Simon King, FSU Jena
Fakultät für Mathematik und Informatik
Henicke, Kraume, Lafeld, Max, Rump

Lineare Algebra für *-Informatik

FMI-MA0022

Wintersemester 2020/21 Übungsblatt 4

Liveaufgaben für 02./03.12.2020

Repetition von HA 3.4: Nullteilerfreie Ringe sind multiplikativ kürzbar.

Präsenzaufgabe 4.1: *Endliche Primkörper*

a) Schulbegriff: $p \in \mathbb{N}_{>1}$ ist ***Primzahl*** $:\Leftrightarrow \nexists a, b \in \mathbb{N}_{>1}\colon\ p = ab$. In der Algebra nennt man dies nicht Primzahl, sondern „unzerlegbare Zahl".

- Sei $p \in \mathbb{N}_{>1}$ prim. Angenommen, $p = ab$ mit $a, b \in \mathbb{N}_{>1}$, insbesondere $p \mid (ab)$. Wegen $a, b > 1$ folgt $a, b < p$, also auch $p \nmid a$ und $p \nmid b$. Widerspruch zu p prim.
- Sei $p \in \mathbb{N}_{>1}$ Primzahl. Sei $p \mid (ab)$. Schulwissen: Primfaktorzerlegung ist eindeutig. Daher gilt $p \mid (ab) \iff p$ tritt in der Primfaktorzerlegung von ab auf. Aber wegen der Eindeutigkeit der Primfaktorzerlegung setzt sich die Primfaktorzerlegung von ab aus denen von a und b zusammen, d.h. der Primfaktor p tritt in a oder in b auf. Mit anderen Worten: $p \mid ab \ \Rightarrow\ (p \mid a \vee p \mid b)$.

Anmerkung: Im Prinzip konnte man sich darüber schon in einer vorigen Aufgabe Gedanken machen.

b) Für $a \in \mathbb{Z}$ heißt $[a] = [0] \in \mathbb{Z}/d\mathbb{Z}$ nichts anderes als $d \mid a$.

$\mathbb{Z}/d\mathbb{Z}$ hat Nullteiler $\iff \exists a, b \in \mathbb{Z}\colon\ [ab] = [0] \wedge [a], [b] \neq [0] \iff \exists a, b \in \mathbb{Z}\colon\ d \mid (ab) \wedge d \nmid a \wedge d \nmid b \iff p$ nicht prim.

c)
- In $\mathbb{Z}/5\mathbb{Z}$: Alles außer $[0]$ invertierbar, nämlich $[1][1] = [1]$, $[2][3] = [3][2] = [1]$, $[4][4] = [1]$
- In $\mathbb{Z}/12\mathbb{Z}$: $[a]$ ist genau dann invertierbar, wenn a teilerfremd zu 12 ist, nämlich $[1][1] = [1]$, $[5][5] = [1]$, $[7][7] = [1]$, $[11][11] = [1]$.

Dahinter steckt übrigens ein allgemeines Prinzip: $a \in \mathbb{Z}^*$ ist modulo $b \in \mathbb{Z}^*$ genau dann invertierbar, wenn a, b teilerfremd sind.

d) Zunächst die leichte Richtung: d nicht prim $\Rightarrow \mathbb{Z}/d\mathbb{Z}$ wie gesehen nicht nullteilerfrei $\Rightarrow$ kein Körper.

Für die umgekehrte Richtung sei d prim. Ich kenne zwei Beweisansätze, aber keiner von beiden ist leicht. Es geht in dieser Teilaufgabe darum, sich über Beweisansätze Gedanken zu machen, aber es wurde nicht erwartet, dass man tatsächlich einen Beweis findet.

