3.5 Faktorielle Ringe

3.5.1 Def Sei R ein kommutativer Ring, $a, b \in R$, a teilt b, $a|b$, falls $\exists\, c \in R: \; ca = b$.

3.5.2 Lemma (Regeln für Teilbarkeit)
Sei R nullteilerfrei, seien $a, b, c, d \in R$.

1) (Kürzungsregel) $c \neq 0, \; ac = bc \Rightarrow a = b$
2) $a|0, \; a|a, \; 1|a$
3) $a|b, \; u \in R^* \Rightarrow au|b, \; a|ub$
4) $R^* = \{a \mid a|1\}$
5) $a|u$ mit $u \in R^* \Rightarrow a \in R^*$
6) $c \neq 0, \quad ca|cb \Leftrightarrow a|b$
7) $c|a, \; c|b \Rightarrow c|xa+yb \quad \forall x, y \in R$
8) $a|b, c|d \Rightarrow ac|bd$

Beweis:

1) $ac = bc \Rightarrow ac - bc = 0 \Rightarrow (a-b)c = 0$
Da R nullteilerfrei ist und $c \neq 0$ folgt $a - b = 0 \Rightarrow a = b$.

2) Da $0 \cdot a = 0, \; 1 \cdot a = a, \; a \cdot 1 = a$

3) $a|b \Rightarrow \exists c: ac = b \Rightarrow a \cdot u \cdot (u^{-1}c) = b \Rightarrow au | b$. $a(cu) = ub \Rightarrow a | ub$

4) $R^* = \{a \mid \exists b: ab = 1\} = \{a \mid a|1\}$

5) $a|u \Rightarrow \exists c: ac = u \Rightarrow a(cu^{-1}) = uu^{-1} = 1 \Rightarrow a \in R^*$

6) „$\Rightarrow$" $ca|cb \Rightarrow \exists d: cad = cb \overset{c \neq 0,\ 1)}{\Longrightarrow} ad = b \Rightarrow a|b$.

„$\Leftarrow$" klar

7) $c|a,\ c|b \Rightarrow \exists d, e: cd = a,\ ce = b \Rightarrow c \cdot (dx + ey) = cdx + cey = ax + by \Rightarrow c | ax + by$

8) $a|b,\ c|d \Rightarrow \exists e, f: ae = b,\ cf = d \Rightarrow ac(ef) = bd \Rightarrow ac | bd$ $\square$

3.5.3 Def

Sei R nullteilerfrei, $a, b \in R$.

a, b heißen <u>assoziiert</u> $:\Leftrightarrow \exists u \in R^*: au = b$.

3.5.4 Lemma Sei R nullteilerfrei.

a, b assoziiert $\Leftrightarrow a|b,\ b|a \Leftrightarrow \langle a \rangle = \langle b \rangle$

Beweis: a, b assoziiert $\Rightarrow \exists\, u \in R^*$:
$au = b \Rightarrow a \mid b$, außerdem gilt
$bu^{-1} = a \Rightarrow b \mid a$.
Es gelte $b \mid a$, $a \mid b \Rightarrow \exists\, c, d$:
$ac = b$, $bd = a \Rightarrow a \in \langle b \rangle$,
$b \in \langle a \rangle \Rightarrow \langle a \rangle \subset \langle b \rangle$, $\langle b \rangle \subset \langle a \rangle$
$\Rightarrow \langle a \rangle = \langle b \rangle$.
Es gelte $\langle a \rangle = \langle b \rangle$. $\Rightarrow b \in \langle a \rangle$
und $a \in \langle b \rangle \Rightarrow \exists\, c, d$:
$a \cdot c = b$, $b \cdot d = a$
1. Fall: Sei $a = 0 \Rightarrow b = c \cdot a = c \cdot 0 = 0$
$\Rightarrow$ a und b sind assoziiert
2. Fall: $a \neq 0$. Aus $a \cdot c \cdot d = a$
folgt dann mit der Kürzungsregel
$cd = 1 \Rightarrow c, d \in R^* \Rightarrow$
a und b sind assoziiert. $\square$

Bsp

1) $a, b \in \mathbb{Z}$ sind assoziiert $\Leftrightarrow |a| = |b|$
2) Sei K ein Körper. Dann sind $a, b \neq 0$ assoziiert.

