Wortprobleme in Ringen (IV)

Moritz Hartlieb

28. Mai 2020

1 Körper

Definition 1. Ein *Körper* ist ein Ring, der zusätzlich folgende Axiome erfüllt:

- $\neg(1 = 0)$
- $\neg(x = 0) \Rightarrow \exists z.z \cdot x = 1$

Aus der Algebra kennen wir die folgenden beiden Sätze:

Satz 2. *Jeder Körper (mit Charakteristik p) ist ein Integritätsring (mit Charakteristik p).*

Satz 3. *Jeder Integritätsring R kann in einen Körper* $\mathrm{Quot}(R)$ *(den Quotientenkörper von R) eingebettet werden. Inbesondere haben R und* $\mathrm{Quot}(R)$ *die gleiche Charakteristik.*

Satz 4. *Eine universelle Formel in der Sprache der Ringe gilt in allen Körpern (mit Charakteristik p), genau dann wenn sie in allen Integritätsringen (mit Charakteristik p) gilt.*

Beweis. Wenn eine Formel in allen Integritätsringen (mit Charakteristik p) gilt, dann gilt sie auch in allen Körpern (mit Charakteristik p), da Körper nach Satz 2 Integritätsringe sind.

Angenommen eine universelle Formel $\phi \in L^{S_{\mathrm{Ring}}}$ gilt in allen Körpern (mit Charakteristik p). Sei R eine Integritätsring (mit Charakteristik p). Dann gilt ϕ im Quotientenkörper von R. Da R in $\mathrm{Quot}(R)$ eingebettet werden kann, und ϕ universell ist, gilt dann schon $R \models \phi$. □

2 Der Rabinowitsch-Trick

Zunächst bemerken wir, dass wir die universelle Theorie der Integritätsringe / Körper auf das Wortproblem zurückführen können:

Satz 5. *Die Gültigkeit einer universellen Formel in der Sprache der Ringe für alle Integritätsringe / Körper kann auf das Wortproblem zurückgeführt werden.*

Beweis. Da Körpern und Integritätsringe nullteilerfrei sind, gilt eine Formel der Form

$$\forall \overline{x}. \bigwedge_{i \in I} p_i(\overline{x}) \Rightarrow \bigvee_{j \in J} q_j(\overline{x}) = 0. \tag{1}$$

in allen Integritätsringen/Körpern genau dann, wenn

$$\forall \overline{x}. \bigwedge_{i \in I} p_i(\overline{x}) \Rightarrow \prod_{j \in J} q_j(\overline{x}) = 0.$$

in allen Integritätsringen/Körpern gilt. Wir haben bereits gesehen, dass jede universelle Formel in der Sprache der Ringe logisch äquivalent zu einer Konjunktion von Formeln der Form (1) umgeformt werden kann. □

Der sogenannte Rabinowitsch-Trick ermöglicht es uns, Instanzen des Wortproblems auf Instanzen des degenerierten Wortproblems zurückzuführen:

Satz 6. *Die Formel*

$$\forall \overline{x}.p_1(\overline{x}) = 0 \wedge \cdots \wedge p_n(\overline{x}) = 0 \Rightarrow q(\overline{x}) = 0 \in L^{S_{\text{Ring}}}$$

gilt in allen Körpern genau dann, wenn

$$\forall \overline{x}z.p_1(\overline{x}) = 0 \wedge \cdots \wedge p_n(\overline{x}) \wedge 1 - q(\overline{x})z = 0 \Rightarrow \bot$$

in allen Körpern gilt.

Beweis. Sei K ein beliebiger Körper. Dann gilt

$$K \models \forall \overline{x}.p_1(\overline{x}) = 0 \wedge \cdots \wedge p_n(\overline{x}) = 0 \Rightarrow q(\overline{x}) = 0$$

genau dann, wenn

$$K \models \forall \overline{x}z.p_1(\overline{x}) = 0 \wedge \cdots \wedge p_n(\overline{x}) = 0 \wedge 1 - q(\overline{x})z = 0 \Rightarrow \bot,$$

da in allen Körpern

$$(\exists z.1 - q(\overline{x})z = 0) \Leftrightarrow (\exists z.q(\overline{x})z = 1) \Leftrightarrow \neg(q(\overline{x}) = 0).$$

gilt. □

Satz 7. $\forall \overline{x}.p_1(\overline{x}) = 0 \wedge \cdots \wedge p_n(\overline{x}) = 0 \Rightarrow \bot \in L^{S_{\text{Ring}}}$ *gilt in allen Integritätsringen / Körpern genau dann wenn* $1 \in \text{Id}_{\mathbb{Z}}\langle p_1, , \ldots, p_n\rangle$

