Theorie der reell abgeschlossenen Körper (RCF)

1 Einführung

Die im Vortrag betrachteten Modelle verwenden die Sprache

$$\mathbb{L}_{ORing}=\{0,1,+,-,\cdot,<\}$$

1.1 Def. Angeordneter Körper

Sei F ein Körper und $<$ eine Relation auf F, die folgende Axiome erfüllt:

1. $\forall x \quad \neg x < x$
2. $\forall x, y, z \quad (x < y \wedge y < z \rightarrow x < z)$
3. $\forall x, y \quad (x < y \vee x = y \vee y < x)$
4. $\forall x, y, z \quad (x < y \rightarrow x + z < y + z)$
5. $\forall x, y \quad (0 < x \wedge 0 < y \rightarrow 0 < x \cdot y)$

Dann heißt (F,<) *angeordneter Körper*

1.2 Def. Reell Abgeschlossener Körper

Ein angeordneter Körper (F,<) heißt *reell abgeschlossen*, falls er folgende Axiome erfüllt:

1. $\forall x \exists y \quad (x < 0 \vee x = y^2)$
2. $\forall x_0, ..., x_{2n} \exists y \quad y^{2n+1} + x_{2n} \cdot y^{2n} + ... + x_1 \cdot y + x_0 = 0$ für alle n $\in \mathbb{N}$

Die Theorie der reell abgeschlossenen Körper wird auch als *RCF (real closed fields)* bezeichnet.
Der relativ algebraische Abschluss eines Teilkörpers in einem reell abgeschlossenen Körper ist offenbar reell abgeschlossen.

1.3 Satz (ohne Beweis) [Pr, S. 211]

Für einen angeordneten Körper (F,<) sind äquivalent:

1. (F,<) erlaubt keinen echten algebraischen und angeordneten Erweiterungskörper
2. (F,<) ist reell abgeschlossen
3. F($\sqrt{-1}$) ist algebraisch abgeschlossen und F $\neq$ F($\sqrt{-1}$)

Die Klasse aller angeordneten Körper ist offenbar abgeschlossen unter der Vereinigung von Ketten (*"induktiv"*). Für einen angeordneten Körper (F,<) betrachte alle algebraischen Erweiterungen (F',<). Mit Zorns Lemma folgt die Existenz einer maximalen algebraischen Erweiterung ($F^*, <^*$), die nach Satz 1.3 reell abgeschlossen ist. F^* wird als *reeller Abschluss* von F bezeichnet.

1.4 Bem.

In RCF gilt der Zwischenwertsatz:
$RCF \vdash \forall a, b, q_0, ..., q_n : a < b \wedge q_n a^n + ... + q_0 < 0 < q_n b^n + ... + q_0 \to \exists c : a < c < b \wedge q_n c^n + ... + q_0 = 0 \quad$ für jedes $n \in \mathbb{N}$

Beweis Sei (F,<) ein reell abgeschlossener Körper. Mit Satz 1.3.3 folgt, dass die irreduziblen Polynome f $\in$ F[X] nur von der Gestalt

$$f = X - a \quad \text{oder} \quad f = (X - b)^2 + c^2 \text{ mit a,b,c} \in \text{F und } c \neq 0$$

sein können. Für ein beliebiges Polynom p $\in$ F[X] ersieht man leicht das Gewünschte aus der Faktorisierung.

1.5 Satz (ohne Beweis) [Pr, S. 212]

Zwei reelle Abschlüsse eines angeordneten Körpers (F,<) sind über F isomorph

2 Der Satz von Tarski

2.1 Satz (ohne Beweis)

Eine Theorie T hat Quantorenelimination gdw. für je zwei Modelle M_1, M_2 von T mit einer gemeinsamen endlich erzeugten Substruktur A und für jede einfache Existenzaussage ϕ der Sprache L(A) gilt: $M_1^A \models \phi \to M_2^A \models \phi$
Eine einfache Existenzaussage hat die Form $\exists x \varphi(x)$, wobei φ eine quantorenfreie Formel ist.

2.2 Satz von Tarski-Seidenberg

RCF hat Quantorenelimination

Beweis Wir zeigen die Bedingung aus Satz 2.1. Seien also $(F_1, <_1)$ und $(F_2, <_2)$ reell abgeschlossene Körper und A eine gemeinsame Substruktur und endlich erzeugt. Dann ist A ein angeordneter Teilring von F_1 und F_2. Bilde den Quotientenkörper F:=Quot(A) in F_1 und F_2. Die beiden (angeordneten) Quotientenkörper sind kanonisch isomorph, da die Anordnung auf dem Quotientenkörper eindeutig fortgesetzt wird (denn $\frac{a}{b} < \frac{c}{d} \Leftrightarrow a \cdot d < c \cdot b$). Sei $\tilde{F}$ der relative algebraische Abschluss von F in F_1 bzw. F_2 (isomorph nach Satz 1.5 und reell abgeschlossen s.o.).

