

Mathematik III - Wintersemester 14/15

16. November 2014

Inhaltsverzeichnis

1	Algebraische Strukturen mit einer Verknüpfung	3
1.1	Definition: Verknüpfung	3
1.2	Beispiel	3
1.3	Definition: Halbgruppe	3
1.4	Bemerkung	3
1.5	Beispiel	4
1.6	Definition: kommutative Halbgruppe	4
1.7	Beispiel	4
1.8	Definition: Unterhalbgruppe	5
1.9	Beispiel	5
1.10	Lemma: Eins eindeutig	5
1.11	Definition: Monoid	5
1.12	Beispiele	5
1.13	Definition: Untermonoid	6
1.14	Lemma: Inverses eindeutig	6
1.15	Definition: Gruppe, Inverse, Ordnung	6
1.16	Bemerkung	6
1.17	Beispiele	6
1.18	Beispiele	7
1.19	Satz: Gleichungen lösen in Gruppen	8
1.20	Beispiel	8
1.21	Definition: Untergruppe	8
1.22	Beispiele	9
1.23	Satz und Definition: Rechtsnebenklassen	9
1.24	Beispiel	10
1.25	Lemma: Mächtigkeit von Untergruppen	10
1.26	Theorem: Satz von Lagrange	10
1.27	Definition: Potenzen	11
1.28	Satz: Potenzgesetze	11
1.29	Satz und Definition: Ordnung, zyklische Gruppe	12
1.30	Beispiel	12
1.31	Korollar	13
1.32	Beweis	13
2	Algebraische Strukturen mit 2 Verknüpfungen: Ringe und Körper	13
2.1	Definition: Ring	13
2.2	Beispiel	14
2.3	Satz: Rechnen mit Ringen	14
2.4	Bemerkung	14
2.5	Definition: Körper	15
2.6	Beispiele	15
2.7	Satz: Rechnen im Körper, Nullteilerfreiheit	15
2.8	Definition: Homomorphismus, Isomorphismus	16
2.9	Beispiel	16
2.10	Satz: Chinesischer Restsatz	16
2.11	Beispiel	16

2.12	Bemerkung	17
2.13	Korollar: Phi-Funktion berechnen	17
2.14	Definition: Polynom	18
2.15	Beispiel	18
2.16	Satz und Definition: Polynomring	18
2.17	Bemerkung	19
2.18	Beispiel	19
2.19	Definition: Grad eines Polynoms	19
2.20	TBD	20
2.21	TBD	20
2.22	TBD	20
2.23	TBD	20
2.24	TBD	20
2.25	TBD	20
2.26	TBD	20
2.27	TBD	20
2.28	TBD	20
2.29	TBD	20
2.30	Satz	20
2.31	Satz	20
2.32	Beispiel	20
2.33	Definition	20
2.34	Beispiel	21
2.35	Abschlussbemerkung	21

1 Algebraische Strukturen mit einer Verknüpfung

HALBGRUPPEN, MONOIDE, GRUPPEN

1.1 Definition

Sei $X \neq \emptyset$ eine Menge.

Eine *Verknüpfung* oder (abstrakte) Multiplikation auf X ist eine Abbildung

$$\begin{aligned} \bullet : X \times X &\rightarrow X \\ (a, b) &\mapsto a \bullet b \end{aligned}$$

$a \bullet b$ heißt *Produkt* von a und b , muss aber mit der üblichen Multiplikation von Zahlen nichts zu tun haben.

Beschreibung bei endlichen Mengen oft durch Multiplikationstabellen.

1.2 Beispiel

$$\text{a) } X = \{a, b\} \quad \begin{array}{c|cc} \bullet & a & b \\ \hline a & b & b \\ b & a & a \end{array}$$

$$(a \bullet a) \bullet a = b \bullet a = a$$

$$a \bullet (a \bullet a) = a \bullet b = b \quad \rightarrow \text{nicht assoziativ}$$

$$\text{b) } X = \mathbb{Z}^- (= \{0, -1, -2, \dots\})$$

Die normale Multiplikation ist auf \mathbb{Z}^- keine Verknüpfung!

(zum Beispiel ist $(-2) \cdot (-3) = 6 \notin \mathbb{Z}^-$)

Aber auf $X = \mathbb{N}$, $X = \mathbb{Z}$ oder $X = \{1\}$, $X = \{0, 1\}$

1.3 Definition

Sei $H \neq \emptyset$ eine Menge mit Verknüpfung.

(H, \bullet) heißt *Halbgruppe*, falls gilt:

$$\forall a, b, c \in H : (a \bullet b) \bullet c = a \bullet (b \bullet c) \quad (\text{Assoziativgesetz (AG)})$$

1.4 Bemerkung

AG sagt aus: bei endlichen Produkten ist die Klammerung irrelevant, z.B.

$$(a \bullet b) \bullet (c \bullet d) = ((a \bullet b) \bullet c) \bullet d = (a \bullet (b \bullet c)) \bullet d \quad (\text{usw.})$$

Deshalb werden Klammern meistens weggelassen.

Die Reihenfolge der Elemente ist i.A. relevant!

1.5 Beispiel

- a) $(\mathbb{N}, \bullet), (\mathbb{Z}, \bullet), (\mathbb{Q}, \bullet), (\mathbb{R}, \bullet)$ ¹ sind Halbgruppen.

Ebenso $(\mathbb{N}, +), (\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ ²

- b) $(\mathbb{Q} \setminus \{0\}, :)$ ³ ist *keine* Halbgruppe, denn z.B. $(12 : 6) : 2 = 1$
 $12 : (6 : 2) = 4$

- c) vgl. Vorlesung Theoretische Informatik

$A \neq \emptyset$ endliche Menge ("Alphabet")

$A^+ = \cup_{n \in \mathbb{N}} A^n =$ Menge aller endlichen Wörter über A

(z.B. $A = \{a, b\}$, dann ist z.B. $\underbrace{(a, a, b)}_{aab} \in A^3$)

Verknüpfung: Konkatenation (Hintereinanderschreiben)

z.B. $aab \bullet abab = aababab$

$A^* = A^+ \cup \{\lambda\}$ λ (oder ϵ) ist das leere Wort

Es gilt: $\lambda \cdot w = w \cdot \lambda = w \quad \forall w \in A^*$

$(A^+, \bullet), (A^*, \bullet)$ *Worthalbgruppe* über A

- d) $M \neq \emptyset$ Menge, $\text{Abb}(M, M)$: Menge aller Abbildungen $M \rightarrow M$ mit \circ (Komposition) ist Halbgruppe.

