Das Wortproblem für Integritätsringe

Definition Ein Integritätsring ist ein kommutativer, nicht trivialer Ring($1 \neq 0$), der nullteilerfrei ist, d.h. zusätzlich das Axiom I erfüllt:

$$x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$$

Motivation Wir möchten zeigen $Ring \cup \{I\} \models \forall \overline{x}.p_1(\overline{x}) = 0 \wedge ... \wedge p_n(\overline{x}) = 0 \Rightarrow q(\overline{x}) = 0$ *g.d.w. es eine Zahl* $k \in \mathbb{N}$ *gibt, s.d.* $q^k \in Id_{\mathbb{Z}}\langle p_1, ..., p_n\rangle$.
Dafür betrachten wir
$Ring \ \cup \ \{I\} \ \cup \ \{p_1(\overline{x}) = 0, ..., p_n(\overline{x}) = 0\} \ \cup \ \{q(\overline{x}) \neq 0\} \models \bot$
Hierbei können wir die $\overline{x}$ als Konstanten betrachten.
Da I keine definite Klausel ist, müssen wir dies auf einem allgemeineren Weg beweisen. Falls die Aussage oben gilt, gibt es einen Beweis per Resolution, der aus den Axiomen einen Widerspruch (leere Klausel) folgert. Die Klauseln der Resolution haben die Form:

$$\bigvee_{i=1}^{r}(e_i \neq e_i') \vee \bigvee_{j=1}^{s}(f_j = f_j').$$

Über die Gleichheit $s = t \Leftrightarrow s - t = 0$ können wir dies in eine einfachere Form schreiben:

$$\bigvee_{i=1}^{r}(e_i \neq 0) \vee \bigvee_{j=1}^{s}(f_j = 0)$$

Satz Es gilt $(q(\prod_{j=1}^{s} f_j))^k \in Id_{\mathbb{Z}}\langle e_1, ..., e_r, p_1, ..., p_n\rangle$ mit $k \in \mathbb{N}$ für jede Klausel der Resolution.
Beweis Erstmal müssen wir dies für die Grundinstanzen zeigen. Für die Ringaxiome der Form $l = r$ gilt immer $l - r \approx 0$ und damit $(l - r) \in Id_{\mathbb{Z}}\langle p_1, ..., p_n\rangle$. Trivialerweise gilt auch für jedes $p_i = 0$: $p_i \in Id_{\mathbb{Z}}\langle p_1, ..., p_n\rangle$. In beiden Fällen genügte es k=1 zu nehmen und da Ideale unter Multiplikation abgeschlossen sind können wir das q überall multiplizieren und erhalten die Aussage. Als nächstes zeigen wir die Aussage für die restlichen Gleichheits -und Kongruenzeigenschaften:

- $x = y \Rightarrow y = x \quad \Leftrightarrow \quad x \neq y \vee y = x \quad \Leftrightarrow \quad x - y \neq 0 \vee y - x = 0$. Also müssen wir zeigen $(y - x) \in Id_{\mathbb{Z}}\langle x - y, p_1, ..., p_n\rangle$, was stimmt, da $(y - x) \approx -1 \cdot (x - y)$.

- $x = y \wedge y = z \Rightarrow x = z \quad \Leftrightarrow \quad x - y \neq 0 \vee y - z \neq 0 \vee x - z = 0$. Also müssen wir zeigen $(x - z) \in Id_{\mathbb{Z}}\langle x - y, x - z, p_1, ..., p_n\rangle$, was stimmt, da $(x - z) \approx 1 \cdot (x - y) + 1 \cdot (y - z)$.

- $x = x' \Rightarrow -x = -x' \quad \Leftrightarrow \quad x - x' \neq 0 \vee -x - (-x') = 0$. Also müssen wir zeigen $(-x - (-x')) \in Id_{\mathbb{Z}}\langle x - x', p_1, ..., p_n\rangle$ was stimmt, da $-x - (-x')) \approx -1 \cdot (x - x')$.

- $x = x' \wedge y = y' \Rightarrow x + y = x' + y' \quad \Leftrightarrow \quad x - x' \neq 0 \vee y - y' \neq 0 \vee (x + y) - (x' + y') = 0$. Also müssen wir zeigen $((x + y) - (x' + y')) \in Id_{\mathbb{Z}}\langle x - x', y - y', p_1, ..., p_n\rangle$ was stimmt, da $((x + y) - (x' + y')) \approx 1 \cdot (x - x') + 1 \cdot (y - y')$.

- $x = x' \wedge y = y' \Rightarrow x \cdot y = x' \cdot y' \quad \Leftrightarrow \quad x - x' \neq 0 \vee y - y' \neq 0 \vee x \cdot y - x' \cdot y' = 0$. Also müssen wir zeigen $(x \cdot y - x' \cdot y') \in Id_{\mathbb{Z}}\langle x - x', y - y', p_1, ..., p_n\rangle$ was stimmt, da $x \cdot y - x' \cdot y' \approx y \cdot (x + x') + x' \cdot (y - y')$.

