

Logik und Diskrete Strukturen

Kapitel 4: Algebra

Prof. Dr. Jasmin Blanchette

Lehr- und Forschungseinheit für Theoretische Informatik und Theorembeweisen

Sommersemester 2026

Basierend auf Folien von PD Dr. Jan Johannsen

Übersicht

Strukturen

Halbgruppen und Monoide

Gruppen

Ringe und Körper

Polynome

Endliche Körper

Algebraische Strukturen

Eine **algebraische Struktur** ist ein Tupel $A = (M, f_1, \dots, f_m)$ mit

- ▶ Menge M
- ▶ $f_i : M^{k_i} \rightarrow M$ für $i \in \{1, \dots, m\}$
- ▶ (k_1, \dots, k_m) ist die **Signatur** von A

M ist die **Trägermenge**, die f_i sind die **Operationen** von A .

Beispiele: $(\mathbb{N}, +, \cdot)$, $(\mathbb{Z}, +, -, \cdot)$, $(\mathcal{P}(M), \cup, \cap)$

Gegenbeispiele: $(\mathbb{N}, +, -)$, $(\mathbb{Z}, +, \cdot, /)$, $(\mathbb{Q}, +, \cdot, /)$

Unterstrukturen

Sei $f : M^k \rightarrow M$ und $U \subseteq M$.

$U \subseteq M$ ist **abgeschlossen** unter f , wenn gilt:

für alle $(x_1, \dots, x_k) \in U^k$ ist $f(x_1, \dots, x_k) \in U$

Dann ist $f|U : U^k \rightarrow U$ die Einschränkung von f auf U .

Ist $A = (M, f_1, \dots, f_m)$ eine algebraische Struktur,

und $U \subseteq M$ abgeschlossen unter allen f_1, \dots, f_m ,

dann ist $A' = (U, f_1|U, \dots, f_m|U)$ eine **Unterstruktur** von A .

Homomorphismen

Seien $A_1 = (M_1, f_1, \dots, f_m)$ und $A_2 = (M_2, g_1, \dots, g_m)$ Strukturen gleicher Signatur (k_1, \dots, k_m) .

$h : M_1 \rightarrow M_2$ ist **Homomorphismus** von A_1 nach A_2 , wenn gilt:

$$g_i(h(x_1), \dots, h(x_{k_i})) = h(f_i(x_1, \dots, x_{k_i})) \quad \text{für alle } i \in \{1, \dots, m\} \text{ und } x_1, \dots, x_{k_i} \in M_1$$

Dann ist $h(A_1) = (h(M_1), g'_1, \dots, g'_m)$ mit $g'_i = g_i|_{h(M_1)}$ Unterstruktur von A_2 .

Isomorphismen

Seien $A_1 = (M_1, f_1, \dots, f_m)$ und $A_2 = (M_2, g_1, \dots, g_m)$ Strukturen gleicher Signatur (k_1, \dots, k_m) .

$h : M_1 \rightarrow M_2$ ist **Isomorphismus** von A_1 nach A_2 , wenn gilt:

- ▶ h ist Homomorphismus von A_1 nach A_2
- ▶ h ist bijektiv

A_1 und A_2 sind **isomorph**, wenn es einen Isomorphismus von A_1 nach A_2 gibt.

Isomorphismus von A nach A heißt Automorphismus.

Ende der 5. Vorlesung

Halbgruppen

Eine Struktur $H = (M, *)$ mit $* : M \times M \rightarrow M$ heißt **Halbgruppe**, wenn $*$ assoziativ ist:

$$a * (b * c) = (a * b) * c \quad \text{für alle } a, b, c \in M$$

$e \in M$ heißt **linksneutrales** Element, wenn gilt:

$$e * x = x \quad \text{für alle } x \in M$$

$e \in M$ heißt **rechtsneutrales** Element, wenn gilt:

$$x * e = x \quad \text{für alle } x \in M$$

$e \in M$ heißt **neutrales Element**, wenn es links- und rechtsneutral ist.

Halbgruppen

Lemma

Ist e linksneutral und e' rechtsneutral, so ist $e = e'$.

Insbesondere gibt es höchstens ein neutrales Element.

Beweis.

$$e = e * e' = e'.$$



Monoide

Eine Halbgruppe $H = (M, *)$ heißt **Monoid**, wenn es ein neutrales Element $e \in M$ gibt.

