ..

Zunächst folgendes: $a \cdot b = 0 \Rightarrow a = 0$ oder $b = 0$ gilt auch nicht immer!

Bsp: Betrachte $\mathbb{Z}/4\mathbb{Z} = \underbrace{\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}}_{\text{Ring}}$ $\qquad \bar{2}\cdot\bar{2} = \bar{0}$

Definition: a) Sei R ein kommutativer Ring mit Einselement. Ein Element $n \in R$ heißt *Nullteiler* $:\iff \exists\, a \in R\setminus\{0\}$ so dass $n \cdot a = 0$

b) Falls R nur den Nullteiler 0 besitzt, dann nennt man R "Nullteilerfrei".

Bemerkung: 0 ist immer Nullteiler: $a \cdot 0 = a\cdot(0+0) = a\cdot 0 + a \cdot 0 \quad \big| -a\cdot 0$

$\Rightarrow \quad 0 = a \cdot 0$

Satz: Die Kürzungsregel $ab = ac \Rightarrow b = c \quad \forall a, b, c \in R,\ a \neq 0$ gilt genau in Ringen die nullteilerfrei sind.

Beweis: "$\Rightarrow$" WA R hat Nullteiler $n \neq 0 \Rightarrow \exists\, b \in R\setminus\{0\}$ mit

$n b = 0 = 0 \cdot b \overset{KR}{\Rightarrow} n = 0$ ↯

"$\Leftarrow$" Sei R nullteilerfrei. WA: Es existieren $a,b,c \in R$ $a \neq 0$ mit
$ab = ac$ aber $b \neq c$

$\Rightarrow ab - ac = 0 \Rightarrow \underbrace{a}_{\neq 0}\,(\underbrace{b-c}_{\neq 0}) = 0 \Rightarrow$ eines von beiden ist Nullteiler $\lightning$

Bsp zum ggT: $30, 42$ gem. Teiler: $\{\pm 1, \pm 2, \pm 3, \pm 6\}$

all diese sind auch Teiler von $+6$ und -6

Dies werden wir verwenden um das ggT zu definieren, ohne dass eine Ordnungsstruktur besteht.

Definition: Sei R ein kommutativer Ring.

a) Man sagt a ist Teiler von b $(a \mid b) :\Leftrightarrow a, b \in R$ $\exists\, x \in R$ mit $ax = b$

b) Ein Element $g \in R$ ist ein ggT von $a, b \in R$ $:\Leftrightarrow$
$g \mid a$, $g \mid b$ und für alle $x \mid a$ und $x \mid b$ gilt $x \mid g$

c) Ein Element $k \in R$ ist ein kgV von $a, b \in R$ $:\Leftrightarrow$
$a \mid k$, $b \mid k$ und für alle x mit $a \mid x$ und $b \mid x$ gilt $k \mid x$.

$ggT(a,b)$ und $kgV(a,b)$ sind dadurch i.A. Mengen.

Satz: Seien $a, b \in R$, R kommutativer Ring. R^* sei die Menge der invertierbaren Elemente von R ("Einheiten"). Dann gilt:

$$ggT(a,b) = \{g \cdot x \mid x \in R^*\} \quad \text{für bel. } g \in ggT(a,b)$$

und $$kgV(a,b) = \{k\, x \mid x \in R^*\} \quad \text{für bel. } k \in kgV(a,b)$$

Beweis folgt.

Satz: a) $a \mid b \Rightarrow \langle a \rangle \supset \langle b \rangle$

b) Folgende Aussagen sind äquivalent:

i) $a \mid b$ und $b \mid a$

ii) $\langle a \rangle = \langle b \rangle$