- e) (WICHTIG)

$n \in \mathbb{N}, \mathbb{Z}_n = \{0, 1, \dots, n-1\}$

Verknüpfung: $\oplus : a \oplus b := (a + b) \bmod n$
 $\odot : a \odot b := (a \cdot b) \bmod n$

$(\mathbb{Z}_n, \oplus), (\mathbb{Z}_n, \odot)$ sind Halbgruppen.

1.6 Definition

Eine Halbgruppe (H, \bullet) heißt *kommutativ*, falls gilt:

$$\forall a, b \in H : a \cdot b = b \cdot a \quad (\text{Kommutativgesetz, KG})$$

1.7 Beispiel

Beispiele 1.5 a), e) sind kommutative Halbgruppe.

(hallo \neq ollah, ab \neq ba, Worthalbgruppe nicht kommutativ)

¹ \bullet normale Multiplikation

² + normale Addition

³: normale Division

1.8 Definition

Sei (H, \bullet) Halbgruppe, $\emptyset \neq U \subseteq H$

U heißt *Unterhalbgruppe* von H , falls $u \cdot v \in U \forall u, v \in U$ gilt.

(U, \odot) ist dann selbst Halbgruppe.

1.9 Beispiel

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

G = Menge aller gerade ganzen Zahlen $\subseteq \mathbb{Z}$

$(G, +)$ ist Unterhalbgruppe von $(\mathbb{Z}, +)$

U = Menge aller ungerade Zahlen $\subseteq \mathbb{Z}$

$(U, +)$ ist keine Unterhalbgruppe!

1.10 Lemma

Sei (H, \bullet) Halbgruppe, $e_1, e_2 \in H$ mit $(*) e_1 \cdot x = x \cdot e_1 = x$ und $(**) e_2 \cdot x = x \cdot e_2 = x \forall x \in H$

Dann ist $e_1 = e_2$

Beweis. $e_1 \stackrel{(**)}{=} e_1 \cdot e_2 \stackrel{(*)}{=} e_2$

□

1.11 Definition

Eine Halbgruppe (H, \bullet) heißt *Monoid*, falls $e \in H$ existiert mit $e \cdot x = x \cdot e = x \forall x \in H$

e heißt *neutrales Element* / Einselement / Eins in H .

Schreibweise: (H, \bullet, e)

Für additive Verknüpfung oft 0 für e (Nullelement)
multiplikative 1

Nach 1.10 ist das neutrale Element eindeutig!

1.12 Beispiele

- a) (\mathbb{N}, \bullet) Monoid mit $e = 1$
 $(\mathbb{N}, +)$ kein Monoid
 $(\mathbb{N}_0, +)$ Monoid mit $e = 0$
 $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ Monoide mit $e = 0$
 $(\mathbb{Z}, \bullet), (\mathbb{N}_0, \bullet), (\mathbb{Q}, \bullet), (\mathbb{R}, \bullet)$ Monoide mit $e = 1$
- b) $(\text{Abb}(M, M), \circ)$ Monoid, $e = \text{id}$
- c) (\mathbb{Z}_n, \oplus) Monoid, $e = 0$
 (\mathbb{Z}_n, \odot) Monoid, $e = 1$
- d) (A^*, \bullet) Monoid, $e = \lambda$ (hallo $\lambda = \lambda$ hallo = hallo)

1.13 Definition

Sei (M, \bullet, e) Monoid. Eine Teilmenge $\emptyset \neq U \subseteq M$ heißt *Untermonoid* von M , falls U mit \bullet selbst ein Monoid mit neutralem Element e ist (also $e \in U$)

1.14 Lemma

Sei (H, \bullet, e) Monoid und es gebe zu jedem Element $h \in H$ Elemente $x, y \in H$ mit $h \cdot x \stackrel{(*)}{=} e \stackrel{(**)}{=} y \cdot h$.

Dann ist $x = y$

Beweis. $y = y \cdot e \stackrel{(*)}{=} y \cdot (h \cdot x) \stackrel{(AG)}{=} (y \cdot h) \cdot x \stackrel{(**)}{=} e \cdot x = x$ □

1.15 Definition

(i) (H, \bullet, e) Monoid, $h \in H$

Falls ein $x \in H$ existiert mit $hx = xh = e$, so nennt man h *invertierbar* und x das *Inverse* zu h , bez. h^{-1} (bei additiven Verknüpfungen oft auch $-h$)

Nach 1.14 ist h^{-1} eindeutig bestimmt!

Es gilt: e ist immer invertierbar, $e^{-1} = e$

(ii) Ein Monoid (G, \bullet, e) heißt *Gruppe*, falls jedes Element in G invertierbar ist.

(iii) Für eine endliche Gruppe G heißt die Anzahl der Elemente in G die *Ordnung* von G , $|G|$

1.16 Bemerkung

(H, \bullet, e) Monoid.

Sei G die Menge aller invertierbaren Elemente von H , dann ist (G, \bullet, e) eine Gruppe.

Es gilt: e invertierbar ($e^{-1} = e$)

und falls g invertierbar, dann ist auch g^{-1} invertierbar: $(g^{-1})^{-1} = g$

falls g, h invertierbar, dann auch $g \cdot h$: $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$

1.17 Beispiele

a) $(\mathbb{N}_0, +, 0)$ ist keine Gruppe aber $(\mathbb{Z}, +, 0), (\mathbb{Q}, +, 0), (\mathbb{R}, +, 0)$ sind Gruppen.

b) $(\mathbb{Z}, \bullet, 1)$ ist keine Gruppe.

Die Menge der invertierbaren Elemente ist $\{1, -1\}$, diese bilden eine Gruppe.

c) $(\mathbb{Q}, \bullet, 1)$ ist keine Gruppe, aber $(\mathbb{Q} \setminus \{0\}, \bullet, 1), (\mathbb{R} \setminus \{0\}, \bullet, 1)$ sind Gruppen.

d) A^* ist keine Gruppe, nur λ ist invertierbar.

