Di 9.3.2021 NACHMITTAG

$\mathbb{Z}/m\mathbb{Z}$ Ring mit m Elementen

nicht negative ganze Zahlen, < 3

$\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$

$0+0=0$
$0+1=1$
$0+2=2$
$1+2=0$
$2+2=1$
$1+1=2$

$1+0=1$
$2+0=2$
$2+1=0$

$0 \cdot 0 = 0$
$0 \cdot 1 = 0$
$0 \cdot 2 = 0$
$1 \cdot 2 = 2$
$2 \cdot 2 = 1$
$1 \cdot 1 = 1$

$1 \cdot 0 = 0$
$2 \cdot 0 = 0$
$2 \cdot 1 = 2$

$\mathbb{Z}/3\mathbb{Z}$ ist ein Ring!

$a, b \in \mathbb{Z}/3\mathbb{Z}$

$a +_{\mathbb{Z}/3\mathbb{Z}} b$ = der Rest von der Teilung von $a +_{\mathbb{Z}} b$ durch 3

$\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z}$ SURJEKTIVER RINGHOMOMORPHISMUS

$a \longmapsto$ der Rest der Teilung von a durch 3

mit Kern $3\mathbb{Z} = \{$ durch 3 teilbare ganze Zahlen $\}$

$1 \longmapsto 1$
$4 \longmapsto 1$
$-2 \longmapsto 1$

$0 \longmapsto 0$
$3 \longmapsto 0$
$6 \longmapsto 0$
$-3 \longmapsto 0$
$-9 \longmapsto$

$2 \longmapsto 2$
$5 \longmapsto 2$
$-1 \longmapsto 2$

Was ist 2^6 in $\mathbb{Z}/3\mathbb{Z}$?

In $\mathbb{Z}$ $2^6 = 64$

$64 = 3 \cdot 21 + 1$

$\Rightarrow 2^6 = 1$ in $\mathbb{Z}/3\mathbb{Z}$

In $\mathbb{Z}/3\mathbb{Z}$ $2^2 = 1 \Rightarrow$

$2^6 = (2^2)^3 = 1^3 = 1$

$m \in \mathbb{Z}$, $m \geq 1$.

$\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, \dots, m-1\}$ Ring:

$a +_{\mathbb{Z}/m\mathbb{Z}} b$:= der Rest der Teilung von $a +_{\mathbb{Z}} b$ durch m

$a \cdot_{\mathbb{Z}/m\mathbb{Z}} b$ " " " $a \cdot_{\mathbb{Z}} b$ durch m

$\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ surjektiver Ringhomomorphismus

$a \longmapsto$ der Rest der Teilung von a durch m

$(m = 0$ in $\mathbb{Z}/m\mathbb{Z})$ Fundamentale Relation

Beispiel $\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$
$3 = -3$, $4 = -2$, $5 = -1$

$2 \neq 0$
$3 \neq 0$
$2 \cdot 3 = 6 = 0$

$5^2 = 25 = 1$ in $\mathbb{Z}/6\mathbb{Z}$

$5 = -1 \Rightarrow 5^2 = (-1)^2 = 1$

Beispiel $\mathbb{Z}/7\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6\}$ Hat 3 ein multiplikatives Inverses?

$2 \cdot 3 = 6$
$3 \cdot 3 = 2$
$4 \cdot 3 = 5$
$5 \cdot 3 = 1 \Rightarrow$ 5 ist das multiplikative Inverse von 3.

Beispiel $\mathbb{Z}/7\mathbb{Z}$

$3^0 = 1$

$3^1 = 3$

$3^2 = 9 = 2$

$3^3 = 27 = 21 + 6 = 6$] $3^3 = 3^1 \cdot 3^2 = 3 \cdot 2 = 6$

$3^4 = (3^2)^2 = 2^2 = 4$

$3^5 = 3^2 \cdot 3^3 = 2 \cdot 6 = 5$

$3^6 = (3^3)^2 = 6^2 = (-1)^2 = 1$ $\quad 1000 = 996 + 4$

$3^{1000} = 3^4 = 4$

In Singular

$\mathbb{Z}/8\mathbb{Z}$

```
int m = 8;
ring r = (integer, m), x, dp;
```

$\mathbb{Z} \longrightarrow \mathbb{Z}/8\mathbb{Z}$

```
number(16);
number(16) == number(0);
```

```
number a = 5;
```

Def Ein Ring R ist ein KÖRPER wenn:

$\forall a \in R, a \neq 0$, a hat ein multiplikatives Inverses

$\forall a \in R \setminus \{0\}, \exists b \in R : ab = 1$

Beispiel $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind Körper

$\mathbb{Z}$ ist kein Körper: 2 hat kein mult. Inverses

$\mathbb{Z}/6\mathbb{Z}$ ist kein Körper: 2, 3, 4 haben kein mult. Inv.

$\mathbb{Z}/3\mathbb{Z}$ ist ein Körper: $1 \cdot 1 = 1$

$2 \cdot 2 = 1$

Satz $m \in \mathbb{Z}$, $m \geq 1$.

$\mathbb{Z}/m\mathbb{Z}$ ist ein Körper $\Leftrightarrow$ m prim

Wenn p prim ist, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$

```
int p = 5;
ring r = p, x, dp;
```

2.3.1

2.3.2

2.3.3

ohne Rechner

2.3.4

2.3.5

2.3.6

mit Singular

2.3.7, 2.3.8, 2.3.9.