K4) $\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$

$\Rightarrow \mathbb{Z}/m\mathbb{Z}$ Gruppe, abelsch

π surjektiv ist klar

π ist Gruppenhomom., denn $\pi(a+b) = \overline{a+b} = \bar{a} + \bar{b} = \pi(a) + \pi(b)$

Außerdem: $\ker(\pi) = m\mathbb{Z}$

$$\pi(a) = \bar{a} \overset{!}{=} \bar{0} = m\mathbb{Z}$$

$$\Leftrightarrow a \in m\mathbb{Z}$$

<u>Behauptung</u>: $(\mathbb{Z}_m, +_m) \cong (\mathbb{Z}/m\mathbb{Z}, +)$

$\mathbb{Z}/m\mathbb{Z}$ heißt zyklische Gruppe der Ordnung m.

15.12.15

(C) Körper (und Ringe)

<u>Def.</u>: Ein <u>Körper</u> ist eine Menge K mit 2 Verknüpfungen $+ : K \times K \to K$, $\cdot : K \times K \to K$ so dass gilt:

a) $(K, +)$ ist eine abelsche Gruppe (neutrales Element: 0, Inverse: $-x$)

b) $(K \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe (neutrales Element: 1, Inverse: $x^{-1} = \frac{1}{x}$ $\forall x \neq 0$)

c) $(a+b) \cdot c = ac + bc$ $\forall a, b, c \in K$ Distributivität

Streng genommen $(ac) + (bc)$

wie in der Schule: $\cdot$ vor $+$. Außerdem lassen wir $\cdot$ oft weg.

Wenn wir in b) auf G3) (Inverse) und K4) (Kommutativität) verzichten, (also gilt für $(K \setminus \{0\}, \cdot)$ nur G1), G2)) so heißt K ein <u>Ring</u> (mit <u>Eins</u>). Mit K4) ist K <u>kommutativer Ring</u>.

$\mathbb{Z} = m\mathbb{Z} \dot\cup (1+m\mathbb{Z}) \dot\cup \dots \dot\cup ((m-1)+m\mathbb{Z})$

Teilen mit Rest: $0 \quad \dots \quad 1 \quad \dots \quad m-1$

Notation: $a + m\mathbb{Z} = a' + m\mathbb{Z}$

$\Leftrightarrow a - a'$ teilbar durch m

$\Leftrightarrow : a \equiv a' \bmod m$

„a ist kongruent zu a' (modulo m)"

$\bar{a} := a + m\mathbb{Z}$

$\mathbb{Z}/m\mathbb{Z} = \{$ Restklassen von $m\mathbb{Z}\}$

$= \{ \bar{0}, \bar{1}, \dots, \overline{m-1} \}$

Addition von Restklassen:

$M + N := \{ a+b \mid a \in M, b \in N \}$

$M + N$ ist wieder Restklasse, denn $\bar{a} + \bar{b} = \overline{a+b}$

"$\subseteq$" $(a+km)+(b+\ell m) = a+b+(k+\ell)m$

$\in a+b$

"$\supseteq$" $a+b+km = (a+km)+b$

$\in \bar{a} \quad \in \bar{b}$

Satz 4.5 $(\mathbb{Z}/m\mathbb{Z}, +)$ ist abelsche Gruppe und

$\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

$a \mapsto \bar{a} = a + m\mathbb{Z}$

ist surjektiver Gruppenhomom.

Beweis:

G1) $(\bar{a}+\bar{b})+\bar{c} = \overline{a+b} + \bar{c} = \overline{a+b+c} \overset{\text{analog}}{=} \bar{a} + (\bar{b}+\bar{c})$

G2) neutrales Element:

$\bar{0} = m\mathbb{Z}$

$\bar{a} + \bar{0} = \overline{a+0} = \bar{a}$

G3) Inverse zu $\bar{a}$:

