Zu Korollar 11.15 und Bemerkung 11.11

Die Aussage in Korollar 11.15 „Damit ist der Satz anwendbar" ist im allgemeinen leider falsch. Beispiel: $\phi\colon \mathbb{Z} \to \mathbb{Z}_p$. Dann ist $\psi(px+1) = 1$, d.h. ein Polynom positiven Grades wird auf eine Einheit abgebildet. Die Voraussetzungen des Satzes sind also insbesondere in dem für uns wichtigen Spezialfall $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$ unerfüllbar.

Für den angesprochenen Spezialfall eignet sich jedoch das folgende Kriterium.

Irreduzibilitätskriterium modulo p.
Sei $f = f_0 + f_1\,x + \ldots + f_k\,x^k \in \mathbb{Z}[x] \setminus \mathbb{Z}$ ein ganzzahliges Polynom mit positivem Grad, dessen Koeffizienten keinen gemeinsamen Teiler besitzen (d.h. keine Primzahl teile alle Koeffizienten). Sei p eine Primzahl, die den Höchstkoeffizienten f_k nicht teilt.

Sei $\phi\colon \mathbb{Z} \to \mathbb{Z}_p$ der Ring-Epimorphismus, der jede ganze Zahl auf ihre Restklasse modulo p abbildet. Sei weiter $\psi\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, $\sum a_i\,x^i \mapsto \phi(a_i)\,x^i$ die Fortsetzung von ϕ auf die Polynomringe.

Ist $\psi(f)$ irreduzibel über $\mathbb{Z}_p$, so ist f irreduzibel über $\mathbb{Z}$.

- Informelle Version: Ist unter den angegebenen Voraussetzungen f irreduzibel über $\mathbb{Z}_p$, so ist f irreduzibel über $\mathbb{Z}$.
- Für monische Polynome sind die Primzahlvoraussetzungen automatisch erfüllt.

Beweis. Sei $f = g\,h$ in $\mathbb{Z}[x]$. Dann gilt auch $\psi(f) = \psi(g)\,\psi(h)$ in $\mathbb{Z}_p[x]$. Da nach Voraussetzung $\psi(f)$ irreduzibel über $\mathbb{Z}_p$ ist, muss einer der Faktoren eine Einheit in $\mathbb{Z}_p[x]$ sein. (Die Einheiten in $\mathbb{Z}_p[x]$ sind die vom Nullpolynom verschiedenen konstanten Polynome.) OBdA sei der erste Faktor g eine Einheit in $\mathbb{Z}_p[x]$, also

$$\psi(g_m x^m + \ldots + g_1 x + g_0) = \phi(g_m)x^m + \ldots + \phi(g_1)x + \phi(g_0) = \phi(g_0) \neq 0 \ .$$

Damit gilt in $\mathbb{Z}[x]$ die Darstellung

$$f_k x^k + \ldots + f_1 x + f_0 = (p\tilde{g}_m x^m + \ldots + p\tilde{g}_1 x + g_0)(h_n x^n + \ldots + h_1 x + h_0) \ .$$

Die rechte Seite hat den „Höchstkoeffizienten" $pg_m h_n$, der entweder null ist oder mit dem Höchstkoeffizienten f_k der linken Seite übereinstimmen muss. Letzteres ist aufgrund der Voraussetzung „p teilt nicht f_k" ausgeschlossen. Folglich ist $\tilde{g}_m = 0$. Da m beliebig war, folgt $g = g_0$ und

$$f_k x^k + \ldots + f_1 x + f_0 = g_0(h_n x^n + \ldots + h_1 x + h_0) \ .$$

Da nach Voraussetzung keine Primzahl alle Koeffizienten von f teilt, kann auch keine Primzahl g_0 teilen. Somit ist $g_0 = \pm 1$ eine Einheit in $\mathbb{Z}$ un damit eine Einheit $\mathbb{Z}[x]$. Wir haben gezeigt, aus dem Ansatz $f = g\,h$ in $\mathbb{Z}[x]$ folgt, dass einer der Faktoren eine Einheit in $\mathbb{Z}[x]$ ist. Das entspricht der Irreduzibilität.

Beispiel zu Bemerkung 11.11 (b) der Vorlesung: Das ganzzahlige Polynom $4x^2 - 1 = (2x-1)(2x+1)$ ist reduzibel über $\mathbb{Z}$, besitzt aber keine Nullstellen in $\mathbb{Z}$.