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.

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 $\operatorname{grad}(f) \geq 1$.

(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 $K[x]$.

Beispiel zu Prop. 13.9, Teil (iii):

- Nachweis der Irreduzibilität von $f = x^4 + 1$ in $\mathbb{Q}[x]$

Auf Grund der Prop. genügt es zu zeigen, dass f in $\mathbb{Z}[x]$ irreduzibel ist. Seien also $g, h \in \mathbb{Z}[x]$ mit $f = gh$. zzg: Eins der Polynome g, h liegt in $(\mathbb{Z}[x])^\times = \mathbb{Z}^\times = \{\pm 1\}$.

Ang.: g und h sind beide keine Einheiten.

1. Fall: Einer der Faktoren (o.B.d.A.) g ist vom Grad 0.

$g \notin \{\pm 1\}$, $g \in \mathbb{Z} \Rightarrow g$ hat einen Primfaktor p.

$f = g\,h \Rightarrow p \mid f \Rightarrow p$ teilt alle Koeff. von f $\lightning$ da f normiert

2. Fall: Faktor vom Grad 1, $\exists$ grad $g = 1$

Dann hätte g und somit auch f in $\mathbb{Q}$ eine Nullstelle $\lightning$

da $f(r) \geq 1 \quad \forall r \in \mathbb{Q}$.

3. Fall: $\text{grad}(g) = \text{grad}(h) = 2$ f normiert $\Rightarrow$ Leitkoeff. von g und h beide 1 oder beide -1 $\Rightarrow$ Nach evtl. Ersetzung von g durch $-g$, h durch $-h$ können wir annehmen, dass g und h beide normiert sind. außerdem: konstanter Term von f ist 1 $\Rightarrow$ konstante Terme von g und h sind beide 1 oder beide -1 damit insgesamt:

Es gibt $a, b \in \mathbb{Z}$ mit $x^4 + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$

oder $x^4 + 1 = (x^2 + ax - 1)(x^2 + bx - 1)$

$\Rightarrow x^4 + 1 = x^4 + (a+b)x^3 + (ab+2)x^2 + (a+b)x + 1$ oder

$x^4+1 = x^4 + (a+b)x^3 + (ab-2)x^2 + (-a-b)x + 1$

$a+b=0 \Rightarrow b=-a$

$x^4+1 = x^4 + (2-a^2)x^2 + 1$

oder $x^4+1 = x^4 + (2+a^2)x^2 + 1 \Rightarrow$

$2-a^2=0$ oder $2+a^2=0$ $\nexists$ da ± 2 keine Quadrate in $\mathbb{Z}$ sind. $\square$

Beweis von Proposition 13.9

geg.: R faktoriell, K Quot.-kop.
$f, g \in R[x]$, $\operatorname{grad}(f) \geq 1$

zu (i) Vor.: $g \mid f$ in $K[x]$, g primitiv
zzg: $g \mid f$ in $R[x]$

Vor. $\Rightarrow \exists h \in K[x]$ mit $f = gh$

bekannt: Es gibt ein $\alpha \in K^\times$, so dass $\tilde{h} = \alpha h$ in $R[x]$ liegt und primitiv ist. Schreibe $\alpha = \frac{a}{b}$ mit $a, b \in R$, a, b teilerfremd

$\tilde{h} = \alpha h \Rightarrow h = \alpha^{-1} \tilde{h} \Rightarrow f = \alpha^{-1} g \tilde{h}$

$= \frac{b}{a} g \tilde{h} \Rightarrow af = b \cdot g \tilde{h}$

$x+1$

$\Rightarrow$

teilen

$\square$

Ang., a besitzt einen Primteiler $p \in R$.

$p \mid af \Rightarrow p \mid bg\tilde{h} \overset{a,b \text{ teilerfremd}}{\Rightarrow} p \mid g\tilde{h} \Rightarrow$

$g\tilde{h}$ ist nicht primitiv. aber: $g, \tilde{h}$ sind primitiv $\overset{\text{Lemma von Gauß}}{\Rightarrow} g\tilde{h}$ primitiv $\lightning$

Also ist $a \in R^\times \Rightarrow a^{-1} \in R \Rightarrow h = a^{-1}\tilde{h} \in R[x]$

Wegen $f = gh$ ist g also Teiler von f in $R[x]$.

zu ii) Vor.: f ist irreduzibel in $R[x]$

zzg.: f ist irreduzibel in $K[x]$

Ang., f ist in $K[x]$ reduzibel $\Rightarrow \exists\, g, h \in K[x]$, beide nicht konstant, mit $f = gh$.

