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.

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 $R[x]$.

Anwendungsbeispiel zu Satz 13.12 (Reduktionskriterium)

Beh.: $f = x^3 + x + 1 \in \mathbb{Z}[x]$ ist irreduzibel (in $\mathbb{Z}[x]$)

Sei $\bar{f}$ das Bild von f in $\mathbb{F}_2[x]$. $\bar{f} = x^3 + x + \bar{1}$

Das Polynom $\bar{f}$ ist irreduzibel, da $\operatorname{grad}(\bar{f}) = 3$ ist und $\bar{f}$ in $\mathbb{F}_2$ keine Nullstellen hat ($\bar{f}(\bar{0}) = \bar{1} \neq \bar{0}$, $\bar{f}(\bar{1}) = \bar{3} = \bar{1} \neq \bar{0}$). außerdem: f ist primitiv und der Leitkoeff. von f (die 1) liegt nicht in (2)

Red.-kriterium $\Rightarrow$ f ist irreduzibel und $\bar{f}$ in $\mathbb{F}_2$ keine Nullstellen hat ($\bar{f}(\bar{0}) = \bar{1} \neq \bar{0}$, $\bar{f}(\bar{1}) = \bar{3} = \bar{1} \neq \bar{0}$). außerdem: f ist primitiv

Achtung: Die Umkehrung des Red.-kriteriums ist im Allgemeinen falsch, d.h. $\bar{f}$ reduzibel $\not\Rightarrow$ f reduzibel

Bsp.: $g = x^4 + 1 \in \mathbb{Z}[x]$, $\bar{g} = x^4 + \bar{1} \in \mathbb{F}_2[x]$

letzte Stunde gezeigt: g ist irreduzibel, aber $\bar{g}$ ist reduzibel, denn $\bar{g} = (x^2 + \bar{1})^2$

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 $a^{p-1} \equiv 1 \mod p$.

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

Beweis von Satz 14.1, Teil (iv)

geg.: Primzahl p, $a \in \mathbb{Z}$, zeige:

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

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

Betrachte das Bild $\bar{a} = a + p\mathbb{Z} \in \mathbb{F}_p$.

<u>zu (1)</u> $p \nmid a \Rightarrow \bar{a} \neq \bar{0} \Rightarrow \bar{a} \in \mathbb{F}_p^\times$

Es ist $\mathbb{F}_p^\times$ eine Gruppe der Ordnung $p-1$.

Gruppentheorie $\Rightarrow \bar{a}^{p-1} = \bar{1} \Rightarrow$
$a^{p-1} \equiv 1 \mod p$.

<u>zu (2)</u> 1. Fall: $p \nmid a \overset{(1)}{\Longrightarrow} a^{p-1} \equiv 1 \mod p$

$\Rightarrow a^{p-1} \cdot a \equiv 1 \cdot a \mod p \Rightarrow a^p \equiv a \mod p$

2. Fall: $p \mid a \Rightarrow a \equiv 0 \mod p$.

$p \mid a^p \Rightarrow a^p \equiv 0 \mod p \Rightarrow a^p \equiv a \mod p$ $\square$

Teilerfremdheit von Idealen

Definition (14.2)

Sei R ein Ring. Zwei Ideale I, J in R werden teilerfremd genannt, wenn $I + J = (1)$ gilt, wobei (1) wie üblich das Einheitsideal in R bezeichnet.

Lemma (14.3)

Sei $R = \mathbb{Z}$, und seien $m, n \in \mathbb{N}$. Genau dann sind die Ideale $I = (m)$ und $J = (n)$ teilerfremd, wenn m, n als natürliche Zahlen teilerfremd sind.

Beweis von Lemma 14.3

Seien $m, n \in \mathbb{N}$.

Beh.: m, n teilerfremd $\Longleftrightarrow$ $(m), (n)$ teilerfremd (als Ideale in $\mathbb{Z}$)

„$\Longleftarrow$" Vor. $\Longrightarrow (m)+(n) = (1) \Longrightarrow 1 \in (m)+(n) \Longrightarrow \exists\, k, l \in \mathbb{Z}$ mit $1 = km + ln$

Sei $d \in \mathbb{N}$ ein gem. Teiler von m und n.

z.zg.: $d = 1$ $\quad d \mid m$ und $d \mid n \Rightarrow d \mid km$ und $d \mid ln \Longrightarrow d \mid (km + ln) \Longrightarrow d \mid 1 \Longrightarrow d = 1$

„$\Longrightarrow$" Vor.: $\mathrm{ggT}(m, n) = 1$ Lemma von Bézout $\Longrightarrow$
$\exists\, k, l \in \mathbb{Z}: km + ln = 1 \Longrightarrow 1 \in (m)+(n) \Longrightarrow (m)+(n) = (1)$ $\square$

Beweis des Chinesischen Restsatzes - Vorbereitungen

Lemma (14.4)

Sei R ein Ring, und seien $I_1, ..., I_m, J$ Ideale in R, wobei $I_1, ..., I_m$ jeweils teilerfremd zu J sind. Dann ist auch das Produkt $I_1 \cdot ... \cdot I_m$ teilerfremd zu J.