- Man kann mit Hilfe des erweiterten euklidischen Algorithmus das Lemma von Bézout beweisen: Wenn $a, d, \in \mathbb{Z}^*$, so gibt es $b, c \in \mathbb{Z}$ mit $ab + cd = \mathrm{ggT}(a, d)$. Ist also a, d teilerfremd, dann $[a][b] = [\mathrm{ggT}(a, d)] = [1]$. Da p prim ist, ist a genau dann teilerfremd zu d, wenn $d \nmid a$, also $[a] \neq [0]$. Es ist also jedes Element von $(\mathbb{Z}/d\mathbb{Z})^*$ invertierbar.
- d prim $\Rightarrow R := \mathbb{Z}/d\mathbb{Z}$ Nullteilerfrei $\Rightarrow R$ hat eine multiplikative Kürzungsregel $\Rightarrow \forall a \in R^*$: die Abbildung $\mu_a \colon R^* \to R^*$ mit $\mu_a(b) := ab$ ist injektiv. R^* ist endlich, und daraus kann man folgern (nicht leicht), dass μ_a auch surjektiv ist. Und dann ist $\mu_a^{-1}([1])$ das Inverse von a.

Präsenzaufgabe 4.2: *Bruchrechnung*

Wenn ich im Folgenden (a, b) schreibe, ist gemeint $(a, b) \in R \times R^*$.

a) Reflexivität: $(a, b) \sim (a, b)$, da $ab = ab$.
Symmetrie: $(a, b) \sim (a', b') \Rightarrow ab' = a'b \Rightarrow a'b = ab' \Rightarrow (a', b') \sim (a, b)$.
Transitivität: $(a, b) \sim (a', b') \wedge (a', b') \sim (a'', b'') \Rightarrow ab' = a'b \wedge a'b'' = a''b'$. Sonderfall: $a = 0 \Rightarrow a'b = 0 \overset{b\neq 0}{\Rightarrow} a' = 0$ wegen Nullteilerfreiheit. Insgesamt gilt: Wenn eines von a, a', a'' Null ist, dann alle. Insbesondere gilt dann auch $0 = ab'' = a''b$. Seien nun $a, a', a'' \neq 0$. Dann: Multiplikation der Gleichungen $ab' = a'b \wedge a'b'' = a''b'$ liefert $aa'b'b'' = a'a''bb' \overset{a'b'\neq 0}{a} b'' = a''b$ (Nullteilerfreiheit und Kürzung), also $(a, b) \sim (a'', b'')$.

Anmerkung: $\frac{a}{b} = \frac{a'}{b'} \iff ab' = a'b$. Unsere Äquivalenzrelation entspricht also Gleichheit von Brüchen.

b) Hier nur ein Beispiel: Sei $(a, b) \sim (a', b')$, also $ab' = a'b$. Wir zeigen $(ad + bc,\, bd) \sim (a'd + b'c,\, b'd)$:

$$(ad + bc) \cdot (b'd) = ab'd^2 + bb'cd \overset{\checkmark}{=} (a'd + b'c) \cdot bd = \underbrace{a'b}_{=ab'} d^2 + bb'cd$$

c) Nullelement $[(0,1)]$, Einselement $[(1,1)]$. Sei $(a,b) \nsim (0,1)$, also insbesondere $a = a \cdot 1 \neq 0 \cdot b = 0$. Dann ist auch $(b,a) \in R \times R^*$, und es gilt $[(a,b)] \cdot [(b,a)] = [(ab,ab)] = [(1,1)]$. **Vgl. Bruchrechnung:** $\frac{a}{b} \cdot \frac{b}{a} = 1$.

Assoziativität und Distributivität sind zugegebenermaßen etwas mühsam nachzurechnen. Das lasse ich in diesen Anmerkungen weg.

d) $R := \mathbb{R}[X]$ ist nullteilerfrei: Seien $f, g \in R^*$. Dann $f = a_0 + a_1X + ... + a_mX^m$ mit $a_m \neq 0$ und $g = b_0 + b_1X + ... + b_nX^n$ mit $b_n \neq 0$, dann ist fg von der Form $a_0b_0 + (a_1b_0 + a_0b_1)X + ... + a_mb_nX^{m+n}$. Wegen $a_m \neq 0 \neq b_n$ ist $a_mb_n \neq 0$ (denn $\mathbb{R}$ ist nullteilerfrei!), also $fg \neq 0$.

Und den Quotientenkörper von $\mathbb{R}[X]$ kennt man im Prinzip dadurch, dass man in der Schule gebrochen-rationale Funktionen behandelt hat.