Definition der faktoriellen Ringe

Definition (12.19)

Ein faktorieller Ring ist ein Integritätsbereich R mit der Eigenschaft, dass jedes Element $r \in R$, das weder gleich Null noch eine Einheit ist, als Produkt von Primelementen dargestellt werden kann. Dies bedeutet:
Es gibt ein $n \in \mathbb{N}$ und Primelemente $p_1, ..., p_n \in R$, so dass

$$r = p_1 \cdot p_2 \cdot ... \cdot p_n \quad \text{gilt.}$$

Charakterisierung der faktoriellen Ringe

Satz (12.22)

Sei R ein Integritätsbereich. Dann sind äquivalent

(i) R ist ein faktorieller Ring.

(ii) Jedes Element $r \in R$, dass weder gleich Null noch eine Einheit ist, kann als Produkt von irreduziblen Elementen dargestellt werden, und diese Darstellung ist im Wesentlichen eindeutig. Dies bedeutet genau: Sind $m, n \in \mathbb{N}$ und $p_1 \cdot \ldots \cdot p_m = r = q_1 \cdot \ldots \cdot q_n$ zwei Darstellungen von r als Produkt irreduzibler Elemente p_i, q_j, dann ist $m = n$, und nach eventueller Umnummerierung der Elemente ist p_i assoziiert zu q_i für $1 \leq i \leq m$.

Hauptidealring $\Rightarrow$ faktorieller Ring

Satz (12.28)

Jeder Hauptidealring R ist faktoriell.

Ergänzungen:

- Der Polynomring $\mathbb{Z}[x]$ ist faktoriell (als Polynomring über einem faktoriellen Ring, siehe nächstes Kapitel), aber kein Hauptidealring, denn das Ideal $I = (2, x)$ in $\mathbb{Z}[x]$ ist kein Hauptideal.
- Es gibt Hauptidealringe, die keine euklidischen Ringe sind (zum Beispiel den Ring $\mathbb{Z}[\frac{1}{2}(1 + \sqrt{-19})]$, siehe Anhang).

Beweis von Satz 12.28:

geg.: ein Hauptidealring R, z.Zg:
R ist faktorieller Ring

- Nach Def. ist R ein Integritätsbereich.
- bereits bekannt: Die irreduziblen Elemente in R sind genau die Primelemente.
Es genügt somit zu zeigen, dass jedes Element aus $R \setminus (R^\times \cup \{0_R\})$ als Produkt von irreduziblen Elementen darstellbar ist.

Angenommen, $a \in R$ ist ein Element mit

$a \notin R^\times \cup \{0_R\}$, das keine solche Produktdarstellung besitzt.

Beh.: Es gibt in R eine Folge $(a_n)_{n \in \mathbb{N}}$ mit folgenden Eigenschaften:

(1) $a_n \notin R^\times \cup \{0_R\}$

(2) a_n hat keine Darstellung als Produkt irreduzibler Elemente

(3) $a_{n+1} \mid a_n$, aber nicht $a_n \mid a_{n+1}$

jeweils für alle $n \in \mathbb{N}$. Setze $a_1 = a$.

Dann sind (1) und (2) nach Def. von a erfüllt.

Ang., es ist $m \in \mathbb{N}$, und wir haben bereits Elemente $a_1, \dots, a_m$ definiert, so dass (1) und (2) für $n \leq m$ und (3) für $n < m$ erfüllt ist.

Wegen (2) ist a_m insb. nicht irreduzibel. $\Rightarrow$
$\exists b, c \in R$, beides keine Einheiten, mit $a_m = bc$.
Dann hat zumindest eines der Elemente b, c keine Darstellung als Produkt irred. Elemente (ansonsten könnte man für a eine solche Produktdarstellung zusammensetzen). O.B.d.A. sei das b. Setze $a_{m+1} = b$.
Es ist $a_{m+1} \notin R^\times$. Ang. $a_{m+1} = 0_R \Rightarrow a_m = a_{m+1} \cdot c$
$= 0_R \cdot c = 0_R$ ↯ also: a_{m+1} erfüllt (1), ebenso die Bed. (2) $a_m = a_{m+1} \cdot c \Rightarrow a_{m+1} \mid a_m$
Ang. $a_m \mid a_{m+1}$. $\Rightarrow a_m, a_{m+1}$ assoziiert $\Rightarrow \exists \varepsilon \in R^\times$
mit $a_m = \varepsilon a_{m+1} \Rightarrow c a_{m+1} = \varepsilon a_{m+1}$ $\overset{\text{Kürzungsregel}}{\Rightarrow}$
$c = \varepsilon \Rightarrow c \in R^\times$ ↯

Also ist Bed. (3) für $n \leq m+1$ erfüllt ($\Rightarrow$ Beh.)