Lemma (14.5)

Sei R ein Ring, und seien $I_1, ..., I_m$ Ideale in R, die paarweise teilerfremd sind. Dann gilt

$$I_1 \cdot ... \cdot I_m = I_1 \cap ... \cap I_m.$$

Beweis von Lemma 14.4

$\square$

Wir zeigen die Aussage nur für $m = 2$. Die allgemeine Aussage erhält man daraus durch vollst. Ind.

geg.: Ring R, I_1, I_2, J Ideale
I_1, I_2 sind beide teilerfremd zu J

z.zg.: $I_1 I_2 + J = (1)$

$$(1) = (1)(1) = (I_1 + J) \cdot (I_2 + J) =$$
$$I_1 I_2 + J I_1 + J I_2 + J^2 \subseteq I_1 I_2 + J(I_1 + I_2 + J)$$
$$\subseteq I_1 I_2 + J \implies (1) = I_1 I_2 + J$$

$\square$

Beweis von Lemma 14.5:

Wir beschränken uns auf den Fall $n = 2$.

Sei R ein Ring, und seien I_1, I_2 teilerfremde Ideale in R.

Beh.: $I_1 \cdot I_2 = I_1 \cap I_2$

„$\subseteq$" Bekanntlich gilt $I_1 I_2 \subseteq I_1$ und $I_1 I_2 \subseteq I_2$

$\Rightarrow I_1 I_2 \subseteq I_1 \cap I_2$.

„$\supseteq$" $I_1 + I_2 = (1) \Rightarrow 1 \in I_1 + I_2 \Rightarrow \exists\, a_1 \in I_1,\ a_2 \in I_2$ mit $1 = a_1 + a_2$. Sei nun $r \in I_1 \cap I_2 \Rightarrow r =$

$r \cdot 1 = r(a_1 + a_2) = \underbrace{ra_1}_{\in I_1 \cdot I_2} + \underbrace{ra_2}_{\in I_1 I_2} \in I_1 I_2$ $\square$

Der Chinesische Restsatz

Satz (14.6)

Sei R ein Ring, $I_1, ..., I_m$ paarweise teilerfremde Ideale in R und $I = I_1 \cdot ... \cdot I_m$. Dann gibt es einen Isomorphismus von Ringen

$$\bar{\phi} : R/I \longrightarrow (R/I_1) \times ... \times (R/I_m)$$

mit

$$\bar{\phi}(a + I) = (a + I_1, ..., a + I_m) \quad \text{für alle} \quad a \in R.$$

Anwendungsbeispiel zum Chin. Restsatz:

Es gibt einen Isom. $\overline{\Phi}: \mathbb{Z}/63\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$

mit $\overline{\Phi}(a + 63\mathbb{Z}) = (a + 7\mathbb{Z}, a + 9\mathbb{Z})$

Da $\overline{\Phi}$ insb. surjektiv ist, gibt es z. B. ein $a \in \mathbb{Z}$

mit $(a + 7\mathbb{Z}, a + 9\mathbb{Z}) = \overline{\Phi}(a + 63\mathbb{Z}) = (2 + 7\mathbb{Z}, 5 + 9\mathbb{Z})$

(nämlich $a = 23$)

Beweis des Chinesischen Restsatzes

gg: Ring R, $m \in \mathbb{N}$ mit $m \geq 2$, $I_1, \dots, I_m$ paarweise teilerfremde Ideale, $I = I_1 \cdot \ldots \cdot I_m$

zzg: Es gibt einen Isom. von Ringen

$$\Phi : R/I \to R/I_1 \times \ldots \times R/I_m \text{ mit}$$
$$\Phi(a+I) = (a+I_1, \dots, a+I_m) \quad \forall a \in R.$$

Betrachte die Abbildung $\phi : R \to R/I_1 \times \ldots \times R/I_m$, $a \mapsto (a+I_1, \dots, a+I_m)$. Es ist leicht zu überprüfen, dass ϕ ein Ringhomomorphismus ist. Damit der Homomorphiesatz die gewünschte Aussage liefert, müssen wir noch zeigen