$-\bar{a} = \overline{-a}$

Bsp.: 1) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ sind Körper

2) $(\mathbb{Z}, +, \cdot)$ ist kommutativer Ring

3) $K = \{0, 1\}$ mit

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

kleinstmöglicher Körper, da in jedem Körper $0 \neq 1 \in K$

Satz 4.6 Sei R Ring, dann gilt:

a) $-(-a) = a$

b) $-(a+b) = -a-b$

c) $a \cdot 0 = 0 \cdot a = 0$

d) $(-a) \cdot b = a \cdot (-b) = -ab$

e) $1 \neq 0$

Ist R Körper, so gilt außerdem:

f) $(a^{-1})^{-1} = a \quad \forall a \neq 0$

g) $a \cdot c = b \cdot c, \; c \neq 0 \Rightarrow a = b$ Kürzungsregel

h) $a \cdot b = 0 \Rightarrow a = 0$ oder $b = 0$

Beweis: Übung

c) $a \cdot 0 = a(0+0) = a \cdot 0 + a \cdot 0 \quad | -a \cdot 0$

$\Rightarrow 0 = a \cdot 0$

Def.: Seien R, G Ringe.

Eine Abbildung $f: R \to G$ heißt Ringhomomorphismus falls gilt:

a) $f(a+b) = f(a) + f(b)$

b) $f(a \cdot b) = f(a) \cdot f(b)$

c) $f(1) = 1$

① Primkörper

$\mathbb{Z}/m\mathbb{Z} = \{a + m\mathbb{Z} \mid a \in \mathbb{Z}\}$

(Wdh. $\bar{a} + \bar{b} = \overline{a+b}$)

jetzt: $\bar{a} \cdot \bar{b} := \overline{a \cdot b}$

⚠ $M \cdot N = \{m \cdot n \mid m \in M, n \in N\}$ ist i. A. keine Restklasse

Zu zeigen: $\cdot$ ist wohldefiniert

$\hat{=}$ unabhängig von Repräsentanten a, b.

Beweis: Sei $a' \in \bar{a}$, $b' \in \bar{b}$

$a' = a + km$, $b' = b + \ell m$

$a' \cdot b' = (a + km)(b + \ell m)$

$= ab + (kb + \ell a + k\ell m)m$

$\Rightarrow \overline{a' \cdot b'} = \overline{ab}$

Für $\bar{a} \cdot \bar{b}$ gilt:

G1) $(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \overline{abc}$ ✓

G2) neutrales Element $\bar{1}$ ✓

K4) $\bar{a} \cdot \bar{b} = \overline{ab} = \overline{ba} = \bar{b} \cdot \bar{a}$ ✓

Axiom c)

$(\bar{a} + \bar{b}) \cdot \bar{c} = \overline{(a+b)c}$ ✓

G3) Inverse?

$\bar{a}$ invertierbar (modulo m) $\Leftrightarrow \exists\, \bar{b}$ mit $\bar{a} \cdot \bar{b} = \bar{1}$

$\Leftrightarrow \exists\, b \in \mathbb{Z}, k \in \mathbb{Z}$ mit $ab + km = 1$

$\overset{(*)}{\Leftrightarrow} ggT(a, m) = 1$

$\in \mathbb{N}$

Beweis (*):

"$\Rightarrow$" Sei $c \in \mathbb{N}$ mit $c \mid a$ und $c \mid m$

$\Rightarrow c \mid ab + km = 1 \Rightarrow c = 1$

"$\Leftarrow$" euklidischer Algorithmus (zur Bestimmung von ggT)

OBdA $m > a$: Teile m durch a mit Rest

(Induktion über $\max(a,m)$) $m = b_1 a + r, \quad 0 \leq r < a$

$\Rightarrow ggT(a,m) = ggT(a,r)$

IV: $\exists\ b_2, k \in \mathbb{Z}$ mit $ab_2 + kr = 1$

teilerfremd $\Rightarrow (b_2 - b_1)a + km = 1$

Bem.: $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ist kommutativer Ring

Kor 4.7 $\mathbb{Z}/m\mathbb{Z}$ ist Körper genau dann, wenn m Primzahl

Beweis:

"$\Rightarrow$" Annahme: $m = a \cdot b$

$\Rightarrow \bar{a} \cdot \bar{b} = \overline{m} = \bar{0}$

$\overset{4.6\ h)}{\Rightarrow} \bar{a} = 0$ oder $\bar{b} = 0$

$\Rightarrow a = m$ oder $b = m$

$\Rightarrow m$ prim.

"$\Leftarrow$" m prim.