1.18 Beispiele

a) $(\mathbb{Z}_n, \oplus, 0)$ ist Gruppe (was ist das Inverse zu $x \in \mathbb{Z}_n$? Siehe PÜ1, A9)

b) Sei $n \geq 2$. $(\mathbb{Z}_n, \odot, 1)$ ist Monoid aber keine Gruppe.

Wann ist ein Element aus \mathbb{Z}_n invertierbar bezüglich \odot ?

$$\begin{aligned} z \in \mathbb{Z}_n \text{ invertierbar} &\Leftrightarrow \exists x \in \mathbb{Z}_n : z \odot x = 1 \\ &\Leftrightarrow \exists x \in \mathbb{Z} : (z \cdot x) \bmod n = 1 \\ &\Leftrightarrow \exists x, q \in \mathbb{Z} : z \cdot x = q \cdot n + 1 \\ &\Leftrightarrow z \cdot x + (-q \cdot n) = 1 \\ &\stackrel{\text{Mathe I}}{\Leftrightarrow} \text{ggT}(z, n) = 1 \end{aligned}$$

also sind nur zu n teilerfremde Elemente invertierbar!

(vgl. $(\mathbb{Z}_6, \odot, 1)$: 0, 2, 3, 4 nicht invertierbar, 1, 5 invertierbar)

Bezeichnung:

$$\mathbb{Z}_n^* = \{z \in \mathbb{Z}_n \mid \text{ggT}(z, n) = 1\}$$

ist Gruppe bezüglich \odot (vgl. Bemerkung ??) mit Ordnung $|\mathbb{Z}_n^*| = \varphi(n)$ ("phi von n ", Eulersche φ -Funktion) = Anzahl aller $z \in \mathbb{N}$, die teilerfremd zu n sind und $1 \leq z \leq n$.

$$\varphi(3) = 2, \varphi(4) = 2, \varphi(7) = 6$$

Wie berechnet man das Inverse von $z \in \mathbb{Z}_n^*$?

Mathe I, Erweiterter Euklidischer Algorithmus (WHK, S. 80/81) liefert zu z und n ($\text{ggT}(z, n) = 1$) Zahlen $s, t \in \mathbb{Z}$ mit

$$\begin{aligned} z \cdot s + n \cdot t &= 1 \\ \Rightarrow (z \cdot s) \bmod n &= 1 \\ \Rightarrow (z^{-1}) &= s \bmod n \end{aligned}$$

Beispiel:

$n = 8$: (\mathbb{Z}_8, \odot) , $z = 5$ ist invertierbar, $\text{ggT}(8, 5) = 1$

$$\text{EEA: } 5 \cdot (-3) + 8 \cdot 2 = 1 \Rightarrow z^{-1} = -3 \bmod 8 \Rightarrow z^{-1} = 5$$

c) $\text{Abb}(M, M)$: invertierbare Elemente sind genau die *bijektiven* Abbildungen auf M , $\text{Bij}(M)$ (Mathe I)

Speziell: $M = \{1, 2, \dots, n\}$, dann heißt $\text{Bij}(M)$ die symmetrische Gruppe von Grad n , S_n

$|S_n| = n!$, Elemente heißen Permutationen.

Bsp: $n = 2$

$$S_2 = \left\{ \underbrace{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}}_{\text{id}}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$n = 3$

$$S_3 = \left\{ \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}}_{\text{id}}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \varrho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_3$$

$$\pi \circ \varrho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \varrho \circ \pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ (nicht kommutativ!)}$$

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \pi, \varrho^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

1.19 Satz (Gleichungen lösen in Gruppen)

Sei G Gruppe, $a, b \in G$

- (i) Es gibt genau ein $x \in G$ mit $ax = b$ (nämlich $x = a^{-1}b$)
- (ii) Es gibt genau ein $y \in G$ mit $ya = b$ (nämlich $y = ba^{-1}$)
- (iii) Ist $ax = bx$ für ein $x \in G$, dann gilt $a = b$ (Kürzungsregel)

Beweis. (i) • $x = a^{-1}$ ist Lösung (prüfe $ax = b$):

$$a \cdot \underbrace{a^{-1}b}_x \stackrel{\text{AG}}{=} (a \cdot a^{-1}) \cdot b = e \cdot b = b$$

- Es gibt genau eine Lösung:

Es gelte $ax = b$

$$\Rightarrow x = ex = (a^{-1}a)x \stackrel{\text{AG}}{=} a^{-1}(ax) = a^{-1}b = b$$

(ii) analog

(iii) Multipliziere von rechts mit x^{-1}
links y^{-1}

□

1.20 Beispiel

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ x = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} - \text{Was ist } x?$$

$$a \cdot x = b \Leftrightarrow x = a^{-1} \cdot b$$

$$x = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}^{-1} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

1.21 Definition

(G, \cdot) Gruppe, $\emptyset \neq U \subseteq G$ Teilmenge.

U heißt *Untergruppe* von G ($U \leq G$), falls U bzgl. \cdot selbst eine Gruppe ist.

Insbesondere gilt dann: $\forall u, v \in U$ ist $u \cdot v \in U$.

e von G ist auch neutrales Element in U . (*)

Inversen in U sind die gleichen wie in G .

(*) Angenommen e ist neutrales Element in G , aber f neutrales Element in U , f^{-1} Inverses von f in G .

