Proposition (13.1)

Sei K ein Körper und $f \in K[x]$ nicht konstant, also $f \notin K$.

(i) Ist $\mathrm{grad}(f) = 1$, dann ist f im Ring $K[x]$ irreduzibel.

(ii) Im Fall $\mathrm{grad}(f) \in \{2, 3\}$ ist f genau dann irreduzibel, wenn f in K keine Nullstelle besitzt.

(iii) Im Fall $\mathrm{grad}(f) \in \{4, 5\}$ ist f genau dann irreduzibel, wenn f in K keine Nullstelle besitzt und durch kein normiertes, irreduzibles Polynom vom Grad 2 teilbar ist.

Anwendungsbeispiel zu Prop. 13.1:

Das Polynom $g = x^5 + x^2 + \bar{1} \in \mathbb{F}_2[x]$ ist irreduzibel,
denn

- $g(\bar{0}) = \bar{1}$, $g(\bar{1}) = \bar{1} \Rightarrow g$ hat in $\mathbb{F}_2$ keine Nullst.
- g hat auch keinen irreduziblen Teiler vom Grad 2, denn: $x^2, x^2 + \bar{1}, x^2 + x, x^2 + x + \bar{1}$

sind die Polynome vom Grad 2 in $\mathbb{F}_2[x]$. irreduzibel ist nur $h = x^2 + x + \bar{1}$ (Alle anderen haben eine Nullst.)

Es gilt aber $h \nmid g$, denn ansonsten wäre h auch Teiler von $g - x^3 h = x^4 + x^3 + x^2 + x + \bar{1}$ und auch von $g - x^3 h - x^2 h = \bar{1}$ ↯ da $h \neq \bar{1}$

Nullstellen in Quotientenkörpern

Satz (13.2)

Sei R ein faktorieller Ring, K sein Quotientenkörper und $f \in R[x]$ ein Polynom vom Grad $n \geq 1$. Sei $f = a_n x^n + ... + a_1 x + a_0$ mit $a_0, ..., a_n \in R$.

(i) Ist $\alpha \in K$ eine Nulstelle von f, $\alpha = \frac{p}{q}$ mit $p, q \in R$ und $q \neq 0$, wobei p und q teilerfremd sind, dann gilt $q \mid a_n$ und $p \mid a_0$.

(ii) Ist insbesondere f normiert, also $a_n = 1$, dann liegt α in R und ist ein Teiler von a_0.

Anwendungsbeispiel:
Das Polynom $f = x^3 - x + 2$ ist irreduzibel in $\mathbb{Q}[x]$.

Es gilt aber $h \neq g$, denn ansonsten wäre h auch

Anwendungsbeispiel zu Satz 13.2:

$f = x^3 - x + 2 \in \mathbb{Q}[x]$ ist irreduzibel, denn

- Wegen $\operatorname{grad}(f) = 3$ genügt es zu überprüfen, dass f in $\mathbb{Q}$ keine Nullstelle hat:
- Ang. $\alpha \in \mathbb{Q}$ ist Nullst. von f. Satz 13.2 $\Rightarrow \alpha \in \mathbb{Z}$ und $\alpha \mid 2 \Rightarrow \alpha \in \{\pm 1, \pm 2\}$. Aber Einsetzen zeigt, dass diese Zahlen keine Nullst. von f sind.

Beweis von Satz 13.2:

Sei $x = \frac{p}{q} \in K$ eine Nullst. von $f = a_n x^n + \ldots + \ldots + a_1 x + a_0$, mit $p, q \in R$, $q \neq 0$, $\mathrm{ggT}(p, q) = 1$ $\Longrightarrow \sum_{k=0}^{n} a_k \left(\frac{p}{q}\right)^k = 0$

$\overset{\cdot q^n}{\Longrightarrow} \sum_{k=0}^{n} a_k p^k q^{n-k} \Longrightarrow a_0 q^n = -\sum_{k=1}^{n} a_k p^k q^{n-k}$

$= p\left(\sum_{k=1}^{n} (-a_k) p^{k-1} q^{n-k}\right) \Longrightarrow p \mid a_0 q^n \overset{\mathrm{ggT}(p,q)=1}{\Longrightarrow}$

$p \mid a_0$ ebenso: $a_n p^n = -\sum_{k=0}^{n-1} a_k p^k q^{n-k}$

$= q\left(\sum_{k=0}^{n-1} (-a_k) p^k q^{n-k-1}\right) \Rightarrow q \mid a_n p^n \Longrightarrow q \mid a_n$

Teil (ii) folgt direkt aus (i) $\square$

Definition der primitiven Polynome

Definition (13.4)

Sei R ein faktorieller Ring und $f = \sum_{k=0}^{n} a_k x^k \in R[x]$. Wir nennen das Polynom f primitiv, wenn $f \neq 0$ ist und die Koeffizienten $a_0, ..., a_n$ keinen gemeinsamen Primteiler besitzen.