3) Seien $f, g \in R[X]$. f, g sind assoziiert $\Leftrightarrow \exists\, u \in R^*: f = ug$.

<u>3.5.5 Def</u> Sei R nullteilerfrei.
Sei $0 \neq a \in R \setminus R^*$
1) a heißt <u>irreduzibel</u> (unzerlegbar) $:\Leftrightarrow$
falls $a = bc$ mit $b, c \in R$ folgt
$b \in R^*$ oder $c \in R^*$
2) a heißt <u>prim</u> $:\Leftrightarrow$
falls $a \mid bc$ für $b, c \in R$ folgt
$a \mid b$ oder $a \mid c$

<u>Bemerkung</u>: In $\mathbb{Z}$ ist prim und irreduzibel äquivalent (Satz 1.12)

<u>3.5.6 Lemma</u> Sei R nullteilerfrei.
$a \in R$ sei prim $\Rightarrow a$ ist irreduzibel.

<u>Beweis</u>: Sei a prim, sei $a = bc$
$\Rightarrow a \mid bc \Rightarrow$ OE $a \mid b \Rightarrow \exists d:$
$ad = b \Rightarrow a = acd \overset{\text{kürzen}}{\Longrightarrow} 1 = cd$
$\Rightarrow c \in R^* \Rightarrow a$ ist irreduzibel.
$\square$

Bemerkung Im Allgemeinen folgt aus irreduzibel nicht prim, ein Bsp davon gibt es in den Übungen:
$2 \in \mathbb{Z}[\sqrt{-5}]$ ist irreduzibel, aber nicht prim.

3.5.7 Lemma Sei R nullteilerfrei, $0 \neq a \in R \setminus R^*$

$\langle a \rangle$ ist Primideal $\Leftrightarrow$ a prim

Beweis: „$\Rightarrow$" Sei $\langle a \rangle$ Primideal,

$a \mid bc \Rightarrow bc \in \langle a \rangle \Rightarrow$ OE $b \in \langle a \rangle$
$\Rightarrow a \mid b \Rightarrow a$ prim.

„$\Leftarrow$" Sei a prim, $bc \in \langle a \rangle \Rightarrow$
$a \mid bc \Rightarrow$ OE $a \mid b \Rightarrow b \in \langle a \rangle$
$\Rightarrow \langle a \rangle$ Primideal. $\square$

3.5.8 Lemma Sei R nullteilerfrei, $0 \neq a \in R \setminus R^*$

$\langle a \rangle$ maximal $\Rightarrow$ a irreduzibel

Beweis: Sei $a = bc \Rightarrow a \in \langle b \rangle$
$\Rightarrow \langle a \rangle \subset \langle b \rangle$

Falls $\langle a \rangle = \langle b \rangle \Rightarrow b \in \langle a \rangle \Rightarrow$
$\exists\, d: \; ad = b \Rightarrow a = adc \overset{\text{kürzen}}{\Rightarrow}$
$dc = 1 \Rightarrow c$ Einheit.

Falls $\langle a \rangle \subsetneq \langle b \rangle \Rightarrow \langle b \rangle = R$
$\Rightarrow 1 \in \langle b \rangle \Rightarrow \exists\, d: \; bd = 1$
$\Rightarrow b$ Einheit

$\Rightarrow a$ ist irreduzibel. $\square$

<u>Bsp</u> Es gibt irreduzible Elemente, die kein maximales Ideal erzeugen.

$f = xy - 1 \in \mathbb{C}[x, y]$

f ist irreduzibel, wäre es zerlegbar, so müßte es in zwei Polynome vom Grad 1 zerfallen $ax + by + c,\; dx + ey + f$
man rechnet nach, daß es das nicht tut.

$xy - 1 \in \langle x-1, y-1 \rangle$, denn
$$xy - 1 = y(x-1) + y - 1$$

$x - 1 \notin \langle xy - 1 \rangle$

$\Rightarrow \langle xy - 1 \rangle \subsetneq \langle x-1, y-1 \rangle \subsetneq \mathbb{C}[x, y]$

3.5.9 Satz

Sei R noethersch, $0 \neq a \in R \setminus R^*$. Dann ist $a = q_1 \cdots q_r$ ein Produkt von irreduziblen Elementen.

