Karlsruher Institut für Technologie

Malte Voß
Larissa Bihr

Vokabeln der Algebra und Zahlentheorie

18. Oktober 2020, `https://github.com/vossmalte`

1 Teilbarkeit

Def. d teilt $n \Leftrightarrow \exists t : t \cdot d = n$
Begriffe: Teiler, Vielfaches, ggT, kgV

Bem. ggT $ggT(0, m) = m$, $ggT(m, n) = ggT(m, n - m)$

Def. Euklidischer Algorithmus. $a \overset{!}{<} b$. Solange $b - a > 0$: $b := b - a$

Bem. mit dem eukl. Alg. kann man auch den ggT als Linearkombination darstellen.

Def. Kongruenz $k \equiv l(\mod n) \Leftrightarrow n|k - l$

Bem.
- $g = ggT(n, m) \Rightarrow ggT(\frac{n}{g}, \frac{m}{g}) = 1$
- m, n teilerfremd und $m \mid nu \Leftrightarrow m \mid u$
- $kgV(m, n) \cdot ggT(m, n) = m \cdot n$

Def. Primzahlen ...

Bem. Fundamentalsatz der Arithmetik: Jede Zahl hat eine Primfaktorzerlegung

Def. p-adische Bewertung. $v_p(k)$ ist die höchste Potenz von p, die k teilt: $p^{v_p(k)} \mid k$

Bem.
- $b \mid a \Leftrightarrow \forall p \in \mathbb{P} : v_p(b) \leq v_p(a)$
- ggT von a und b ist $\prod_{p \in \mathbb{P}} p^{\min(v_p(a), v_p(b)}$
- kgV von a und b ist $\prod_{p \in \mathbb{P}} p^{\max(v_p(a), v_p(b)}$

Satz. kl. von Fermat: $p \in \mathbb{P}$ und $c \in \mathbb{Z} \Rightarrow p \mid c^p - c$ (hiermit kann prim wiederlegt werden)

Bem. Lücken: $k \in \mathbb{N}$. Zwischen $M := (k + 2)! + 2$ und $M + k$ liegt keine Primzahl

2 Gruppen

2.1 Magmen

Def. Magma $(M, *)$ ist eine Menge mit einer Verknüpfung $* : M \times M \to M$
- ist die Verknüpfung assoziativ, so nennt man das Magma Halbgruppe
- Eine Halbgruppe mit neutralem Element heißt Monoid
- es gibt auch kommutative Magmen
- Bsp: Abb(D,D) mit Komposition ist ein Magma. Leeres Magma. Triviales Magma.
- $U \subset M$ heißt Untermagma wenn $U * U \subset U$. Untermagmen kann man schneiden und diese bleiben Untermagmen
- Sei $X \subset M$, das Magmenerzeugnis $\langle X \rangle$ von X ist der Schnitt alles Untermagmen, die X enthalten.
- für assoz. Magmen gilt: $\langle X \rangle = \cup_{n \in \mathbb{N}} X_n$ mit $X_1 = X, X_{n+1} = X * X_n$

2.2 Der Gruppenbegriff

Def. Gruppe

- Sei $(M, *)$ ein Monoid mit neutralem Element e. Ein Element x heißt invertierbar, wenn ein $y \epsilon M$ exisitiert, sodass $x * y = y * x = e$. Bezeichne mit M^x die Menge aller invertierbaren Elemente in M.
- Eine Gruppe ist ein Monoid, in dem jedes Element invertierbar ist.
- Sei $(M, *)$ eine Gruppe. $(M, *)$ ist kommutativ/abelsch wenn sie als Magma kommutativ ist.

Def. Untergruppe Sei $(G, *)$ eine Gruppe. Dann ist eine Untergruppe von G ein nichtleeres Untermagma U, das unter der Inversenbildung abgeschlossen ist.
Schreibe: $U \leq G$

- Die Gruppe $(\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Q}, +)$.
- Die Gruppe der ganzen Zahlen $\mathbb{Z}$ mit der Addition als Verknüpfung. Die triviale Untergruppe ist die 0. AUßerdem gilt für jede natürliche Zahl n die Teilmenge
  $n\mathbb{Z} := nk | k \epsilon \mathbb{Z}$
  Wir halten fest: Die Untergruppen von $\mathbb{Z}$ sind genau die Mengen $n\mathbb{Z}$ mit $n \epsilon \mathbb{N}_0$

Bem. Durchschnitt von Untergruppen: Sei G Gruppe, I nichtleere Menge und für jedes $i \epsilon I$ gibt es eine Untergruppe U_i von G geben. Dann ist $\cap_{i \epsilon I} U_i$ eine Untergruppe von G.

Def. Gruppenerzeugnis: Sei M Teilmenge der Gruppe G, sei I die Menge aller Untergruppen von G, die M enthalten.
$\langle M \rangle := \cap_{i \epsilon I} i$ ist Gruppenerzeugnis von M oder die von M erzeugte Untergruppe von G.

- Es ist die kleinste Untergruppe von G, die M enthält.

Def. zyklisch: Eine Gruppe G heißt zyklisch, wenn es ein Element $a \epsilon G$, sodass $G = \langle a \rangle$

Def. Ordnung Die Mächtigkeit/Kardinalität einer Gruppe nennt man auch Ordnung. Die Ordnung eines Elemtens $g \epsilon G$ ist definiert als die Ordnung der von g erzeugten Untergruppe.

