<u>Beweis:</u> Sei R ein Hauptidealring.

Zuerst zeigen wir, dass jedes Element aus R in irred. Faktoren zerlegbar ist:

- Sei $\tilde{R} := \{ r \in R : r \neq 0$ und r ist <u>nicht</u> in irred. Faktoren zerlegbar$\}$.
  Wir führen die Annahme $\tilde{R} \neq \emptyset$ zu einem Widerspruch.
- Sei $r_0 \in \tilde{R}$. Dann ist $r_0 \neq 0$ und r_0 ist nicht irred., d.h. es ex. r_1, r_1' mit $r_1 \notin R^*$, $r_1' \notin R^*$ und $r = r_1 \cdot r_1'$, und weil $r_0 \in \tilde{R}$, ist mindestens einer der Faktoren r_1, r_1' in $\tilde{R}$ (denn wenn $r_1, r_1' \notin \tilde{R}$, dann sind r_1 und r_1' beide in irred. Faktoren zerlegbar, somit auch $r_0 = r_1 \cdot r_1'$).
- OEdA sei $r_1 \in \tilde{R}$. Dann gilt $(r_0) \subsetneq (r_1)$:
  - Weil $r_0 \in (r_1)$ gilt $(r_0) \subseteq (r_1)$.
  - Ist $(r_0) = (r_1)$, dann ist $r_1 = r_0 \cdot s$, d.h. $r_0 = r_1 \cdot r_1' = r_0 \cdot s \cdot r_1'$
    $\Rightarrow r_0(1 - s r_1') = 0 \Rightarrow 1 = s \cdot r_1' \Rightarrow r_1' \in R^* \lightning_{r_1' \notin R^*}^{\text{zu}}$
- Weil $r_1 \in \tilde{R}$ gilt analog, dass ein $r_2 \in \tilde{R}$ ex. mit $(r_1) \subsetneq (r_2)$.
- So weiter gefahren, erhalten wir aus $\tilde{R} \neq \emptyset$ eine unendliche Kette $(r_0) \subsetneq (r_1) \subsetneq \ldots \subsetneq (r_n) \subsetneq \ldots$ von Idealen in R.
- Sei $I := \bigcup_{n \in \mathbb{N}} (r_n) \subseteq R$. Dann ist I ein Ideal in R:
  - $a, b \in I$, dann ex. $m \in \mathbb{N}$ mit $a, b \in (r_m)$ und es ist $a + b \in (r_m) \subseteq I$ und $s \cdot a \in (r_m) \subseteq I$ (für alle $s \in R$).
- Weil R ein Hauptidealring ist, ex. $a \in R$ mit $I = (a)$, und weil $a \in I$ ex. $n_0 \in \mathbb{N}$ mit $a \in (r_{n_0}) \subsetneq (r_{n_0+1}) \subsetneq I = (a) \lightning_{(a) \subseteq (r_{n_0})}^{\text{zu}}$
- Somit muss die Kette $(r_0) \subsetneq \ldots$ abbrechen $\lightning_{\tilde{R} \neq \emptyset}^{\text{zu}}$

Nun zeigen wir, dass die Zerlegung eindeutig ist:

- Sei $r \in R$ mit $r = a \cdot u_1 \cdot \ldots \cdot u_n = b \cdot v_1 \cdot \ldots \cdot v_m$ wobei $a, b \in R^*$ und u_i, v_j irreduzibel sind.
- Mit Kor. 13.5 sind u_i, v_j Primelemente, d.h. $v_j \mid a \cdot u_1 \cdot \ldots \cdot u_n$
  $\Rightarrow v_j$ teilt einen Faktor. ∘ $v_j \mid a \Rightarrow v_j \cdot s = a \Rightarrow v_j \cdot (s a^{-1}) = 1 \Rightarrow v_j \in R^* \lightning$
  ∘ $v_j \mid u_i \Rightarrow u_i = s \cdot v_j$ und weil u_i, v_j irred., ist $s \in R^*$, d.h. u_i, v_j assoz. ⊣

<u>Def.</u> Sei R ein faktorieller Ring und $q \in R[X]$ mit $q \neq 0$. Dann heisst q <u>primitiv</u>, falls ein ggT der Koeffizienten von q gleich 1 ist.

