Algebra Zusammenfassung

Jan Arends

1 Die Menge der ganzen Zahlen

1.1 Die Rechenstruktur $\mathbb{Z}$

1.2 Teilbarkeit

1.2.1 Division mit Rest

Seien $a \in \mathbb{Z} \wedge b \in \mathbb{N}$:

$$\exists q \in \mathbb{Z} \wedge \exists r \in \mathbb{N}_0 : a = b \cdot q + r$$

mit $0 \leq r < b$

Modulo Alternative Schreibweisen:

$$a = r(m) \Leftrightarrow a = m \cdot q + r \Leftrightarrow m | a - r$$

1.2.2 Division ohne Rest

Ess gilt für $b \neq 0$

$$b|a \Leftrightarrow \exists q \in \mathbb{Z} : a = b \cdot q$$

$$a|b(m) \Leftrightarrow a = m \cdot q + b$$

Korollar 1.2 Seiten $a, b, c, d, x, y \in \mathbb{Z}$:

	Aussage	Bemerkung
a)	$0 \| a$ nur dann, wenn $a = 0$	
b)	$a \| 0$	Für $a \in \mathbb{Z}$: $\frac{0}{a} = 0$
c)	$1 \| a$ und $a \| a$	triviale Teiler, $\frac{a}{1} = a$, $\frac{a}{a} = 1$
d)	$a \| b \wedge b \| c \Rightarrow a \| c$	Transitivität
e)	$a \| b \wedge c \| d \Rightarrow ac \| bd$	
f)	$ca \| cb \Rightarrow a \| b$	Kürzungsregel (Für $c \neq 0$)
g)	$a \| b \wedge a \| c \Rightarrow a \| xb + yc$	Linearkombinationsregel
h)	$a \| b \wedge a \| b + c \Rightarrow a \| c$	
i)	$a = bc + d \wedge b \| a \implies b \| d$	
j)	$a \| b, b \| a \implies a = b \vee a = -b$	
k)	$bc \| a \implies b \| a \wedge c \| a$	

1.2.3 Restklassen

Äquivalenzrelation

1.3 Größter gemeinsamer Teiler

1.3.1 Das Lemma von Bézout - Linearkombination

Seien $a, c \in \mathbb{Z}$. Dann gilt

- $\exists x, y \in \mathbb{Z} : ax + by = (a, b)$
- $(a, b) = 1 \Rightarrow \exists x, y \in \mathbb{Z} : ax + by = 1$

Die Koeffizienten $x, y \in \mathbb{Z}$ erhält man mit dem erweiterten euklidischen Algorithmus.

1.3.2 Berechnung des GGTs

- Euklidischer Algorithmus
- Anhand von Primfaktorzerlegung

Erweiteter euklidischer Algorithmus Zum Berechnen von:

- Linearkombination (s.o.)
- Modularen Inversen

2 Gruppen

Definition 2.2 - Gruppenaxiome Sei $\mathcal{A}(M, *)$. Falls $\mathcal{G}$:

$$\begin{aligned}
abgeschlossen &\implies algebraischeStruktur & \forall a, b \in M : a * b \in M \\
assoziativ &\implies Halbgruppe & \forall a, b, c \in M : (a * b) * c = a * (b * c) \\
Einselement &\implies Monoid & \forall a \in M : a * e = e * a = a \\
Inverse &\implies Gruppe & \forall a \in M \exists a^{-1} \in M : a * a^{-1} = a^{-1} * a = e \\
Kommutativ &\implies zusatzabelsch & \forall a, b \in M : a * b = b * a
\end{aligned}$$

$\mathcal{G}$ endlich $\implies ord_{\mathcal{G}} = |\mathcal{G}|$ die Ordnung von $\mathcal{G}$ (Gruppenordnung).
Sei $a \in \mathcal{G}$ und e das Einselement von $\mathcal{G}$. Dann heißt

$$ord_{\mathcal{G}}(a) = min\{k \in \mathbb{N} | a^k = e\}$$

die Ordnung von a in $\mathcal{G}$.

2.1 Untergruppen

$$< a >= \left\{a^1, a^2, \ldots, a^n\right\}$$

wobei $a^{n+1} = a(m)$. Der einfachhalthalber: Jeweils Vorgänger mit a multiplizieren.

