§5 Faktorielle Ringe

In $\mathbb{Z}$ hat jedes Element $n \neq 0$ eine bis auf Reihenfolge eindeutige Darstellung $n = \pm p_1 \cdots p_r$
wobei p_i Primzahlen sind.
Ein solches Resultat gilt nicht in beliebigen Ringen.

5.1 Definition R Ring, $a, b \in R$
a teilt b ($a \mid b$) wenn ein $c \in R$ existiert mit $a \cdot c = b$
Ist $c \in R^*$ eine Einheit, dann gilt auch
$a = c^{-1} \cdot b$, also auch $b \mid a$ und in diesem Fall heißen
b und a assoziiert. In Zeichen $a \sim b$

Bem In Integritätsring gilt $a \mid b$ und $b \mid a \Rightarrow a \sim b$
In der Tat $ac_1 = b$ und $bc_2 = a \Rightarrow b = c_1 c_2 b$
Kürzungsregel $b = 0$ und $a = 0$ oder $1 = c_1 c_2 = 0$ d.h. $c_1, c_2 \in R^\times$.

5.2 Definition: Ein Element $q \in R$, $q \notin R^\times$, $q \neq 0$
heißt irreduzibel, wenn aus $a \mid q$ $a \in R^\times$ auch $a \sim q$ folgt.
Ein Element $p \in R$, $p \notin R^\times$, $p \neq 0$ heißt prim (Primelement),
wenn $p \mid ab \Rightarrow p \mid a$ oder $p \mid b$ äquivalent wenn $R/(p)$ ein
Integritätsring bzw $(p) \subset R$ ein Primideal ist.

5.3 Satz In Integritätsringen gilt
p prim $\Rightarrow$ p irreduzibel

Beweis $p = a \cdot b$ und p prim
$\Rightarrow$ $p \mid a$ oder $p \mid b$ etwa $p \mid a$ $p \cdot c = a$
$\Rightarrow p = pcb \xrightarrow{\text{Kürzungsgesetz}} cb = 1 \Rightarrow b \in R^\times$ und $a \sim p$.

Die Umkehrung ist i. A. falsch.

5.4 Beispiel Betrachte $\sqrt{-5} = i\sqrt{5} \in \mathbb{C}$ und $R = \mathbb{Z}[\sqrt{-5}]$
$= \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$, da $(\sqrt{-5})^2 = -5 \in \mathbb{Z}$

In $\mathbb{Z}[\sqrt{-5}]$ gilt
$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}) = 4 + 5 = 9$
$3, 2 \pm \sqrt{-5}$ sind irreduzibel:

Dazu betrachten wir den Betragsquadrat.

$|a+b\sqrt{-5}|=a^2+5b^2 \in \mathbb{Z}$

Wegen $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$ sind die Einheiten in $\mathbb{Z}[\sqrt{-5}]$ die Menge $\{\pm 1\}$.

Wegen $|3|^2 = |2 \pm \sqrt{-5}|^2 = 9$ haben echte Teiler von 3 bzw. $2 \pm \sqrt{-5}$ Betragsquadrat ein echter Teiler von 9.

Also 3 aber $a^2+5b^2=3$ hat keine ganzzahlige Lösung

Da $\frac{2 \pm \sqrt{-5}}{3} \notin \mathbb{Z}[\sqrt{-5}]$ sind die Elemente zueinander nicht assoziiert. Die Zerlegung

$3 \cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5})$,

ist eine Zerlegung irreduzibel die sich nicht nur durch Reihenfolge und Einheiten voneinander unterscheidet.

5.5 Def

Ein Integritätsring R heißt Hauptidealring, wenn jedes Ideal $I \subset R$ ein Hauptideal ist, (also der form $I=(a)$,

Beispiele 1) $\mathbb{Z}$ ist Hauptidealring; (n).

2) $K[x]$, K Körper ist Hauptidealring.

In der Tat: $I \subset K[x]$ Ideal, $I \neq (0)$, dann betrachten wir in I ein normiertes Polynom f kleinsten Grades.

