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

WS 2007/08
29.11.2007

Lineare Algebra (und analytische Geometrie) I

Musteraufgabenblatt 06

Musteraufgabe 10 (endliche zyklische Gruppen)**.** Es sei C eine endliche zyklische Gruppe, erzeugt von $c \in C$, und es sei $n := \operatorname{ord} C$.

(e) Es seien $k, l \in \mathbb{Z}$. Zeigen Sie, dass genau dann $c^l \in [c^k]$ ist, wenn $\operatorname{ggT}(k, n) \mid l$.

(f) Nun seien $k, l \in \mathbb{Z}$ mit $\operatorname{ggT}(k, n) \mid l$ und es seien $a, b, q \in \mathbb{Z}$ mit $\operatorname{ggT}(k, n) = ak + bn$ und $l = q \operatorname{ggT}(k, n)$ gegeben. Dann ist $c^l = (c^k)^{qa}$.

Lösung.

(e) Es ist $c^l \in [c^k]$ genau dann, wenn es ein $p \in \mathbb{Z}$ gibt mit $c^l = (c^k)^p = c^{kp}$ bzw. $c^{kp-l} = \mathrm{e}$. Dies ist aber genau dann der Fall, wenn $n \mid kp - l$, d.h. wenn es ein $q \in \mathbb{Z}$ gibt mit $kp - l = nq$ bzw. $l = kp - nq$. Nach Musteraufgabenblatt 05, Musteraufgabe 9 ist das wiederum äquivalent zu $l \in k\mathbb{Z} + n\mathbb{Z} = \operatorname{ggT}(k, n)\mathbb{Z}$ bzw. $\operatorname{ggT}(k, n)\mathbb{Z} \mid l$.

(f) Aus der Darstellung $\operatorname{ggT}(k, n) = ak + bn$ folgt

$$l = q \operatorname{ggT}(k, n) = q(ak + bn) = qak + qbn$$

und damit

$$c^l = c^{qak+qbn} = c^{qak} = (c^k)^{qa}.$$