Sei nun φ eine quantorenfreie Formel der Sprache $\mathbb{L}_{ORing}(A)$ mit $F \models \exists x\varphi(x)$. Wir können annehmen, dass φ in disjunktiver Normalform ist und ersetzen

$$\neg(t_1 = t_2) \text{ durch } (t_1 < t_2 \vee t_2 < t_1)$$

$$\neg(t_1 < t_2) \text{ durch } (t_1 = t_2 \vee t_2 < t_1)$$

Damit hat φ(x) nach Aufteilung des Existenzquantors ohne Einschränkung die Form

$$(\bigwedge_{i=1}^{r} p_i(x) = 0 \wedge \bigwedge_{j=1}^{s} 0 < q_i(x))$$

wobei p_i und q_j Polynome mit Koeffizienten in A sind.
Ist nun mindestens eines der $p_i \neq 0$, so muss ein $d \in F_1$, das φ erfüllt, schon in $\tilde{F}$ liegen. Es folgt $\tilde{F} \models \exists x\varphi(x)$ und damit $F_2 \models \exists x\varphi(x)$.
Seien nun alle $p_i = 0$ oder r=0. Seien weiter $a_1 < ... < a_m$ alle Nullstellen der q_i. Angenommen $F_1 \models \varphi(d)$ für ein $d \in F_1 \setminus A$. Dann gibt es genau drei Möglichkeiten der Lage von d in Bezug auf $a_1 < ... < a_m$:

1. Fall: $d < a_1$ In diesem Fall haben $q_j(d)$ und $q_j(a_1 - 1)$ dasselbe Vorzeichen, da es andernfalls nach dem Zwischenwertsatz (Bem. 1.4) eine weitere Nullstelle $q_j(a') = 0$ zwischen d und a_1 geben müsste.
2. Fall: $a_m < d$ Analog für $a_m + 1$
3. Fall: $a_v < d < a_{v+1}$ Hier haben $q_j(d)$ und $q_j(\frac{a_v + a_{v+1}}{2})$ wieder mit dem Zwischenwertsatz dasselbe Vorzeichen.

In allen drei Fällen finden wir also ein $d' \in \tilde{F}$, das ebenso wie d alle Ungleichungen $0 < q_j(x)$ erfüllt, d.h. $\tilde{F} \models \varphi(d')$ und es folgt $F_2 \models \varphi(d')$ und damit $F_2 \models \exists x\varphi(x)$.

□

2.3 Kor.

RCF ist vollständig und modellvollständig

Beweis Eine Theorie die Quantorenelimination hat und eine Primsubstruktur besitzt, ist vollständig. $\mathbb{Q}$ ist eine solche Primsubstruktur, da aus den Axiomen direkt folgt, dass ein reell abgeschlossener Körper Charakteristik 0 haben muss, also $\mathbb{Z}$ einbettet und als Körper damit auch $\mathbb{Q}$. Die Anordnung auf $\mathbb{Q}$ ist eindeutig mit dem obigen Argument für Quotientenkörper. Modellvollständigkeit folgt direkt aus Quantorenelimination.

3 Konsequenzen

3.1 Kor.

Die Theorie der angeordneten Körper hat RCF als Modellbegleiter.

Beweis Nach dem Satz von Tarski ist RCF modellvollständig und wie oben gesehen besitzt jeder angeordnete Körper einen reellen Abschluss.

3.2 Def. o-minimal (Wdh.)

Sei (F,<,...) eine Struktur, sodass < auf F eine lineare Ordnung definiert. F heißt *o-minimal*, falls jede (in einer Variablen) definierbare Teilmenge $X \subseteq F$ eine endliche Vereinigung von Intervallen ist.
Eine Theorie ist o-minimal, falls jedes ihrer Modelle o-minimal ist.

3.3 Kor.

RCF ist o-minimal

Beweis Ein Modell (F,<,...) ist o-minimal gdw. jede Formel mit einer freien Variablen und Parametern in F äquivalent ist zu einer quantorenfreien Formel, die nur < verwendet und Parameter in F hat (klar!). Aus der Quantorenelimination von RCF folgt damit direkt das Gewünschte.

3.4 Bem. (Wdh.)

Eine o-minimale Theorie ist NIP (Beweis im NIP-Vortrag)

3.5 Lemma

Sei (K,<) ein angeordneter Körper und $(K^*, <^*)$ sein reeller Abschluss. Dann gibt es in K^* keine *bezüglich K infinitesimalen* Elemente (d.h. $k \in K^*_{0<}$ mit $\forall x \in K_{0<} : k < x$).