Beispiel 1

$M := \Sigma^*$ Menge der Strings über Alphabet Σ

$*$:= Konkatenation

Neutrales Element: leerer String ε

Beispiel 2

$M :=$ Menge der unären Funktionen von A nach A (d.h. $\{f \mid f : A \rightarrow A\}$)

$*$:= Komposition

Neutrales Element: Identität id

Inverse Elemente

Sei $H = (M, *)$ ein Monoid mit neutralem Element e , und $a \in M$.

$b \in M$ heißt zu a **linksinverses** Element, wenn gilt:

$$b * a = e$$

$b \in M$ heißt zu a **rechtsinverses** Element, wenn gilt:

$$a * b = e$$

$b \in M$ heißt zu a **invers**, wenn es zu a links- und rechtsinvers ist.

Inverse Elemente

Lemma

Ist b zu a linksinvers und b' zu a rechtsinvers, so ist $b = b'$.

Insbesondere hat jedes $a \in M$ höchstens ein inverses Element.

Beweis.

$$b' = e * b' = (b * a) * b' = b * (a * b') = b * e = b. \quad \square$$

Gruppen

Ein Monoid $H = (M, *)$ mit neutralem Element e heißt **Gruppe**, wenn es zu jedem $a \in M$ ein inverses Element $a^{-1} \in M$ gibt.

Eine Gruppe heißt **abelsch**, wenn $*$ kommutativ ist, also für alle $a, b \in M$ gilt:

$$a * b = b * a$$

Beispiele:

- ▶ $(\mathbb{Z}, +)$ ist eine abelsche Gruppe
- ▶ $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe
- ▶ $(\mathbb{Z}_n, +)$ ist eine abelsche Gruppe

Gegenbeispiele:

- ▶ $(\mathbb{N}, +)$ ist ein Monoid, aber keine Gruppe
- ▶ (\mathbb{Z}, \cdot) und (\mathbb{Q}, \cdot) sind keine Gruppen

Weitere Gruppen

$(\mathbb{Z}_6 \setminus \{0\}, \cdot)$ ist keine Gruppe.

$$\mathbb{Z}_n^* := \{a \in \mathbb{Z}_n \setminus \{0\} \mid \text{ggT}(a, n) = 1\}$$

(\mathbb{Z}_n^*, \cdot) ist eine abelsche Gruppe.

Insbesondere ist $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ eine abelsche Gruppe, für jede Primzahl p .

S_n ist die Menge der Permutationen von $[n]$, also der bijektiven Funktionen $\pi : [n] \rightarrow [n]$.

(S_n, \circ) ist eine Gruppe, die **symmetrische Gruppe** vom Grad n .

Für $n \geq 3$ ist (S_n, \circ) nicht abelsch.

Rechenregeln in Gruppen

In allen Gruppen gelten die folgenden Rechenregeln und -gesetze:

- ▶ Involutionsgesetz: $(a^{-1})^{-1} = a$
- ▶ Kürzungsregeln:
 - aus $a * b = c * b$ folgt $a = c$
 - aus $a * b = a * c$ folgt $b = c$
- ▶ Lösbarkeit linearer Gleichungen:
 - aus $a * x = b$ folgt $x = a^{-1} * b$
 - aus $x * a = b$ folgt $x = b * a^{-1}$
- ▶ Injektivität von $*$:
 $a \neq b$ gdw. $a * c \neq b * c$ gdw. $c * a \neq c * b$
- ▶ Surjektivität von $*$:
es gibt x mit $a * x = b$ und es gibt y mit $y * a = b$

Potenzen

Für $z \in \mathbb{Z}$ definiere die Potenz a^z durch:

▶ $a^0 = e$

▶ $a^{i+1} = a^i * a$ für $i \geq 0$

▶ $a^{-k} = (a^{-1})^k$ für $k \geq 2$

Potenzen

Lemma (Potenzgesetze)

1. $a^m * a^n = a^{m+n}$
2. $(a^m)^n = a^{mn}$
3. aus $a^m = a^n$ folgt $a^{m-n} = e$

Beweis.

Wir beschränken uns auf Punkt 1. Der Beweis ist durch vollständige Induktion über n .

