8 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir den im Skript 7 angekündigten Beweis von Satz 8.1 führen. Der letzte Abschnitt 11 im Kapitel 1 wird für Irreduzibilitätsteste und Beispiele gewidmet. Damit beenden wir Kapitel 1.

Sei hier R stets ein integer Ring.

Satz 8.1.
R ist genau dann faktoriell wenn $R[x]$ faktoriell ist.

Beweis:
Die Rückrichtung ist Lemma 7.1 und wurde bereits gezeigt.
Sei R faktoriell. Seien $F = \text{Quot}\,(R)$ und $0 \neq p(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. Setze $d = \text{ggT}\{a_0, \ldots, a_n\}$ (d existiert weil R faktoriell ist wegen Proposition 6.6). Schreibe $p(x) = dq(x)$ (für ein geeignetes $q(x) \in R[x]$). Der ggT der Koeffizienten von q ist nun 1.
Da R faktoriell ist lässt sich d in R als Produkt $d = d_1 \cdots d_m$ von Irreduziblen faktorisieren und diese Irreduziblen in R sind auch in $R[x]$ irreduzibel (Beweis Lemma 7.1 $(**)$).
Nun wollen wir $q(x)$ als Produkt von irreduziblen Polynomen aus $R[x]$ schreiben. Da $F[x]$ faktoriell ist (Beispiel 5.7(ii)), existieren $q_1(x), q_2(x), \ldots, q_n(x) \in F[x]$, irreduzibel in $F[x]$ mit $q(x) = q_1(x) \cdots q_n(x)$. Nach dem Lemma von Gauß können wir annehmen dass $q_i \in R[x]$ für alle $i = 1, \cdots, n$. Da der ggT der Koeffizienten von $q(x)$ 1 ist, ist der ggT der Koeffizienten von q_i auch 1 , für alle $i = 1, \cdots, n$. Nach Korollar 7.4 ist q_i irreduzibel in $R[x]$, für alle $i = 1, \cdots, n$. Wir können also $p(x)$ als Produkt von irreduziblen Polynomen aus $R[x]$ schreiben:
$p(x) = d_1 \cdots d_m q_1(x) \cdots q_n(x)$.
Es bleibt noch zu zeigen, dass diese Faktorisierung eindeutig bis auf Reihenfolge der Faktoren und Multiplikation mit Einheiten ist. Das wird als ÜA gemacht. □

Induktion auf n ergibt:

Korollar 8.2.
Ist R faktoriell so ist $R[x_1, \ldots, x_n]$ auch faktoriell.

Beweis: ÜA.

§ 11 Irreduzibilitätskriterien

Wir untersuchen hier weiter die Irreduzibilität eines Polynoms in einem Integerring. Wir beginnen mit einer Bemerkung:

Bemerkung 8.3. Sei $R = K$ ein Körper, und $0 \neq p(x) \in K[x] \setminus K$. Wenn $\deg p = 1$ dann ist p irreduzibel. Wenn $\deg p = 2$ oder $\deg p = 3$, dann ist p reduzibel genau dann, wenn p einen linearen Faktor in $K[x]$ hat, genau dann, wenn p eine Nullstelle in K hat (s. LA II Skript 4 Korollar 4.1).

Lemma 8.4. Sei $p(x) \in R[x] \setminus R$ ein normiertes Polynom. Dann ist p irreduzible in $R[x]$ genau dann, wenn $p(x)$ kein Produkt $p(x) = a(x)b(x)$ von normierten Polynomen $a(x)$, $b(x)$ mit $\deg a(x) < \deg p(x)$ und $\deg b(x) < \deg p(x)$ ist.

Beweis:
Sei $p(x) \in R[x]$ nicht-konstant, so dass $p(x) = a(x)b(x)$ mit $\deg a(x) < \deg p(x)$ und $\deg b(x) < \deg p(x)$. Da R integer ist, ist $\deg p(x) = \deg a(x) + \deg b(x)$ (s. Beweis Satz 4.8). Da $\deg p(x) > 0$, sind $\deg a(x) > 0$ und $\deg a(x) > 0$, also sind $a(x) \notin R$ und $b(x) \notin R$. Da $R[x]^\times = R^\times$ (s. Beweis Lemma 7.1 $(**)$) sind insbesondere $a(x) \notin R[x]^\times$ und $b(x) \notin R[x]^\times$. Also ist $p(x)$ reduzibel.

