<u>Bsp</u> Sei K ein Körper

Sei S ein Ring mit $0_S \neq 1_S$.

Sei $K \xrightarrow{\varphi} S$ ein Ringmorphismus.

Dann ist φ <u>injektiv</u>.

Dazu überprüfen wir $\operatorname{Kern}(\varphi) \stackrel{!}{=} 0$.

Es ist $\operatorname{Kern}(\varphi) \trianglelefteq K$.

Es ist $1_K \notin \operatorname{Kern}(\varphi)$, da

$$1_K \stackrel{\varphi}{\longmapsto} 1_S \neq 0_S .$$

Annahme, es ist $\operatorname{Kern}(\varphi) \neq 0$.

Sei $x \in \operatorname{Kern}(\varphi) \setminus \{0\}$.

Dann ist $x \in U(K)$.

Wegen $\mathrm{Kern}(\varphi) \trianglelefteq K$ ist mit $x \in \mathrm{Kern}(\varphi)$ auch $\mathrm{Kern}(\varphi) \ni x \cdot x^{-1} = 1_K$. ↯

<u>Bsp</u> Sei K ein Körper.

Dann ist $\mathrm{char}(K) = 0$ oder $\mathrm{char}(K) =: p > 0$ mit p prim.

Denn sei $\mathrm{char}(K) =: p > 0$.

Wir haben zu zeigen, daß p prim ist.

Homomorphiesatz:

$$\begin{tikzcd}
 & 1 \arrow[rr, mapsto] & & 1_K \\
\mathrm{Kern}(\varphi) \arrow[r, hook] \arrow[d, equal] & \mathbb{Z} \arrow[rr, "\varphi"] \arrow[dr, "\rho_{\mathbb{Z},p\mathbb{Z}}"'] & & K \\
p\mathbb{Z} & & \mathbb{Z}/p\mathbb{Z} \arrow[r, "\sim", "\bar{\varphi}"'] & \varphi(\mathbb{Z}) \arrow[u, hook]
\end{tikzcd}$$

Wäre $p = a \cdot b$ mit

$a, b \in \mathbb{Z}_{\geq 2}$, dann wären

$a + p\mathbb{Z}, \; b + p\mathbb{Z} \neq 0$,

also $\varphi(a) = \bar{\varphi}(a + p\mathbb{Z}) \neq 0$

$\varphi(b) = \bar{\varphi}(b + p\mathbb{Z}) \neq 0$,

Aber $\varphi(a) \cdot \varphi(b) = \varphi(a \cdot b) = \varphi(0) = 0$,

im Widerspruch zu K Körper.

Bsp Es ist $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$,

da $2 \cdot (-1) + 3 \cdot 1 = 1$.

Es ist $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$,

da eine ganze Zahl genau dann durch 2 und durch 3 teilbar ist, wenn sie durch 6 teilbar ist.

Also haben wir den Ringisomorphismus

$$\mathbb{Z}/6\mathbb{Z} \xrightarrow[\sim]{\varphi} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

$$z + 6\mathbb{Z} \longmapsto (z + 2\mathbb{Z},\ z + 3\mathbb{Z})$$

Wir wollen dessen Bijektivität durch eine direkte Betrachtung bestätigen.

$$
\begin{aligned}
0 + 6\mathbb{Z} &\longmapsto (0 + 2\mathbb{Z},\ 0 + 3\mathbb{Z}) \\
1 + 6\mathbb{Z} &\longmapsto (1 + 2\mathbb{Z},\ 1 + 3\mathbb{Z}) \\
2 + 6\mathbb{Z} &\longmapsto (0 + 2\mathbb{Z},\ 2 + 3\mathbb{Z}) \\
3 + 6\mathbb{Z} &\longmapsto (1 + 2\mathbb{Z},\ 0 + 3\mathbb{Z}) \\
4 + 6\mathbb{Z} &\longmapsto (0 + 2\mathbb{Z},\ 1 + 3\mathbb{Z}) \\
5 + 6\mathbb{Z} &\longmapsto \underbrace{(1 + 2\mathbb{Z},\ 2 + 3\mathbb{Z})}_{\text{jedes Paar ist genau einmal aufgetreten}}.
\end{aligned}
$$

Eine Formel für die Umkehrabbildung:

$$\mathbb{Z}/6\mathbb{Z} \xleftarrow[\sim]{\varphi^{-1}} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

$$3+6\mathbb{Z} \longleftarrow\!\shortmid (1+2\mathbb{Z},\ 0+3\mathbb{Z})$$

$$4+6\mathbb{Z} \longleftarrow\!\shortmid (0+2\mathbb{Z},\ 1+3\mathbb{Z})$$

Also:

$$3a+4b+6\mathbb{Z} \longleftarrow\!\shortmid (a+2\mathbb{Z},\ b+3\mathbb{Z})$$

<u>Bsp</u> (1) Sei K ein Körper mit $\operatorname{char}(K) =: \underbrace{p}_{\text{prim}} > 0$.

Georg Frobenius

Sei

$$\mathrm{Frob}_K : K \longrightarrow K : x \longmapsto x^p,$$

d.h. $\mathrm{Frob}_K(x) = x^p$ für $x \in K$.

Dann ist Frob_K ein Ringmorphismus. Da K ein Körper ist und da $0_K \neq 1_K$, ist Frob_K dann auch injektiv; cf. 26.04.21-1

Frob_K ist Ringmorphismus:

- $\mathrm{Frob}_K(1) = 1^p = 1$
- $\mathrm{Frob}_K(a \cdot b) = (a \cdot b)^p$
  $= a^p \cdot b^p = \mathrm{Frob}_K(a) \cdot \mathrm{Frob}_K(b)$
- $\mathrm{Frob}_K(a+b) = (a+b)^p$

$$= \underbrace{\binom{p}{0}}_{=1} a^p b^0 + \underbrace{\binom{p}{1}}_{=0 \text{ in } K} a^{p-1} b^1 + \underbrace{\binom{p}{2}}_{=0 \text{ in } K} a^{p-2} b^2 + \ldots + \underbrace{\binom{p}{p}}_{=1} a^0 b^p = \ldots$$

$$\ldots = a^p + b^p$$

$$= \mathrm{Frob}_K(a) + \mathrm{Frob}_K(b).$$

(2) $\mathrm{Frob}_{\mathbb{F}_p} = \mathrm{id}_{\mathbb{F}_p}$,

da $\mathrm{Frob}_{\mathbb{F}_p}(1) = 1$

und also $\mathrm{Frob}_{\mathbb{F}_p}(\underbrace{1 + \ldots + 1}_{a \text{ Summanden}})$

$$= 1 + \ldots + 1$$

(3) $\mathrm{Frob}_{\mathbb{F}_p(X)}$ ist nicht surjektiv, da z.B.

$$\mathrm{Frob}_{\mathbb{F}_p(X)}\left(\frac{u(X)}{v(X)}\right) = \left(\frac{u(X)}{v(X)}\right)^p \overset{!}{=} X$$

unlösbar ist aus Gradgründen:

$$\underbrace{u(X)^p}_{\deg \equiv_p 0} \overset{!}{=} \underbrace{X \cdot v(X)^p}_{\deg \equiv_p 1}$$