Dann ist $f^{-1} \cdot f = f \cdot f^{-1} = e$ und $f \cdot f = f$.

$$\Rightarrow f = e \cdot f = (f^{-1} \cdot f) \cdot f = f^{-1} \cdot (f \cdot f) = f^{-1} \cdot f = e$$

1.22 Beispiele

a) $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$

b) $(\{-1, 1\}, \cdot) \leq (\mathbb{Q} \setminus \{0\}, \cdot) \leq (\mathbb{R} \setminus \{0\}, \cdot)$

c) (e, \cdot) ist Untergruppe jeder beliebigen Gruppe mit Verknüpfung \cdot und neutralem Element e .

d) $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$, $\pi^{-1} = \pi$, $\pi^{-1} \circ \pi = \text{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$
 $\Rightarrow (\pi, \text{id}) \leq S_3$

1.23 Satz und Definition

G Gruppe, $U \leq G$

- (i) Durch $x \sim y \Leftrightarrow x \cdot y^{-1} \in U$
 $x + (-y) \in U$ (bei additiver Verknüpfung)
 wird auf G eine Äquivalenzrelation definiert

Beweis

\sim ist reflexiv: $x \sim x$ gilt $\forall x \in G$, denn $x \cdot x^{-1} = e \in U$ ✓

\sim ist symmetrisch: $x \sim y \Rightarrow y \sim x$

Sei $x \sim y$, also $x \cdot y^{-1} \in U$ (zzg.: $y \sim x$, also $y \cdot x^{-1} \in U$)

dann ist $y \cdot x^{-1} = (x \cdot y^{-1})^{-1} \in U$, da auch $x \cdot y^{-1} \in U$.

\sim ist transitiv: $x \sim y, y \sim z \Rightarrow x \sim z$

Sei $x \sim y$, also $x \cdot y^{-1} \in U$ und $y \sim z$, also $y \cdot z^{-1} \in U$ (zzg.: $x \sim z$, d.h. $x \cdot z^{-1} \in U$)

$$x \cdot z^{-1} = x e z^{-1} = x (y^{-1} y) z^{-1} = \underbrace{(x \cdot y^{-1})}_{\in U} \cdot \underbrace{(y \cdot z^{-1})}_{\in U} \in U, \text{ also } x \sim z. \quad \square$$

- (ii) Für $x \in G$ ist $Ux = \{u \cdot x \mid u \in U\}$ die Äquivalenzklasse von x bzgl. \sim und heißt *Rechtsnebenklasse* von U in G .

Also (Eigenschaften von Äquivalenzklassen siehe Mathe I):

(a) $Ux = Uy \Leftrightarrow x \sim y$, also $x \cdot y^{-1} \in U$

(b) $x, y \in G$, dann ist entweder $Ux = Uy$ oder $Ux \cap Uy = \emptyset$

Beweis

(a) Seit $x \sim y \Rightarrow y \sim x \Rightarrow y \cdot x^{-1} \in U \Rightarrow y = y(x^{-1} \cdot x) = \underbrace{(y \cdot x^{-1})}_{\in U} x \in Ux$

(b) Sei $y \in Ux$, dann zeige: $x \sim y$
 $y \in Ux \Rightarrow y = u \cdot x$ für ein $u \in U$
 $\Rightarrow x \cdot y^{-1} = x \cdot (ux)^{-1} = x \cdot x^{-1} \cdot u^{-1} = u^{-1} \in U$
 Es wurde gezeigt, dass $x \sim y$ gilt.

□

1.24 Beispiel

$$G = (\mathbb{Z}, +), 3\mathbb{Z} = \{\dots, -3, 0, 3, 6, \dots\}$$

$$U = (3\mathbb{Z}, +) \leq G \text{ (ÜA, Blatt 2)}$$

Inverses zu y in $(\mathbb{Z}, +)$ ist $-y$.

$$x \sim y \Leftrightarrow x \cdot y^{-1} \in U$$

bzw.: $x - y \in U$

$$x = 0 : U + 0 = \{u + 0 \mid u \in U\} = \{\dots, -3, 0, 3, 6, \dots\} = U = 3\mathbb{Z}$$

$$x = 1 : U + 1 = \{u + 1 \mid u \in U\} = \{\dots, -2, 1, 4, 7, 10, \dots\} = 3\mathbb{Z} + 1$$

$$x = 2 : U + 2 = \{u + 2 \mid u \in U\} = \{\dots, -1, 2, 5, 8, 11, \dots\} = 3\mathbb{Z} + 2$$

$$x = 3 : U + 3 = U + 0 = 0$$

...

1.25 Lemma

G Gruppe, U endliche Untergruppe von G , $x \in G$

Dann ist $|U| = |Ux|$

Beweis

$$\begin{aligned} \text{Abb } \varphi : U &\rightarrow Ux \\ u &\mapsto ux \end{aligned}$$

ist surjektiv und injektiv (falls $u_1x = u_2x$, dann ist $u_1 = u_2$ (Satz 1.19 (iii), Kürzungsregel))

Also ist φ bijektiv, also U, Ux gleich mächtig.

1.26 Theorem (Satz von Lagrange)

G endliche Gruppe, $U \leq G$

Dann gilt $|U|$ ist Teiler von $|G|$ und $q = \frac{|G|}{|U|}$ ist die Anzahl der Rechtsnebenklassen von U in G

Beweis

Seien Ux_1, \dots, Ux_q die q verschiedenen Rechtsnebenklassen von U in G

$$\text{Mathe I \& ??} \Rightarrow G = \bigcup_{i=1}^q Ux_i \text{ (disjunkte Vereinigung der Äquivalenzklassen)}$$

$$\Rightarrow |G| = \sum_{i=1}^q \underbrace{|Ux_i|}_{|U|} \stackrel{1.25}{=} q \cdot |U|$$

1.27 Definition

(G, \bullet, e) Gruppe, $a \in G$

$$\begin{aligned} \text{Definiere } a^0 &:= e \\ a^1 &:= a \\ a^m &:= a^{m-1} \cdot a \quad \text{für } m \in \mathbb{N} \\ a^m &:= (a^{-1})^{-1} \quad \text{für } m \in \mathbb{Z}^- \end{aligned}$$

(Potenzen von a)

$$\begin{aligned} \text{Bei additiver Schreibweise: } 0 \cdot a &= e \\ 1 \cdot a &= a \\ m \cdot a &= \begin{cases} (m-1) \cdot a + a & \text{für } m \in \mathbb{N} \\ (-m) \cdot (-a) & \text{für } m \in \mathbb{Z}^- \end{cases} \end{aligned}$$

1.28 Satz

G, a wie oben

- (i) $(a^{-1})^m = (a^m)^{-1} = a^{-m} \quad \forall m \in \mathbb{Z}$
- (ii) $a^m \cdot a^n = a^{m+n} \quad \forall m, n \in \mathbb{Z}$
- (iii) $(a^m)^n = a^{m \cdot n} \quad \forall m, n \in \mathbb{Z}$