Beweis Ist a irreduzibel, ist nichts zu zeigen. Ist a zerlegbar $\Rightarrow \exists\, a_1, b_1 \in R \setminus R^*$, $a = a_1 b_1$. Sind a_1, b_1 irreduzibel, fertig. Sonst OE a_1 zerlegbar $\Rightarrow \exists\, a_2, b_2 : a_1 = a_2 b_2$ usw.

So produzieren wir eine Kette

$$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots$$

die wegen noethersch stationär wird

$\Rightarrow \exists\, k : \langle a_k \rangle = \langle a_{k+1} \rangle$

$\Rightarrow \exists\, c : a_{k+1} = a_k \cdot c$

$\Rightarrow a_k = a_{k+1} b_{k+1} = a_k c\, b_{k+1}$

$\Rightarrow c\, b_{k+1} = 1 \Rightarrow b_{k+1} \in R^*$

$\Rightarrow a_k$ ist irreduzibel

und $a = a_1 \cdots a_k$ ist ein Produkt von irreduziblen Elementen.

$\square$

3.5.10 Def Ein nullteilerfreier Ring, in dem jedes $0 \neq a \in R \setminus R^*$ eine bis auf Vertauschung und Einheiten eindeutige Darstellung $a = p_1 \cdot \ldots \cdot p_r$ mit p_i prim besitzt, heißt <u>faktoriell</u> (ZPE „Zerlegung in Primfaktoren ist eindeutig", UFD „unique factorization domain")

Bsp $\mathbb{Z}$ ist faktoriell.

3.5.11 Prop Sei R faktoriell.
a irreduzibel $\Rightarrow$ a prim.

Insbesondere sind wegen Lemma 3.5.6 die beiden Begriffe in faktoriellen Ringen äquivalent.

Beweis: Sei a irreduzibel, schreibe $a = p_1 \cdots p_r$ als Produkt von Primfaktoren, dann muß $r = 1$ und $a = p_1$ gelten. $\square$

3.5.12 Satz Sei R nullteilerfrei.

R faktoriell $\iff$ jedes $0 \neq a \in R \setminus R^*$ besitzt eine bis auf Vertauschung und Einheiten eindeutige Darstellung als Produkt von irreduziblen Elementen.

Beweis:

„$\Rightarrow$" Existenz: a besitzt eine Darstellung als Produkt von Primfaktoren, jedes Primelement ist irreduzibel.

Eindeutigkeit: Jede Zerlegung in irreduzible Faktoren ist auch eine Zerlegung in Primfaktoren und letztere ist n. V. eindeutig.

„$\Leftarrow$" Beh: jedes irreduzible Element ist prim.

Dann folgen Existenz und Eindeutigkeit der Zerlegung in Primfaktoren aus der Existenz und Eindeutigkeit der Zerlegung in irreduzible Faktoren.

Sei p irreduzibel und $p \mid ab$

Ist $a \in R^* \Rightarrow p \mid b$.

Ist $a = 0 \Rightarrow p \mid a$

Also können wir annehmen,

$a, b \in R \setminus (R^* \cup \{0\})$.

$\exists\, c: \; pc = ab$. Beide Seiten haben eindeutige Zerlegungen in irreduzible Elemente, p ist n. V. irreduzibel, damit ist p einer der Faktoren von a oder b (bis auf Einheit) $\Rightarrow$

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

$\Rightarrow p$ ist prim. $\square$

<u>Bsp</u>

1) $R = \mathbb{C}[x,y,z,w] / (xy - zw)$ ist nullteilerfrei, da $xy - zw \in \mathbb{C}[x,y,z,w]$ prim.

R ist nicht faktoriell:

x, y, z, w sind irreduzibel, aber

$xy = zw$ ist nicht eindeutig als Produkt von irreduziblen Elementen.

Wegen Satz 3.5.12 kann R daher nicht faktoriell sein.

2) $R = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$

<u>Beh</u>: R ist nicht faktoriell.

Wir bestimmen die Einheiten von R:

$$(a+b\sqrt{-3})(c+d\sqrt{-3}) = 1 \Rightarrow$$

$$|a+b\sqrt{-3}|\,|c+d\sqrt{-3}| = 1 \Rightarrow b, d = 0,$$

$$a, c \in \{\pm 1\} \Rightarrow R^* = \{\pm 1\}.$$

<u>Bew</u>: 2 ist irreduzibel.