$\Rightarrow \forall\ a \in \mathbb{Z}$ gilt: $ggT(a,m) = m$ oder $ggT(a,m) = 1$

1. Fall: $a = km \Rightarrow \bar{a} = \bar{0}$

2. Fall: $\exists\ \bar{b}$ mit $\bar{a} \cdot \bar{b} = \bar{1}$

$\Rightarrow ((\mathbb{Z}/m\mathbb{Z}) \setminus \{\bar{0}\}, \cdot)$ erfüllt G3)

Def: Sei $p \in \mathbb{N}$ prim. Dann heißt

$\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ der Primkörper der Ordnung p.

Notation: Sei $n \in \mathbb{N}$. Setze $n \cdot 1 = \underbrace{1+\ldots+1}_{n\text{-fache}} \in K$

Def: Sei K Körper. Die Charakteristik von K ist die kleinste Zahl $n \in \mathbb{N}$ mit $n \cdot 1 = 0$

$$\operatorname{char}(K) := \begin{cases} 0 & \text{falls } n+1 \neq 0 \ \forall n \\ n & \text{falls } \underset{n \in \mathbb{N}}{\exists} \text{ minimal mit } n \cdot 1 = 0 \end{cases}$$

Bsp.: $\operatorname{char}(\mathbb{F}_p) = p$

$\operatorname{char}(\mathbb{Q}) = \operatorname{char}(\mathbb{R}) = 0$

Bsp:

$m = 6$

$\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

invertierbar: $\bar{1}, \bar{5}$

$\bar{1} \cdot \bar{1} = \bar{1} = \bar{5} \cdot \bar{5}$

nicht invertierbar: $\bar{0}, \bar{2}, \bar{3}, \bar{4}$

$\bar{2} \cdot \bar{3} = \bar{3} \cdot \bar{4} = \bar{0}$

(E) Komplexe Zahlen

Def: Der Körper der komplexen Zahlen $\mathbb{C}$ ist definiert wie folgt:

Als Menge $\mathbb{R}^2$

Addition: $(x,y) + (u,v) = (x+u, y+v)$

Multipl.: $(x,y)(u,v) = (x \cdot u - y \cdot v, xv + yu)$

Satz 4.8

$(\mathbb{C}, +, \cdot)$ ist Körper.

Beweis: a) $(\mathbb{R}^2, +)$ ist abelsche Gruppe.

b) $(\mathbb{R}^2 \setminus \{0\}, \cdot)$ ist abelsche Gruppe.

G1) Übung

G2) neutrales Element $(1, 0)$

$(1, 0) \cdot (u, v) = (u, v)$

G3) $(x, y)^{-1} = \left(\frac{x}{x^2+y^2}, -\frac{y}{x^2+y} \right)$ nachrechnen!

für $(x, y) \neq (0, 0)$

K4) klar

Distributivität: nachrechnen.

Notation:

$0 := (0, 0)$

$1 := (1, 0)$

$i := (0, 1)$

$1, i \triangleq$ Standardbasis von $\mathbb{R}^2$

$\mathbb{R} \to \mathbb{C}$, $x \mapsto (x, 0)$ ist injektiver Ringhomom.

denn $(x, 0) + (y, 0) = (x+y, 0)$

$(x, 0) \cdot (y, 0) = (xy, 0)$

Wir können uns $\mathbb{R}$ als Teilmenge von $\mathbb{C}$ vorstellen

Wir schreiben statt (x, y) meist $x + iy$, da

$x + iy = (x, 0) + (0, 1)(y, 0)$

$\Rightarrow = (x, 0) + (0, y) = (x, y)$

$xe_1 + ye_2$

$i^2 = (0, 1) \cdot (0, 1) = (-1, 0) = -1$

K4) $\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$

$\Rightarrow \mathbb{Z}/m\mathbb{Z}$ Gruppe (abelsch)

π surjektiv ist klar.