Beweis

$$(i) \ m \in \mathbb{N} : (a^{-1})^m \cdot a^m = \underbrace{a^{-1} \cdot a^{-1} \cdot \dots \cdot a^{-1}}_{m \text{ mal}} \cdot \underbrace{a \cdot \dots \cdot a}_{m \text{ mal}} = e$$

$$\Rightarrow (a^{-1})^m = (a^m)^{-1} \text{ (Inverses von } a^m)$$

$$\text{nach Definition ist } a^{-m} = (a^{-1})^m$$

$$\Rightarrow (i) \text{ gilt } \forall m \in \mathbb{N}$$

$$m = 0 : e = e = e \checkmark$$

$$m \in \mathbb{Z}^- : \text{dann ist } -m \in \mathbb{N}$$

Wende den bewiesenen Teil an auf a^{-1} statt a und $-m$ statt m , Behauptung folgt.

(ii), (iii) per Induktion und mit (i)

□

1.29 Satz und Definition

G endliche Gruppe, $g \in G$

- (i) Es existiert eine kleinste natürliche Zahl n mit $g^n = e$, diese heißt die *Ordnung* $o(g)$ von g
- (ii) Die Menge $\{g^0 = e, g^1 = g, g^2, \dots, g^{n-1}\}$ ist eine Untergruppe von G , die von g erzeugte zyklische Gruppe $\langle g \rangle$
Es gilt $o(g) = |\langle g \rangle| = n$ teilt $|G|$
- (iii) $g^{|G|} = e$

Bemerkung: Eine endliche Gruppe heißt *zyklisch*, falls sie von einem Element erzeugt werden kann.

Beweis

- (i) G endlich $\Rightarrow \exists i, j \in \mathbb{N}, i > j$ mit $g^i = g^j$
Dann ist $g^{i-j} \stackrel{1.28ii)}{=} g^i \cdot g^{-j} \stackrel{1.28}{=} \underbrace{g^i}_{=g^j} \cdot (g^j)^{-1} = e$
- (ii) Das Produkt zweier Elemente aus $\langle g \rangle$ liegt wieder in $\langle g \rangle$
Neutrales Element ist $g^0 = e$
Inverses Element zu g^i ist $(g^i)^{-1} = g^{n-i}$
 $\Rightarrow \langle g \rangle \leq G$
- (iii) Satz von Lagrange (1.26): $n = o(g) = |\langle g \rangle| \mid |G|$
Also ist $|G| = n \cdot k$ für ein $k \in \mathbb{N}$
 $g^{|G|} = g^{n \cdot k} = (g^n)^k = e^k = e$

□

1.30 Beispiel

$(\mathbb{Z}_3 \setminus \{0\}, \odot, 1)$

$$g = 1: \langle 1 \rangle = \{g^0 = 1^0 = 1\}, o(1) = 1$$

$$g = 2: \langle 2 \rangle = \{g^0 = 1, g^1 = 2\}, o(2) = 2$$

$(\mathbb{Z}_5 \setminus \{0\}, \odot, 1)$

$$g = 2: \langle 2 \rangle = \{2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 3\}, o(2) = 4$$

1.31 Korollar

(i) Satz von Euler

Sei $n \in \mathbb{N}, a \in \mathbb{Z}, \text{ggT}(a, n) = 1$

Dann ist

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

(ii) Kleiner Satz von Fermat

Ist p eine Primzahl, $a \in \mathbb{Z}, p \nmid a$, dann gilt

$$a^{p-1} \equiv 1 \pmod{p}$$

1.32 Beweis

- a) Wir können annehmen, dass $1 \leq a < n$ (denn $a^{\varphi(n)} \pmod{n} = (a \pmod{n})^{\varphi(n)}$)
wegen $\text{ggT}(a, n) = 1$ ist $a \in \mathbb{Z}_n^*$, das ist eine endliche Gruppe.

$$\begin{aligned} \stackrel{?(iii)}{\Rightarrow} a^{|\mathbb{Z}_n^*|} &= 1 (= e) & a \odot a \odot \dots \\ \Rightarrow a^{\varphi(n)} &\equiv 1 \pmod{n} & a \cdot a \cdot \dots \end{aligned}$$

- b) Folgt aus (i) ($n = p, \varphi(p) = -1$)

2 Algebraische Strukturen mit 2 Verknüpfungen: Ringe und Körper

2.1 Definition

Sei $R \neq \emptyset$ eine Menge mit zwei Verknüpfungen $+$ und \bullet .

- (i) Wir nennen $(R, +, \cdot)$ einen *Ring*, falls gilt:

- (a) $(R, +)$ ist eine abelsche Gruppe (Eselsbrücke: KAIN)

Das neutrale Element bezeichnen wir hier mit 0, das zu $a \in R$ Inverse mit $-a$
(schreibe auch $a - b$ für $a + (-b)$).

- (b) (R, \cdot) ist eine Halbgruppe.

- (c) Es gelten die Distributivgesetze:

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) = ab + ac \\ (a + b) \cdot c &= (a \cdot c) + (b \cdot c) = ac + bc \quad \forall a, b, c \in R \end{aligned}$$

- (ii) Ein Ring $(R, +, \cdot)$ heißt *kommutativ* falls \cdot ebenfalls kommutativ ist, also falls $\forall a, b \in R : a \cdot b = b \cdot a$

- (iii) Ein Ring $(R, +, \cdot)$ heißt *Ring mit Eins*, falls (R, \cdot) ein Monoid ist mit neutralen Element $1 \neq 0$ ($\forall a \in R : a \cdot 1 = 1 \cdot a = a$).

- (iv) Ist $(R, +, \cdot)$ Ring mit Eins, dann heißen die bezüglich \cdot invertierbaren Elemente *Einheiten*. Das zu a bezügliche \cdot invertierbare Element bezeichnen wir mit a^{-1} .
 $R^* :=$ Menge der Einheiten in R .