Untergruppenkriterium Sei $\mathcal{G} = (M, *)$und $U \subseteq M$. Dann ist $\mathcal{G}_U$ eine Untergruppe von $\mathcal{G}$ genau dann. wenn gilt: $a, b, \in \mathcal{G}_U$, dann ist auch

$$a^{-1} * b \in \mathcal{G}_U$$

bzw.

$$a * b^{-1} \in \mathcal{G}_U$$

Zyklische Gruppen Gdw. $\exists a :< a >= \mathcal{G}.a$ heißt Generator.
Zyklische Gruppen sind abelsch.

2.2 Faktorisierung von Gruppen

Nebenklassen Sei $G = (M, *)$ Gruppe, $U \subseteq M$ und $\mathcal{G}_U$ Untergruppe von G sowieso $a \in G$ Linksnebenklasse:

$$a * G_U$$

Rechtsnebenklasse:

$$G_U * a$$

a heißt Repräsentant der Nebenklasse.
Gilt $\forall a \in \mathcal{G} : a * \mathcal{G}_U = \mathcal{G}_U * a$, dann heißt G_U Normalteiler von $\mathcal{G}$ (automatisch, wenn Operator kommutativ). Außerdem: Nebenklassen sind unabhängig vom Repräsentaten.

Faktorgruppen Sei $\mathcal{G}_\mathcal{U}$ Normalteiler von $\mathcal{G}$. Dann bildet $\mathcal{G}/\mathcal{G}_U$bzw. $\mathcal{G}/ < a >$ mit:

$$(a * \mathcal{G}_U) *_U (b * \mathcal{G}_U) = (a * b) * \mathcal{G}_U$$

die sog. Faktorgruppe.
Am einfachsten dann Verknüpfungstafel aufstellen.

Satz von Lagrange (Ausschnitt)

- Nebenklassen sind entweder identisch oder disjunkt.
- Die Nebenklassen legen eine Äquivalenzrelation und damit eine Partition auf $\mathcal{G}$ fest.
- Alle Links- und alle Rechtsnebenklassen haben dieselbe Anzahl an Elementen, nämlich die der Untergruppe.
- Die Ordnungen von Untergruppen sind also immer Teiler der Gruppenordnung.

Funktionen/Abbildungen Total: $\forall_{x \in A} \exists_{y \in B}$
Injektivität: Jedes Element der Zielmenge hat höchstens ein Urbild.
Surjektivität: Jedes Element der Zielmenge hat mindestens ein Urbild.
Bijektivität: Abbildung ist total, injektiv und surjektiv

Gruppenhomomorphismus Seien $\mathcal{G}_1 = (M_1, *_1)$ und $\mathcal{G}_2 = (M_2, *_2)$ zwei Gruppen sowie $\varphi : \mathcal{G}_1 \to \mathcal{G}_2$ eine Abbildung. φ heißt (Gruppen-)Homomorphismus von $\mathcal{G}_1$ nach $\mathcal{G}_2$, falls

- φ total ist
- $\forall_{a,b \in \mathcal{G}_1}$ die Strukturgleichung $\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b)$ erfüllt ist.

Isomorphismus falls φ bijektiv, d.h.:

- injektiv
- surjektiv

Schreibweise: $\mathcal{G}_1 \cong \mathcal{G}_2$

Automorphismus Isomorphismus auf sich selbst: $\mathcal{G} \cong \mathcal{G}$

Kerne von Homomorphismen Sei $\varphi : \mathcal{G}_1 \to \mathcal{G}_2$ Homomorphismus. Der Kern von φ enthält alle Elemente von $\mathcal{G}_1$, die auf das Einselement von $\mathcal{G}_2$ abgebildet werden:

$$Kern(\varphi) = \{x \in \mathcal{G}_1 | \varphi(x) = e_2\}$$

$|Kern(\varphi)| = 1 \Rightarrow \varphi$ ist injektiv.

