Beweis des Satzes von Gauß

Bem Es genügt z.z., dass $R[x]$ fakt. ist (denn dann auch $(R[x])[y] = R[x,y]$ usw.)

Bem Satz 5.4.15 sagt: wir brauchen nur die Eindt.keit von Darst. zeigen.

Beweis durch Widerspruch: ang. $\exists$ $r(x) \in R[x]$, das zwei nicht-äquiv. Darst. existieren

$$r(x) = p_1(x) \cdots p_r(x) = q_1(x) \cdots q_s(x)$$

Können OE annehmen

1) $\deg r(x)$ ist min. unter allen Polynomen mit nicht-eindt. Darstellung

2) $m = \deg p_1 \geq \deg p_2 \geq \ldots$

3) $n = \deg q_1 \geq \deg q_2 \geq \ldots$

4) $n \geq m$

Ausserdem gilt:

5) $\deg r > 0$ (... denn sonst wäre r ein Elt. von R und in R sind je zwei Darst. äquivalent)

6) r ist nicht irreduzibel in $R[x]$ (denn sonst gäbe es keine interessanten Darstellungen)

7) p_1 ist zu keinem der q_i assoziiert (denn sonst könnte ich p_1 kürzen, erhielte Polynom mit untersch. Darstellungen vom Grad $< \deg r$)

Schreibe

$a :=$ Leitkoeff. von p_1, d.h. $p_1(x) = a \cdot x^m +$ (Terme kleinerer Ordnung)

$b :=$ — " — q_1

$$s(x) = a \cdot r - b \cdot p_1 x^{n-m} \cdot q_2 \cdots q_s$$

$$= \underbrace{(a \cdot q_1 - b \cdot p_1 x^{n-m})}_{\deg < \deg q_1} q_2 \cdots q_s \qquad \deg < \deg r \qquad (*)$$

$$= p_1 (a \cdot p_2 \cdots p_r - b \cdot x^{n-m} \cdot q_2 \cdots q_s) \qquad (**)$$

Fall 1 $s = 0$ Dann ist $a \cdot q_1 = b \cdot p_1 \cdot x^{n-m}$

Fall 2 $s \neq 0$ Verfeinere $(*)$ und $(**)$ zu Darstellungen; diese müssen äquivalent sein, weil $\deg s < \deg r$. Weil p_1 nicht zu $q_2, \dots, q_s$ assoziiert ist, muss es zu einem Faktor von $(a \cdot q_1 - b \cdot p_1 x^{n-m})$ assoziiert sein

$$p_1 \mid (a q_1 - b \cdot p_1 \cdot x^{n-m}) \Rightarrow p_1 \mid a \cdot q_1$$

In jedem Fall: $\exists\, h \in R[x]$: $p_1(x) \cdot h(x) = a \cdot q_1(x)$.

Beob: Wenn f ein irred. Faktor von a ist (d.h. $f \in R$ ist prim), dann ist $f \mid p_1 \cdot h$; also nach Lemma: $f \mid p_1$ oder $f \mid h$.

Aber: p_1 ist irreduzibel, hat keine echten Teiler. Also: $f \mid h$

$\Rightarrow a \mid h$

Kann also a kürzen, erhalte

$$p_1(x) \cdot h'(x) = q_1(x)$$

irreduzibel, hat keine echten Teiler $\Rightarrow h'$ ist Einheit

Also: $p_1 \sim q_1$, Widerspruch ↯ □