Überblick über Kapitel 2

Gruppe $(+, -, 0)$
$(\cdot, a^{-1}, 1)$

Ring $(+, -, \cdot, 0, 1)$
Bsp: $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, Polynomringe

Körper $(+, -, \cdot, a^{-1}, 0, 1)$
Bsp: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$

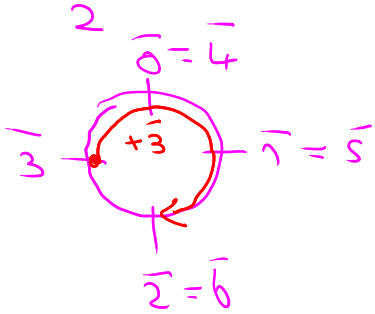
---

zu 2.1.12:

$\mathbb{Z}/4\mathbb{Z} = \{\underbrace{\{\ldots -4, 0, 4, 8, 12\}}_{\bar{0} = \bar{4}}, \underbrace{\{-3, 1, 5, 9, \ldots\}}_{\bar{1}}, \underbrace{\{\ldots -2, 2, 6, \ldots\}}_{\bar{2}}, \underbrace{\{\ldots -1, 3, 7, 11, \ldots\}}_{\bar{3}}\}$

In $\mathbb{Z}/4\mathbb{Z}$:

$\bar{3} + \bar{3} = \bar{6} = \bar{2}$



7 durch, da $4|7-3$

11 durch, da $4|11-3$

Zahlen, die beim Teilen durch 4 den Rest 3 haben.

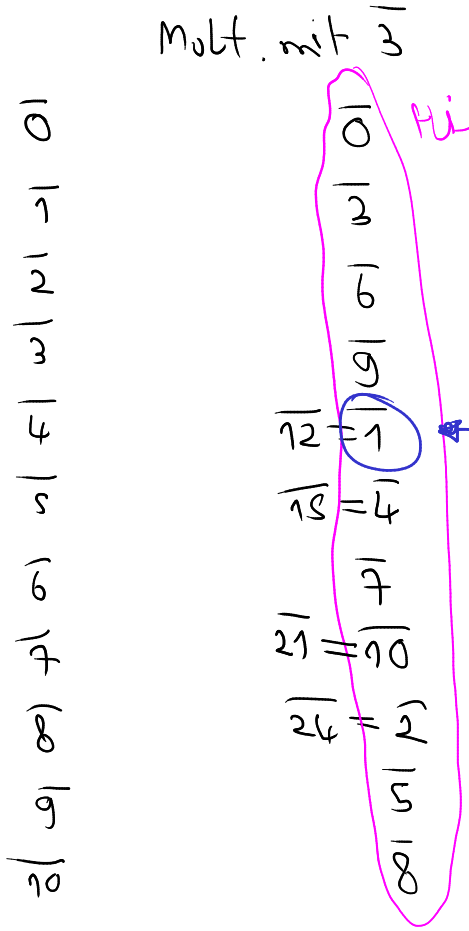
$\bar{3} \cdot \bar{3} = \bar{9} = \bar{1}$

$\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$ ← Kann in einem Körper nicht passieren.

Beweis dass $\mathbb{Z}/11\mathbb{Z}$ ein Körper ist.

Betrachte $\bar{3} \in \mathbb{Z}/11\mathbb{Z}$.

Suche mult. Inverses, d.h. $\bar{b} \in \mathbb{Z}/11\mathbb{Z}$ s.d. $\bar{3} \cdot \bar{b} = \bar{1}$



---

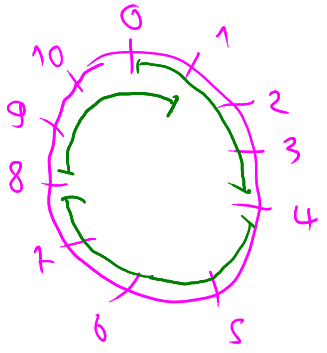
nicht die normalen Zahlen $0,1,\dots,10$!

$\mathbb{F}_{11} = \mathbb{Z}/11\mathbb{Z} = \{0,1,2,\dots,10\}$

In $\mathbb{F}_{11}$: $3^{-1} = 4$

$\frac{1}{3}$

Zahl, die, wenn man sie mit 3 multipliziert, 1 ergibt.



0-Element von $\mathbb{F}_{11}$: $0+9=9$, $0+3=3$, $0+5=5$

1-Element von $\mathbb{F}_{11}$: $1\cdot 9=9$, $1\cdot 3=3$, $1\cdot 5=5$

Informatik

char byte: $0,\dots,255$ $\quad 200+60=4$

Rechnung in $\mathbb{Z}/256\mathbb{Z}$

Ist $\mathbb{F}_{11}$ ein Unterring von $\mathbb{Z}/256\mathbb{Z}$?

$\{0,1,\dots,10\} \subseteq \{0,1,\dots,255\}$

$1+1=2$ $\quad$ $1+1=2$ passt

$6+6=1$ $\quad$ $6+6=12$ passt nicht, also kein Unterring.

Ist $\mathbb{R}$ ein Unterkörper von $\mathbb{C}$?

$3 \cdot 7 = 21$ $\qquad (3+0i)\cdot(7+0i) = 21+0i$

Das geht immer ... und auch für $+$; also: ja.