<u>Lemma 13.7</u> (Gauss) Sei R ein faktorieller Ring und $q \in R[X]$ primitiv. Weiter sei $Q := \mathrm{Quot}(R)$ der Quotientenkörper von R. Dann gilt:

$$q \text{ irreduzibel in } R[X] \iff q \text{ irreduzibel in } Q[X]$$

<u>Beweis:</u> Mit Kontraposition.

($\Rightarrow$) Wir nehmen an, dass q zerlegbar in $Q[X]$ ist.

- Sei $q = s \cdot t$ mit $s, t \notin Q[X]^* = Q^* = Q \setminus \{0\}$ (Prp. 12.5(b)).
- Weil $q \neq 0$ ist $s \neq 0 \neq t$, somit $s, t \notin Q$, aber $s, t \in Q[X]$.
- Sei $s = a_0 + a_1 X + \ldots + a_n X^n$ mit $a_i \in Q$, $a_n \neq 0$, $n \geq 1$. Dann ist $a_i = \frac{c_i}{d_i}$ mit $c_i, d_i \in R$, $d_i \neq 0$, und für den Hauptnenner $a := d_0 \cdot \ldots \cdot d_n$ ist dann $a \in R$ und $a \cdot s \in R[X]$.
- Analog finden wir $b \in R$ mit $b \cdot t \in R[X]$.
- Somit ist $(a \cdot s) \cdot (b \cdot t) = (a \cdot b) \cdot (s \cdot t) = (a \cdot b) \cdot q$ mit $a \cdot b \in R$.
- Weil R faktoriell ist gilt $a \cdot b = e \cdot u_1 \cdot \ldots \cdot u_k$ mit $e \in R^*$ und u_i irreduzibel in R, also u_i Primelement in R (Faktum 13.2).
- Es gilt somit $(a \cdot s) \cdot (b \cdot t) = (e \cdot u_1 \cdot \ldots \cdot u_k) \cdot q$
- Weil alle u_i's Primelemente sind und für alle u_i gilt $u_i \mid a \cdot b$, folgt für alle u_i: $u_i \mid a$ oder $u_i \mid b$. D.h. wir können alle u_i's kürzen und erhalten

$$(e_s \cdot s) \cdot (e_t \cdot t) = e \cdot q \quad \text{wobei } e_s, e_t, e \in R^*.$$

Somit ist $\underbrace{(e^{-1} \cdot e_s \cdot s)}_{\in R[X]} \cdot \underbrace{(e_t \cdot t)}_{\in R[X]} = q$ und q ist zerlegbar in $R[X]$.

($\Leftarrow$) Wir nehmen an, dass q zerlegbar in $R[X]$ ist.

- Sei $q = s \cdot t$ mit $s, t \in R[X]$ und $s, t \notin R[X]^* = R^*$.
- Ist $s \in R \setminus R^*$ oder $t \in R \setminus R^*$, so ist q nicht primitiv $\lightning$ zur Voraussetzung
- Also $s, t \notin R$, und weil $s, t \in R[X]$, ist $\operatorname{grad}(s), \operatorname{grad}(t) \geq 1$.
- D.h. $s, t \in Q[X] \setminus Q$ und $q = s \cdot t$ ist zerlegbar in $Q[X]$.