3 Ringe, Integritätsbereiche und Körper

3.1 Ringe

Die alg. Struktur $R = (M, *_1, *_2)$ heißt Ringe, falls

- $(M, *_1)$ abelsche Gruppe
- $(M, *_2)$ Halbgruppe
- Distributivgesetze erfüllt sind: $\forall_{a,b,c \in M}$:

$$a *_2 (b *_1 c) = (a *_2 b) *_1 (a *_2 c)$$

$$(b *_1 c) *_2 a = (b *_2 a) *_1 (c *_2 a)$$

Sonstige Eigenschaften

- $*_2$ kommutativ $\implies$ kommutativer Ring
- $(M, *_2)$ Monoid $\implies$ Ring mit Einselement

Bsp: $(\mathbb{Z}_m, +, \cdot)$ der ganzen Addition und Multiplikation bildet kommutativen Ring mit Einselement.

$(M, *_1)$ ein abelsches Monoid und $(M, *_2)$ ein Monoid $\implies$ Semiring

Einheiten

- $\mathcal{R}$ Ring, $a \in \mathcal{R}$ (multiplikativ) invertierbar $\implies$ Einheit.
- $\mathcal{R}^*$ ist die Menge aller Einheiten von $\mathcal{R}$.
- $\mathcal{R}$ Ring mit Einselement $\implies$ $\mathcal{R}^*$ bildet (multiplikative) Gruppe, die sog. Einheitsgruppe.

Nullteiler Sei $\mathcal{R}$ ein Ring, $a \in \mathcal{R}$ mit $a \neq 0$.
$\exists_{b \in \mathcal{R}} a \cdot b = 0 \implies$ Nullteiler in R.
Enthält $\mathcal{R}$ keine Nullteiler $\implies$ $\mathcal{R}$ nullteilerfrei.

Bsp: Besitzen Nullteiler: $\mathbb{Z}_4, \mathbb{Z}_6, \mathbb{Z}_8, \mathbb{Z}_{14}$

3.2 Integritätbereich

Ring mit folgenden Eingeschaften:

- kommutativ
- nullteilerfrei

Bsp: $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7$

3.3 Körper

$\mathcal{A} = (\mathcal{M}, *_1, *_2)$ ist ein Körper, falls:

- $(\mathcal{M}, *_1)$ abelsche Gruppe mit Einselement e_1,
- $(\mathcal{M} - \{e_1\}, *_2)$ abelsche Gruppe mit Einselement e_2,
- Distributivgesetz gilt: $\forall_{a,b,c \in \mathcal{M}}$:

$$a *_2 (b *_1 c) = a *_2 b *_1 a *_2 c$$

Alternativ:

Körper Sei $\mathcal{A} = (\mathcal{M}, *_1, *_2)$ ein Ring. Falls

- $(\mathcal{M} - \{e_1\}, *_2)$ abelsche Gruppe

dann ist $\mathcal{R}$ ein Körper. Beispiele: $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$
Korollar:
Sei $\mathcal{K}$ Körper, dann ist $\mathcal{K}^* = \mathcal{K} - 0$
Jeder Körper ist ein Integritätsbereich $\rightarrow$ nullteilerfrei

3.4 Sätze von Euler und Fermat

Eulersche φ-Funktion

$$\varphi : \mathbb{N} \rightarrow \mathbb{N} : \varphi(m) = ord_{\mathbb{Z}_m^*} = |\mathbb{Z}_m^*|$$

Korollar 3.7:

a) Es ist $\varphi(m) = \{a \in \mathbb{Z}_m | (a, m) = 1\}$

b) Für $p \in \mathbb{P} : \varphi(p) = p - 1$

Korollar 3.8: Sei $p \in \mathbb{P}, \alpha \in \mathbb{N}, \alpha \geq 2$, dann gilt $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$

Sei $a = c \cdot b$ und c und b teilerfremd, dann gilt: $\varphi(a) = \varphi(b \cdot c) = \varphi(b) \cdot \varphi(c)$ Weitere Beobachtung: Ergebnis von φ ist immer eine gerade Zahl.