Beispiele für primitive Polynome

(i) Normierte Polynome in $R[x]$ sind primitiv.

(ii) Das Polynom $2x^2 + 4x + 6$ ist nicht primitiv, denn es gilt $\mathrm{ggT}(2, 4, 6) = 2$.

(iii) Ist R ein Integritiätsbereich und $f \in R[x]$ ein irreduzibles Element vom Grad ≥ 1, dann ist f primitiv.

Polynome als Vielfache von primitiven Polynomen

Lemma (13.3)

Sei R ein faktorieller Ring und K sein Quotientenkörper. Sind $a_1, ..., a_n \in K^\times$ beliebig vorgegeben, dann gibt ein $\alpha \in K^\times$, so dass die Elemente $a_i' = \alpha a_i$ in R liegen und $\mathrm{ggT}(a_1', ..., a_n') = 1$ gilt.

Folgerung (13.5)

Sei R ein faktorieller Ring, K sein Quotientenkörper und $f \in K[x]$ ein Polynom mit $f \neq 0$. Dann gibt es ein $\alpha \in K^\times$, so dass αf in $R[x]$ liegt und primitiv ist.

Beweis des Gauß'schen Lemmas (Vorbereitungen)

Notation:
Sei R ein Integritätsbereich, $\mathfrak{p} \subseteq R$ ein Primideal, $\bar{R} = R/\mathfrak{p}$ und $\pi : R \to \bar{R}$ der kanonische Epimorphismus. Dann bezeichnet

$$\mathfrak{p}[x] \quad = \quad \mathfrak{p}R[x]$$

die Menge aller Polynome, deren Koeffizienten in $\mathfrak{p}$ enthalten sind.

Lemma (13.6)

Der Homomorphismus $\phi : R[x] \to \bar{R}[x]$ gegeben durch

$$\sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \pi(a_i) x_i$$

induziert einen Isomorphismus $R[x]/\mathfrak{p}[x] \cong \bar{R}[x]$ von Ringen.

Folgerung (13.7)

Das Ideal $\mathfrak{p}[x]$ ist ein Primideal in $R[x]$.

Beweis von Folgerung 13.7:

Lemma 13.6 $\Rightarrow$ $R[x]/\mathfrak{p}[x] \cong \bar{R}[x]$

$\mathfrak{p} \subseteq R$ ist ein Primideal $\Rightarrow$ $\bar{R} = R/\mathfrak{p}$

ist ein Integritätsbereich $\Rightarrow$ $\bar{R}[x]$

ist Integritätsbereich $\Rightarrow$ $R[x]/\mathfrak{p}[x]$ ist

ein Integritätsbereich $\Rightarrow$ $\mathfrak{p}[x]$ ist Prim-

ideal (in $R[x]$). $\square$

q^{n-k}

$(p,q)=1$

$\Rightarrow$

q^{n-k}

$\Rightarrow q \mid a_n$

$\square$

Das Gauß'sche Lemma

Satz (13.8)

Sei R ein faktorieller Ring, und seien $f, g \in R[x]$ primitive Polynome. Dann ist auch fg primitiv.

Dieser Satz ist unter dem Namen „Lemma von Gauß“ bekannt.

Satz (13.9)

Sei R ein faktorieller Ring, K sein Quotientenkörper und $f \in R[x]$ ein Polynom mit $\mathrm{grad}(f) \geq 1$.

(i) Ist $g \in R[x]$ ein primitives Polynom mit der Eigenschaft, dass g ein Teiler von f in $K[x]$ ist, so ist g bereits ein Teiler von f in $R[x]$.

(ii) Ist f irreduzibel in $R[x]$, dann auch in $K[x]$.

