(2). Körper + Ringe

Bisher Gruppen

(z.B. $(\mathbb{R}, +)$, $(\mathbb{R} - \{0\}, \cdot)$)

jetzt Ringe und Körper gemischt

Grundrechenarten:

Ring: $+, -, \cdot$: $\begin{cases} (R, +) \text{ Gruppe} \\ \text{Distributivgesetze} \end{cases}$

Körper: $+, -, \cdot, :$ $\begin{cases} (R, +) \text{ Gruppe} \\ (R - \{0\}, \cdot) \text{ Gruppe} \\ \text{Distributivgesetze} \end{cases}$

(2.1) Ringe

Def Sei R eine Menge und $+ : R \times R \to R$
und $\cdot : R \times R \to R$ zwei abgeschlossene Operationen
$(R, +, \cdot)$ heißt Ring wenn

(i) $(R, +)$ ist kommut. Gruppe
(ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle $a, b, c \in R$
(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ "
(iv) $(a + b) \cdot c = a \cdot c + b \cdot c$ "

- Achtung $(R, \cdot)$ ist nicht notwendig Gruppe
- Ist $(R, \cdot)$ kommutativ, so heißt $(R, +, \cdot)$ kommutativer Ring
- Gibt es ein $e \in R$ mit $a \cdot e = e \cdot a = a$ für alle $a \in R$
  dann heißt $(R, +, \cdot)$ Ring mit 1

Notation

Sei $(R,+,\cdot)$ Ring

- Neutrales Element bezüglich $(R,+)$ heißt „0"
- Inverses zu a bezgl. $(R,+)$ heißt „$-a$"
- Falls $(R,+,\cdot)$ Ring mit 1 dann heißt das neutrale El. bzgl $(R,\cdot)$ „1"

Beispiele

Ringe $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$

$(\mathbb{Z}_p,\oplus_p,\odot_p)$ ist Ring $\forall p\in\mathbb{N}$

$(p\mathbb{Z},+,\cdot)$

$(\{\frac{a}{2^i}\mid a\in\mathbb{Z},\ i\in\mathbb{N}\},+,\cdot)$ ist Ring

Einige Rechenregeln:

Satz Sei $(R,+,\cdot)$ Ring mit 1 dann gilt

(i) $0 \cdot x = x \cdot 0 = 0$ für alle $x \in R$

(ii) $(-1) \cdot x = -x$ für alle $x \in R$

(iii) $(-1) \cdot (-1) = 1$

Bew (i) $0 \cdot x + x = 0 \cdot x + 1 \cdot x = (0+1) \cdot x = 1 \cdot x = x$

$\Rightarrow 0 \cdot x = 0$

(ii) $(-1) \cdot x + x = (-1) \cdot x + 1 \cdot x = (-1+1) \cdot x = 0 \cdot x = 0$

$\Rightarrow (-1) \cdot x = -x$

(iii) .... selber machen

Endliche Ringe

$(\mathbb{Z}_4, \oplus_4, \odot_4)$

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- Ring mit 1
- $(\mathbb{Z}_4 - \{0\}, \odot_4)$ ist keine Gruppe
- 2 ist „Nullteiler"
  $2 \odot_4 2 = 0$
- 2 hat kein multiplikatives Inverses.

$(\mathbb{Z}_5, \oplus_5, \odot_5)$

$\oplus_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\odot_5$	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

- Ring mit 1
- $(\mathbb{Z}_5 - \{0\}, \odot_5)$ ist Gruppe
- abgeschlossen bzgl $\odot_5$
- keine Nullteiler
- jedes Element hat Inverses

(2.2) Körper

Def. $(K,+,\cdot)$ heißt Körper wenn gilt

(i) $(K,+,\cdot)$ ist Ring

(ii) $(K-\{0\},\cdot)$ ist kommutativ. Gruppe

Beispiele

$(\mathbb{Q},+,\cdot)$

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

$(\mathbb{C},+,\cdot)$

Äquivalent:

(i) $(K,+)$ ist komm. Gruppe

(ii) $(K-\{0\},\cdot)$ ist kommutative Gruppe

(iii) $a\cdot(b+c)=a\cdot b+a\cdot c$ für alle $a,b,c\in K$

Notation

Neutrales El in $(K,+)$ → „0"

Inverse zu a → „$-a$"

Neutrale El in $(K-\{0\},\cdot)$ → „1"

Inverse zu a $(K-\{0\},\cdot)$ → „a^{-1}" (bzw $\frac{1}{a}$)

Der kleinste Körper

$(\{0,1\}, +, \cdot) \cong$ zu $(\mathbb{Z}_2, \oplus_2, \odot_2)$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Allgemein $(\mathbb{Z}_p, \oplus_p, \odot_p)$ ist Körper genau dann wenn p ist Primzahl.