Satz von Euler

$$\forall_{a \in \mathbb{Z}_m^*} : a^{\varphi(m)} = 1(m)$$

Kleiner Satz von Fermat Sei $p \in \mathbb{P}$

$$\forall_{a \in \mathbb{F}_p^*} : a^{p-1} = 1(p)$$

Äquivalent dazu: $a^m = a(m)$
Korollar:

a) Sei $p \in \mathbb{P}$ und $a \in \mathbb{N} = 1$, dann ist $a^{p-1} = 1(p)$

b) Sei $n \in \mathbb{N}$ und $a \in \mathbb{N}$ mit $(a, b) = 1$ und $a^{n-1} \neq 1(n)$, dann ist $n \notin \mathbb{P}$

3.5 Polynome

4 Erweiterung endlicher Körper

...

5 Modulare Arithmetik

5.1 Algorithmus, der aus dem Chinesischen Restsatz resultiert

Bedingung: gewählte Module müssen paarweile teilerfremd sein, also $(m_i, m_j) = 1$.

1. Lineares Kongruenzgleichungssystem aufstellen

$$\begin{aligned} x &= a_1(m_1) \\ x &= a_2(m_2) \\ &\dots \\ x &= a_n(m_n) \end{aligned}$$

2. Produkt $M = m_1 \cdot m_2 \cdot \ldots \cdot m_n$ der Moduln und $M_i = \frac{M}{m_i}$ berechnen

3. Inversen b_i der M_i modulo m_i bestimmen

$$\begin{aligned} b_1 \cdot M_1 &= 1(m_1) \\ b_2 \cdot M_1 &= 1(m_2) \\ &\dots \\ b_n \cdot M_n &= 1(m_n) \end{aligned}$$

4. Gleichung lösen

$$x = a_1 \cdot b_1 \cdot M_1 + a_2 \cdot b_2 \cdot M_2 + \ldots + a_n \cdot b_n \cdot M_n$$

5.2 Modulare Addition und Multiplikation

5.3 Effizientes Protenzieren

$b^e(m)$

1. Exponenten in Binärdarstellung umwandeln. Länge n feststellen
2. Faktoren $a_i, 0 \leq i < n$ mitels wiederholten Quadrieren berechnen. Alles modulo m

$$
\begin{aligned}
a_0 &= b^{2^0} = b^1 = b \\
a_1 &= b^{2^1} = b^2 = b \cdot b \\
a_2 &= b^{2^2} = b^4 = b^2 \cdot b^2 \\
a_3 &= b^{2^3} = b^8 = b^4 \cdot b^4 \\
&\vdots \\
a_n &= b^{2^n} = b^{\cdots} = b^{2^{k-1}} \cdot b^{2^{k-1}}
\end{aligned}
$$

3. Produkt der a_i berechnen, bei denen das i in der Binärdarstellung des Exponenten auf 1 gesetzt sind. Am einfachsten: Schrittweise bei gleichzeitiger Reduktion.

6 Primzahlen und Primzahltests

Pseudoprimzahl Ist $m \in \mathbb{N} - \mathbb{P}$ mit $(2, m) = 1$ und $2^m = 2(m) \Rightarrow$ Pseudoprimzahl.
Anders ausgedrückt also Zahlen, bei denen der Fermat-Test *prim?* ausgeben würde, es aber keine Primzahlen sind.

Andere Basen auch möglich: Dann pseudoprim zur Basis a.

Carmichael-Zahlen Eine zusammengesetze Zahl $m \in \mathbb{N}$, $m \geq 3$ heißt Carmichel-Zahl $\Leftrightarrow$ für alle Basen a mit $(m, a) = 1$ der Fermat-Test *prim?* ausgibt.

Fermat-Test m soll untersucht werden: Wähle (zufällig) $a \in \mathbb{Z}$ mit $(a, m) = 1$. Gilt:

- $a^{m-1} = 1(m)$ bzw. $a^m = a(m) \Rightarrow$ Ja $\rightarrow$ prim?
- ansonsten Nein $\rightarrow$ nicht prim!!

Miller-Rabin Seien $m \in \mathbb{N}$ (die zu untersuchende Zahl).

- Bestimme s und d anhand Zerlegung, sodass gilt $m-1 = 2^s \cdot d$ gilt mit s als größt möglichen Wert.
- $b \in \mathbb{Z}_m^*$ ist die vorgegebene Basis.
- Ermittel Anzahl Elemente in b-Sequenz und stell ggf. Exponenten auf
- Bilde die b-Sequenzen. Angefangen bei b^d kann man daraufhin immer das Ergebnis quadrieren.
- Letzes Element der b-Sequenzen ist $b^{2^s \cdot d}$

7 Kryptographie

...