Jedes weitere Polynom g lässt sich darstellen

$g = q \cdot f + r$ mit $\deg r < \deg f$ (Polynomdiv.)

(Division mit Rest). Für $g \in I$ ist auch $r \in I$ und somit nach Wahl von f r=0 d.h. $g \in (f)$ d.h. $I=(f)$

5.6 Satz 3) $\mathbb{Z}[\sqrt{-5}]$ ist kein Hauptidealring

$(3, 2+\sqrt{-5})$ ist kein Hauptideal

(Warum ist dies nicht das 1-Ideal?)

5.6 Satz In einem Hauptidealring ist jedes irreduzible Element prim.

Beweis: Sei p irreduzibel und $p | a \cdot c$

Dann sind die Ideale (p,a) bzw (p,b) nicht beide das Ideal (1)

Sonst hätten wir $1 = \alpha_1 p + \beta_1 a \equiv \alpha_2 p + \beta_2 b$

$1 = (\alpha_1 p + \beta_1 a)(\alpha_2 p + \beta_2 b) = \underbrace{\alpha_1\alpha_2 p^2 + \beta_1\alpha_2 ap + \alpha_1\beta_2 bp}_{\in (p)} + \underbrace{\beta_1\beta_2 ab}_{\in (p)} \in (p)$

Sei also etwa $(a,p) \neq (1)$. Da $(a,p) = (q)$ ein Hauptideal ist und p irreduzibel. Ist $q \sim p$ da $q \mid p$. Also $(a,p) = (p)$ und damit gilt $p \mid a$. □

5.7 Definition Ein Integritätsr heißt faktoriell (UFD unique factorization domain) wenn jedes Element $a \in R$, $a \in R^\times$, $a \neq 0$ eine Faktorisierung

$$a = p_1 \cdots p_r$$

in irreduzible Faktoren besitzt und diese bis auf Reihenfolge und Einheiten eindeutig ist.

Bem In faktoriellen Ringen ist jedes irreduzible Element auch prim:

$p \mid ab$ etwa $p \cdot c = a \cdot b$

so können wir c, a, b in irreduzible Faktoren zerlegen und die Eindeutigkeit der Zerlegung von ab besagt, dass p zu einem Faktor von a oder b assoziiert ist, also

$p \mid a$ oder $p \mid b$

5.8 Satz Sei R ein Integritätsring und $a = p_1 \cdots p_s = q_1 \cdots q_r$ eine Faktorisierung von a in Primelemente p_i bzw. irreduzible Elemente q_j.

Dann gilt $s = r$ und nach Umnummerierung $p_i \sim q_i$.

Beweis Da p_s prim ist teilt p_s einen. Faktor q_j. Nach Umnummerierung können wir $p_s \mid q_r$ annehmen. Da q_r irreduzibel ist folgt $q_r = \varepsilon p_s$ wobei $\varepsilon \in R^\times$, also $q_r \sim p_s$ Kürzungsregel gibt

$$p_1 \cdots p_{r-1} = q_1 \cdots q_{s-2}(q_{s-1} \cdot \varepsilon)$$

Mit Induktion nach s folgt $s-1 = r-1$ und nach Umnummerierung

$p_i \sim q_i$

IA: $s=1$ gilt, da $1 = q_1 \cdots q_{r-2}(q_{r-1}, \varepsilon)$ die Faktoren falls vorhanden keine Einheiten sind.

Für die Eindeutigkeit ist die prim Eigenschaft günstig.
Für Existenz Irreduzibilität.

5.9 Satz Sei R ein noetherscher Integritäts Ring.
Dann besitzt jedes Element $a \in R \setminus (R^\times \cup \{0\})$ eine Zerlegung $a = q_1 \cdots q_s$ in irreduzible Faktoren.

