IP 30.4.19 Beweis zu Satz 2.1

- Für $y \in \mathbb{Q}^n$ sei $\alpha(y) \in \{1, 2, \dots\}$ das Produkt der Nenner der Komponenten von y.
- $\tilde{Y} := \{\alpha(y) \cdot y : y \in Y\} \subseteq \mathbb{Z}^n$
  - $\operatorname{ccone}(\tilde{Y}) = \operatorname{ccone}(Y)$
  - $k(\tilde{Y})$ ist polynomial beschränkt in $k(Y)$
- $\tilde{X} := \mathbb{Z}^n \cap \left(\operatorname{conv}(X) + Q\right)$ mit $Q := \left\{\sum_{y \in Y'} \lambda_y \cdot y : 0 \le \lambda_y \le 1,\ Y' \subseteq \tilde{Y},\ |Y'| \le n\right\}$
- Für alle $z \in \operatorname{conv}(X) + Q$ gilt:

$$\|z\|_\infty \le \max\{\|x\|_\infty : x \in X\} + n \cdot \max\{\|y\|_\infty : y \in \tilde{Y}\}$$

- Also für alle $z \in \tilde{X}$: $\langle z \rangle$ polynomial beschränkt in $k(X \cup \tilde{Y})$, also in $k(X \cup Y)$.

- Daher genügt es, $P \cap \mathbb{Z}^n = \tilde{X} + \Lambda^{\geq 0}(\tilde{Y})$ zu zeigen.
- "$\supseteq$": klar, da $\tilde{X} \subseteq P$ und $\tilde{Y} \subseteq \operatorname{dcar}(P)$ (und $\tilde{X}, \tilde{Y} \subseteq \mathbb{Z}^n$).
- "$\subseteq$": Sei $p \in P \cap \mathbb{Z}^n$ $\quad (P = \operatorname{conv}(X) + \operatorname{dcar}(P))$
  - $\operatorname{ccone}(\tilde{Y}) = \operatorname{dcar}(P) \Rightarrow p = x + v$ mit $x \in \operatorname{conv}(X)$, $v \in \operatorname{ccone}(\tilde{Y})$
  - Carathéodory's Theorem $\Rightarrow \exists Y' \subseteq \tilde{Y}$, $|Y'| \leq n$ $\exists \mu_y \in \mathbb{R}_+$ $(y \in Y')$:
    $$v = \sum_{y \in Y'} \mu_y \cdot y = \lfloor \mu_y \rfloor + (\mu_y - \lfloor \mu_y \rfloor)$$
  - $p = x + \underbrace{\sum_{y \in Y'} (\mu_y - \lfloor \mu_y \rfloor) \cdot y}_{=: r \in Q} + \underbrace{\sum_{y \in Y'} \lfloor \mu_y \rfloor \cdot y}_{=: \tilde{v} \in \Lambda^{\geq}(\tilde{Y})}$
  - mit $\tilde{x} := \underbrace{x + r}_{\in \operatorname{conv}(X) + Q} = p - \tilde{v} \in \mathbb{Z}^n \in \tilde{X}$ also $p = \tilde{x} + \tilde{v}$
    $\in \tilde{X} + \Lambda^{\geq}(\tilde{Y})$

□

Kor. 2.2: Für $A \in \mathbb{Q}^{m \times n}$, $b \in \mathbb{Q}^m$ gibt es $\tilde{X}, \tilde{Y} \subseteq \mathbb{Z}^n$, $|\tilde{X}|, |\tilde{Y}| < \infty$ mit:

- $P^{\leq}(A,b) \cap \mathbb{Z}^n = \tilde{X} + \Lambda^{\geq 0}(\tilde{Y})$
- $\text{ccone}(\tilde{Y}) = \dim(P^{\leq}(A,b))$ $\quad (= P^{\leq}(A,0))$
- $k(\tilde{X} \cup \tilde{Y})$ polynomial beschränkt in $k(A,b)$.

Bemerkungen:

- Kor. 2.2 liefert Parametrisierung von $\{x \in \mathbb{Z}^n : Ax \leq b\}$ oder $\{x \in \mathbb{Z}^n : Ax = b, x \geq 0\}$, die analog zu den Sätzen 1.8(ii) und 1.2(ii) sind.
- $|\tilde{X}|, |\tilde{Y}|$ sind i.a. nicht polynomial beschränkt in $\langle A,b \rangle$.
- $P^{\leq}(A,b) \cap \mathbb{Z}^n \neq \emptyset \iff \tilde{X} \neq \emptyset$

Beobachtg: Für $\tilde{X} \neq \emptyset$, $\tilde{Y} \subseteq \mathbb{R}^n$, $|\tilde{X}|, |\tilde{Y}| < \infty$, $c \in \mathbb{R}^n$ gilt:

- $$\inf \{ \langle c, x+y \rangle : x \in \tilde{X}, y \in \Lambda^{\geq 0}(\tilde{Y}) \} = -\infty$$
  $$\Leftrightarrow \exists y \in \tilde{Y} : \langle c, y \rangle < 0$$

- Andernfalls: $$\inf \{ \langle c, x+y \rangle : x \in \tilde{X}, y \in \Lambda^{\geq 0}(\tilde{Y}) \}$$
  $$= \min \{ \langle c, x \rangle : x \in \tilde{X} \}$$

Kor. 2.3: Seien $A \in \mathbb{Q}^{m \times n}$, $b \in \mathbb{Q}^m$.

(i) Falls $P^{=}(A,b) \cap \mathbb{Z}^n \neq \emptyset$, so gibt es $x \in \mathbb{Z}^n$ mit $Ax \leq b$ und $\langle x \rangle$ polynomial beschränkt in $k(A,b)$.

(ii) Falls für $c \in \mathbb{R}^n$ der Optimalwert von $\min \{ \langle c, x \rangle : Ax \leq b, x \in \mathbb{Z}^n \}$ (*) endlich ist, so hat (*) eine Optimallösung x^* mit $\langle x^* \rangle$ polynomial beschränkt in $k(A,b)$.

Bemerkungen:

- Kor. 2.3(i) liefert ein polynomial großes Zertifikat für die Lösbarkeit rationaler Diophantischer linearer Ungleichungssysteme

  $\rightsquigarrow$ "IP-Zulässigkeit" ist in NP (es ist NP-vollständig)

- Es gibt aber kein polynomial großes Zertifikat für die Unlösbarkeit (es sei denn NP = coNP).

Definition: Ein Hilbert-Basis eines polyedrischen Kegels $K \subseteq \mathbb{R}^n$ ist eine endliche Menge $H \subseteq \mathbb{Z}^n$ mit

$$K \cap \mathbb{Z}^n = \Lambda^{\geq 0}(H).$$

Kor. 2.4 :

(i) Jeder rationale polyedrische Kegel hat eine Hilbert-Basis.

(ii) Jeder spitze rationale polyedrische Kegel k hat eine endliche inklusionsminimale Hilbert-Basis.

Linealitätsraum $= \{0\}$, d.h. es gibt $c \in \mathbb{R}^n$ mit

$\langle c, x \rangle \geq 0 \quad \forall x \in k$, $\quad (\langle c, x \rangle = 0, x \in k) \Rightarrow x = 0$