▶ **Induktionsanfang:** $a^m * a^0 = a^m * e = a^m = a^{m+0}$.

▶ **Induktionsschritt:**

$$\begin{aligned} & a^m * a^{n+1} \\ &= a^m * a^n * a \\ &= a^{m+n} * a \quad (\text{durch die Induktionshypothese}) \\ &= a^{m+n+1}. \end{aligned}$$



Ordnung eines Elements

Die **Ordnung** von a ist

$$\text{ord}(a) = \min\{r \in \mathbb{N} \setminus \{0\} \mid a^r = e\}$$

falls diese Menge nichtleer ist, sonst $\text{ord}(a) = \infty$.

Lemma

Ist G endlich, so ist $\text{ord}(a)$ endlich für alle $a \in G$.

Ordnung eines Elements

Lemma

Ist $\text{ord}(a)$ endlich für $a \in G$, so gilt: $a^k = e$ gdw. $\text{ord}(a) \mid k$.

Beweis.

Richtung \leftarrow : Wenn $\text{ord}(a) \mid k$, dann gibt es q , sodass $k = q \cdot \text{ord}(a)$.

Daher $a^k = a^{q \cdot \text{ord}(a)} = (a^{\text{ord}(a)})^q = e^q = e$.

Richtung \rightarrow : Wenn $a^k = e$ ist, dann ist $k \geq \text{ord}(a)$.

Das heißt, $k = q \cdot \text{ord}(a) + r$ für q und $0 \leq r < \text{ord}(a)$.

$e = a^k = a^{q \cdot \text{ord}(a) + r} = a^{q \cdot \text{ord}(a)} * a^r = (a^{\text{ord}(a)})^q * a^r = e^q * a^r = e * a^r = a^r$.

Da $r < \text{ord}(a)$, muss $r = 0$.

Daher $k = q \cdot \text{ord}(a)$, d.h. $\text{ord}(a) \mid k$. □

Zyklische Gruppen

Eine Gruppe G ist **zyklisch**, wenn es ein $a \in G$ gibt mit $G = \{a^i \mid i \in \mathbb{Z}\}$.

In diesem Fall heißt a **Erzeuger** von G .

Beispiele:

- ▶ $(\mathbb{Z}, +)$ ist eine unendliche zyklische Gruppe
- ▶ $(\mathbb{Z}_n, +)$ ist eine zyklische Gruppe, für jedes $n \in \mathbb{N}$

Dies sind die einzigen zyklischen Gruppen.

Zyklische Gruppen

Theorem

Sei G eine zyklische Gruppe. Ist G unendlich, so ist G isomorph zu $(\mathbb{Z}, +)$.

Beweis.

Da G zyklisch ist, gibt es einen Erzeuger $a \in G$, sodass $G = \{a^i \mid i \in \mathbb{Z}\}$.

Wir definieren $f : \mathbb{Z} \rightarrow G$ mit $f(i) = a^i$. Wir werden zeigen, dass f ein Isomorphismus ist.

► **Surjektivität:** Klar.

► **Injektivität:** Seien $m, n \in \mathbb{Z}$ mit $m < n$ und $f(m) = f(n)$.

Das heißt, $a^m = a^n$, also $a^{n-m} = e$.

Sei a^k eine beliebige Potenz von a . Wir haben $k = q(n-m) + r$ für q und $0 \leq r < n-m$.

Dann $a^k = a^{q(n-m)} * a^r = a^r$. Das heißt, es gibt nur $n-m$ Elemente.

Widerspruch zur Annahme, dass G unendlich ist.

► **Homomorphismus:** $f(i+j) = a^{i+j} = a^i * a^j = f(i) * f(j)$.



Zyklische Gruppen

Theorem

Sei G eine zyklische Gruppe. Ist G endlich, so ist G isomorph zu $(\mathbb{Z}_n, +)$, für $n = |G|$.

Beweis.

Sei $n = |G|$. Da G zyklisch ist, gibt es einen Erzeuger $a \in G$, sodass $G = \{a^i \mid i \in \mathbb{Z}\}$.

Wir definieren $f : \mathbb{Z}_n \rightarrow G$ mit $f(i) = a^i$. Wir werden zeigen, dass f ein Isomorphismus ist.