Beweis Ist a irreduzibel, so ist nichts zu zeigen.
Andernfalls zerlegen wir $a = b \cdot c$, $b, c \notin R^\times$
Indem wir b und c ggf weiter zerlegen, bis wir nur noch irreduzible Faktoren haben erhalten wir eine Zerlegung
Im Fall $R = \mathbb{Z}$ oder $R = K[x]$ ist hierdas dieses Verfahren nach endlich vielen Schritten abbricht, da
$|b|, |c| < |a|$ bez. $\deg b, \deg c < \deg a$.
Im Allgemeinen ist dies nicht so offensichtlich.
Wir verwenden eine sogenannte Noethersche Induktion.
Sei $M = \{(a) \mid a \notin R^\times, a \neq 0$ und a ist kein endl. Produkt von irreduziblen$\}$
Wir wollen $M = \emptyset$ zeigen. Angenommen $M \neq \emptyset$.
Da R noethersch ist existiert ein bzgl. Inklusion maximales Element $(a) \in M$. Nach Voraussetzung ist a zerlegbar $a = b \cdot c$ mit $b, c \notin R^\times$.
Dann gilt $(a) \subset (b)$ und $(a) \subset (c)$
Nach der Kürzungsregel gilt $(a) \subsetneq (b)$ $(a) \subsetneq (c)$
Also $(b) \notin M, (c) \notin M$ d.h. b, c sind endl. Produkte von irreduziblen. $a = b \cdot c$ ebenfalls ein Widerspruch, also $M = \emptyset$

□

((a)=(b) erzwingt in beliebigen Ringen nicht dass $a \sim b$)

Beispiel $R = k[x,y]/(xy^2)$

~~$\bar{x}, \bar{y} \in R$~~ ~~$(\bar{x}) \subset (\bar{x},\bar{y})$~~

$\bar{x}, \bar{x}(1+\bar{y})$

$(\bar{x}) \supset (\bar{x}+1+\bar{y})\,\bar{x}(1+\bar{y})(1-\bar{y}) = \bar{x}-\bar{x}\bar{y}^2 = \bar{x}$

aber $1+\bar{y}$ ist keine Einheit.

$1+\bar{x}\bar{y} \in R^\times$ $\quad 1-\bar{x}\bar{y}$

$\bar{x} \mid \bar{x}$

5.10 Korollar

Hauptidealringe sind faktoriell. Insbesondere sind $\mathbb{Z}$ und $K[x]$ faktoriell

Beweis: Hauptidealringe sind noethersche Integritätsringe also eine Zerlegung existiert und $p \in R$ ist irreduzibel $\Leftrightarrow$ p ist prim.

Also folgt auch die Eindeutigkeit □

5.11 Def Sei R ein faktorieller Ring und $P \subset R$ ein vollständiges Repräsentantensystem für die Klassen zueinander assoziierter irreduzibler Elemente.

Jedes $a \in R \setminus (R^\times \cup \{0\})$ hat eine eindeutige Darstellung $a = \varepsilon\, p_1^{\nu_1} \cdots p_r^{\nu_r}$

wobei $\mu_i \in \mathbb{N}_{>0}$ $p_1, \dots, p_r \in P$ paarweise verschiedene irreduzible und ε eine Einheit in R ist.

Erlauben wir $\nu_i \geq 0$ so können wir für ein weiteres Element $b \in R \setminus (R^\times \cup \{0\})$ die gleichen $p_1, \dots, p_r$ verwenden, etwa $b = \varepsilon \cdot p_1^{\mu_1} \cdots p_r^{\mu_r}$, $\mu_i \geq 0$

Wir definieren den größten gemeinsamen Teiler

$$ggT(a,b) = \prod_{i=1}^{r} p_i^{\min(\nu_i,\mu_i)} \quad \text{und}$$

$$kgV(a,b) = \prod_{i=1}^{r} p_i^{\max(\nu_i,\mu_i)}$$

Die Definition hängt ab von der Wahl des Repräsentantensystems. Bei Wahl eines anderen Repräsentantensystem erhalten wir assoziierte Elemente.