Beweis. Wir beobachten, dass $0 = 1$ in Körpern und Integritätsringen äquivalent zu $\bot$ ist. Wir können also den starken Nullstellensatz mit $q(\overline{x}) = 1$ anwenden. Dann haben wir

$$\forall \overline{x}.p_1(\overline{x}) = 0 \wedge \cdots \wedge p_n(\overline{x}) = 0 \Rightarrow \bot$$

genau dann, wenn $1 = q^k \in \text{Id}_{\mathbb{Z}}\langle p_1, , \ldots, p_n\rangle$. □

Satz 8. $\forall \overline{x}.p_1(\overline{x}) = 0 \wedge \cdots \wedge p_n(\overline{x}) = 0 \Rightarrow \bot \in L^{S_{\text{Ring}}}$ *gilt in allen Integritätsringen / Körpern mit Charakteristik 0 genau dann wenn* $1 \in \text{Id}_{\mathbb{Q}}\langle p_1 \ldots p_n\rangle$

Beweis. Wende wie oben den starken Nullstellensatz mit $q(\overline{x}) = 1$ an. □

Die Kombination von Satz 5-7 zeigt, dass wir die universelle Theorie der Integritätsringe / Körper lösen können, wenn wir entscheiden können, ob die 1 in bestimmten Idealen enthalten ist.

3 Algebraisch abgeschlossene Körper

Definition 9. Ein Körper heißt *algebraisch abgeschlossen*, wenn jedes Polynom mit Grad $n \geq 1$ mindestens eine Nullstelle hat.

Aus der Algebra kennen wir den folgenden Satz:

Satz 10. *Jede Körper ist in einem algebraisch abgeschlossenen Körper enthalten.*

Satz 11. *Eine universelle Formel in der Sprache der Ringe gilt in allen algebraisch abgeschlossenen Körpern (mit Charakteristik p) gdw. sie in allen allen Körpern (mit Charakteristik p) gilt.*

Beweis. Wenn eine Formel in allen Körpern (mit Charakteristik p) gilt, dann gilt sie auch in allen algebraisch abgeschlossenen Körpern (mit Charakteristik p).

Angenommen eine universelle Formel $\phi \in L^{S_{\text{Ring}}}$ gilt in allen algebraisch abgeschlossenen Körpern (mit Charakteristik p). Sei K eine Körper (mit Charakteristik p). Dann gilt ϕ im algebraischen Abschluss von K. Da ϕ universell ist, gilt dann schon $K \models \phi$. □

Zusammenfassend haben wir nun folgenden Satz:

Korollar 12. *Folgende Aussagen sind äquivalent für eine universelle Formel $\phi \in L^{S_{\text{Ring}}}$.*

- *ϕ gilt in allen Integritätsringen mit Charakteristik 0*
- *ϕ gilt in allen Körpern mit Charakteristik 0*
- *ϕ gilt in allen algebraisch abgeschlossen Körpern mit Charakteristik 0*
- *ϕ gilt in einem beliebigen algebraisch abgeschlossenen Körper mit Charakteristik 0*
- *ϕ gilt in $\mathbb{C}$*

Beweis. Die ersten beiden Äquivalenzen wurden in diesem Vortrag gezeigt.

Die letzten beiden Äquivalenzen folgen aus dem Beweis der Quantorenelimination über algebraisch abgeschlossenen Körpern mit Charakteristik 0, die im letzten Vortrag gezeigt wurden. □

4 Abelsche Monoide und Gruppen

Bis jetzt haben wir aussgehend vom Wortproblem für allgemeine Ringe in jedem Schritt algebraische Strukturen mit mehr Axiomen und erlaubten Rechenoperationen betrachtet. Im Folgenden werden wir nun algebraische Strukturen mit weniger Axiomen betrachten.

4.1 Abelsche Monoide

Definition 13. Sei $S_{\text{Monoid}} := \{1, \cdot\}$ wobei $\cdot$ ein zweistelliges Funktionssymbol ist. Ein *abelsches Monoid* ist ein S_{Monoid}-Modell, dass folgende Axiome erfüllt:

- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$,
- $x \cdot y = y \cdot x$
- $1 \cdot x = x$.

Satz 14. *Jedes abelsche Monoid lässt sich in einen Ring einbetten.*

Beweis. Sei M ein abelsches Monoid. Sei

$$\mathbb{Z}[M] := \{\text{Abbildungen } a : M \to \mathbb{Z} \mid a(i) \neq 0 \text{ nur für endlich viele } i \in M\}$$

Für $a, b \in \mathbb{Z}[M]$ definieren wir

$$a + b := m \mapsto a(m) + b(m)$$

und

$$a \cdot b := m \mapsto \sum_{n,n' \in M, n \cdot n' = m} a(n) \cdot b(n')$$

Durch Nachrechnen der Ring-Axiome sieht man, dass $\mathbb{Z}[M]$ ein Ring ist, also insbesondere ein abelsches Monoid bezüglich $(\cdot)$.

