Prof. Dr. H.-G. Gräbe, Uni Leipzig; Prof. Dr. J. Waldmann, HTWK Leipzig
Vorlesung Symbolisches Rechnen, Wintersemester 2014

Anmerkungen zur Übung vom 15. 1.

Aufgabenblatt 8 (Lösungen)

Ü8-2 Gitter Γ, Basis B, GSO von B ist B^*. Zeige: wenn $\forall i : |b_1| \leq |b_i^*|$, dann ist b_1 ein kürzester Vektor in Γ.

Lösung:

Bezeichung: $O_i(v)$ = die Gram-Schmidt-Reduktion von v bzgl $b_1, \ldots, b_{i-1}$. D.h. $O_i(v) = v - \pi_{\mathrm{span}(b_1,\ldots,b_{i-1})}(v)$. Es gilt $b_i^* = O_i(b_i)$.

Für alle v, i gilt $|O_i(v)| \leq |v|$. (betrachte rechtw. Dreieck mit Katheten $O_i(v), \pi_{\mathrm{span}(b_1,\ldots,b_{i-1})}(v)$ und Hypotenuse v)

Sei $v \in \Gamma \setminus \{0\}$ beliebig. Wir zeigen $|v| \geq |b_1|$:

Da B eine Basis für Γ ist, gibt es $c_j \in \mathbb{Z}$ mit $v = \sum_j c_j b_j$. Sei $i = \max\{j : c_j \neq 0\}$. (wegen $v \neq 0$ ist das ein max über nichtleere Menge)

$O_i(v) = O_i(\sum_j c_j b_j) = \sum_j c_j \cdot O_i(b_j) = 0 + \ldots + 0 + c_i \cdot O_i(b_i) = c_i b_i^*$

Dann $|v| \geq |O_i(v)| = |c_i||b_i^*| \geq 1 \cdot |b_1|$.