Beh.: $\forall n \in \mathbb{N}: (a_n) \subsetneq (a_{n+1})$

denn: $a_{n+1} \mid a_n$ impliziert $(a_n) \subseteq (a_{n+1})$ (Satz 10.8)

Ang. $(a_{n+1}) \subseteq (a_n) \overset{(10.8)}{\Rightarrow} a_n \mid a_{n+1}$ ↯ ($\Rightarrow$ Beh.)

Beh.: $I = \bigcup_{n \in \mathbb{N}} (a_n)$ ist ein Ideal in R

$0_R \in (a_1) \Rightarrow 0_R \in I$ Seien nun $a, b \in I$ und $r \in R$ z.Zg.: $a+b \in I$ und $ra \in I$

$a, b \in I \Rightarrow \exists m, n \in \mathbb{N}$ mit $a \in (a_m)$, $b \in (a_n)$

o.Bd.A. $m \leq n \overset{\text{Beh. s.o.}}{\Rightarrow} (a_m) \subseteq (a_n) \Rightarrow a, b \in (a_n)$

Da (a_n) ein Ideal ist, folgt $a+b \in (a_n)$, $ra \in (a_n)$

$\overset{(a_n) \subseteq I}{\Rightarrow} a+b \in I$ und $ra \in I$ ($\Rightarrow$ Beh.)

Da R ein Hauptidealring ist, existiert ein $c \in I$ mit $I = (c)$. $\Rightarrow c \in (a_n)$ für ein $n \in \mathbb{N}$

$c \in (a_n) \Rightarrow I = (c) \subseteq (a_n) \Rightarrow (a_{n+1}) \subseteq I \subseteq (a_n) \Rightarrow$

$(a_n) = (a_{n+1})$ ↯

□

Beh: $I = (2, x)$ ist kein Hauptideal in $\mathbb{Z}[x]$

Ang I ist ein Hauptideal $\Rightarrow \exists f \in \mathbb{Z}[x]$ mit $I = (f)$

$(2, x) = (f) \Rightarrow 2 \in (f)$ und $x \in (f) \Rightarrow \exists g, h \in \mathbb{Z}[x]$

mit $2 = f \cdot g$, $x = f \cdot h \Rightarrow \operatorname{grad}(f) \leq \operatorname{grad}(2) = 0$

$\Rightarrow f \in \mathbb{Z}$ $\quad x = f h$, $f \in \mathbb{Z} \Rightarrow \operatorname{grad}(h) = 1 \Rightarrow \exists a, b \in \mathbb{Z}$

mit $h = ax + b$ einsetzen $\Rightarrow x = (ax + b) f = af x + bf$

$\Rightarrow b = 0$ oder $f = 0$, und außerdem $af = 1 \Rightarrow f \in \{\pm 1\}$

$\Rightarrow f \in \mathbb{Z}^\times \Rightarrow f \in \mathbb{Z}[x]^\times \Rightarrow I = (f)$ ist das Einheitsideal $\Rightarrow 1 \in I \Rightarrow 1 \in (2, x) \Rightarrow \exists u, v \in \mathbb{Z}[x]$

mit $1 = 2u + vx$ ↯ da der konstante Term des Polynoms $2u + vx$ gleich $2u$, also eine gerade ganze Zahl ist □

Proposition (13.1)

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

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

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

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

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 $\mathbb{Q}[x]$.

Beweis von Satz 13.2

klar: Teil (ii) folgt aus (i)

zu (i) Vor.: R faktorieller Ring, K Quotientenkörper

$f = \sum_{k=0}^{n} a_k x^k \in R[x]$, $x = \frac{p}{q}$ Nullstelle von f (mit $p, q \in R$, $q \neq 0_R$ und p, q teilerfremd) z.Z.: $p \mid a_0$, $q \mid a_n$

$$f\left(\frac{p}{q}\right) = 0_R \Rightarrow \sum_{k=0}^{n} a_k \left(\frac{p}{q}\right)^k = 0_R \Rightarrow \sum_{k=0}^{n} a_k p^k q^{n-k} = 0_R$$

$$\Rightarrow a_0 q^n = \sum_{k=1}^{n} (-a_k) p^k q^{n-k} = p\left(\sum_{k=1}^{n} (-a_k) p^{k-1} q^{n-k}\right) \Rightarrow$$