Beweis Angenommen es gäbe ein solches Element k. Für beliebige $n \in \mathbb{N}$ folgt sofort $k^{n+1} < ak^n$ für beliebige $a \in K$. Da K^* algebraisch über K ist, existieren $a_0, ..., a_i \in K$, sodass

$$a_0 + ... + a_i k^i = 0 \quad \Leftrightarrow \quad k^i = \tfrac{-a_0}{a_i} + ... + \tfrac{-a_{i-1}}{a_i} k^{i-1}$$

k^i muss jedoch immer strikt kleiner als eine solche Summe sein. Widerspruch.

3.6 Bem.

Jeder o-minimale angeordnete Körper ist reell abgeschlossen

Beweis Sei $(K, <)$ ein angeordneter und o-minimaler Körper. Wir zeigen, dass in K der Zwischenwertsatz gilt.
Seien also $p \in K[X]$ und außerdem $b, c \in K$, sodass ohne Einschränkung $p(b) < 0 < p(c)$. Bezeichne $(K^*, <^*)$ den reellen Abschluss von $(K, <)$. Wie bereits gesehen, gilt in K^* der Zwischenwertsatz, d.h. es gibt $(d_i) \in K^*$ mit $b <^* d_i <^* c$

und $p(d_i) = 0$. Setze $d = \max_<\{d_i\}$.
Wir nehmen an $d \notin K$. Betrachte die Formel

$$\varphi(x) = b < x \wedge p(x) < 0 \wedge \forall y \quad (b < y < x \rightarrow 0 < f(y))$$

Da K o-minimal ist gibt es Intervalle $I_1, ..., I_k$, sodass die von φ definierte Menge als (disjunkte) Vereinigung dieser Intervalle geschrieben werden kann. Sei nun $I := (k_1, k_2)$ das Intervall, welches das nach $<$ größte Element enthält. (I darf sowohl offen als auch abgeschlossen sein!). Offenbar muss $k_2 <^* d$ sein.
Nach Lemma 3.5 gibt es nun $i \in K_{0<}$ mit $i < d - k_2$ (da sonst $d - k_2$ infinitesimal bzgl. K wäre). Es folgt $k_2 < k_2 + i < d$. Das Element $k_2 + i$ läge aber schon in der von φ definierten Menge, was der Maximalität von I widerspräche. Also muss bereits $d \in K$ gewesen sein.
Mit dem Zwischenwertsatz sieht man sofort, dass jedes Polynom ungeraden Grades eine Nullstelle besitzt. Die Existenz der Quadratwurzel einer positiver Zahl $a \in K^{>0}$ sieht man durch die Betrachtung des Polynoms $x^2 - a$ auf dem Intervall (0,a+1). Damit folgt, dass K reell abgeschlossen ist.

□

3.7 Satz Hilberts 17tes Problem

Sei R ein reell abgeschlossener Körper (z.B. $\mathbb{R}$) und $p \in R[X_1, ..., X_n]$ ein *positiv semidefinites* Polynom ($p(a_1, ..., a_n) \geq 0$ für alle $a_1, ..., a_n \in R$). Dann gibt es rationale Funktionen $f_1, ..., f_k \in R(X_1, ..., X_n) = R(\bar{X})$, sodass

$$p = \sum_{i=1}^{k} f_i^2$$

Beweis Nach einem Satz von Artin und Schreier sind in jedem Körper die Quadratsummen genau die Elemente, die für alle Anordnungen des Körpers positiv sind.
Angenommen p ist in $R(\bar{X})$ keine Quadratsumme, dann gäbe es nach diesem Satz eine Anordnung $<$ von $R(\bar{X})$, sodass $p < 0$ ist. Sei (R',$<'$) der reelle Abschluss von $(R(\bar{X}), <)$. In R' gilt dann ebenfalls $p <' 0$, also die Existenzaussage

$$\varphi = \exists x_1, ..., x_n \quad \underline{p}(x_1, ..., x_n) < 0$$

wobei in p alle Koeffizienten durch Konstanten ersetzt wurden. R ist Substruktur in R'. Wegen der Modellvollständigkeit folgt $R \prec R'$. Damit gilt φ auch in R. Dies widerspricht jedoch der Semidefinitheit von p. Also ist p doch eine Quadratsumme in $R(\bar{X})$.

□

Literaturverzeichnis

[Pr] Prestel, Alexander: Einführung in die Mathematische Logik und Modelltheorie, vieweg 1986