$\dashv$

[Bem. $q = \underbrace{4X^5 - 12X^3 + 18X^2 - 30}_{2 \cdot (2X^5 - 6X^3 + 9X^2 - 15)}$ ist zerlegbar in $\mathbb{Z}[X]$ aber irreduzibel in $\mathbb{Q}[X]$]

Kriterium von Schönemann-Eisenstein 13.9

Sei R ein faktorieller Ring, $q \in R[X]$, q primitiv, $\operatorname{grad}(q) = n \geq 1$,

$$q = a_0 + a_1 X + \ldots + a_n X^n, \quad a_n \neq 0.$$

Existiert ein Primelement $p \in R$ mit

- $p \mid a_i$ für $0 \leq i < n$,
- $p \nmid a_n$,
- $p^2 \nmid a_0$,

dann ist q irreduzibel in $R[X]$ (und mit Gauss' Lemma auch in $Q[X]$).

Beweis: Seien $s, t \in R[X]$ mit $q = s \cdot t$.

zu zeigen: $s \in R^*$ oder $t \in R^*$, wobei $R^* = R[X]^*$.

- Seien $s = b_0 + \ldots + b_k X^k$, $t = c_0 + \ldots + c_\ell X^\ell$ mit $k, \ell \leq n$ und $b_k, c_\ell \neq 0$.
- Dann ist $q = s \cdot t = \underbrace{b_0 \cdot c_0}_{a_0} + \underbrace{(b_0 \cdot c_1 + b_1 \cdot c_0)}_{a_1} \cdot X + \ldots + b_k c_\ell X^{k+\ell}$
$= a_0 + a_1 \cdot X + \ldots + a_n X^n$

  mit $n = k + \ell$.

- p Primelement $\left.\begin{array}{l} p \mid b_0 \cdot c_0 \Rightarrow p \mid b_0 \vee p \mid c_0 \\ p^2 \nmid b_0 \cdot c_0 \Rightarrow \neg(p \mid b_0 \wedge p \mid c_0) \end{array}\right\}$ entweder $p \mid b_0$ oder $p \mid c_0$

- OBdA $p \mid b_0 \wedge p \nmid c_0$.
- $p \nmid \underbrace{a_n}_{= b_k \cdot c_\ell} \Rightarrow p \nmid b_k \wedge p \nmid c_\ell$
- Weil $p \mid b_0$ und $p \nmid b_k$ ex. kleinstes $j \leq k$ mit $p \mid b_i$ für $0 \leq i < j$ und $p \nmid b_j$.
- Für a_j gilt dann $a_j = \underbrace{b_0 c_j}_{p \text{ teilt}} + \underbrace{b_1 c_{j-1}}_{p \text{ teilt}} + \dots + \underbrace{b_{j-1} \cdot c_1}_{p \text{ teilt}} + \underbrace{b_j c_0}_{p \text{ teilt } \underline{\text{nicht}}}$

  $\Rightarrow p \nmid a_j \Rightarrow j = n = k + \ell \Rightarrow j = k = n \wedge \ell = 0.$
- Somit ist $\operatorname{grad}(t) = 0$, also $t \in R$, und weil $q = s \cdot t$ und q primitiv ist, ist $t \in R^*$.
- Unter der Annahme $p \nmid b_0 \wedge p \mid c_0$ folgt analog $s \in R^*$.
- Somit folgt aus $q = s \cdot t$, dass $s \in R^*$ oder $t \in R^*$, d.h. q ist irreduzibel in $R[X]$.

$\dashv$

<u>Beispiel:</u> $q = 2X^5 - 6X^3 + 9X^2 - 15 \in \mathbb{Z}[X]$

- q ist primitiv
- Für $p = 3$ gilt: $p \mid \overbrace{15}^{a_0}$, $p \mid \overbrace{0}^{a_1}$, $p \mid \overbrace{9}^{a_2}$, $p \mid \overbrace{6}^{a_3}$, $p \mid \overbrace{0}^{a_4}$

  $p \nmid \overbrace{2}^{a_5}$

  $p^2 \nmid \overbrace{15}^{a_0}$

Somit ist q irred. in $\mathbb{Z}[X]$ und weil $\mathbb{Q} = \operatorname{Quot}(\mathbb{Z})$ ist q auch irred. in $\mathbb{Q}[X]$.