$p \mid a_0 q^n \overset{p,q \text{ teilerfremd}}{\Longrightarrow} p \mid a_0$ $\quad a_n p^n = \sum_{k=0}^{n-1} (-a_k) p^k q^{n-k} =$

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

p, q teilerfremd $\Rightarrow q \mid a_n$. $\square$

wobei

Beh.

dem

überp

zu (1)

Beh: $f = x^3 - x + 2$ ist irreduzibel in $\mathbb{Q}$

Ang. f ist reduzibel. $\operatorname{grad}(f) = 3 \overset{\text{Prop 13.1 (ii)}}{\Rightarrow}$ f hat in $\mathbb{Q}$ eine Nullstelle r $f \in \mathbb{Z}[x]$ und ist normiert $\Rightarrow$ Satz 13.2 (ii) $\Rightarrow r \in \mathbb{Z}$ und $r \mid 2 \Rightarrow r \in \{\pm 1, \pm 2\}$

aber: $f(1) = 2 \neq 0$, $f(-1) = 2 \neq 0$, $f(2) = 8 \neq 0$

und $f(-2) = -4 \neq 0$ $\lightning$ $\Rightarrow$ f ist irreduzibel

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.

Primideale in Polynomringen

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 Lemma 13.6:

geg: R Int. bereich, $\mathfrak{p} \subseteq R$ Primideal,

$\bar{R} = R/\mathfrak{p}$, $\phi : R[x] \to \bar{R}[x]$

$$\sum_{k=0}^{n} a_k x^k \mapsto \sum_{k=0}^{n} \pi(a_k) x^k$$

wobei $\pi : R \to \bar{R}$, $a \mapsto a + \mathfrak{p}$ (kan. Epimorphismus)

Beh.: $R[x]/\mathfrak{p}[x] \cong \bar{R}[x]$ Dies folgt aus dem Homomorphiesatz für Ringe, sobald wir überprüft haben: (1) Der Hom. ϕ ist surjektiv.

(2) $\ker(\phi) = \mathfrak{p}[x]$

zu (1) Sei $\bar{f} \in \bar{R}[x]$, $\bar{f} = \sum_{k=0}^{n} \bar{a}_k x^k$

mit $n \in \mathbb{N}_0$, $\bar{a}_0, \dots, \bar{a}_n \in \bar{R}$. π ist surjektiv

$\Rightarrow \exists\, a_k \in R$ mit $\pi(a_k) = \bar{a}_k$, für $0 \leq k \leq n$

Sei $f = \sum_{k=0}^{n} a_k x^k$. Dann gilt $\phi(f) = \bar{f}$.

zu (2) Sei $f = \sum_{k=0}^{n} a_k x^k$ $(n \in \mathbb{N}_0, a_0, \dots, a_n \in R)$.

Dann gilt die Äquivalenz $f \in \ker(\phi) \iff$

$\phi(f) = 0_{\bar{R}} \iff \sum_{k=0}^{n} \pi(a_k) x^k = 0_{\bar{R}} \iff$

$\pi(a_k) = \bar{0}$ für $0 \leq k \leq n \iff a_k \in \mathfrak{p}$ für $0 \leq k \leq n$

$\Rightarrow f \in \mathfrak{p}[x]$

□

Beweis von Folgerung 13.7:

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

$\mathfrak{p}$ ist R-mideal in $R \Rightarrow \bar{R} = R/\mathfrak{p}$ ist Integritätsbereich $\overset{\S 12}{\Rightarrow} \bar{R}[x]$ ist Integritätsbereich

$\Rightarrow \mathfrak{p}[x]$ ist R-mideal $\square$

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

(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 $K[x]$.

Beweis des Gaußschen Lemmas (Satz 13.8)

geg.: faktorielle Ring R, $f, g \in R[x]$ primitiv

z.zg.: fg ist primitiv. Ang., dies ist nicht der Fall

$\Rightarrow$ Die Koeff. von fg haben einen gem. Primteiler p. Setze $\mathfrak{p} = (p)$

Dann gilt $fg \in \mathfrak{p}[x]$ $\overset{(13.7)}{\Longrightarrow}$ $f \in \mathfrak{p}[x]$ oder $g \in \mathfrak{p}[x]$

$\mathfrak{p}[x]$ ist Primideal

$\Rightarrow$ f nicht primitiv oder g nicht primitiv $\lightning$

□