(1) $\ker(\phi) = I$ (2) ϕ ist surjektiv

zu (1) Sei $a \in R$. Dann gilt die Äquivalenz

$$a \in \ker(\phi) \iff \phi(a) = (0+I_1, \ldots, 0+I_m)$$

$$\iff (a+I_1, \ldots, a+I_m) = (0+I_1, \ldots, 0+I_m)$$

$$\iff \forall k \in \{1, \ldots, m\} : a+I_k = 0+I_k = I_k$$

$$\iff \forall k \in \{1, \ldots, m\} : a \in I_k$$

$$\iff a \in I_1 \cap \ldots \cap I_k \overset{\text{Lemma 14.5}}{\iff} a \in I_1 \cdot \ldots \cdot I_m$$

$$\iff a \in \underline{I}$$

zu (2) Beweis durch vollst. Induktion

Ind.-anf. $m=2$: Sei $(a_1+I_1, a_2+I_2) \in$
$R/I_1 \times R/I_2$. z.zg. $\exists a \in R$ mit

$(a+I_1, a+I_2) = \phi(a) = (a_1+I_1, a_2+I_2)$

$I_1+I_2 = (1) \Rightarrow 1 \in I_1+I_2 \Rightarrow \exists\, b_1 \in I_1,\ b_2 \in I_2$

mit $b_1 + b_2 = 1 \Rightarrow 1 - b_1 = b_2 \Rightarrow$

$\phi(b_2) = (b_2+I_1, b_2+I_2) = (1-b_1+I_1, b_2+I_2)$

$= (1+I_1, 0+I_2)$ genauso: $1-b_2 = b_1$

$\Rightarrow \phi(b_1) = (0+I_1, 1+I_2)$

Sei $a = a_1 b_2 + a_2 b_1 \Rightarrow \phi(a) = \phi(a_1)\phi(b_2) +$

$\phi(a_2)\phi(b_1) = (a_1+I_1, a_1+I_2)\cdot(1+I_1, 0+I_2) +$

$(a_2+I_1, a_2+I_2)\cdot(0+I_1, 1+I_2) = (a_1+I_1, 0+I_2) +$

$(0+I_1, a_2+I_2) = (a_1+I_1, a_2+I_2)$

Ind-Schritt $m \mapsto m+1$:

geg.: paarweise teilerfremde Ideale $I_1, \dots, I_{m+1}$

$a_1, \dots, a_{m+1} \in R$

zzg.: $\exists a \in R$ mit $\phi(a) = (a_1 + I_1, \dots, a_m + I_m, a_{m+1} + I_{m+1})$

Setze $J = I_1 \cdot \ldots \cdot I_m \overset{\text{Lemma 14.4}}{\Longrightarrow} J, I_{m+1}$ sind teilerfremd

Ind-V. $\Rightarrow \exists b \in R$ mit $(b + I_1, \dots, b + I_m) \overset{(**)}{=} (a_1 + I_1, \dots, a_m + I_m)$

Fall $m = 2$ $\Rightarrow \exists a \in R$ mit

$(a + J, a + I_{m+1}) = (b + J, a_{m+1} + I_{m+1})$ (*)

zu zeigen: $a + I_k = a_k + I_k$ für $1 \leq k \leq m+1$

Für $k = m+1$ folgt dies direkt aus (*). Sei nun $k \in \{1, \dots, m\}$. $b + I_k = a_k + I_k$ wegen (**) $\Rightarrow$

$b - a_k \in I_k$, außerdem (*) $\Rightarrow a + J = b + J$

Lösbarkeit von Kongruenzsystemen

Satz (14.7)

Seien $r \in \mathbb{N}$ mit $r \geq 2$, außerdem $n_1, ..., n_r \in \mathbb{N}$ paarweise teilerfremde natürliche Zahlen und $n = \prod_{j=1}^{r} n_j$. Seien $c_1, ..., c_r \in \mathbb{Z}$. Dann ist die Lösungsmenge $\mathcal{L} \subseteq \mathbb{Z}$ des Kongruenzsystems

$$x \equiv c_1 \bmod n_1 \quad , \quad x \equiv c_2 \bmod n_2 \quad , \quad ... \quad , \quad x \equiv c_r \bmod n_r$$

nicht leer. Ist $a \in \mathcal{L}$ beliebig gewählt, dann gilt $\mathcal{L} = a + n\mathbb{Z}$.

Anwendung von Satz 14.7 auf das Kongruenz-
system $x \equiv 2 \bmod 7$, $x \equiv 5 \bmod 9$ (*)

Sei $\Phi: \mathbb{Z}/63\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ der Isomorphismus aus
dem Chin. Restsatz s.o. $\Rightarrow (23+7\mathbb{Z}, 23+9\mathbb{Z}) = \Phi(23+63\mathbb{Z})$
$= (2+7\mathbb{Z}, 5+9\mathbb{Z})$ $\quad 23+7\mathbb{Z} = 2+7\mathbb{Z} \Rightarrow 23 \equiv 2 \bmod 7$
$23+9\mathbb{Z} = 5+9\mathbb{Z} \Rightarrow 23 \equiv 5 \bmod 9$

<u>also</u>: 23 ist Lösung von (*)

Aus Satz 14.7 folgt, dass $\mathcal{L} = 23+63\mathbb{Z}$ die gesamte
Lösungsmenge von (*) ist.