Vorlesung Algebra

SoSe'21, hhu
K. Halupczok

A0: Einleitung und Sätze in $\mathbb{Z}$

Stichworte: Über die Vorlesung Algebra,
Satz von der eindeutigen PFZ in $\mathbb{Z}$, Satz von der Division mit Rest in $\mathbb{Z}$,
Erklärung des Farbcodes des Skripts,
Notationen und gängige Bezeichnungen / Abkürzungen

0.1. Einleitung: Dieses Pflichtmodul bietet eine Einführung in die Grundideen der modernen Algebra und vermittelt die für jede Mathematikerin und jeden Mathematiker nützlichen Werkzeuge dieser Strukturwissenschaft.

Wir folgen dem Standardkonzept "Gruppe – Ringe – Körper – und zurück". Der Vorlesungsteil "und zurück" kann noch als Teil des Kapitels "Körper" verstanden werden, das die Brücke zur Gruppentheorie zurückschlägt, indem es die Galoistheorie behandelt.

In dieser Vorlesung stellen wir nach und nach ein Skript bereit, das knapp und kurz den Stoff in Form eines beinahe perfekten mathematischen Textes darstellt. Zum Verständnis ist aber der Besuch der eigentlichen Vorlesungstermine unerlässlich, da dort dieses Skript ausgeführt, erläutert, ergänzt, in Beispielen besprochen, und in die mündliche Kommunikation der Algebra eingeführt wird. Dies wird in den Übungen gefestigt. Die Übungen dienen darüberhinaus zur Vertiefung, Festigung und Beherrschung des Stoffs. Ziel ist es, dabei die "Werkzeuge" der Algebra anwenden zu lernen.
Wesentliche Voraussetzung zum Verständnis der Veranstaltung "Algebra" ist ein früherer Besuch der Veranstaltungen "Lineare Algebra I und II".
Es werden Grundlagen über das Rechnen mit $\mathbb{Z}$ benutzt, die wir hier nennen.

0.2. Def.: $a, b \in \mathbb{Z}$. a heißt Teiler von b, falls $\exists c \in \mathbb{Z}: b = ac$.

Notation: $a|b$, lies "a teilt b". (↑ c heißt gelegentlich "Gegenteiler")

Gilt $a|b$, heißt b Vielfaches von a.

$p \in \mathbb{Z}$ heißt prim, falls sie genau zwei natürliche Teiler besitzt.

(Eine prime natürliche Zahl heißt Primzahl (Kurz: PZ).)

0.3. Bem.: Ist p prim, so ist also $p \in \mathbb{Z} \setminus \{\pm 1, 0\}$, und $\pm 1, \pm p$ sind die einzigen Teiler von p. Die Menge $\mathbb{P} := \{p \in \mathbb{N};\ p \text{ prim}\} = \{2, 3, 5, 7, 11, 13, \ldots\}$ bezeichnet die Menge aller Primzahlen.

Es gilt der Satz über die eindeutige Primfaktorzerlegung (PFZ) in $\mathbb{Z}$, auch: "Fundamentalsatz der Arithmetik":

0.4. Satz: Jede ganze Zahl $a \neq 0$ ist eindeutig Produkt von Primzahlen. D.h.:
$\forall a \in \mathbb{Z}\ \exists p_1, \ldots, p_m > 0$ prim: $a = \pm p_1 \cdots p_m$, und die Folge $p_1, \ldots, p_m$ ist bis auf Permutation ihrer Glieder eindeutig bestimmt.

[Beweis: s. lineare Algebra oder elementare Zahlentheorie oder später in Kapitel A13]
↳ dort kurz: "$\mathbb{Z}$ ist faktoriell"

Weiter werden wir die Division mit Rest verwenden:

0.5 Satz (Division mit Rest in $\mathbb{Z}$):

1.) $\forall a \in \mathbb{Z}\ \forall m \in \mathbb{N}\ \exists r \in \mathbb{N}_0,\ r < m: a = \lfloor \frac{a}{m} \rfloor m + r$,

wo $\lfloor x \rfloor := \max\{m \in \mathbb{Z};\ m \leq x\}$ die Gaußklammer bezeichnet.

2.) In der Darstellung $a = bm + r$ mit $b \in \mathbb{Z}$, $r \in \mathbb{N}_0$, $r < m$, sind b und r für alle $a \in \mathbb{Z}$ und alle $m \in \mathbb{N}$ eindeutig festgelegt.

Bew.: 1.): Es ist $\lfloor \frac{a}{m} \rfloor \leq \frac{a}{m} < \lfloor \frac{a}{m} \rfloor + 1$, also $0 \leq a - \lfloor \frac{a}{m} \rfloor m < m$.

Dies ist die Ungleichung für r, es folgt 1.).

2.): Es gelte $bm + r = a = b'm + r'$ mit $0 \leq r, r' < m$.

Dann ist $(b - b')m = r' - r$, wobei $-m < r - r' < m$,

was nur mit $b - b' = 0 = r' - r$ möglich ist. $\square$

0.6. Erklärung des Farbcodes des Skripts: (kann nicht immer konsequent angewendet werden)

rot unterstrichen: (ausgeführte) Definitionen

gelb unterstrichen: definierte Kurznotationen, Symbole und Kurzformeln in Definitionen

rot und schwarz unterstrichen: Begriffe, die definiert werden

blau unterstrichen: Referenzen

grün unterstrichen: Aussagen, die behauptet werden, etwa Sätze/Lemmas/Beispiele ...

rosa unterstrichen: markiert verwendete Beweisideen, wesentliche Beweisschritte

Ü Übungssmiley: vgl. Übungen/Übungsaufgaben

0.7. Notationen/gängige Bezeichnungen/Abkürzungen (weitere Abkürzungen werden im Skript definiert)

OE ohne Einschränkung (für o.B.d.A. = ohne Beschränkung der Allgemeinheit)

VI	vollständige Induktion	bel.	beliebig	Univ. Eig.	
IV	Induktionsvoraussetzung	(gen.) z.z.	(genügt,) zu zeigen	Universelle Eigenschaft	
□	qed, Beweisende	El.	Element	min/max	mini/maximum

$\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ die Zahlbereiche der natürlichen Zahlen, der nat. Zahlen mit 0, der ganzen Zahlen, der rationalen Zahlen, der reellen Zahlen, der komplexen Zahlen

PFZ	Primfaktorzerlegung	PZ	Primzahl	max.	maximal
$\leq$ UG	Untergruppe	wohldef.	wohldefiniert	deg	Grad
$\trianglelefteq$ NT	Normalteiler	eind.	eindeutig	assoz.	assoziiert
$\hookrightarrow$ inj.	injektiv	eind. best.	eind. bestimmt	(un)endl.	(un)endlich
$\twoheadrightarrow$ surj.	surjektiv	Eind.	Eindeutigkeit	endl. erz.	endlich erzeugt
bij.	bijektiv	Ex./ex.	Existenz/existiert	paarw.	paarweise
det	Determinante	Bez.	Bezeichnung	pwv.	paarweise verschieden
Hom.	Homomorphismus	Div.	Division	betr.	betrachte
Aut.	Automorphismus	im	Bild	r.S.	rechte Seite
Iso(m.)	Isomorphismus	ker	Kern	l.S.	linke Seite
$\cong$ isom.	isomorph	Ann.	Annahme	Endo	Endomorphismus
Gruppenop.	Gruppenoperation	$\lightning$	Widerspruch	lin. Abb.	lineare Abbildung
op.	operiert	#	Kardinalität	Komm.	kommutativ
ab.	abelsch	Gr.	Gruppe	K-VR	K-Vektorraum