Für $q \neq 0$ gilt $q \in Id_{\mathbb{Z}}\langle q, p_1, ..., p_n\rangle$. Bei allen benutzen wir k=1.
Das Axiom I, welches der Form $xy \neq 0 \vee x = 0 \vee y = 0$ entspricht müssen wir jetzt nur noch zeigen. Im Normalfall $x \neq y$ haben wir $x \cdot y = xy \in Id_{\mathbb{Z}}\langle xy, p_1, ..., p_n\rangle$, also gilt dies mit k=1. Da allerdings Klauseln Mengen sind, müssen wir den Spezialfall $x = y$ unterscheiden, in dem I: $x^2 \neq 0 \vee x = 0$ enspricht, und wir brauchen k=2: $(qx)^2 \in Id_{\mathbb{Z}}\langle x^2, p_1, ..., p_n\rangle$.
Jetzt müssen wir nur noch die Resolution überprüfen, also den Induktionsschritt machen: Erstmal fällt auf, da Klauseln Mengen sind, das gleiche Literale zusammengefasst werden. Dabei gibt es zwei Fälle den negierten und unnegierten Fall:

$$\{e \neq 0, e \neq 0, ...\} \to \{e \neq 0, ...\}$$

$$\frac{e \neq 0 \vee e \neq 0 \vee \Gamma}{e \neq 0 \vee \Gamma}$$

Das gilt, da $Id_{\mathbb{Z}}\langle e, e, ...\rangle$ ist das selbe Ideal wie $Id_{\mathbb{Z}}\langle e, ...\rangle$. Nun betrachten wir den unnegierten Fall:

$$\{f = 0, f = 0, ...\} \to \{f = 0, ...\}$$

$$\frac{f = 0 \vee f = 0 \vee \Gamma}{f = 0 \vee \Gamma}$$

Das heißt wir haben nach Induktionshypothese $(p \cdot P \cdot f \cdot f)^k \in I$, was impliziert: $(p \cdot f)^{2k} \in I$, wie gefordert. Hierbei sind durch P die Gleichheiten in der Klausel angedeutet.
Jetzt bleibt nur noch der kompliziertere Resolutionsschritt:

$$\{e \neq 0, \Gamma\} \text{ mit } \{e = 0, \Gamma'\} \text{ resolviert zu } \{\Gamma, \Gamma'\}$$

$$\frac{e \neq 0 \vee \bigvee_{i=1}^{r} e_i \neq 0 \vee \bigvee_{j=1}^{s} f_j = 0 \quad e = 0 \vee \bigvee_{i=1}^{t} g_i \neq 0 \vee \bigvee_{j=1}^{u} h_j = 0}{\bigvee_{i=1}^{r} e_i \neq 0 \vee \bigvee_{j=1}^{s} f_j = 0 \vee \bigvee_{i=1}^{t} g_i \neq 0 \vee \bigvee_{j=1}^{u} h_j = 0}$$

Wenn wir die Induktionhypothese einsetzen erhalten wir:

$$(qF)^k \in Id_{\mathbb{Z}}\langle e, e_1, ..., e_r, p_1, ..., p_n\rangle. \quad (1)$$
$$(qeH)^l \in Id_{\mathbb{Z}}\langle g_1, ..., g_t, p_1, ..., p_n\rangle. \quad (2)$$

mit $F = \prod_{j=1}^{s} f_j$ und $H = \prod_{j=1}^{u} h_j$. Aus (1) folgt für ein Polynom d:

$(qF)^k = d \cdot e + z_1 \cdot e_1 + ...| - d \cdot e$
$(qF)^k - de \in Id_{\mathbb{Z}}\langle e_1, ..., e_r, p_1, ..., p_n\rangle$ $\quad |(x-y)\ teilt\ (x^l - y^l)$
$(qF)^{kl} - d^l e^l \in Id_{\mathbb{Z}}\langle e_1, ..., e_r, p_1, ..., p_n\rangle$ $\quad | \cdot (qH)^l$
$(qF)^{kl}(qH)^l - d^l(qeH)^l \in Id_{\mathbb{Z}}\langle e_1, ..., e_r, p_1, ..., p_n\rangle$ $\quad |\ (2)$
$(qF)^{kl}(qH)^l \in Id_{\mathbb{Z}}\langle e_1, ..., e_r, g_1, ..., g_t, p_1, ..., p_n\rangle$ $\quad | \cdot F^l H^{kl}$
$(qFH)^{kl+l} \in Id_{\mathbb{Z}}\langle e_1, ..., e_r, g_1, ..., g_t, p_1, ..., p_n\rangle.$ $\quad \square$