8 Vektorräume

Anzahl Elemte im Vektorraum über $\mathcal{K}$ mit $|K| = k$ und $dim(\mathcal{V}) = n$ ist:

$$|\mathcal{V}| = k^n$$

Lin. Unabhängigkeit Verschiedene Möglichkeiten zur Prüfung:

1. Schnellste Lösung:
Man sieht, dass sich ein Vektor aus den anderen erzeugen lässt. Dann lin. unab.
2. Falls eine quadratische Matrix erzeugt werden kann und Determinate $\neq 0$, dann lin. unab.
3. Prüfe, ob für jede Linearkombination der Vektoren gilt:

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots \lambda_n v_n = \vec{0}$$

$$\Leftrightarrow \lambda_1, \lambda_2, \cdots \lambda_n = 0$$

D.h. LGS aufstellen und auflösen.

Erzeugendensystem Menge an Vektoren $\mathcal{U} \subseteq \mathcal{V}$ durch welche jeder Vektor im Raum dargestellt werden kann:

$$Span_{\mathcal{U}} = \mathcal{V}$$

Basis

- Erzeugendensystem mit linear unabhängigen Vektoren
- Lösung für einen Ergebnisvektor ist eindeutig

Standardbasen: Z.b. für $\mathbb{R}^2 : \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Dimension Die Anzahl Basisvektoren ist die Dimension des Vektorraums: $dim(\mathcal{V})$

Unterraum $\mathcal{U} \subseteq \mathcal{V}$ Bedingungen:

- $\mathcal{U} \neq 0$
- $\forall a, b \in \mathcal{U} : a + b \in \mathcal{U}$ - Abgeschlossen
- $\forall \lambda \in \mathcal{K}, \forall a \in \mathcal{U} : \lambda a \in \mathcal{U}$ - Linearkombination wieder im Unterraum

8.1 Lineare Gleichungssysteme und Matrizen

Matrixmultiplikation Die Anzahl an Spalten von A muß mit der Anzahl an Zeilen von B übereinstimmen. Die Matrixmultiplikation ist assoziativ, aber im allgemeinen nicht kommutativ.

Lineare Abbildung falls

Zeilenreduktion Elementaroperationen:

- $C(i,j)$: Vertauschen der Zeilen i und j
- $M(i,\alpha)$ Multiplikation aller Elemente von Zeile i mit dem α-fachen
- $S(i,j,\alpha)$ Addition aller Elemente von Zeile i mit den α-fachen der Elemente der j-ten Zeile

Für eine Matrix in *Zeilenstufenform* gelten folgende drei Eigenschaften:

1. Das erste von Null verschiedene Element einer Zeile ist 1. Dieses Element heißt *Pivot* oder Pivotelement
2. Das Pivotelement in Zeile i + 1 steht rechts von dem in Zeile i.
3. Alle Spaltenelemente oberhalb eines Pivots sind Null.

Rang einer Matrix Die maximale Anzahl linear unabhängiger Zeilen- bzw. Spaltenvektoren einer Matrix.

Invertierbarkein von Matrixen Gdw die Determinate ungleich Null ist.

Gaußsches Eliminationsverfahren Zum Lösem von LGS in Matrixform.

1. Erweiterte Koeffizientenmatrix $(A|b)$ aufstellen.
2. Zeilenreduktionen anwenden bis Einheitsmatrix eingebaut ist
3. Rang bestimmen
4. Anhand dessen kann man feststellen, ob LGS
   - keine: $rang(A|b) > rang(A)$ (bedeutet, dass in der b-Spalte steht ein Pivot)
   - eine eindeutige: $rang(A|b) = rang(A) = n$
   - oder mehrdeutige Lösungen: $rang(A|b) = rang(A) < n$

   hat.
5. Dimension feststellen: $dim() = n - rang(A)$. Nun weiß man die Anzahl Basisvektoren.
6. Wähle allgemeine λ Lösung (?!)