- Wenn $g \epsilon G$ endliche Ordnung, dann ist diese gleich der kleinsten natürlichen Zahl k, für die $g_k = e_G$ gilt.

Bem. Satz von Lagrange: Sei G endl. Gruppe und H Untergruppe von G. Dann gilt: $\#H \mid \#G$

Def. Index: Wenn $H \leq G$ zwei Gruppen, dann heißt die Anzahl der Äquivalenzklassen der Index von H in G. Schreibe $(G : H)$.
Es gilt demnach für alle Gruppen $(G : H) = \frac{\#G}{\#H}$.

2.3 Homomorphismen zwischen Gruppen

Def. Gruppenhomomorphismus: Sei $(G, *)$ und $(H, \cdot)$ zwei Gruppen. Ein Homomorphismus von G nach H ist eine Abbildung $f : G \to H$, für die gilt:

3 Teilbarkeit und Primelemente

3.1

Def. Assoziert sind a und b wenn $\exists e \in R^\times : b = a \cdot e$

Bem. Ordnung entsteht durch Teilbarkeit: $aR^\times \leq bR^\times \Leftrightarrow a|b$

Bem. teilerfremd sind a und b, wenn die einzigen Teiler Einheiten sind.

Def. Hauptideal I ist ein Ideal, für das gilt: $I = Rg = (g)$

Def. Hauptidealring ist ein nullteilerfreier kommutativer Ring, in dem jedes Ideal Hauptideal ist.

Bem. ggT: für $I = Rg = ax + by \mid x, y \in R$ ist $g = \mathrm{ggT}(a, b)$

Korollar. Erzeuger $Rg = Rh \Leftrightarrow g, h$ sind assoziert.

Def. Euklidischer Ring ist ein nullteilerfreier kommutativer Ring R mit $\gamma : R \to \mathbb{N}_0$, wobei $\gamma(r) = 0 \Leftrightarrow r = 0$ und $\forall a, b \neq 0 \exists c : \gamma(a - bc) < \gamma(b)$

Bem. Euklidische Ringe sind Hauptidealringe

Bem. Chinesischer Restsatz: $R/(Rrs) \cong R/(Rr) \times R/(Rs)$

3.2 Arithmetik in Hauptidealringen

Def. m irreduzibel: $\Leftrightarrow \forall a, b : m = ab \Rightarrow a$ oder $b \in R^\times$

Def. p prim: $\Leftrightarrow \forall a, b : p \mid ab \Rightarrow p|a$ oder $p \mid b$

Korollar. Primelemente von 0 verschieden sind immer irreduzibel

Korollar. Im Hauptidealring sind irreduzible Elemente prim.

Satz. Primzerlegung $\mathbb{P}_R$ ist Vertretersystem der Primelemente. Dann ist $\forall r \in R$ ein eindeutiges Produkt assoziert aus Elementen in $\mathbb{P}_R$.

Bem. Restklassenkörper R/Rg ist Körper $\Leftrightarrow g$ irreduzibel

Def. Primideal: $xy \in I \Rightarrow x \in I$ oder $y \in I$

4 Übersicht über Strukturen und Homomorphismen

Struktur	Homomorphismus
Magma: $(M, *)$	$\phi(m * n) = \phi(m) * \phi(n)$
Halbgruppe ist assoziatives Magma.	
Monoid ist Halbgruppe mit neutralem Element.	$\phi(e) = e$
Gruppe ist Monoid und alle Elemente sind invertierbar.	$\phi(x^{-1}) = \phi(x)^{-1}$ Kern$\phi = \phi^{-1}(\{e\})$ ist Untergruppe $\phi(G)$ ist Untergruppe ϕ injektiv $\Leftrightarrow \phi^{-1}(\{e\}) = \{e\}$
Normalteiler N von G: $\forall g : gNg^{-1} = N$	Jeder Kern ist Normalteiler
Faktorgruppe G/N mit $(gN) \cdot (hN) := ghN$	Kern$\phi = N \Rightarrow gN \mapsto \phi(g)$ ist Isomorphismus H Untergruppe: $H/(N \cap H) \cong (HN)/N$
Gruppenoperationen $G \times M \to M$ mit $e \cdot m = m$ und $(gh)m = g(hm)$ Bahn, Stabilisator, Fixpunkt, transitiv	
Ring $(R, +, \cdot)$ ist bzgl + abelsche Gruppe und bzgl $\cdot$ Monoid mit Distributivgesetzen.	Kern$\phi = \phi^{-1}(0)$ $\phi(R^\times) \subset S^\times$
Integritätsbereich ist kommutativer, nullteilerfreier Ring.	
Körper ist kommutativer Ring und $R^\times = R \setminus 0$	
Ideal: $\forall x \in I, r \in R : xr, rx \in I$ ist ein Normalteiler bzgl +	
Faktorring R/I	$I \subset$ Kern$\phi \Rightarrow \exists \tilde{\phi} : \phi = \tilde{\phi} \circ \phi$
R-Modul M ist abelsche Gruppe mit $(r + s)m = rm + sm$ $r(m + n) = rm + rn$ $(rs)m = r(sm)$ $1m = m$	Module über Körpern sind Verktorräume
R-Algebra A mit $\sigma : R \to A$ mit $\sigma(r)a = a\sigma(r)$	