Beweis von Satz 13.8:

geg: R faktorieller Ring

$f, g \in R[x]$ primitive Polynome

Ang. fg ist nicht primitiv $\Rightarrow \exists$ Primelement $p \in R$ mit $p \mid (fg) \Rightarrow \mathfrak{p} = (p)$ ist Primideal in $R \overset{(13.7)}{\Longrightarrow} \mathfrak{p}[x]$ ist Primideal in $R[x]$

$p \mid (fg) \Longrightarrow fg \in \mathfrak{p}[x] \underset{\text{Primideal}}{\overset{\mathfrak{p}[x]}{\Longrightarrow}} f \in \mathfrak{p}[x]$ oder $g \in \mathfrak{p}[x] \Rightarrow p \mid f$ oder $p \mid g$

↯ da f, g beide primitiv. $\square$

Anwendungsbeispiel zu Satz 13.9:

$x^4 + 1$ ist in $\mathbb{Q}[x]$ irreduzibel

- Satz 13.9 $\Rightarrow$ genügt z.zg., dass $f = x^4 + 1$ in $\mathbb{Z}[x]$ irreduzibel ist
- Sei $f = gh \in \mathbb{Z}[x]$ mit $g, h \in \mathbb{Z}[x]$.
  z.zg.: $g \in (\mathbb{Z}[x])^\times$ oder $h \in (\mathbb{Z}[x])^\times$, wobei $(\mathbb{Z}[x])^\times = \{\pm 1\}$ ist

1. Fall: $\operatorname{grad}(g) = 0$ oder $\operatorname{grad}(h) = 0$

f normiert $\Rightarrow g \in \{\pm 1\}$ oder $h \in \{\pm 1\}$

2. Fall: $\operatorname{grad}(g) = 1$ oder $\operatorname{grad}(h) = 1$

Dann hätte f in $\mathbb{Q}$ eine Nullst. f normiert $\Rightarrow$

g

An

ele

Prim

$p \mid$

oder

$\lightning$ d

Die Nullstelle liegt in $\mathbb{Z}$ und ist ein Teiler von 1.

aber: $f(1) \neq 0$, $f(-1) \neq 0$ $\lightning$

3. Fall: $\operatorname{grad}(g) = \operatorname{grad}(h) = 2$

f normiert $\Rightarrow$ g, h haben Leitkoeff. in $\{\pm 1\}$

o.B.d.A. g, h beide normiert

Außerdem muss das Produkt der konstanten Terme von g und h gleich 1 sein $\Rightarrow \exists\, a, b \in \mathbb{Z}$ mit

$g = x^2 + ax + 1$ und $h = x^2 + bx + 1$ oder

$g = x^2 + ax - 1$ und $h = x^2 + bx - 1$

$\Rightarrow gh \in \{x^4 + (a+b)x^3 + (ab \pm 2)x^2 - (a+b)x + 1$

Vergleich mit $f = x^4 + 1 \Rightarrow a + b = 0 \Rightarrow b = -a$

Wegen $ab \pm 2 = 0$ folgt $-a^2 + 2 = 0$ bzw. $-(a^2+2) = 0$

↯ da ± 2 keine Quadrate in $\mathbb{Z}$ sind. $\square$

Beweis von Satz 13.9

geg. faktorieller Ring R, Quotientenkörper K
$f, g \in R[x]$

zu ii) Vor.: $g \mid f$ in $K[x]$ und g primitiv
z.zg.: $g \mid f$ in $R[x]$

Vor. $\Rightarrow \exists \tilde{h} \in K[x]$ mit $f = g\tilde{h}$ s.o. $\Rightarrow \exists \alpha \in K^*$,
so dass $h = \alpha\tilde{h}$ in $R[x]$ und primitiv ist.
Schreibe $\alpha = \frac{a}{b}$ mit $a, b \in R$, $b \neq 0$ und $ggT(a, b) = 1$
$f = g\tilde{h} = g(\alpha^{-1}h) \Rightarrow \alpha f = gh \Rightarrow \frac{a}{b} f = gh$
$\Rightarrow af = bgh$ Nach dem Gauß'schen Lemma ist

gh ein primitives Polynom. Daraus folgt $a \in R^\times$, denn:
Ang. a besitzt ein Primteiler p $\Rightarrow p \mid (af) \Rightarrow p \mid (bgh)$
$\overset{ggT(a,b)=1}{\Longrightarrow}$ $p \mid (gh)$ $\lightning$ zu gh primitiv.
also: $f = a^{-1} b g h = g(a^{-1} b h)$, $a^{-1} b h \in R[x] \Rightarrow g$ teilt f im Ring $R[x]$

zu (ii) Vor: f ist irred. in $R[x]$ z.zg: f ist irred. in $K[x]$
Sei $f = gh$ mit $g, h \in K[x]$. z.zg: $g \in (K[x])^\times$ oder $h \in (K[x])^\times$
(wobei $(K[x])^\times = K^\times$) Sei $\alpha \in K^\times$ so gewählt, dass $\tilde{g} = \alpha g$ in $R[x]$ liegt und primitiv ist $\Rightarrow f = \tilde{g}(\alpha^{-1} h)$
$\Rightarrow \tilde{g}$ ist Teiler von f in $K[x]$ $\xrightarrow[\text{Teil (i)}]{\tilde{g} \text{ ist prim.}}$ $\tilde{g}$ teilt f in $R[x]$
$\Rightarrow \exists \tilde{h} \in R[x]$ mit $f = \tilde{g}\tilde{h}$ $\xrightarrow[\text{in } R[x]]{f \text{ irred.}}$ $\tilde{g}$ oder $\tilde{h}$ liegt in