- ▶ **Surjektivität:** Klar.
- ▶ **Injektivität:** Jede Funktion auf einer endlichen Menge, die surjektiv ist, ist auch injektiv.
- ▶ **Homomorphismus:** $f(i + j) = a^{i+j} = a^i * a^j = f(i) * f(j)$. □

Untergruppen

Eine Unterstruktur H einer Gruppe G heißt **Untergruppe**, wenn sie eine Gruppe ist, also wenn $e \in H$ ist, und für jedes $h \in H$ auch $h^{-1} \in H$ ist.

Gegenbeispiel: $(\mathbb{N}, +)$ ist Unterstruktur von $(\mathbb{Z}, +)$, aber keine Untergruppe.

Untergruppen

Lemma

Jede Unterstruktur einer endlichen Gruppe ist auch eine Untergruppe.

Beweis.

Sei H eine Unterstruktur von G .

Sei $h \in H$ ein beliebiges Element.

Dann $h^n \in H$ für alle $n \in \mathbb{N}$ wegen Abgeschlossenheit.

Als Element einer endlichen Gruppe hat h eine endliche Ordnung $\text{ord}(h) = k$.

$h^k = e \in H$ ist das neutrale Element.

$h^{k-1} \in H$. Da $h^{k-1} * h = e = h * h^{k-1}$, ist h^{k-1} das inverse Element zu h . □

Untergruppen

Lemma

Sind H_1 und H_2 Untergruppen von G , dann ist auch $H_1 \cap H_2$ Untergruppe von G .

Beweis.

Für das neutrale Element:

$e \in H_1$ und $e \in H_2$, daher $e \in H_1 \cap H_2$.

Für ein beliebiges Element $a \in H_1 \cap H_2$:

$a^{-1} \in H_1$ und $a^{-1} \in H_2$, daher $a^{-1} \in H_1 \cap H_2$.



Nebenklassen

Sei H eine Untergruppe von G .

Die Relation \sim_H ist definiert als $a \sim_H b$ gdw. $a^{-1} * b \in H$.

Nebenklassen

Lemma

\sim_H ist eine Äquivalenzrelation auf G .

Beweis.

- ▶ **Reflexivität:** $a^{-1} * a = e \in H$. Somit $a \sim_H a$.
- ▶ **Transitivität:** Aus $a \sim_H b$ und $b \sim_H c$ folgen $a^{-1} * b \in H$ und $b^{-1} * c \in H$.
Deshalb ist $a^{-1} * b * b^{-1} * c \in H$.
Somit $a^{-1} * c \in H$.
Mit anderen Worten, $a \sim_H c$.
- ▶ **Symmetrie:** Aus $a \sim_H b$ folgt $a^{-1} * b \in H$.
Daher $(a^{-1} * b)^{-1} \in H$.
Daher $b^{-1} * a \in H$.
Somit $b \sim_H a$.



Nebenklassen

Sei H eine Untergruppe von G .

Für $a \in G$ ist $a * H := \{a * h \mid h \in H\}$ eine **linke Nebenklasse** zu H .

Die linken Nebenklassen $a * H$ sind die Äquivalenzklassen von \sim_H .

\rightsquigarrow Partition von G

Analog könnten wir die rechten Nebenklassen $H * a$ definieren.

Nebenklassen

Lemma

Für alle linken Nebenklassen gilt $|a * H| = |H|$.

Beweis.

Aus $a * H = \{a * h \mid h \in H\}$ folgt $|a * H| \leq |H|$.

Nehmen wir an, dass $h_1, h_2 \in H$ mit $a * h_1 = a * h_2$.

Dann $h_1 = h_2$ nach Wegkürzen von a .

Daher ist die Funktion $h \mapsto a * h$ injektiv.

Somit $|a * H| \geq |H|$. □

Satz von Lagrange

Theorem (Satz von Lagrange)

Ist H Untergruppe einer endlichen Gruppe G , so ist $|H|$ ein Teiler von $|G|$.

Beweis.

Seien H_1, \dots, H_k die Nebenklassen von H , die eine Partition von G bilden.
Sie sind alle gleich groß: $|H_i| = |H|$ für $i \in \{1, \dots, k\}$.
Somit $|G| = k|H|$. □

Der Quotient $|G|/|H|$ heißt Index von H in G .

Folgerung:

Für jedes $a \in G$ ist $\text{ord}(a)$ ein Teiler von $|G|$.