Außerdem ist

$$\begin{aligned} &M \hookrightarrow \mathbb{Z}[M] \\ &m \mapsto \left(n \mapsto \begin{cases} 1 & \text{falls } m = n \\ 0 & \text{sonst} \end{cases} \right) \end{aligned}$$

eine S_{Monoid}-Einbettung von M in $\mathbb{Z}[M]$. □

Satz 15. *Eine universelle Formel in der multiplikativen Sprache der Monoide gilt in allen abelschen Monoiden gdw. sie in allen Ringen gilt*

Beweis. Da $S_{\text{Monoid}} \subset S_{\text{Ring}}$, ist die Aussage sinnvoll. Insbesondere ist jeder Ring eine abelsches Monoid in Bezug auf die multiplikative Operation, da $\Psi_{\text{Monoid}} \subset \Psi_{\text{Ring}}$. Also gilt eine solche Formel in allen Ringen, wenn sie in allen abelschen Monoiden gilt.

Sei nun ϕ eine universelle Formel in der Sprache der Monoide, die in allen Ringen gilt. Sei M ein beliebiges abelsches Monoid. Dann gilt $\mathbb{Z}[M] \models \phi$. Da M bezüglich der multiplikativen Struktur in $\mathbb{Z}[M]$ eingebettet werden kann und ϕ universell ist, gilt schon $M \models \phi$. □

Korollar 16. *Eine Formel* $\forall \overline{x}. s_1(\overline{x}) = t_1(\overline{x}) \wedge \cdots \wedge s_n(\overline{x}) = t_n(\overline{x}) \Rightarrow s(\overline{x}) = t(\overline{x})$ *in der Sprache* S_{Monoid} *gilt in allen Monoiden gdw.* $s - t \in \text{Id}_{\mathbb{Z}}\langle s_1 - t_1, \ldots, s_n - t_n \rangle$.

Beweis. Kombiniere den vorherigen Satz und den betreffenden Satz für allgemeine Ringe. □

4.2 Abelsche Gruppen

Die additive Struktur des Ringes ist eine abelsche Gruppe. Diesen Umstand nutzen wir nun, um das Wortproblem für abelsche Gruppen auf das Wortproblem für Ringe zurückzuführen.

Definition 17. Sei $S_{\mathrm{Grp}} = \{0, +, -\}$. Eine abelsche Gruppe ist ein S_{Grp}-Modell, das folgende Axiome erfüllt:

- $x + (y + z) = (x + y) + z$
- $x + y = y + x$
- $x + 0 = x$
- $x + (-x) = 0$

Satz 18. *Die folgenden Aussagen sind äquivalent:*

(i) $\forall \overline{x}.s_1(\overline{x}) = t_1(\overline{x}) \wedge \cdots \wedge s_n(\overline{x}) = t_m(\overline{x}) \Rightarrow s(\overline{x}) = t(\overline{x})$ *gilt in allen abelschen Gruppen*

(ii) $\forall \overline{x}.s_1(\overline{x}) = t_1(\overline{x}) \wedge \cdots \wedge s_n(\overline{x}) = t_m(\overline{x}) \Rightarrow s(\overline{x}) = t(\overline{x})$ *gilt in allen Ringen*

(iii) $s - t \in \mathrm{Id}_{\mathbb{Z}}\langle s_1 - t_1, \ldots, s_n - t_n\rangle$

(iv) Es gibt ganze Zahlen $c_1, \ldots, c_n \in \mathbb{Z}$*, sodass* $s - t = c_1 \cdot (s_1 - t_1) + \cdots + c_n \cdot (s_n - t_n)$

Beweis. (i)⇒ (ii) gilt, da jeder Ring eine abelsche Gruppe ist. (ii) ⇒ (iii) ist ein Satz, den wir bereits gesehen haben. (iv) ⇒(i) ist eine einfache Folgerung in der Gruppentheorie. Wir müssen also nur noch (iii) ⇒ (iv) zeigen:

Wenn die Idealzugehörigkeit gilt, dann können wir

$$s - t = (c_1 + q_1)(s_1 - t_1) + \cdots + (c_n + q_n)(s_n - t_n)$$

schreiben, wobei $c_i \in \mathbb{Z}$ und die q_i Polynome mit Koeffizienten in $\mathbb{Z}$ ohne Konstantenteil sind. Durch Vergleich der Koeffizienten auf beiden Seiten gilt dann schon

$$s - t = c_1(s_1 - t_1) + \cdots + c_n(s_n - t_n)$$

□