

46. Sei R ein direktes Produkt abzählbar vieler Kopien von \mathbb{Z} , d. h.

$$R = \bigotimes_{i=1}^{\infty} \mathbb{Z},$$

und $M = \text{Hom}(R, R)$ der Endomorphismenring von R . Sei $n \in \mathbb{N}$. Zeigen Sie, dass M als M -Modul eine Basis aus n Elementen hat.

47. Sei L ein Gitter im \mathbb{R}^n mit Basis b_1, \dots, b_n . Zeigen Sie, dass die Länge aller Gittervektoren $v \neq 0$ durch den kleinsten Eigenwert der Gram-Matrix $(\langle b_i, b_j \rangle)_{1 \leq i, j \leq n}$ von unten beschränkt ist.

48.  Effiziente Bestimmung kürzester Gittervektoren in \mathbb{R}^2 : Sei L ein Gitter in \mathbb{R}^2 mit Basis b_1, b_2 , wobei $\|b_1\| \leq \|b_2\|$. Betrachten Sie folgenden Algorithmus:

```

loop
  wähle  $k \in \mathbb{Z}$ , sodass  $-\|b_1\|^2 < 2\langle b_2 - kb_1, b_1 \rangle \leq \|b_1\|^2$ 
   $b_2 := b_2 - kb_1$ 
  if  $\|b_1\| \leq \|b_2\|$  then
    return  $b_1, b_2$ 
  else
    vertausche  $b_1$  und  $b_2$ 
  end if
end loop

```

- (a) Zeigen Sie, dass der Algorithmus terminiert und Vektoren v_1, v_2 liefert, sodass v_1 ein kürzester Vektor ($\neq 0$) von L ist und v_2 ein kürzester Vektor von $L \setminus \text{span}(v_1)$ ist.
- (b) Zeigen Sie, dass der Algorithmus nach $O(\log(\|b_1\|/l))$ Iterationen endet, wobei l die Länge eines kürzesten Vektors ($\neq 0$) in L ist.