Satz von Euler

Theorem (Satz von Euler)

Für alle $n \in \mathbb{N} \setminus \{0\}$ gilt:

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad \text{für alle } a \in \mathbb{Z}_n^*$$

Beweis.

Zur Erinnerung: $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \setminus \{0\} \mid \text{ggT}(a, n) = 1\}$ ist eine multiplikative Gruppe und $\varphi(n) = |\mathbb{Z}_n^*|$.

Sei $a \in \mathbb{Z}_n^*$. Sei $k = \text{ord}(a)$.

Dann $k \mid \varphi(n)$ aus dem Satz von Lagrange.

Das heißt, $\varphi(n) = tk$ für ein t .

Somit $a^{\varphi(n)} = a^{tk} = (a^k)^t \equiv 1 \pmod{n}$. □

Ende der 6. Vorlesung

Ringe

Eine Struktur $R = (R, +, \cdot)$ ist ein **Ring**, wenn gilt:

- ▶ $(R, +)$ ist eine abelsche Gruppe mit neutralem Element 0.
- ▶ (R, \cdot) ist ein Monoid mit neutralem Element 1.
- ▶ Es gelten die Distributivgesetze:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

für alle $a, b, c \in R$.

Ein Ring ist **kommutativ**, wenn das Monoid (R, \cdot) kommutativ ist.

Beispiele: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind kommutative Ringe.

Gegenbeispiel: $(\mathbb{N}, +, \cdot)$ ist kein Ring.

Ringe

Lemma

In jedem Ring gilt Absorption der 0:

$$a \cdot 0 = 0$$

Beweis.

$$a \cdot 0 + 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

Dann $0 = a \cdot 0$ nach Wegkürzen von $a \cdot 0$. □

Weitere Ringe

\mathbb{Z}_n mit Addition $+$ und Multiplikation \cdot modulo n

Die Menge $\mathbb{R}^{2 \times 2}$ der reellen 2×2 -Matrizen

- ▶ Addition und Multiplikation von Matrizen wie üblich.
- ▶ Neutrale Elemente sind:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ bezüglich } + \quad \text{und} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ bezüglich } \cdot$$

$\mathbb{R}^{2 \times 2}$ ist nicht kommutativ.

Die Menge $\mathbb{Q}[x]$ der Polynome mit rationalen Koeffizienten

- ▶ Addition und Multiplikation von Polynomen wie üblich.
- ▶ Neutrale Elemente sind die konstanten Polynome 0 und 1.

Körper

Ein kommutativer Ring $K = (K, +, \cdot)$ ist ein **Körper**, wenn gilt:

$(K \setminus \{0\}, \cdot)$ ist eine (abelsche) Gruppe

D.h. für jedes $a \in K \setminus \{0\}$ gibt es ein Inverses $a^{-1} \in K \setminus \{0\}$ mit

$$a^{-1} \cdot a = 1$$

Beispiele: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind Körper.

Gegenbeispiele: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}^{2 \times 2}, +, \cdot)$ und $(\mathbb{Q}[x], +, \cdot)$ sind keine Körper.

Lemma

In jedem Körper gilt Nullteilerfrei:

Ist $a \cdot b = 0$, so ist $a = 0$ oder $b = 0$

Beweis.

Sei $a \cdot b = 0$. Zu zeigen: $a \neq 0$ impliziert $b = 0$.

Da $a \neq 0$, hat a ein Inverses a^{-1} .

$$b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0. \quad \square$$

Weitere Körper

Theorem

$(\mathbb{Z}_n, +, \cdot)$ ist ein Körper gdw. n eine Primzahl ist.

Beweis.

- ▶ **Fall 1:** n ist keine Primzahl.

Dann ist $n = pm$, wobei $p > 1$ und $m > 1$.

Dann $p \in \mathbb{Z}_n$ und $m \in \mathbb{Z}_n$, aber $pm \equiv 0 \pmod{n}$.

$(\mathbb{Z}_n, +, \cdot)$ ist nicht nullteilerfrei und deshalb kein Körper.

- ▶ **Fall 2:** n ist eine Primzahl.

Dann gilt $\text{ggT}(a, n) = 1$ für jedes $a \in [n - 1]$.

