Prof. Dr. Franz Kalhoff
Dipl.-Math. Sebastian Thomas

WS 2007/08
22.11.2007

Lineare Algebra (und analytische Geometrie) I

Musteraufgabenblatt 05

Musteraufgabe 8 (Teilbarkeit)**.** Gegeben seien ganze Zahlen $m, n \in \mathbb{Z}$. Es heißt m ein *Teiler* von n, geschrieben $m \mid n$, wenn es ein $q \in \mathbb{Z}$ gibt mit $n = qm$. Zeigen Sie die Äquivalenz der folgenden Aussagen:

(a) Es gilt $m \mid n$.

(b) Es ist $n \in m\mathbb{Z}$.

(c) Es ist $n\mathbb{Z} \subset m\mathbb{Z}$.

Lösung. Es gelte zunächst $m \mid n$. Dann gibt es ein $q \in \mathbb{Z}$ mit $n = qm$ und damit ist $n = qm \in m\mathbb{Z}$.
Da $m\mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$ ist, folgt aus $n \in m\mathbb{Z}$ auch, dass die von n erzeugte Untergruppe in $m\mathbb{Z}$ liegt, also $n\mathbb{Z} \subset m\mathbb{Z}$.
Aus $n\mathbb{Z} \subset m\mathbb{Z}$ folgt schließlich $n = n \cdot 1 \in n\mathbb{Z} \subset m\mathbb{Z}$, d.h. es gibt ein $q \in \mathbb{Z}$ mit $n = qm$ und damit gilt $m \mid n$.

Musteraufgabe 9 (Lemma von Bézout)**.** Es seien $m, n \in \mathbb{Z}$ mit $(m, n) \neq (0, 0)$. Eine ganze Zahl $g \in \mathbb{Z}$ heißt ein *größter gemeinsamer Teiler* von m und n, falls einerseits $g \mid m$ und $g \mid n$ und andererseits $d \mid g$ für alle $d \in \mathbb{Z}$ mit $d \mid m$ und $d \mid n$. Wir schreiben $\operatorname{ggT}(m, n) \in \mathbb{N}$ für den positiven größten gemeinsamen Teiler von m und n. Zeigen Sie:

(a) Es ist $m\mathbb{Z} + n\mathbb{Z} = \operatorname{ggT}(m, n)\mathbb{Z}$.

(b) Es existieren $a, b \in \mathbb{Z}$ mit $\operatorname{ggT}(m, n) = am + bn$.

Lösung. Es sei $g := \operatorname{ggT}(m, n)$.

(a) Dann gilt $g \mid m$ und $g \mid n$, also $m\mathbb{Z} \subset g\mathbb{Z}$ und $n\mathbb{Z} \subset g\mathbb{Z}$. Da aber $g\mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$ ist, impliziert dies $m\mathbb{Z} + n\mathbb{Z} \subset g\mathbb{Z}$. Umgekehrt ist auch $m\mathbb{Z} + n\mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$, so dass es nach Übung 5, Aufgabe 18, ein $k \in \mathbb{Z}$ gibt mit $m\mathbb{Z} + n\mathbb{Z} = k\mathbb{Z}$. Dann folgt aber $m\mathbb{Z} \subset m\mathbb{Z} + n\mathbb{Z} = k\mathbb{Z}$ und $n\mathbb{Z} \subset m\mathbb{Z} + n\mathbb{Z} = k\mathbb{Z}$ bzw. $k \mid m$ und $k \mid n$. Da g ein größter gemeinsamer Teiler von m und n ist, impliziert dies nun $k \mid g$ und damit $g\mathbb{Z} \subset k\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$. Insgesamt haben wir also $m\mathbb{Z} + n\mathbb{Z} = g\mathbb{Z}$.

(b) Nach (a) ist $m\mathbb{Z} + n\mathbb{Z} = g\mathbb{Z}$, so dass insbesondere auch $g \in g\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$ ist. Dies bedeutet aber nichts anderes, als dass es $a, b \in \mathbb{Z}$ gibt mit $g = am + bn$.