2.2 Beispiel

- a) $(\mathbb{Z}, +, \cdot)$ ist kommutativer Ring mit Eins (1)
 $\mathbb{Z}^* = \{1, -1\}$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ ebenso
 $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.
- b) $(2\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring ohne Eins
- c) trivialer Ring $(\{0\}, +, \cdot)$ ohne Eins
- d) $n \in \mathbb{N}, n \geq 2, (\mathbb{Z}_n, \oplus, \odot)$ kommutativer Ring mit Eins
- e) $(\mathbb{R}^n, \underbrace{+, \cdot}_{\text{Komponentenweise}})$; allgemein: R_1, \dots, R_n Ringe, dann $R_1 \times \dots \times R_n$ Ring.
- f) $M_n(\mathbb{R})$ - Menge aller $n \times n$ -Matrizen über \mathbb{R} , mit Matrixaddition und -multiplikation ist Ring mit Eins ($=E_n$), nicht kommutativ für $n \geq 2$.

2.3 Satz (Rechnen mit Ringen)

Sei $(R, +, \cdot)$ ein Ring, $a, b, c \in R$. Dann gilt:

- (i) $a \cdot 0 = 0 \cdot a = 0$
- (ii) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$
- (iii) $(-a) \cdot (-b) = a \cdot b$

Beweis

- (i) $a \cdot 0 = a \cdot (0 + 0) \stackrel{2.1(3)}{=} a \cdot 0 + a \cdot 0$
 addiere $-(a \cdot 0)$ (Inverses von $a \cdot 0$) auf beiden Seiten, erhalte $0 = a \cdot 0$
 Analog $0 \cdot a = 0$
- (ii) $(-a) \cdot b + a \cdot b \stackrel{2.1(3)}{=} (-a + a) \cdot b = 0 \cdot b \stackrel{(i)}{=} 0$
 also ist $(-a \cdot b)$ Inverses zu $a \cdot b$, also $= -(a \cdot b)$.
 Analog $a \cdot (-b) = -(a \cdot b)$
- (iii) $(-a) \cdot (-b) \stackrel{(ii)}{=} -(a \cdot (-b)) \stackrel{(ii)}{=} -(-(a \cdot b)) = a \cdot b$

□

2.4 Bemerkung

- a) In jedem Ring mit Eins sind 1 und -1 Einheiten (denn $(-1) \cdot (-1) = 1$, siehe 2.3(iii))
 Es kann mehr geben (z.B. in \mathbb{Z}_5 usw.). Es kann auch $-1 = 1$ gelten (z.B. in $(\mathbb{Z}_2, \oplus, \odot)$)
- b) 0 kann nach 2.3(i) nie Einheit sein (da $1 \neq 0$)

c) In einem kommutativen Ring R gilt der *Binomialsatz*,

$$(a + b)^n = \sum_{i=0}^n \binom{n}{i} a^i b^{n-i} \quad (n \in \mathbb{N}, a, b \in \mathbb{R})$$

...

2.5 Definition

Ein kommutativer Ring $(K, +, \cdot)$ heißt *Körper*, wenn jedes Element $0 \neq x \in K$ eine Einheit ist, also wenn

$$K^* = K \setminus \{0\}$$

2.6 Beispiele

a) $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ sind Körper. $(\mathbb{Z}, +, \cdot)$ ist kein Körper.

b) vgl. Beispiel 1.18 b)

$$\mathbb{Z}_n^* = \{z \in \mathbb{Z}_n \mid \text{ggT}(z, n) = 1\}$$

ist Gruppe bezüglich \odot

$\Rightarrow (\mathbb{Z}_n, \oplus, \odot)$ ist genau dann ein Körper, wenn n eine Primzahl ist.

2.7 Satz (Rechnen im Körper, Nullteilerfreiheit)

Sei $(K, +, \cdot)$ ein Körper, $a, b \in K$

Dann gilt

$$a \cdot b = 0 \Leftrightarrow a = 0 \text{ oder } b = 0$$

Gegenbeispiel: $(\mathbb{Z}_6, \oplus, \odot)$ ist kein Körper. Hier gilt $2 \odot 3 = 0$, aber weder $2 = 0$, noch $3 = 0$

Beweis

" \Leftarrow ": klar: $0 \cdot b = 0$ oder $a \cdot 0 = 0$ (Satz 2.3 (i), Rechenregeln für Ringe)

" \Rightarrow ": Sei $a \cdot b = 0$. Angenommen $a \neq 0$ (d.h. a hat Inverses)

$$\begin{aligned} \text{Dann ist } b &= 1 \cdot b = (a^{-1} \cdot a) \cdot b \\ &= a^{-1} \cdot (a \cdot b) \\ &= a^{-1} \cdot 0 \\ &\stackrel{2.3(i)}{=} 0 \end{aligned}$$

□

2.8 Definition

Seien $(R, +, \cdot)$ und $(\tilde{R}, \boxplus, \boxdot)$ Ringe.

(i) $\varphi : R \rightarrow \tilde{R}$ heißt (Ring-)Homomorphismus, falls gilt:

$$\underbrace{\varphi(x+y)}_{\in R} = \underbrace{\varphi(x)}_{\in \tilde{R}} \boxplus \underbrace{\varphi(y)}_{\in \tilde{R}} \quad \text{und} \quad \varphi(x \cdot y) = \varphi(x) \boxdot \varphi(y) \quad \forall x, y \in R$$

2.9 Beispiel

$$\varphi(\mathbb{Z}, +, \cdot) \rightarrow (\mathbb{Z}_n, \oplus, \odot)$$

$x \mapsto x \bmod n$ ist Ringhomomorphismus (kein Isomorphismus), da φ nicht injektiv ist, z.B. $n = 5 : \varphi(1) = \varphi(6) = \varphi(11) \dots$

2.10 Satz (Chinesischer Restsatz)

Seien $m_1, \dots, m_n \in \mathbb{N}$ paarweise teilerfremd, $M := m_1 \cdot \dots \cdot m_n$, $a_1, \dots, a_n \in \mathbb{Z}$

Dann existiert ein x , $0 \leq x < M$ mit

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ \dots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

Beweis

Für jedes $i \in \{1, \dots, n\}$ sind die Zahlen m_i und $M_i := \frac{M}{m_i}$ teilerfremd.