Umgekehrt sei $p(x)$ nicht-konstant, normiert und reduzibel in $R[x]$.
Also gibt es Polynome $a'(x) \in R[x] \setminus R[x]^\times$ und $b'(x) \setminus R[x]^\times$ mit $p(x) = a'(x)b'(x)$. Insbesondere sind $a'(x) \notin R^\times$ und $b'(x) \notin R^\times$. Wir bemerken dass der Leitkoeffizient von $p = 1 = a_m b_n$, wobei $a_m \in R$ der Leitkoeffizient von $a'(x)$ und $b_n \in R$ der Leitkoeffizient von $b'(x)$ sind (s. Beweis Satz 4.8). Also sind $a_m, b_n \in R^\times$ (es gelten $b_n = a_m^{-1}$ und $a_m = b_n^{-1}$). Es folgt dass $a'(x) \notin R$ (sonst wäre $a'(x) = a_m \in R^\times$) und analog $b'(x) \notin R$. Also sind $\deg a'(x) < \deg p(x)$ und $\deg b'(x) < \deg p(x)$.

Nun setze $a(x) := a_m^{-1} a'(x)$ und $b(x) := b_n^{-1} b'(x)$. Dann sind $a(x)$ und $b(x)$ normiert mit $\deg a(x) < \deg p(x)$ und $\deg b(x) < \deg p(x)$. Ferner gilt

$$p(x) = a_m b_n p(x) = b_n^{-1} a_m^{-1} a'(x) b'(x) = a_m^{-1} a'(x) b_n^{-1} b'(x) = a(x)b(x).$$

□

Proposition 8.5.
Sei I ein echtes Ideal in R und sei $p(x)$ ein normiertes Polynom aus $R[x] \setminus R$. Wenn $\varphi(p) = \overline{p}(x)$ in $(R/I)[x]$ sich nicht als Produkt $\overline{p}(x) = \overline{a}(x)\overline{b}(x)$ von Polynomen in $(R/I)[x]$ mit $\deg \overline{a}(x) < \deg \overline{p}(x)$ und $\deg \overline{b}(x) < \deg \overline{p}(x)$ darstellen lässt, dann ist $p(x)$ irreduzibel in $R[x]$.

Beweis:
Sei $p(x) \in R[x]$ nicht-konstant, normiert und reduzibel. Aus Lemma 8.4 ist $p(x) = a(x)b(x)$, $a(x)$, $b(x) \in R[x]$ normiert und nicht-konstant. Seien $\overline{p}(x), \overline{a}(x)$ und $\overline{b}(x)$ die Bilder von $p(x), a(x)$ und $b(x)$ in $(R/I)[x]$ (s. Beweis Lemma 7.2). Dann $\overline{p}(x) = \overline{a}(x)\overline{b}(x)$. Da I echt ist, $a(x)$ und $b(x)$ normiert und nicht-konstant sind, so sind auch $\overline{a}(x)$ und $\overline{b}(x)$. Es folgt, dass $\deg \overline{a}(x) < \deg \overline{p}(x)$ und $\deg \overline{b}(x) < \deg \overline{p}(x)$. □

Proposition 8.5 kann man anwenden um zu prüfen ob ein Polynom über $\mathbb{Z}$ irreduzibel ist.

Beispiel:
Betrachte das Polynom $x^4 + 9x^3 + 10x^2 + 22x + 1 \in \mathbb{Z}[x]$.
Das Bild in $\mathbb{Z}_2[x]$ ist $x^4 + x^3 + 1$. Dieses Polynom besitzt keine Nullstelle in $\mathbb{Z}_2$ (prüfe 0 und 1). Daher, wenn es reduzibel ist, dann zerfällt es als Produkt zweier irreduziblen Polynomen aus $\mathbb{Z}_2[x]$ von Grad 2. (Wir arbeiten über $\mathbb{Z}_2 = \mathbb{F}_2$ und können Bemerkung 8.3 ausnutzen). Wenn $p(x) \in \mathbb{Z}_2[x]$ irreduzibel von Grad 2 ist, dann ist das Leitkoeffizient 1 und das konstante Koeffizient ist auch 1 (weil 0 keine Nullstelle ist). Das Polynom x^2+1 hat die Nullstelle 1. Somit gibt es nur ein irreduzibles Polynom von Grad 2 aus $\mathbb{Z}_2[x]$, und zwar $x^2 + x + 1$ (prüfe, dass 0 und 1 keine Nullstelle sind). Aber $(x^2 + x + 1)^2 = x^4 + x^2 + 1$. Somit ist $x^4 + x^3 + 1$ irreduzibel über $\mathbb{Z}_2$ und, daher ist $x^4 + 9x^3 + 10x^2 + 22x + 1$ irreduzibel über $\mathbb{Z}$.