Satz $Ring \cup \{I\} \models \forall \overline{x}.p_1(\overline{x}) = 0 \wedge ... \wedge p_n(\overline{x}) = 0 \Rightarrow q(\overline{x}) = 0$
$g.d.w.\ es\ eine\ Zahl\ k \in \mathbb{N}\ gibt,\ s.d.\ q^k \in Id_{\mathbb{Z}}\langle p_1, ..., p_n\rangle$.
Beweis⇒: Die erste Aussage ist, wie oben schon beschrieben, äquivalent zu: $Ring \cup \{I\} \cup \{p_1(\overline{x}) = 0, ..., p_n(\overline{x}) = 0\} \cup \{q(\overline{x}) \neq 0\} \models \bot$. Dann muss man nur noch die leere Klausel in die eben bewiesene Aussage einsetzen.
⇐: Sobald alle $p_i(\overline{x}) = 0$, gilt $q^k = 0$. Falls k nichtnull ist, folgt aus I, das $q = 0$, was die Aussage beweist. Falls k=0 ist befinden wir uns im trivialen Ring, und dort gilt sowieso jede Gleichheit. □
Nun zeigen wir einige Korollare, die aus der Aussage folgern.

Korollar $Ring \cup \{I\} \cup C_1 \models \forall \overline{x}.p_1(\overline{x}) = 0 \wedge ... \wedge p_n(\overline{x}) = 0 \Rightarrow q(\overline{x}) = 0\ g.d.w.\ es\ ein\ k \in \mathbb{N}\ gibt,\ so\ dass\ q^k \in Id_{\mathbb{Z}}\langle p_1, ..., p_n\rangle$.
Beweis Benutze vorherigen Satz und den Satz, das der Ausschluss des trivialen Rings nichts an der Aussage ändert. □

Korollar $Ring \cup \{I\} \cup C_p \models \forall \overline{x}.p_1(\overline{x}) = 0 \wedge ... \wedge p_n(\overline{x}) = 0 \Rightarrow q(\overline{x}) = 0\ g.d.w.\ es\ ein\ k \in \mathbb{N}\ und\ ein\ c \in \mathbb{Z},\ mit\ p \nmid c\ gibt,\ so\ dass\ cq^k \in Id_{\mathbb{Z}}\langle p, p_1, ..., p_n\rangle,\ wobei\ p\ im\ Ideal \approx p$.
Beweis: ⇐: Ist erneut trivial, siehe alle anderen "Ideal Beweise".
⇒: Nun haben wir $Ring \cup \{I\} \cup C_1 \cup \{c_1 \neq 0, ..., c_m \neq 0, p = 0\} \models \forall \overline{x}.p_1(\overline{x}) = 0 \wedge ... \wedge p_n(\overline{x}) = 0 \Rightarrow q(\overline{x}) = 0$ für endliche viele $c_1, ..., c_m$, wobei keine durch p teilbar sind. Falls die Charakteristik nicht null ist beschreiben die $c_i \neq 0$ und $p = 0$ genau C_p. Falls die Charakteristik 0 ist, können wir endlich viele $c_i \neq 0$ anschauen und Kompaktheit ausnutzen.
Dieses Argument ist äquivalent zu:
$Ring \cup \{I\} \cup C_1 \models p_1(\overline{x}) = 0 \wedge ... \wedge p_n(\overline{x}) = 0 \wedge p = 0 \Rightarrow c_1...c_m q(\overline{x}) = 0$
Nach dem Satz gilt $(c_1...c_m q)^k \in Id_{\mathbb{Z}}\langle p, p_1, ..., p_n\rangle$, und das Ergebnis folgt, in dem wir $c = (c_1...c_m)^k$ setzen, da p null oder prim ist, und da es keine der c_i teilt, teilt es damit auch nicht c.
p ist null oder prim, denn falls $p = n \cdot m \ \ (n, m > 1) \Rightarrow$
$n \cdot m = 0 \Rightarrow_I n = 0 \vee m = 0$ was ein Widerspruch zur Minimalität von p wäre. □
Anmerkung Diese Aussage ist tatsächlich äquivalent zum bekannten Hilbert (starken) Nullstellensatz aus der Algebra.

Korollar $Ring \cup \{I\} \cup C_0 \models \forall \overline{x}.p_1(\overline{x}) = 0 \wedge ... \wedge p_n(\overline{x}) = 0 \Rightarrow q(\overline{x}) = 0\ g.d.w.\ es\ ein\ k \in \mathbb{N}\ gibt,\ so\ dass\ q^k \in Id_{\mathbb{Q}}\langle p_1, ..., p_n\rangle$.
Beweis Es gilt $q^k \in Id_{\mathbb{Q}}\langle p_1, ..., p_n\rangle$, falls es eine positive Zahl c gibt mit
$cq^k \in Id_{\mathbb{Z}}\langle p_1, ..., p_n\rangle$.
⇐: Falls alle $p_i = 0$, so ist $cq^k = 0$ und damit $q = 0$, da $k = 0$ zu einem Widerspruch führen würde.
⇒: Hierfür wenden wir den vorherigen Satz für $p = 0$ an und müssen p nicht ins Ideal aufnehmen, da die 0 schon in jedem Ideal enthalten ist. □