π ist Grp homom. (denn

$$\pi(a+b) = \overline{a+b} = \bar{a} + \bar{b} = \pi(a) + \pi(b)$$

Außerdem: $\ker(\pi) = m\mathbb{Z}$

$$\pi(a) = \bar{a} \overset{!}{=} \bar{0} = m\mathbb{Z} \iff a \in m\mathbb{Z}$$

Behauptung:

$$(\mathbb{Z}_m, +_m) \cong (\mathbb{Z}/m\mathbb{Z}, +)$$

$\mathbb{Z}/m\mathbb{Z}$ heißt zyklische Gruppe der Ordnung m

15.12.2015

15. Januar: Robokrauser

(C) Körper (und Ringe)

Def: Ein Körper ist eine Menge K mit 2 Verknüpfungen

$+ : K \times K \to K$

$\cdot : K \times K \to K$, sodass gilt:

a) $(K, +)$ ist eine abelsche Gruppe. neutrales Element: 0, Inverse: $-x$

b) $(K \setminus \{0\}, \cdot)$ ist abelsche Gruppe. neutrales Element: 1, Inverse: x^{-1} $\forall x \neq 0$

c) $(a+b)c = ac + bc \quad \forall a, b, c \in K$ Distributivität

Wenn wir in b) auf G3) (Inverse) und K4) (Kommutat.) verzichten, also gilt für $(K \setminus \{0\}, \cdot)$ nur G1), G2)] so heißt K ein **Ring** (mit Eins)

Mit K4) ist K **kommutativer Ring**

Bsp: 1) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ sind Körper

2) $(\mathbb{Z}, +, \cdot)$ ist kein Körper, aber kommutat. Ring

3) $K = \{0, 1\}$ mit Ring

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Kleinstmöglicher Körper, da jeder Körper $0 \neq 1 \in K$

Satz 4.6: Sei R Ring. Dann gilt:

a) $-(-a) = a$

b) $-(a+b) = -a-b$

c) $a \cdot 0 = 0 \cdot a = 0$

d) $(-a) \cdot b = a(-b) = -ab$

e) $1 \neq 0$

Ist R Körper, so gilt außerdem:

f) $(a^{-1})^{-1} = a \quad \forall a \neq 0$

g) $ac = bc, \ c \neq 0 \Rightarrow a = b$ Kürzungsregel

h) $ab = 0 \Rightarrow a = 0$ oder $b = 0$

Beweis: Übung

c) $a \cdot 0 = a \cdot (0+0) = a0 + a \cdot 0 \quad \| + a \cdot 0$

$\Rightarrow 0 = a \cdot 0$

Def: Seien R, G Ringe. Eine Abbildung $f: R \to G$ heißt Ringhomomorphismus, falls gilt:

a) $f(a+b) = f(a) + f(b)$

b) $f(a \cdot b) = f(a) \cdot f(b)$

c) $f(1) = 1$

(2) Primkörper

$\mathbb{Z}/m\mathbb{Z} = \{a + m\mathbb{Z} \mid a \in \mathbb{Z}\}$

(Wohl: $\bar{a} + \bar{b} = \overline{a+b}$)

Ja: $\bar{a} \cdot \bar{b} := \overline{a \cdot b}$

Frage: $M \cdot N = \{m \cdot n \mid m \in M, n \in N\}$

ist i.A. keine Restklasse

Zu zeigen: „$\cdot$" ist wohldef.

Beweis: Sei $a' \in \bar{a}$, $b' \in \bar{b}$

$a' = a + km$, $b' = b + lm$

$a' \cdot b' = (a+km)(b+lm) = ab + (kb + la + kl(m)) \cdot m$

$\Rightarrow \overline{a'b'} = \overline{ab}$

Für $\bar{a} \cdot \bar{b}$ gelt: G1) $(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \overline{abc}$ ✓

G2) neutrales Element $\bar{1}$ ✓

K4) $\bar{a} \cdot \bar{b} = \overline{ab} = \overline{ba} = \bar{b} \cdot \bar{a}$ ✓

Axiom c)

$(\bar{a} + \bar{b}) \cdot \bar{c} = \overline{(a+b)c}$ ✓

G3) Inverse??