Zu 2.3.5:

$f = 3 + 5x + x^2$ $\qquad \deg f = 2$

$g = 4x^2 + 2x^{11}$ $\qquad \deg g = 11$

$f \cdot g = (3 + 5x + x^2)(4x^2 + 2x^{11})$

$2 \cdot x^2 \cdot x^{11} = 2x^{13}$

$= 12x^2 + 20x^3 + 4x^4 + 6x^{11} + 10x^{12} + 2x^{13}$

$\deg(f \cdot g) = 2 + 11 = 13$

$f = a_0 + a_1 x + \dots + a_n x^n$

$g = b_0 + b_1 x + \dots + b_m x^m$

$f \cdot g = a_0 b_0 + a_0 b_1 x + a_0 b_2 x^2 + \dots + a_0 b_m x^m$

$+ a_1 b_0 x + a_1 b_1 x^2 + \dots + a_1 b_m x^{m+1}$

$+ \dots$

$+ a_n b_0 x^n + \dots + a_n b_m x^{m+n}$

$a_1 x \cdot b_1 x = a_1 \cdot b_1 \cdot x \cdot x$ da Ring kommutativ

höchste vorkommende x-Potenz

Bsp für $\deg(f \cdot g) < \deg f + \deg g$:

$R = \mathbb{Z}/4\mathbb{Z}$

$f = 1 + 2x^2$ $\qquad \deg f = 2$

$g = 3 + 2x$ $\qquad \deg g = 1$

$f \cdot g = 1 \cdot 3 + 1 \cdot 2 \cdot x + 3 \cdot 2 \cdot x^2 + 2 \cdot 2 \cdot x^3$

$= 3 + 2x + 2x^2 (+ 0x^3)$

$\deg(f \cdot g) = 2$

Potenzen:

$a \in (G, \cdot, e)$ $\quad n \in \mathbb{Z}$ $\rightsquigarrow$ a^n definiert:

Gruppe, multiplikativ geschrieben.

$a^n := \underbrace{a \cdot \dots \cdot a}_{n\text{-mal}}$ falls $n \geq 1$

$a^{-0} = a^0 := 1$

$a^{-n} = \underbrace{a^{-1} \cdots a^{-1}}_{n \text{ Anal.}} = \underbrace{(a \cdot \ldots \cdot a)^{-1}}_{n \text{ Anal}}$ falls $n \geq 1$

Warum nicht $a^0 = 0$?

a^{-3}	a^{-2}	a^{-1}	a^0	a^1	a^2	a^3	...
	$a^{-1} \cdot a^{-1}$	Inverses von a = a^{-1}	1	a	$a \cdot a$	$a \cdot a \cdot a$	

$\cdot a$ $\cdot a$ $\cdot a$ $\cdot a$ $\cdot a$ $\cdot a$

$\mathbb{F}_{11}$:

3^{-2}	3^{-1}	3^0	3^1	3^2	3^3	...
5	4	1	3	9	5	

$3^{-2} = 3^{-1} \cdot 3^{-1} = 4 \cdot 4 = 5$

$\cdot 3$ $\cdot 3$ $\cdot 3$ $\cdot 3$ $\cdot 3$

Satz: $(a \cdot b)^{-1} = a^{-1} b^{-1}$ in beliebigen abelschen Gruppen.

---

zu 2.3.2; zu zeigen:

(1) $(R, +, 0)$ ist ab. Grp
- (1.1) Assoz. von +
- (1.2) 0 ist neutr. Elem für +
- (1.3) Ex. von addit. Inversen
- (1.4) + ist kommutativ

(2) $\cdot$ ist assoziativ und 1 ist ein neutr. Elem.

In der Vorlesung → (3) distrib.

(4) $\cdot$ ist kommutativ

→ Z.z.: Sind $f = \sum_{i \in \mathbb{N}} a_i x^i$, $g = \sum_i b_i x^i \in R[x]$, so gilt: $f \cdot g = g \cdot f$

$f = 2x + 3x^2$ $\quad a_0 = 0 \quad a_1 = 2 \quad a_2 = 3 \quad a_3 = 0, \ldots$

$g = 4x^2 + 5x^3$ $\quad b_0 = 0, b_1 = 0, b_2 = 4 \quad b_3 = 5 \quad b_4 = 0, \ldots$

$f \cdot g = a_0 b_0 + (a_0 b_1 + a_1 b_0) x^1 + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \ldots$

$g \cdot f = b_0 \cdot a_0 + (b_0 a_1 + b_1 a_0) x^1 + (b_0 a_2 + b_1 a_1 + b_2 a_0) x^2 + \ldots$

$f = \sum a_i x^i \qquad g = \sum b_i x^i \qquad h = \sum c_i x^i$

$(f \cdot g) \cdot h \overset{?}{=} f \cdot (g \cdot h)$

$\sum a_i x^i \cdot \sum b_i x^i = \sum_i \left(\sum_{\substack{j,k \in \mathbb{N} \\ j+k=i}} a_j \cdot b_k \right) \cdot x^i$

Beh:

Danach analog:

$$\sum_i \left(\sum_{\substack{j,k,l \in \mathbb{N} \\ j+k+l=i}} a_j b_k c_l \right) x^i$$

$$(f \cdot g) \cdot h = \left(\sum_i \left(\sum_{\substack{j,k \in \mathbb{N} \\ j+k=i}} a_j b_k \right) x^i \right) \cdot h$$

$$= \sum_i \sum_{m+l=i} \left(\left(\sum_{j+k=m} a_j \cdot b_k \right) c_l \right) x^i$$

Bsp: $i=3$

$m=0, l=3$	$a_0 \cdot b_0 \cdot$	$\cdot c_3$
$m=1, l=2$	$(a_0 b_1 + a_1 b_0)$	$\cdot c_2$
$m=2, l=1$	$(a_0 b_2 + a_1 b_1 + a_2 b_0)$	$\cdot c_1$
$m=3, l=0$	$(a_0 b_3 + \dots + a_3 b_0)$	$\cdot c_0$

---

deg $f = 2$ bedeutet „genau 2", d.h. x^2 kommt wirklich vor

f ist quadratisch — " — „höchstens 2", d.h. x^2 muss nicht unbedingt vorkommen.