\Rightarrow EEA liefert s_i und $t_i \in \mathbb{Z}$ mit $t_i \cdot m_i + s_i \cdot M_i = 1$

Setze $e_i := s_i \cdot M_i$, dann gilt:

$$\begin{aligned} e_i &\equiv 1 \pmod{m_i} \\ e_i &\equiv 0 \pmod{m_j} \quad (j \neq i) \end{aligned}$$

Die Zahl $x := \sum_{i=1}^n a_i e_i \pmod{M}$ ist dann die Lösung der simultanen Kongruenz. □

2.11 Beispiel

$$\text{a) Finde } 0 \leq x < 60 \text{ mit } x \equiv \begin{cases} 2 \pmod{3} \\ 3 \pmod{4} \\ 2 \pmod{5} \end{cases}$$

$$M = 3 \cdot 4 \cdot 5 = 60$$

$$\begin{aligned} M_1 &= \frac{60}{3} = 20 & 7 \cdot 3 + (-1) \cdot 20 &= 1 & \Rightarrow e_1 &= -20 \\ M_2 &= \frac{60}{4} = 15 & 4 \cdot 4 + (-1) \cdot 15 &= 1 & \Rightarrow e_2 &= -15 \\ M_3 &= \frac{60}{5} = 12 & 5 \cdot 5 + (-2) \cdot 12 &= 1 & \Rightarrow e_3 &= -24 \end{aligned}$$

$$x = (2 \cdot (-20) + 3 \cdot (-15) + 2 \cdot (-24)) \bmod 60 = 47$$

b) Was ist $2^{1000} \bmod \underbrace{1155}_{3 \cdot 5 \cdot 7 \cdot 11}$

(a) Berechne $2^{1000} \bmod 3, 5, 7, 11$

$$\begin{aligned} 2^{1000} \bmod 3 &= (-1)^{1000} \bmod 3 = 1 \\ 2^{1000} \bmod 5 &= 4^{500} \bmod 5 = (-1)^{500} \bmod 5 = 1 \\ 2^{1000} \bmod 7 &= 2^{3 \cdot 333 + 1} \bmod 7 = (8^{333} \cdot 2) \bmod 7 = (1 \cdot 2) \bmod 7 = 2 \\ 2^{1000} \bmod 11 &= 2^{5 \cdot 200} \bmod 11 = 32^{200} \bmod 11 = (-1)^{200} \bmod 11 = 1 \end{aligned}$$

$$(b) \text{ Suche } 0 \leq x < 1155 \text{ mit } x \equiv \begin{cases} 1 & (\bmod 3) \\ 1 & (\bmod 5) \\ 2 & (\bmod 7) \\ 1 & (\bmod 11) \end{cases}$$

Der chinesische Restsatz liefert $x = 331$

2.12 Bemerkung

Man kann auch zeigen, dass die Lösung x aus Satz 2.10 eindeutig ist:

$$\begin{aligned} \text{Durch } \psi : \mathbb{Z}_M &\rightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n} \\ x &\mapsto (x \bmod m_1, \dots, x \bmod m_n) \end{aligned}$$

wird ein Ringisomorphismus definiert:

ψ ist surjektiv (zu jedem n -Tupel aus $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$ gibt es eine Lösung x , siehe Restsatz) und es gilt:

$$\underbrace{|\mathbb{Z}_M|}_M = \underbrace{|\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}|}_{m_1 \cdots m_n = M}$$

also ist ψ bijektiv, also auch injektiv, also ist Lösung x eindeutig.

2.13 Korollar

$M = m_1 \cdot \dots \cdot m_n$, m_i paarweise teilerfremd.

Dann ist $\varphi(M) = \varphi(m_1) \cdot \dots \cdot \varphi(m_n)$, insbesondere:

$$n = p_1^{a_1} \cdot \dots \cdot p_k^{a_k} \quad (p_i \text{ Primzahlen, } a_1 > 0, p_i \neq p_j \text{ für } i \neq j)$$

Beweis

Nach 2.12 ist $\mathbb{Z}_M \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$ mittels ψ

$$\Rightarrow x \text{ Einheit} \Leftrightarrow \psi(x) = (x \bmod m_1, \dots, x \bmod m_n) \text{ Einheit}$$

$$\Leftrightarrow x \bmod m_i \text{ Einheit } \forall i = 1 \dots n$$

$$\Rightarrow \varphi(M) = \varphi(m_1) \cdot \dots \cdot \varphi(m_n)$$

$$\varphi(p^a) \underbrace{=}_{\text{Überlegen}} p^a - p^{a-1} = p^{a-1}(p-1)$$

Überlegen

2.14 Definition

Sei K Körper mit Nullelement 0 und Einselement 1:

- (i) Ein *Polynom über K* ist Ausdruck $f = a_0x^0 + a_1x^1 + \cdots + a_nx^n$, $n \in \mathbb{N}_0, a_i \in K$.
 a_i heißen *Koeffizienten* des Polynoms.
 - (a) Ist $a_i = 0$, so kann man $0 \cdot x^i$ bei der Beschreibung weglassen.
 - (b) Statt a_0x^0 schreibt auch a_0
 - (c) Sind alle $a_i = 0$, so schreibt man $f = 0$, das Nullpolynom.
 - (d) Ist $a_i = 1$, so schreibt man x^i statt $1 \cdot x^i$
 - (e) Die Reihenfolge der a_ix^i kann verändert werden, ohne dass das Polynom sich verändert ($x^4 + 2x^3 + 3 = 2x^3 + 3 + x^4$)
- (ii) Zwei Polynome f und g sind *gleich*, wenn ($f = 0$ und $g = 0$) oder ($f = a_0 + a_1x^1 + \cdots + a_nx^n$,
 $g = b_0 + b_1x^1 + \cdots + b_mx^m, a_n \neq 0, b_m \neq 0$ und $n = m, a_i = b_i$ für $i = 0, \dots, n$) gilt.
- (iii) Die Menge aller Polynome über K bezeichnet man als $K[x]$

2.15 Beispiel

- a) $\underbrace{f}_{f(x)} = 3x^2 + \frac{1}{2}x - 1 \in \mathbb{Q}[x] \wedge f \in \mathbb{R}[x]$
- b) $g = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$

Wir wollen in $K[x]$ wie in einem Ring rechnen können. Wir brauchen dazu $+$ und \cdot für Polynome.