$\bar{a}$ invertierbar $\Leftrightarrow \exists \bar{b}$ mit $\bar{a} \cdot \bar{b} = \bar{1}$ (modulo m)

$\Leftrightarrow \exists b \in \mathbb{Z}, k \in \mathbb{Z}$ mit

$ab + km = 1$ teilerfremd

$\overset{(*)}{\Leftrightarrow}$ $ggT(a,m) = 1$, $\in \mathbb{N}$

Beweis (*):

„$\Rightarrow$" Sei $c \in \mathbb{N}$ mit $c \mid a$ & $c \mid m$

$\Rightarrow c \mid ab + km = 1 \Rightarrow c = 1$

„$\Leftarrow$" euklidischer Algorithmus (Zeige Best. von ggT)

OBdA: $m > a$; Teile m oder a mit Rest

(Induktion über $\max(a,m)$) $m = b_1 a + r$, $0 \leq r < a$

$\Rightarrow ggT(a,m) = ggT(a,r) = 1$

IV: $\exists\, b_2, k \in \mathbb{Z}$ mit $ab_2 + kr = 1$

$\Rightarrow (b_2 - b_1)a + km = 1$

Bem $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ist kommutativer Ring

Kor 4.7.: $\mathbb{Z}/m\mathbb{Z}$ ist Körper genau dann, wenn m Primzahl ist.

Beweis: „$\Leftarrow$" Sei $m = a \cdot b$

$$\Rightarrow \bar{a} \cdot \bar{b} = \overline{m} = \bar{0}$$

$$\overset{4.6\ h)}{\Rightarrow} \bar{a} = 0 \text{ oder } \bar{b} = 0$$

$$\Rightarrow a = m \text{ oder } b = m$$

$\Rightarrow m$ prim

„$\Rightarrow$" m prim

$\Rightarrow \forall a \in \mathbb{Z}$ gilt: $ggT(a, m) = m$ oder

$ggT(a, m) = 1$.

1. Fall: $a = km \Rightarrow \bar{a} = \bar{0}$

2. Fall: $\exists b$ mit $\bar{a} \cdot \bar{b} = \bar{1}$

$\Rightarrow ((\mathbb{Z}/m\mathbb{Z}) \setminus \{\bar{0}\}, \cdot)$ erfüllt G3)

Def Sei $p \in \mathbb{N}$ prim. Dann heißt

$\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ der Primkörper der Ordnung p.

Notation: Sei $n \in \mathbb{N}$. Setze $n \cdot 1 = \underbrace{1 + \dots + 1}_{n\text{-fach}} \in K$

Def: Sei K Körper. Die Charakteristik von K ist die kleinste Zahl $n \in \mathbb{N}$ mit $n \cdot 1 = 0$

$$\operatorname{char}(K) := \begin{cases} 0 & \text{falls } n \cdot 1 \neq 0 \ \forall n \\ n & \text{falls } n \in \mathbb{N} \text{ minimal mit } n \cdot 1 = 0 \end{cases}$$

Bsp: $\text{char}(\mathbb{F}_p) = p$

$\text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = 0$

Bsp: $m = 6$

$\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

invertierbar: $\bar{1}, \bar{5}$

$\bar{1}\cdot\bar{1} = \bar{1}$, $\bar{5}\cdot\bar{5} = \bar{1}$

nicht invertierbar: $\bar{0}, \bar{2}, \bar{3}, \bar{4}$

$\bar{2}\cdot\bar{3} = \bar{3}\cdot\bar{4} = \bar{0}$

(E) Komplexe Zahlen

Def: Der Körper der <u>komplexen Zahlen</u> $\mathbb{C}$ ist definiert wie folgt:

Als Menge $\mathbb{R}^2$

Addition $(x,y) + (u,v) = (x+u, y+v)$

Satz 4.8

$(\mathbb{C}, +, \cdot)$ ist Körper.

Beweis: a) $(\mathbb{R}^2, +)$ ist abelsche Gruppe.

b) $(\mathbb{R}^2 \setminus \{0\}, \cdot)$ ist " "

G1) Übung

G2) neutrales Element $(1,0)$

$(1,0)\cdot(u,v) = (u,v)$

G3) $(x,y)^{-1} = \left(\frac{x}{x^2+y^2}, -\frac{y}{x^2+y^2}\right)$

nachrechnen! für $(x,y) \neq (0,0)$

K4) klar

Distributivität: nachrechnen

Notation: $0 := (0,0)$

$1 := (1,0)$

$i := (0,1)$

$1, i \hat{=}$ Standardbasis von $\mathbb{R}^2$