Es gilt $ggT(a,b) \cdot kgV(a,b)$ ist assoziiert zu $a\,b$

Wir definieren

$$\nu_p : R\setminus\{0\} \to \mathbb{N} \quad \text{falls } p^k \mid a \text{ aber } p^{k+1} \nmid a$$
$$a \longmapsto k$$

Wir können dann $a = \varepsilon \cdot \prod_{p \in P} p^{\nu_p(a)}$

schreiben, da nur endlich viele Exponenten $\neq 0$

Durch $\nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b)$

wird $\nu_p : Q(R) \to \mathbb{Z} \cup \{\infty\}$

fortgesetzt, wobei $\nu_p(0) = \infty$

Unser nächstes Ziel ist zu zeigen, dass mit R faktoriell auch $R[x]$ faktoriell ist.

Dazu setzen wir ν_p auf $R[x]$ fort indem wir

$a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 = f$

$\nu_p(f) = \min\{\nu_p(a_0), \dots, \nu_p(a_n)\}$ setzen

Dann gilt $f \in Q(R)[x]$ liegt in $R[x]$

$\iff \nu_p(f) \geq 0 \quad \forall p$ Prim.

5.12 Def Ein Polynom $f \in R[x]$ heißt primitiv wenn $\nu_p(f) = 0 \quad \forall p$, d.h.

$$ggT(a_0, \dots, a_n) = 1$$

Für Anwendungen ist die folgende Aussage sehr nützlich.

"Ein primitives Polynom $f \in R[x]$ ist irreduzibel in $R[x]$ genau dann, wenn es irreduzibel in $Q(R)[x]$ ist."

Bem Die Irreduzibilität von $f \in \mathbb{Z}[x]$ lässt sich algorithmisch entscheiden. Hat f den Grad n und sind $b_0, \dots, b_n \in \mathbb{Z}$ paarweise verschieden, dann ist

f durch Werte $c_j = f(b_j)$ wegen Lagrangeinterpolationspolynome eindeutig bestimmt.

$$f = \sum_{j=0}^{n} c_j \prod_{i \neq j} \frac{x - b_i}{b_j - b_i}$$

Ist nun $g \in \mathbb{Z}[x]$ ein Teiler, dann teilt $g(b_j)$ den Wert $c_j = f(b_j)$. Da die c_j nur endlich viele Teiler haben, kommen nur endlich viele $g \in \mathbb{Z}[x]$ als Teiler in Frage und diese können wir durch probieren.
Irreduzibilität von $f \in \mathbb{Q}[x]$ folgt dann aus Irr. von $f \in \mathbb{Z}[x]$.

Beispiel $f = x^3 + ax + 1 \in \mathbb{Z}[x]$. $f \in \mathbb{Q}[x]$ irreduzibel $\Leftrightarrow a \neq -2, 0$.
Als Faktoren in $\mathbb{Z}[x]$ kommen nur Polynome mit Leitkoeffizienten ± 1 in Frage und Konstantenterm eben ± 1.
Also als Linearfaktor kann nur $\pm x \pm 1$ in Frage kommen.

$x=1$ in f einsetzen $\quad 1+a+1=0 \Leftrightarrow a=2$

$x=-1$ " $\quad -1+a+1=0 \Leftrightarrow a=0$

5.13 Lemma (Gauß)
Sei R faktoriell $p \in R$ prim und $f, g \in Q(R)[x]$.
Dann gilt $v_p(fg) = v_p(f) + v_p(g)$
Beweis: Ist $a \in Q(R) \subset Q(R)[x]$ dann ist
$v_p(af) = v_p(a) + v_p(f)$ klar, da
$v_p(a \cdot a_i) = v_p(a) \cdot v_p(a_i)$ für jeden Koeffizienten a_i von f gilt.
Indem wir f mit dem kgV der Nenner der Koeffizienten multiplizieren und anschließend durch ggT der Koeffizienten teilen können wir $v_p(f) = 0 \; \forall p$ bzw $f \in R[x]$ primitiv erreichen. Analog für g. Wir dürfen also f, g in $R[x]$ und $v_p(f) = v_p(g) = 0$ voraussetzen.