$(R[x])^\times = R^\times \quad \tilde{g}\tilde{h} = f = \tilde{g}(\alpha^{-1}h) \Rightarrow$

$\tilde{h} = \alpha^{-1}h$, außerdem $\tilde{g} = \alpha g \Rightarrow g$ oder h liegt in $K^\times$ $\square$

Polynomringe über faktoriellen Ringen

Satz (13.10)

Ist R ein faktorieller Ring, dann ist auch $R[x]$ faktoriell.

Das Eisenstein-Kriterium

Satz (13.11)

Sei R ein faktorieller Ring, $p \in R$ ein Primelement und $f \in R[x]$ ein primitives Polynom vom Grad $n > 0$. Es sei $f = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ mit $a_0, ..., a_n \in R$, und wir setzen voraus, dass die Koeffizienten von f folgende Bedingungen erfüllen.

(i) $p | a_i$ für $0 \leq i < n$

(ii) $p \nmid a_n$

(iii) $p^2 \nmid a_0$

Dann ist f in $R[x]$ irreduzibel.

Anwendungsbeispiel für das Eisenstein-Krit.

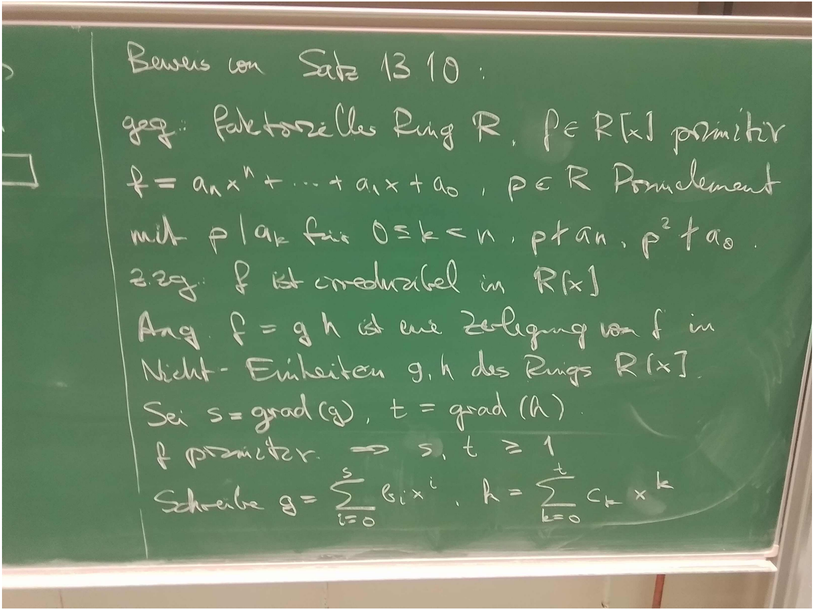
$f = x^2 + 2x + 6$ ist irreduzibel in $\mathbb{Z}[x]$ (und nach Satz 13.9 damit auch in $\mathbb{Q}[x]$), denn:

Setze $a_0 = 6$, $a_1 = 2$, $a_2 = 1$ und $p = 2$.

Es gilt $p \mid a_0$, $p \mid a_1$, $p \nmid a_2$ und $p^2 \nmid a_0$.

Also ist f in $\mathbb{Z}[x]$ irred. nach dem Eisenstein-Kriterium

Korrektur: Beweis von Satz 13.11



$a_0 = b_0 c_0$, $p^2 \nmid a_0$, $p \mid a_0 \Rightarrow$ o.B.d.A.
$p \mid b_0$ und $p \nmid c_0$. $a_n = b_s c_t$, $p \nmid a_n$
$\Rightarrow p \nmid b_s$. Sei $u \in \{1, \dots, n-1\}$ minimal gewählt,
so dass $p \nmid b_u$. Es gilt $a_u = \sum_{k=0}^{u} b_{u-k} c_k$

$u < n \Rightarrow p \mid a_u$, außerdem $p \mid b_{u-k} c_k$ für $1 \leq k < u-1$
(wegen $p \mid b_{u-k}$ für diese k) $\Rightarrow p \mid b_u c_0$
$\lightning$, da $p \nmid c_0$ und $p \nmid b_u$. $\square$