Dann gibt es ein Inverses $a^{-1} \in \mathbb{Z}_n$ mit $a^{-1} \cdot a \equiv 1 \pmod{n}$.



Weitere Körper

Die Menge $\{0, 1, a, b\}$ mit den folgenden Operationen ist ein Körper.

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

\cdot	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Primitive Elemente

Für einen Körper K bezeichnet K^* die multiplikative Gruppe $(K \setminus \{0\}, \cdot)$.

Theorem

Für jeden endlichen Körper K ist die Gruppe K^ zyklisch.*

Ein Erzeuger der Gruppe K^* heißt **primitives Element** von K^* .

Primitive Elemente sind nicht eindeutig:

- ▶ In \mathbb{Z}_5^* sind 2 und 3 primitiv.
- ▶ Sei K der Körper der vorherigen Folie. In K^* sind a und b primitiv.

Charakteristik und Primkörper

Für einen Körper K ist die **Charakteristik** $\text{char}(K)$ definiert als

$$\begin{cases} \text{ord}(1) \text{ in der additiven Gruppe } (K, +) & \text{wenn } \text{ord}(1) \neq \infty \\ 0 & \text{wenn } \text{ord}(1) = \infty \end{cases}$$

Ist $\text{char}(K) = n > 0$, so betrachte die Menge

$$P := \{0, 1, 1 + 1, \dots, \underbrace{1 + \dots + 1}_{(n-1)\text{-mal}}\}$$

$(P, +, \cdot)$ ist ein Unterkörper (**Primkörper**) von K , der isomorph zu \mathbb{Z}_n ist.

Daher ist $\text{char}(K) = 0$ oder $\text{char}(K) = p$ für eine Primzahl p .

Theorem

Für jeden endlichen Körper K ist $|K|$ der Form p^n , wobei $p = \text{char}(K)$ und $n \in \mathbb{N} \setminus \{0\}$.

Polynome

Sei K ein Körper und x eine Variable.

Ein **Polynom** über K in x ist ein Ausdruck

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

für $n \in \mathbb{N}$ und $a_i \in K$ für $i \in \{0, \dots, n\}$.

$K[x]$ bezeichnet die Menge der Polynome über K in x .

Der **Grad** von $p(x)$ ist $\deg p(x) = \max \{d \in \mathbb{N} \mid a_d \neq 0\}$.

Ausnahme: das Polynom $p(x) = 0$ hat Grad $\deg p(x) = -1$.

Ein Polynom $p(x)$ definiert eine Funktion $f_p : K \rightarrow K$

$$f_p(b) := a_n \cdot b^n + a_{n-1} \cdot b^{n-1} + \cdots + a_1 \cdot b + a_0$$

Für $f_p(b)$ schreiben wir auch $p(b)$.

Auswertung von Polynomen

Es gilt: $p(b)$ lässt sich berechnen als

$$\begin{aligned} p(b) &= a_n \cdot b^n + a_{n-1} \cdot b^{n-1} + \dots + a_1 \cdot b + a_0 \\ &= ((\dots((a_n b + a_{n-1})b + a_{n-2})b + \dots)b + a_1)b + a_0 \end{aligned}$$

Dieses **Horner-Schema** als Algorithmus:

```
 $p := a_n$   
for  $i := n - 1$  to 0 do  
   $p := p \cdot b + a_i$   
return  $p$ 
```

Rechnen mit Polynomen

Seien $a(x) = a_n x^n + \cdots + a_1 x + a_0$ und $b(x) = b_m x^m + \cdots + b_1 x + b_0$.

Die Summe $c(x) = a(x) + b(x)$ ist $c(x) = c_k x^k + \cdots + c_1 x + c_0$ mit
 $k = \max(n, m)$ und $c_i = a_i + b_i$ für $i \in \{0, \dots, k\}$

Das Produkt $c(x) = a(x) \cdot b(x)$ ist $c(x) = c_k x^k + \cdots + c_1 x + c_0$ mit
 $k = n + m$ und $c_i = \sum_{j=0}^i a_j b_{i-j}$ für $i \in \{0, \dots, k\}$

$K[x]$ bildet mit diesen Operationen $+$ und \cdot einen kommutativen Ring.