2.16 Satz und Definition

K Körper, dann wird $K[x]$ zu einem kommutativen Ring mit Eins durch folgende Verknüpfungen:

$$f = \underbrace{\sum_{i=0}^n a_i x^i}_{\text{z.B. } x+2}, \quad g = \underbrace{\sum_{j=0}^m b_j x^j}_{x^3+2x+1}$$

dann

$$f + g = \underbrace{\sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i}_{x^3+3x+3}$$

$$f \cdot g = \sum_{i=0}^{n+m} c_i x^i$$

$$\text{mit } c_i = a_0b_i + a_1b_{i-1} + \cdots + a_ib_0 = \sum_{j=0}^i a_j b_{i-j} \quad (\text{Faltungsprodukt})$$

(setze a_i mit $i > n$ bzw. b_j mit $j > m$ gleich 0)

- Einselement: $f = 1$ ($a_0 = 1, a_j = 0$ für $j \geq 1$)
- Nullelement: $f = 0$

$K[x]$ heißt der *Polynomring* in einer Variablen über K .

Beweis: Ringeigenschaften nachrechnen.

2.17 Bemerkung

Die $+$ -Zeichen in der Beschreibung der Polynome entsprechen der Ring-Addition der *Monome* $a_0, ax, a_2x^2, \dots, a_nx^n$

2.18 Beispiel

a) in $\mathbb{Q}[x], \mathbb{R}[x]$ Addition, Multiplikation klar

b) in $\mathbb{Z}_3[x]$: $f = 2x^3 + 2x + 1, g = 2x^3 + x$

$$\begin{aligned} f + g &= x^3 + 1 \\ f \cdot g &= (2x^3 + 2x + 1)(2x^3 + x) \\ &= x^6 + 2x^4 + x^4 + 2x^2 + 2x^3 + x \\ &= x^6 + 2x^3 + 2x^2 + x \end{aligned}$$

c) in $\mathbb{Z}_2[x]$: $f = x^2 + 1, g = x + 1$

$$\begin{aligned} f + g &= x^2 + x \\ f + f &= 0 \\ g \cdot g &= x^2 + 1 \end{aligned}$$

2.19 Definition

Sei $0 \neq f \in K[x]$

$f = a_0 + a_1x + \dots + a_nx^n$ mit $a_n \neq 0$

Dann heißt n der *Grad* von f $\text{Grad}(f)$

$\text{Grad}(0) := -\infty$

$\text{Grad}(f) = 0$ *konstante Polynome* $\neq 0$

2.20 TBD

2.21 TBD

2.22 TBD

2.23 TBD

2.24 TBD

2.25 TBD

2.26 TBD

2.27 TBD

2.28 TBD

2.29 TBD

2.30 Satz

Euklidischer Algorithmus in $K[x]$ → siehe „Blatt“

2.31 Satz

EEA in $K[x]$ → siehe „Blatt“

2.32 Beispiel

$g = x^4 + x^3 + 2x^2 + 1, h = x^3 + 2x^2 + 2 \in \mathbb{Z}_3[x]$
... TBD ...

2.33 Definition

k Körper. Ein Polynom $p \in K[x]$, $\text{Grad}(p) \geq 1$ (d.h. $p \neq 0$, p nicht konst., also keine Einheit) heißt *irreduzibel*, falls gilt:

Ist $p = f \cdot g$ ($f, g \in K[x]$), so ist $\text{Grad}(f) = 0$ oder $\text{Grad}(g) = 0$ (d.h. f oder g ist konst. Polynom).

Bemerkung: $p = a \cdot a^{-1} \cdot p$ für $a \in K \setminus \{0\}$ geht immer.

2.34 Beispiel

- a) $ax + b$ ($a \neq 0$) ist irreduzibel in $K[x]$ für jeden Körper K
- b) $x^2 - 2 \in \mathbb{Q}[x]$ ist irreduzibel:
angenommen nicht, dann $(x^2 - 2) = (ax + b)(cx + d)$ mit $a, b, c \in \mathbb{Q} \wedge a, c \neq 0$
 $(ax + b)$ hat Nullstelle $-\frac{b}{a}$, also müsste auch $(x^2 - 2)$ Nullstelle $\underbrace{-\frac{b}{a}}_{\in \mathbb{Q}}$ haben. Nullstellen von $(x^2 - 2)$ sind aber nur $\sqrt{2}$ und $-\sqrt{2}$, beide nicht in \mathbb{Q} !
- c) $x^2 - 2 \in \mathbb{R}[x]$ ist nicht irreduzibel.

$$x^2 - 2 = \underbrace{(x + \sqrt{2})}_{\in \mathbb{R}[x]} \cdot \underbrace{(x - \sqrt{2})}_{\in \mathbb{R}[x]}$$
- d) $x^2 + 1 \in \mathbb{R}[x]$ ist irreduzibel
- e) $x^2 + 1 \in \mathbb{Z}_5[x]$ ist nicht irreduzibel:
 $(x^2 + 1) = (x + 2) \cdot (x + 3) = (x^2 + 3x + 2x + 1) = (x^2 + 1)$
 $2 \Rightarrow (x^2 + 1)$ ist teilbar durch $(x - 2) \hat{=} (x + 3)$

2.35 Abschlussbemerkung

- a) Irreduzibel Polynome in $K[x]$ entsprechen den Primzahlen in \mathbb{Z} . Man kann zeigen:
 $f = \sum_{i=0}^n a_i x^i \in K[x], a_n \neq 0, n \geq 1$.
Dann existieren eindeutig bestimmte irreduzibel Polynome p_1, \dots, p_e und natürlichen Zahlen $m_1, \dots, m_e \in \mathbb{N}$ mit $f = a_n \cdot p_1^{m_1} \cdot \dots \cdot p_e^{m_e}$
- b) geg: Primzahl p , dann gibt es Körper mit p Elementen:
 $(\mathbb{Z}_p, \oplus, \odot)$
Man kann zeigen: zu jeder Primzahlpotenz p^a gibt es Körper mit p^a Elementen, diesen konstruiert man über irreduzible Polynome in $\mathbb{Z}_p[x]$.