Algebraische Rechenmodelle

Prof. Dr. Klaus Meer, Ameen Naif

Aufgabenblatt 1
16 Oktober 2018

Aufgabe 1.

Gegeben seien $a, b, c \in \mathbb{Q}$ und die Formel $\psi(a, b, c) := (\exists x \in \mathbb{Q} : ax^2 + bx + c = 0)$. Gibt es ein *quantorenfreies* $\phi(a, b, c)$, das äquivalent zu ψ ist?

Aufgabe 2.

Sei $\Phi(X_1, \ldots, X_n)$ eine 3-SAT Formel. Finde ein Polynom $f \in \mathbb{Z}[y_1, \ldots, y_m]$, sodass f eine reelle Nullstelle $y \in \mathbb{R}^m$ genau dann hat, wenn Φ erfüllbar ist. Gesucht ist also eine allgemeine Reduktion von das Erfüllbarkeitsproblem auf die Frage der Existenz reeller Nullstellen von Polynomen.

SAT steht für "satisfiability" und ist die Menge der erfüllbaren Bool'schen Formeln. Das sind alle Ausdrücke bestehend aus $\wedge$, $\vee$, X_i und $\neg X_i$, für die es eine Belegung $X_i \in \{0, 1\}$ für alle i gibt, welche den Ausdruck erfüllt. *3-SAT* ist eine normalisierte Variante mit Ausdrücken in der Form $(r_1 \vee r_2 \vee r_3) \wedge (r_4 \vee r_5 \vee r_6) \wedge \cdots$ mit $r_i \in \{X_1, \ldots, X_n, \neg X_1, \ldots, \neg X_n\}$.

Aufgabe 3.

Wir wollen ein Verfahren studieren um Polynome $f, g \in \mathbb{R}[x]$ zu dividieren, d.h. um einen Quotienten $q \in \mathbb{R}[x]$ und einen Rest $r \in \mathbb{R}[x]$ zu finden mit $\forall x \in \mathbb{R} : f(x) = q(x)g(x) + r(x)$ und $\text{grad}(r) < \text{grad}(g)$ oder $\forall x \in \mathbb{R} : r(x) = 0$. Dieses Verfahren ist als Polynomdivision bekannt.

(a) Beweisen sie die Existenz solcher Polynome q, r für beliebige Polynome f und g. Sind diese eindeutig? Hinweis: Nutzen Sie Induktion über $\text{grad}(f)$.

(b) Zeigen sie mit Hilfe der Polynomdivision: Wenn $f(a) = 0$ für ein $a \in \mathbb{R}$, dann ist $(x - a)$ ein Faktor von f, d.h. bei obiger Division von f durch $(x - a)$ ergibt sich das Rest $r(x)$ das Nullpolynom. Wie lautet $r(x)$, falls $f(a) \neq 0$?

(c) Welche Rechenoperationen werden benutzt. Welche Probleme gibt es z.B. in $\mathbb{Z}[x]$?

Aufgabe 4.

(a) Wie ist der größte gemeinsame Teiler $\text{ggT}(a, b)$ für $a, b \in \mathbb{N}$ definiert? Warum berechnet der Euklidische Algorithmus den ggT? Welche Operationen werden dabei benutzt und welche Eigenschaften müssen diese erfüllen?

(b) Betrachten wir nun den Euklidischen Algorithmus auf Polynomen. Wie ist der größte gemeinsame Teiler $\text{ggT}(f, g)$ für $f, g \in \mathbb{R}[x]$ definiert? Ist er eindeutig?