Neutrales Element bezüglich $+$: Nullpolynom $p(x) = 0$

Neutrales Element bezüglich \cdot : konstantes Polynom $p(x) = 1$

Polynomdivision

Theorem

Für $a(x), b(x) \in K[x]$, wobei $b(x) \neq 0$, gibt es eindeutige $q(x), r(x) \in K[x]$ mit $\deg r(x) < \deg b(x)$ und $a(x) = q(x) \cdot b(x) + r(x)$

Damit lassen sich Begriffe der Zahlentheorie auf Polynome übertragen.

► Teilbarkeit:

$d(x)$ ist Teiler von $p(x)$, wenn $p(x) = d(x) \cdot q(x)$ für ein $q(x)$

► Äquivalenz:

$a(x) \equiv b(x) \pmod{m(x)}$, wenn $m(x)$ die Differenz $a(x) - b(x)$ teilt

ggT und Irreduzibilität

Seien $p(x), q(x) \in K[x]$.

$d(x) \in K[x]$ heißt ggT von $p(x)$ und $q(x)$, wenn gilt:

- ▶ $d(x)$ teilt $p(x)$ und $q(x)$.
- ▶ Für jedes $d'(x)$, das $p(x)$ und $q(x)$ teilt, ist $d'(x)$ Teiler von $d(x)$.

Der ggT ist nur bis auf Multiplikation mit einer Konstante eindeutig bestimmt.

Der erweiterte euklidische Algorithmus berechnet:

- ▶ einen ggT $d(x)$ von $p(x), q(x)$
- ▶ $s(x), t(x)$ mit $d(x) = s(x)p(x) + t(x)q(x)$.

$p(x) \in K[x]$ mit $\deg p(x) > 0$ heißt **irreduzibel**, wenn gilt:

Ist $p(x) = a(x)b(x)$, dann ist $\deg a(x) = 0$ oder $\deg b(x) = 0$

Nullstellen

Ein $a \in K$ mit $p(a) = 0$ heißt **Nullstelle** von $p(x)$.

Lemma

a ist Nullstelle von $p(x)$ gdw. $x - a$ Teiler von $p(x)$ ist.

Beweis.

- ▶ **Richtung \leftarrow** : Wenn $(x - a) \mid p(x)$, dann ist $p(x) = (x - a) \cdot q(x)$ für ein $q(x)$.
Dann ist a natürlich eine Nullstelle: $p(a) = (a - a) \cdot q(a) = 0$.
- ▶ **Richtung \rightarrow** : Wenn a eine Nullstelle ist, dann dividieren wir $p(x)$ durch $x - a$.
Das heißt, es gibt $q(x), r(x)$, sodass $p(x) = (x - a) \cdot q(x) + r(x)$.
Dabei gilt, dass $\deg r(x) < \deg(x - a) = 1$, also $\deg r(x) \in \{-1, 0\}$, d.h. $r(x) = c$ für eine Konstante $c \in K$.

$$p(a) = (a - a) \cdot q(a) + c = 0 \text{ (da } a \text{ eine Nullstelle ist), d.h. } c = 0.$$

$$\text{Dann } (x - a) \mid p(x).$$



Nullstellen

Theorem

Ein Polynom $p(x) \neq 0$ mit $\deg p(x) = n$ hat höchstens n Nullstellen.

Beweis (durch vollständige Induktion über n).

- ▶ **Induktionsanfang:** Wenn $\deg p(x) = 0$, dann hat $p(x)$ keine Nullstellen.
- ▶ **Induktionsschritt:** Dann $\deg p(x) = n + 1$.
 - ▶ **Fall 1:** $p(x)$ hat keine Nullstellen. Trivial.
 - ▶ **Fall 2:** $a \in K$ ist eine Nullstelle von $p(x)$.

Nach dem letzten Lemma:

Es gibt $q(x)$, sodass $p(x) = (x - a) \cdot q(x)$ und $\deg q(x) = n$.

Ist $b \neq a$ eine Nullstelle, da $b - a \neq 0$, muss $q(b) = 0$.

Durch die Induktionshypothese gibt es maximal n Nullstellen von $q(x)$.

Somit gibt es maximal $n + 1$ Nullstellen von $p(x)$.



Nullstellen

Theorem (Fundamentalsatz der Algebra)

Jedes Polynom $0 \neq p(x) \in \mathbb{C}[x]$ mit $\deg p(x) > 0$ hat mindestens eine Nullstelle.