Sei $\alpha \in K^\times$ so gewählt, dass $\tilde{g} = \alpha g$ in $R[x]$ liegt und primitiv ist $\Rightarrow f = \tilde{g}\tilde{h}$ mit $\tilde{h} = \alpha^{-1} h$

also: $\tilde{g}$ primitiv und Teiler von f in $K[x]$ $\xRightarrow{(1)}$

$\tilde{g}$ ist Teiler von f in $R[x] \Rightarrow \exists h_1 \in R[x]$ mit

$f = \tilde{g} h_1 \Rightarrow \tilde{g}\tilde{h} = f = \tilde{g} h_1 \overset{\text{Kürzungs-regel}}{\Rightarrow} \tilde{h} = h_1 \in R[x]$

$f = \tilde{g}\tilde{h}$, f irred. in $R[x] \Rightarrow \tilde{g} \in R^\times$ oder $\tilde{h} \in R^\times$

$\tilde{h} = \alpha h \Rightarrow g \in K^\times$ oder $h \in K^\times$. $\lightning$ zur Vor. $\square$

Polynomringe über faktoriellen Ringen

Satz (13.10)

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

Beweis von Satz 13.10 (m. die Eindeutigkeit der Zerlegung in irreduzible Faktoren):

Ang., $f \in R[x]$ mit $f \notin R^\times \cup \{0\}$ hat die beiden Zerlegungen $g_1 \cdot \ldots \cdot g_r = h_1 \cdot \ldots \cdot h_s$, (*)
g_i, h_j irreduzibel in $R[x]$ $\forall i, j$.
Sei $c \in R$ das Produkt der konstanten g_i, $g \in R[x]$ das Produkt der restlichen Faktoren. Definiere $d \in R$ und $h \in R[x]$ analog. $cg = f = dh$
Die nicht-konstanten g_i, h_j sind irreduzibel somit primitiv. Lemma von Gauß $\Rightarrow$ g, h primitiv $\Rightarrow$

c ist ggT der Koeff von f, ebenso d $\Rightarrow c \sim d$, $\exists\, c = d$

$\rightarrow$ können c, d aus der Gleichung kürzen und annehmen, daß alle g_i, h_j nicht-konstant sind (**)

Betrachte (*) in $K[x]$, wobei K Quot.körp. von R

$K[x]$ ist Hauptidealring, also faktoriell $\Rightarrow r = s$, nach Umnummerierung $g_i \sim h_i$ in $K[x]$ für $1 \le i \le r$.

Prop. 13.9 ii) $\Rightarrow g_i \sim h_i$ in $R[x]$ □

Da R faktoriell ist, ist die Zerlegung von $c = d$ in R (**) evidenterweise bis auf Einheiten und Reihenfolge.

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 $f = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ mit $a_0, \ldots, a_n \in R$, 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.

Anwendungsbeispiele für das Eisenstein-Kriterium:

- $x^2 - 5$ ist irreduzibel in $\mathbb{Z}[x]$ ($a_0 = -5$, $a_1 = 0$, $a_2 = 1$
  $\Rightarrow$ Kriterium ist erfüllt für $p = 5$)
- $x^3 + 2x + 6$ ist irred. in $\mathbb{Z}[x]$ ($a_0 = 6$, $a_1 = 2$, $a_2 = 0$, $a_3 = 1$
  $\Rightarrow$ Kriterium ist erfüllt für $p = 2$)

Beweis des Eisenstein-Kriteriums: geg. R faktoriell, $f \in R[x]$ primitiv, $f = a_n x^n + \dots + a_1 x + a_0$, $p \in R$ prim mit $p \mid a_k$ für $0 \le k < n$, $p \nmid a_n$, $p^2 \nmid a_0$.
Ang., $f = gh$ ist eine Zerlegung in $R[x]$ in Nicht-Einh.
f primitiv $\rightarrow$ g, h nicht konstant Schreibe

$g = \sum_{i=0}^{r} b_i x^i$, $h = \sum_{j=0}^{s} c_j x^j$ $(r+s = n)$ mit $b_i, c_j \in R$.

$a_0 = b_0 c_0$, $p \mid a_0$, $p^2 \nmid a_0 \Rightarrow$ o.B.d.A. $p \mid b_0$, $p \nmid c_0$

Für $0 \le k \le n$ gilt $a_k = \sum_{j=0}^{k} b_{k-j} c_j$

Es gilt $p \nmid b_r$, da sonst p Teiler $a_n = b_r c_s$ wäre.