(2.3) Polynomringe

Wichtiger Ring: Polynomring über $(R,+,\cdot)$

Sei $(R,+,\cdot)$ Ring und X ein neues „formales" Symbal

Polynom: Formaler Ausdruck der Form:

$$P(X) := a_0 + a_1 \cdot X + a_2 \cdot X^2 + \ldots + a_n X^n \quad \text{mit } a_i \in R$$

Polynom in X über R

Bsp

		Koeffizienten
$R = (\mathbb{Z},+,\cdot)$	$-10 + 7 \cdot X + 1 \cdot X^2$	$(-10, 7, 1)$
$R = (\mathbb{Q},+,\cdot)$	$\frac{4}{17} + \frac{1}{5} \cdot X + 8 \cdot X^2 + (-\frac{1}{2}) \cdot X^3$	$(\frac{4}{17}, \frac{1}{5}, 8, -\frac{1}{2})$

Polynom ist vollständig charakterisiert durch die Liste seiner Koeffizienten.

Wir modellieren übliche Rechenoperationen mit Polynomen.

grad(P) ist der höchste Exponent eines Polynoms mit nicht-verschwindendem Koeffizienten.

$$\text{grad}(1 + 2\cdot X + 4\cdot X^2 + 0\cdot X^3) = 2$$

(i) Wir identifizieren $a_0 + a_1 \cdot X + \dots a_n X^n + 0\cdot X^{n+1} + \dots + 0\cdot X^m$ mit $a_0 + a_1 \cdot X + \dots + a_n X^n$

(ii) Addition:
$$(a_0 + a_1 \cdot X + a_2 X^2 + \dots + a_n X^n) + (b_0 + b_1 X + b_2 X^2 + \dots + b_n X^n)$$
$$= (a_0 + b_0) + (a_1 + b_1)\cdot X + (a_2 + b_2)\cdot X^2 + \dots + (a_n + b_n) X^n$$

(iii) Multiplikation:
$$(a_0 + a_1 X + \dots a_n X^n) \cdot (b_0 + b_1 X + \dots b_n X^n)$$
$$= (a_0 \cdot b_0 + (a_0 b_1 + a_1 b_0) X + (a_0 b_2 + a_1 b_1 + a_2 \cdot b_0)\cdot X^2 + \dots + a_n b_n X^{2n}$$

Beispiel

$P = 1 - 2x^2 + 4x^3$ grad 3 $(1, 0, -2, 4)$

$Q = 0 + 1 \cdot x + 2 \cdot x^2$ grad 2 $(0, 1, 2)$

$P + Q = 1 + 1 \cdot x + 0 \cdot x^2 + 4x^3$ grad 3 $(1, 1, 0, 4)$

$P \cdot Q = 0 + 1 \cdot x + 2 \cdot x^2 + (-2) \cdot x^3 + 0 \cdot x^4 + 8 \cdot x^5$

$= x + 2x^2 - 2x^3 + 8x^5$

Mit dieser Addition und Multiplikation bildet die Menge der Polynome wieder einen Ring

Polynomring über R : $R[X]$

Jedes Polynom $P \in R[X]$ definiert eine Abb

$= a_0 + a_1 X + \dots + a_n X^n$

$$P : R \to R$$

$$x \mapsto a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

Achtung aus $P(x) = Q(x)$ für alle $x \in R$ folgt nicht $P = Q$

Beispiel $R = (\mathbb{Z}_2, \oplus_2, \odot_2)$ $P = 0$, $Q = x + x^2$

$P(0) = P(1) = 0$, $Q(0) = 0 + 0^2 = 0$, $Q(1) = 1 + 1^2 = 0$