Körpererweiterung

Sei K ein Körper und $p(x) \in K[x]$.

Die Menge

$$K[x]/p(x) := \{q(x) \in K[x] \mid \deg q(x) < \deg p(x)\}$$

ist ein Vertretersystem für die Äquivalenzklassen von $K[x]$ modulo $p(x)$.

$K[x]/p(x)$ mit der Addition und Multiplikation modulo $p(x)$ bildet einen kommutativen Ring.

Körpererweiterung

Theorem

Ist $p(x)$ irreduzibel, so bildet $K[x]/p(x)$ mit der Addition und Multiplikation modulo $p(x)$ einen Körper.

Beweis.

Sei $a(x) \neq 0$ in $K[x]/p(x)$. Wir müssen zeigen, dass es $a^{-1}(x)$ gibt mit $a^{-1}(x) \cdot a(x) \equiv 1 \pmod{p(x)}$.

- ▶ **Fall 1:** $\deg a(x) = 0$, d.h. $a \in K$. Dann nehmen wir $a^{-1} \in K$ als Inverses: $a^{-1} \cdot a = 1$.
- ▶ **Fall 2:** $\deg a(x) \geq 1$. Da $p(x)$ irreduzibel ist, ist 1 ein ggT($a(x), p(x)$). Es gibt $s(x), t(x)$, sodass $1 = s(x)a(x) + t(x)p(x)$. Das heißt, $s(x)a(x) \equiv 1 \pmod{p(x)}$, wobei $s(x)$ das gesuchte Inverse ist. □

Der Körper $K[x]/p(x)$ enthält K als Unterkörper.

Beispiel: Erweiterung von \mathbb{Z}_2

Das Polynom $x^2 + x + 1$ ist irreduzibel in $\mathbb{Z}_2[x]$.

Betrachte den Körper $\mathbb{Z}_2[x]/(x^2 + x + 1)$.

Elemente sind lineare Polynome $0, 1, x, x + 1$.

Für das Polynom x gilt: $x^2 \equiv x + 1 \pmod{x^2 + x + 1}$.

Addition und Multiplikation:

+	0	1	x	x + 1
0	0	1	x	x + 1
1	1	0	x + 1	x
x	x	x + 1	0	1
x + 1	x + 1	x	1	0

·	0	1	x	x + 1
0	0	0	0	0
1	0	1	x	x + 1
x	0	x	x + 1	1
x + 1	0	x + 1	1	x

Also ist $\mathbb{Z}_2[x]/(x^2 + x + 1)$ isomorph zum Körper $\{0, 1, a, b\}$.

Beispiel: Erweiterung von \mathbb{R}

Betrachte den Körper $\mathbb{R}[x]/(x^2 + 1)$, wobei $x^2 + 1$ irreduzibel in $\mathbb{R}[x]$ ist.

Elemente sind lineare Polynome $ax + b$ für $a, b \in \mathbb{R}$

Für das Polynom x gilt: $x^2 \equiv -1 \pmod{x^2 + 1}$.

Addition:

$$(a_1x + b_1) + (a_2x + b_2) = (a_1 + a_2)x + (b_1 + b_2)$$

Multiplikation:

$$(a_1x + b_1)(a_2x + b_2) = a_1a_2x^2 + a_1b_2x + a_2b_1x + b_1b_2$$

Also:

$$(a_1x + b_1)(a_2x + b_2) \equiv (a_1b_2 + a_2b_1)x + (b_1b_2 - a_1a_2) \pmod{x^2 + 1}$$

Also ist $\mathbb{R}[x]/(x^2 + 1)$ isomorph zu \mathbb{C} .

Endliche Körper

Theorem

Für jede Primzahlpotenz p^n , wobei $n \in \mathbb{N} \setminus \{0\}$, gibt es einen (bis auf Isomorphie eindeutigen) Körper K mit $\text{char}(K) = p$ und $|K| = p^n$.

Beweis.

Konstruktion:

1. Wähle Primkörper \mathbb{Z}_p .
2. Sei $p(x)$ irreduzibel in $\mathbb{Z}_p[x]$ mit $\deg p(x) = n$.
3. Der gesuchte Körper ist $K = \mathbb{Z}_p[x]/p(x)$.

Eindeutigkeit ohne Beweis. □

Ende der 7. Vorlesung