Korrektheit des Algorithmus von Buchberger zur Berechnung von Gröbner-Basen

(Nachtrag zur Vorlesung vom 17.12.2001 zu "Computergestütztes Symbolisches Rechnen", LMU München)

Falls etwas ausgegeben wird, handelt es sich um eine Gröbnerbasis G von I mit $F \subseteq G$.

Offenbar gilt jederzeit während des Programmlaufs, daß $F \subseteq G \subseteq I$, denn es werden nur Elemente hinzugefügt, und diese sind Reste bei der Division von Elementen von I durch jeweils endlich viele Elemente von I.
Dann $I = \langle F \rangle \subseteq \langle G \rangle \subseteq I$, also $\langle G \rangle = I$.
Abgebrochen wird erst, wenn für alle $p \neq q$ in G gilt $\overline{S(p,q)}^G = 0$ (da in der `FOR`-Schleife G unverändert blieb), also nach dem Satz G eine Gröbner-Basis von $\langle G \rangle$ ist.

Der Algorithmus terminiert.

Am Ende eines Durchlaufs durch die `REPEAT`-Schleife ist $G' \subseteq G$, also

$$\langle LT(G') \rangle \subseteq \langle LT(G) \rangle.$$

Falls die Abbruchbedingung nicht erfüllt ist, ist $G \neq G'$.
Behauptung: Dann ist $\langle LT(G') \rangle \neq \langle LT(G) \rangle$.
Beweis: In diesem Fall wurde ein Divisionsrest r zu G' hinzugefügt. r ist Rest bei Division durch G', also kein Term von r durch einen der Leitterme von G' teilbar. Dies gilt insbesondere für $LT(r)$. Also ist $LT(r)$ nicht im Monomideal $\langle LT(G') \rangle$, wohl aber wegen $r \in G$ in $\langle LT(G) \rangle$.
Wegen des Lemmas über die Stabilisierung wachsender Idealfolgen muß die Abbruchbedingung nach endlich vielen Schleifendurchläufe erfüllt sein, weil wir sonst eine unendliche echt wachsende Folge von Idealen bekämen.