Ringe: Unterringe
Ringhomomorphismen
Ideale

Homomorphiesatz:

- Kerne von Homomorphismen sind Ideale:
  $I = \ker(\varphi)$, $\varphi: R \to S$

z.Z.: $i \in I, r \in R \quad r \cdot i \in I$?

$\Uparrow$ (!)

$\varphi(r) \cdot 0 = \varphi(r) \cdot \varphi(i) = \varphi(r \cdot i) = 0$ ✓

- $I \trianglelefteq R$, dann kann man auf R/I Multiplikation definieren durch $(r + I)(s + I) := rs + I$

z.Z. unabhängig von Repräsentantenwahl!

ang. $r + \overline{I} = r' + \overline{I}$ $\quad \not\Rightarrow \quad rs + \overline{I} = r's' + \overline{I}$?

$s + \overline{I} = s' + \overline{I}$

$r' = r + i_r$ $\quad r's' = (r + i_r)(s + i_s) = r \cdot s + \underbrace{i_r \cdot s + r i_s + i_r \cdot i_s}_{\in \overline{I}}$

$s' = s + i_s$

da $\overline{I}$ Ideal

noch zu zeigen: Ringaxiome gelten!

$1 + \overline{I}$ ist neutrales Element der Multiplikation!

Bsp: • $m\mathbb{Z}$ sind Ideale in $(\mathbb{Z}, +, \cdot)$

• allgemeiner: $r_0 \in R$, $r_0 \cdot R = \{r_0 \cdot s \mid s \in R\}$

Ideal

Bsp: $(\mathbb{R}, +, \cdot)$

$\mathbb{R}[X]$ = Ring des Polynome mit Koeffizienten in $\mathbb{R}$ und Unbekannter X

$$\mathbb{R}[X] / \underbrace{(X^2+1)\cdot\mathbb{R}[X]}_{\text{Ideal, Vielfachen von } (X^2+1)} = \mathbb{C}$$

z.z in R/I

$-(r+I)$

$= (-r)+I$

man kann zeigen:

- $\mathbb{C}$ ist nicht nur ein Ring, sondern ein Körper
- $\mathbb{R}$ ist ein Unterring von $\mathbb{C}$

$$r \in \mathbb{R} \longmapsto r + \underbrace{(X^2+1)\cdot\mathbb{R}[X]}_{I} = r + I$$

- $(X+I)^2 = X^2 + I$

$= (-1) + I$, da $(X^2+I) - ((-1)+I)$

$= \underbrace{(X^2+1)+I}_{I} = 0 + I$

Einheiten und Körper

Ring R: „a teilt b", $a \mid b$, falls es $c \in R$ gibt mit $c \cdot a = b$

$r \in R$ heißt Einheit, falls es $r^{-1} \in R$ gibt mit $r \cdot r^{-1} = 1$ ($= r^{-1} r$ falls R nicht komm.)

d.h. es gibt ein multiplikatives Inverses

Falls es existiert, ist es eindeutig).

Einheiten sind genau die Teiler der 1!

$R^* :=$ Menge der Einheiten von R

$(R^*, \cdot)$ ist Gruppe denn wenn $r \in R^*$, dann auch $r^{-1} \in R^*$

Def: Ein Körper $(K, +, \cdot)$ ist ein Ring mit

- $0 \neq 1$ (d.h. nicht der triviale Ring)
- jedes Element $\neq 0$ ist eine Einheit,

d.h. $K = K^* \cup \{0\}$

Bsp: 1) $\mathbb{Z}_m^* = \{x \mid x \text{ teilerfremd zu } m\}$

$ggT(x, m) = 1 \Rightarrow \exists a, b \quad ax + bm = 1$

$bm = 0$ in $\mathbb{Z}_m$

Rest a von m ist Inverses zu x!

2) (nicht kommt) $M_{n \times n}(\mathbb{R})^* = GL(n, \mathbb{R})$

Matrizen mit Determinante $\neq 0$

3) Körper: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$,

rationaler Funktionenkörper über $\mathbb{R}$, $\mathbb{R}(X)$

$$\mathbb{R}(X) = \left\{ \frac{P}{Q} \mid P, Q \in \mathbb{R}[X] \right\}$$

- $\mathbb{Z}_p$ p Primzahl ist Körper, denn:

$$\mathbb{Z}_p^* = \{ x \mid 0 \leq x < p-1, \; x \text{ teilerfremd zu } p \}$$

$$= \mathbb{Z}_p \setminus \{0\}$$

als Körper heißt $\mathbb{Z}_p$ auch $\mathbb{F}_p$ (engl. field = Körper)

$\mathbb{F}_2 = \mathbb{Z}_2$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

$\mathbb{Z}_3$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

in $\mathbb{Z}_6$

$2 \cdot 3 = 0$

$(\mathbb{Z}_5^*, \cdot) \cong (\mathbb{Z}_4, +)$

$\langle 2 \rangle = \langle 3 \rangle$

$\mathbb{Z}_4$

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

$2 \cdot 2 = 0$ d.h. 2 ist Nullteiler, Nullteiler können keine Inversen haben!