Leider funktioniert dieses Verfahren nicht immer.

Bemerkung 8.6. Seien $a(x), b(x)$ nicht-konstante Polynome $\in R[x]$ so dass $f(x) := a(x)b(x) = x^n$ für ein $n \in \mathbb{N}$. Dann sind $a(x)$ und $b(x)$ Monome, das heißt, es gibt $\alpha, \beta \in R^\times$ und $p, q \in \mathbb{N}$ so dass $a(x) = \alpha x^p$ und $a(x) = \beta x^q$ (und $\alpha\beta = 1$, $p + q = n$). In der Tat kann man zeigen, dass nur die Leitkoeffiziente von $a(x)$ und $b(x)$ ungleich Null sind. Siehe ÜA.

Hier zeigen wir dass die konstante Koeffiziente gleich Null sind. Bemerke dass der konstante Koeffizient $f(0)$ von $f(x) := a(x)b(x)$ das Produkt der konstante Koeffiziente $a(0)$ und $b(0)$ von $a(x)$ and $b(x)$ ist. Wir behaupten dass $b(0) = a(0) = 0$. In der Tat, $0 = f(0) = a(0)b(0)$. Da R ein Integritätsbereich ist, gilt $a(0) = 0$ oder $b(0) = 0$. Angenommen $a(0) = 0$. Sei $F = \text{Quot}\,(R)$ und $m \in \mathbb{N}$ maximal mit $a(x) = x^m a'(x)$ für gewisses $a'(x) \in F[x]$ (m ist die Vielfachheit der Nullstelle $x = 0$ von $a(x)$). Dann $a'(0) \neq 0$ und somit $a'(x)b(x) = x^{n-m}$. Da $b(x)$ nicht konstant ist, dann gilt $n - m > 0$. Daher $a'(0)b(0) = 0$ also $b(0) = 0$ und die Behauptung wurde bewiesen.

Proposition 8.7. (Eisensteinkriterium)
Seien P ein Primideal in R, $n \in \mathbb{N}$ und $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in R[x]$. Angenommen $a_{n-1}, \ldots, a_0 \in P$ aber $a_0 \notin P^2$. Dann ist $f(x)$ irreduzibel in $R[x]$.

Beweis:
Angenommen $f(x) = a(x)b(x)$ in $R[x]$ wobei $a(x)$ und $b(x)$ nicht-konstante normierte Polynome sind (s. Lemma 8.4).
Seien $\overline{f}(x), \overline{a}(x), \overline{b}(x)$ die Bilder von $f(x), a(x)$ bzw. $b(x)$ in $(R/P)[x]$ (s. Beweis Lemma 7.2). Also $x^n = \overline{f}(x) = \overline{a}(x)\overline{b}(x)$. Dann gilt $\overline{a}(0) = \overline{b}(0) = 0$ (man kann Bemerkung 8.6 anwenden weil R/P ein Integerring ist). Aber dann liegen die konstante Koeffizienten von $a(x)$ und $b(x)$ in P und somit liegt der konstante Koeffizient a_0 von $f(x)$ in P^2. Widerspruch. Somit ist $f(x)$ irreduzibel. □

Korollar 8.8.
Sei p prim in $\mathbb{Z}$, $n \geq 1$ und sei $f(x) := x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Angenommen p teilt a_i für alle $0 \leq i \leq n-1$ aber p^2 teilt nicht a_0. Dann ist $f(x)$ irreduzibel in $\mathbb{Z}[x]$ sowie in $\mathbb{Q}[x]$.

Beweis:
Für $\mathbb{Z}[x]$: Wende das Eisensteinkriterium auf das Primideal $< p >$ an. Für $\mathbb{Q}[x]$: Korollar 7.4 zu Gauß Lemma anwenden. □

Beispiel:

1. Das Polynom $x^5 + 10x^4 + 25x^2 + 35 \in \mathbb{Z}[x]$ ist irreduzibel nach Eisensteinkriterium auf $p = 5$ angewandt.

2. Sei $f(x) := x^4 + 1 \in \mathbb{Z}[x]$. Wir dürfen das Eisensteinkriterium nicht direkt anwenden. Sei $g(x) = f(x + 1)$, also $g(x) = x^4 + 4x^3 + 6x^2 + 4x + 2$. Nun, nach Eisenstein angewandt auf 2, ist $g(x)$ irreduzibel und, wenn f als Produkt von nicht-konstanten Faktoren zerfällt, dann auch g. Daher ist f irreduzibel.