Wir betrachten nun die Koeffizientenreduktion modp.

$\overline{\Phi} : R[x] \to R/(p)[x]$

$\overline{\Phi}$ ist ein Ringhomomorphismus und

$\ker \overline{\Phi} = \{h \in R[x] \mid v_p(h) > 0\}$

$\overline{\Phi}(f), \overline{\Phi}g \neq 0 \in R/(p)[x]$.

$h = f \cdot g \in R[x]$ und da $R/(p)[x]$ ein Integritätsring ist gilt $\overline{\Phi}(h) = \overline{\Phi}(f) \cdot \overline{\Phi}(g) \neq 0$

Also $v_p(h) = 0 = v_p(f) + v_p(g)$ □

5.14 Korollar Sei R ein faktorieller Ring, $h \in R[x]$ ein normiertes Polynom. Ist $h = f \cdot g$ eine Faktorisierung von h durch normierte Polynome $f, g \in Q(R)[x]$, dann gilt schon $f, g \in R[x]$

Beweis: Für jedes Primelement $p \in R$ gilt

$v_p(h) = 0$ und $v_p(f), v_p(g) \leq 0$ da h, f, g normiert sind.

Aus dem Lemma von Gauß folgt

$0 = v_p(h) + v_p(g) + v_p(f)$ Also

$v_p(g) = 0 = v_p(f)$ $\forall p$ d.h. $g, f \in R[x]$ □

5.15 Satz von Gauß. Es sei R ein faktorieller Ring. Dann ist auch $R[x]$ faktoriell.

Ein Polynom $q \in R[x]$ ist irreduzibel genau dann, wenn entweder

(1) $q \in R$ irreduzibel und (2) q ist primitiv und ein Primelement in $Q(R)[x]$

Insbesondere ist ein primitives Polynom $q \in R[x]$ prim genau dann, wenn $q \in Q(R)[x]$ prim ist.

Beweis Wir zeigen zunächst, dass die Elemente in (1) und (2) prim in $R[x]$ sind.

(1): Ist $q \in R$ prim, dann ist $R/(q)$ Integritätsring und

$R/(q)[x] = R[x]/qR[x]$ ist Integritätsring, also $qR[x]$ ein Primideal und damit q prim.

(2) Sei nun $q \in R[x]$ ein primitives Polynom, sodass in $Q(R)[x]$ prim ist und $f, g \in R[x]$ Polynome mit $q \mid fg$ in $R[x]$

Dann gilt $q \mid f$ oder $q \mid g$ in $Q(R)[x]$, etwa $q \mid f$.

Es gibt also ein $h \in Q(R)[x]$ sodass $q \cdot h = f$

Auf diese Gleichung wenden wir das Gaußsche Lemma an. $0 \leq v_p(f) = v_p(q) + v_p(h) \Rightarrow v_p(h) \geq 0 \ \forall p$ prim

$\Rightarrow h \in R[x]$ und $q \mid f$ in $R[x]$.

Es bleibt zu zeigen, dass $R[x]$ faktoriell ist und jedes Primelement von $R[x]$ von der Gestalt (1) und (2) ist. Dazu reicht es zu zeigen, dass jedes Element $f \in R[x]$ ein Produkt in Elementen von Typ (1) und (2) ist.

Wir schreiben $f = a\tilde{f}$ wobei a der ggT des Koeffizienten von f ist und $\tilde{f}$ primitiv.

a ist Produkt von Primelementen vom Typ (1), da R faktoriell ist. Es reicht $\tilde{f}$ zu zerlegen. $Q(R)[x]$ ist Hauptidealring, wir können also $\tilde{f} = c f_1 \cdots f_r$, wobei die $\tilde{f}_i$ prim in $Q(R)[x]$ und $c \in Q(R)^\times$. Bei geeigneter Wahl von c können wir $\tilde{f}_i$ als primitive Polynome in $R[x]$ voraussetzen.