Sei $u \in \{1, \dots, r\}$ minimal mit $p \nmid b_u$.

$a_u = \sum_{j=0}^{u} b_{u-j} c_j = \underbrace{b_u c_0}_{\text{nicht durch } p \text{ teilbar}} + \underbrace{\sum_{j=1}^{u} b_{u-j} c_j}_{\text{teilbar durch } p} \Rightarrow p \nmid a_u$

$\Rightarrow u = n \Rightarrow \operatorname{grad} g = r = n = \operatorname{grad}(f)$ $f = gh \Rightarrow$

h ist konstant ↯ □

Das Reduktionskriterium

Satz (13.12)

Sei R ein faktorieller Ring, $p \in R$ ein Primelement und $\bar{R} = R/(p)$. Es sei $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ ein primitives Polynom mit $a_n \notin (p)$ und $\bar{f}$ das Bild von f in $\bar{R}[x]$. Ist $\bar{f}$ in $\bar{R}[x]$ irreduzibel, dann auch das Polynom f in $R[x]$.

Erinnerung: Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$.
$a \equiv b \bmod n$ bedeutet: $n \mid (b - a)$

Proposition (14.1)

Seien $m, n \in \mathbb{N}$, außerdem $a, b, c, d \in \mathbb{Z}$ und p eine Primzahl.

(i) Aus $a \equiv c \mod n$ und $b \equiv d \mod n$ folgt
$a + b \equiv c + d \mod n$ und $ab \equiv cd \mod n$.

(ii) Gilt $a \equiv b \mod n$ und ist m ein Teiler von n,
dann folgt $a \equiv b \mod m$.

(iii) Es gilt $a \equiv b \mod n$ genau dann, wenn $ma \equiv mb \mod mn$ erfüllt ist.

(iv) Es gilt $a^p \equiv a \mod p$. Unter der zusätzlichen Voraussetzung $p \nmid a$ gilt darüber hinaus $a^p \equiv 1 \mod p$.

Die Aussage (iv) ist auch als Kleiner Satz von Fermat bekannt.

Beweis von Prop. 14.1 nur (iii), (iv)

zu (iii) geg. $a, b \in \mathbb{Z}$, $m, n \in \mathbb{N}$

Beh: $a \equiv b \bmod n \iff ma \equiv mb \bmod mn$

$ma \equiv mb \bmod mn \iff mn \mid (mb - ma) \iff$

$\exists r \in \mathbb{Z}$ mit $mb - ma = r\,mn \iff$

$\exists r \in \mathbb{Z}$ mit $b - a = r\,n \iff n \mid b - a$

$\iff a \equiv b \bmod n$

zu (iv) geg: ~~Primzahl~~ p, $a \in \mathbb{Z}$ zeige:

(1) $p \nmid a \Rightarrow a^{p-1} \equiv 1 \bmod p$

zu (iv) geg. Primzahl p, $a \in \mathbb{Z}$ beliebig.

(2) $a^p \equiv a \bmod p$

zu (1) Erinnerung: Für alle $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$ ist die Kongruenz $a \equiv b \bmod n$ gleichbedeutend mit der Gleichung $\bar{a} = \bar{b}$ in $\mathbb{Z}/n\mathbb{Z}$, wobei $\bar{a} = a + n\mathbb{Z}$ und $\bar{b} = b + n\mathbb{Z}$.

Sei $\bar{a} = a + p\mathbb{Z}$. $p \nmid a \Rightarrow \bar{a} \neq \bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$

$\Rightarrow \bar{a} \in \mathbb{F}_p^\times$ $\mathbb{F}_p^\times$ ist Gruppe der Ordnung $p-1$

$\Rightarrow \bar{a}^{p-1} = \bar{1} \Rightarrow a^{p-1} \equiv 1 \bmod p$

zu (2) 1. Fall: $p \nmid a \xRightarrow{(1)} a^{p-1} \equiv 1 \bmod p \xRightarrow{ii)} a^{p-1} \cdot a \equiv$

$1 \cdot a \bmod p \Rightarrow a^p \equiv a \bmod p$

2. Fall: $p \mid a \Rightarrow a \equiv 0 \bmod p \Rightarrow a^p \equiv 0^p \equiv 0 \equiv a \bmod p$ □