$\mathbb{Z}_5$

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_p$ ist Körper $\Leftrightarrow$ p Primzahl

$\mathbb{Z}_m$ m keine Primzahl: es gibt Nullteiler, d.h.

Zahlen $a \neq 0 \neq b$ mit $a \cdot b = 0$

$\Rightarrow$ $\mathbb{Z}_m$ kann nicht zu einem Körper erweitert werden

Bem: es gibt noch andere endliche Körper, und zwar

für jede Primzahl p und jede $n \in \mathbb{N} \setminus \{0\}$ gibt es bis

auf Isomorphie genau einen Körper $\mathbb{F}_{p^n}$ mit p^n Elementen

$n = 1$: $\mathbb{F}_p = \mathbb{Z}_p$

$n > 1$ $\mathbb{F}_{p^n} \not\cong \mathbb{Z}_{p^n}$

$\mathbb{F}_{p^n}$ ist etwas schwierig zu definieren, sind von der Art $\mathbb{F}_p[X]/I$

$(\mathbb{Z}_5^\times, \cdot)$

$1 \mapsto e$
$2 \mapsto a$
$3 \mapsto b$
$4 \mapsto c$

zyklisch
$\langle a \rangle \cong \langle b \rangle$

$(\mathbb{Z}_4, +)$

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\circ$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

2 Isomorphismen

$0 \mapsto e$
$1 \mapsto a$
$2 \mapsto c$
$3 \mapsto b$

$0 \mapsto e$
$1 \mapsto b$
$2 \mapsto c$
$3 \mapsto a$

K Körper, I Ideal in K

- $\{0\}$ ist immer Ideal

$$K/\{0\} \cong K$$

$$\{k\} = k + \{0\} \longleftrightarrow k$$

- K ist immer Ideal

$$K/K \cong \text{trivialer Ring } \{0\}$$

- Körper haben keine weiteren Ideale

denn I Ideal, $I \neq \{0\}$, sei $i \in I$, $i \neq 0$

$\Rightarrow$ dann ex. i^{-1} und $1 = i \cdot i^{-1} \in I$

$k \in K$ beliebig: $k = k \cdot 1 \in I$ $\Rightarrow I = K$

insbesondere

$\varphi: K \to R$ nicht trivial Ringhomomorphismus

$\ker(\varphi)$ Ideal von K

$1_K \notin \ker(\varphi)$,

da $\varphi(1_K) = 1_R \neq 0_R$

$\ker(\varphi) \neq K$, damit

$\ker(\varphi) = \{0\}$

also ist φ injektiv

Die endlichen Ringe $(\mathbb{Z}_m, +, \cdot)$

Wie sieht die multiplikative Gruppe $(\mathbb{Z}_m^*, \cdot)$ aus?
Wieviele Elemente hat sie?

$$|\mathbb{Z}_m^*| = |\{x \in \mathbb{N} \mid 0 \leq x \leq m-1, (x,m) \text{ teilerfremd}\}|$$
$$= \varphi(m)$$ Euler'sche φ-Funktion

Bsp: $\varphi(p) = p-1$ für Primzahlen p
$\varphi(4) = 2$
$\varphi(6) = 2$
$\varphi(8) = 4$

Ausblick

Falls $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_\ell^{\alpha_\ell}$

dann $\varphi(m) = (p_1 - 1) \cdot p_1^{\alpha_1 - 1} \cdot \ldots \cdot (p_\ell - 1) \cdot p_\ell^{\alpha_\ell - 1}$

Beweis später!

$m = 8 = 2^3 \quad \varphi(8) = (2-1) \cdot 2^2 = 4$

$m = 6 = 2 \cdot 3 \quad \varphi(6) = (2-1) \cdot (3-1) = 2$

$m = 2^3 \cdot 3^2 \cdot 5^3 \cdot 7 \quad \varphi(\ldots) = (2-1) \cdot 2^2 \cdot (3-1) \cdot 3 \cdot (5-1) \cdot 5^2 \cdot (7-1)$

$= 4 \cdot 2 \cdot 3 \cdot 4 \cdot 25 \cdot 6 = 14400$

bis auf Rechenfehler

11

63.000