Nach dem Lemma von Gauß gilt

$$0 = v_p(\tilde{f}) = v_p(c) + v_p(\tilde{f}_1) + \dots + v_p(\tilde{f}_r)$$

$\Rightarrow v_p(c) = 0 \ \forall p \in R$ Prim, d.h. $c \in R^\times$

Indem wir $\tilde{f} = (c\tilde{f}_1) \cdots \tilde{f}_r$ haben wir eine Zerlegung in f in Elemente von Typ (2) gefunden

5.16 Korollar $\mathbb{Z}[x_1, \dots, x_n]$ und $K[x_1, \dots, x_n]$, K Körper, sind faktoriell

Beweis: Induktion nach n. □

5.17 Satz (Eisensteinsche Irreduzibilitätskriterium)
Sei R ein faktorieller Ring und $f = a_n x^n + \dots + a_0 \in R[x]$ ein primitives Polynom und $p \in R$ ein Primelement.
Gilt $p \nmid a_n$, $p \mid a_i$ für $i < n$ und $p^2 \nmid a_0$. Dann ist f irreduzibel in $R[x]$ und somit auch in $Q(R)[x]$.

Beweis: Angenommen f ist reduzibel in $R[x]$ etwa $f = gh$ mit $g = \sum_{i=1}^{r} b_i x^i$, $h = \sum_{j=1}^{s} c_j x^j$, wobei $r+s = n$ und $r > 0$, $s > 0$
Es folgt:

$a_n = b_r c_s$ und $p \nmid b_r$ $p \nmid c_s$

$a_0 = b_0 c_0$ mit $p \mid b_0 c_0$ aber $p^2 \nmid b_0 c_0$

Wir dürfen $p \mid b_0$ und $p \nmid c_0$ annehmen.

Sei $t < r$ maximal mit der Eigenschaft ~~$p \nmid b_t$~~ $p \mid b_i$ für $0 \le i \le t$

$a_{t+1} = b_0 c_{t+1} + b_1 c_t + \dots + b_{t+1} c_0$, wobei $b_i = 0$ für $i > r$ und $c_j = 0$ für $j > s$

Dann ist a_{t+1} nicht durch p teilbar, da ~~$b_0 c_{t+1}$~~ $b_0 c_{t+1}, \dots, b_t c_1$ durch p teilbar sind aber $b_{t+1} c_0$ nicht.

$\Rightarrow t+1 = n$, $t+1 \le r$

$\Rightarrow r \le n \le r$, also Gleichheit, was $s = n - r > 0$ widerspricht. □

Beispiel 1) p Primzahl und $F = x^{p-1} + x^{p-2} + \dots + 1$ ist irreduzibel in $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$.

Zum Nachweis der Irreduzibilität betrachten wir den Isomorphismus $\mathbb{Z}[x] \to \mathbb{Z}[x]$, $x \mapsto x+1$

Es reicht also $F(x+1)$ irreduzibel zu zeigen.

$$F(x) = \frac{x^p - 1}{x - 1} \Rightarrow f(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1} x^{p-2} + \dots + \binom{p}{p-1}$$

$p \mid \binom{p}{\nu}$ für $\nu = 1, \dots, p-1$ da $\binom{p}{\nu} = \frac{p(p-1)\cdots(p-\nu+1)}{\nu \cdot (\nu-1) \cdots 1}$

p nicht im Nenner hat. $p = \binom{p}{p-1} = a_0$ $p \mid a_0$ aber $p^2 \nmid a_0$

$\overset{\text{Einsetzen}}{\Longrightarrow}$ $f(x+1)$ ist irreduzibel

2) $R = k[t]$, $K = Q(k[t]) = k(t)$ der Körper der rationalen Funktionen $x^n - t \in K[x]$ ist irreduzibel,

$t \in k[t]$ ist prim $k[t]/(t) \cong k$, $t \mid a_{n-1}, \dots, a_0$,

$t \nmid a_n = 1$, $t^2 \nmid a_0 = t$

Einsetzen $\Rightarrow$ $x^n - t \in K[x]$ ist irreduzibel