Angenommen, $2 = (a+b\sqrt{-3})(c+d\sqrt{-3})$

$$\Rightarrow 4 = (a^2+3b^2)(c^2+3d^2)$$

Einer dieser Faktoren muß 1 sein, also OE $a \in \{\pm 1\}$, $b = 0 \Rightarrow a+b\sqrt{-3}$ ist Einheit

Analog sieht man $1 \pm \sqrt{-3}$ ist irreduzibel.

Damit sind

$$2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$$

verschiedene Zerlegungen in irreduzible Elemente.

Wegen Satz 3.5.12 kann R daher nicht faktoriell sein.

<u>3.5.13 Satz</u>

Ein noetherscher nullteilerfreier Ring ist faktoriell $\Leftrightarrow$ jedes irreduzible Element ist prim.

Beweis:

„⇒" 3.5.11.

„⇐" Wegen Satz 3.5.9 besitzt $a \in R \setminus (R^* \cup \{0\})$ eine Darstellung als Produkt von irreduziblen Elementen, damit besitzt es auch eine als Produkt von Primfaktoren.

Eindeutigkeit: wie im Satz 1.12 über die Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}$:

Induktion über k = Anzahl Faktoren.

Sei $k = 1$, $a = p_1$ prim.

Falls $p_1 = p_1' \cdots p_l'$ so folgt $l = 1$ und $p_1 = p_1'$, da p_1 irreduzibel.

Sei $k > 1$, $a = p_1 \cdots p_k = p_1' \cdots p_l'$

$\Rightarrow p_k \mid p_1' \cdots p_l' \xRightarrow{p_k \text{ prim}} \exists i:$

$p_k \mid p_i'$. Da beide prim sind, folgt p_k ist assoziiert zu p_i'.

$\Rightarrow \exists u \in R^*: \; u \, p_1 \cdots p_{k-1} =$

$p_1' \cdots p_{i-1}' \, p_{i+1}' \cdots p_l'$

Da nach Induktionsvoraussetzung für Produkte von $k-1$ Primelementen die Eindeutigkeit gegeben ist, folgt, daß diese Faktoren gleich sind (bis auf Einheiten). $\square$

<u>3.5.14 Def</u> Sei R nullteilerfrei, $a, b \in R$.

d ist ein <u>größter gemeinsamer Teiler</u> von a, b, $ggT(a,b)$, wenn

1) $d | a$, $d | b$
2) $\forall d'$: $d' | a$, $d' | b \Rightarrow d' | d$

m ist ein <u>kleinstes gemeinsames Vielfaches</u> von a, b, $kgV(a,b)$, wenn

1) $a | m$, $b | m$
2) $\forall m'$: $a | m'$, $b | m' \Rightarrow m | m'$

Analog für mehr als zwei Elemente.

<u>Bemerkung</u>

1) ggT und kgV sind nur bis auf Einheiten bestimmt

2) Falls d und d' ggT, so folgt $d \mid d'$, $d' \mid d$ also sind sie assoziiert

3) ggT und kgV müssen nicht existieren

4) Existiert $ggT(a,b)$, dann auch
$$kgV(a,b) = \frac{ab}{ggT(a,b)}$$

5) $ggT(a,b) \cdot kgV(a,b)$ und ab sind assoziiert.

<u>3.5.15 Satz</u> Sei R faktoriell, $a = p_1^{s_1} \cdots p_k^{s_k}$, $b = p_1^{r_1} \cdots p_k^{r_k}$ Darstellungen als Produkt von Primfaktoren. Dann existieren $ggT(a,b)$, $kgV(a,b)$ und
$$ggT(a,b) = \prod p_i^{\min(s_i, r_i)}$$
$$kgV(a,b) = \prod p_i^{\max(s_i, r_i)}$$

Beweis Übung.

3.6 Hauptidealringe

3.6.1 Def

Ein Ideal I, das von einem Element erzeugt wird, $I = \langle a \rangle$, heißt Hauptideal.
Ein nullteilerfreier Ring, in dem alle Ideale Hauptideale sind, heißt Hauptidealring.

Bsp $\mathbb{Z}$ ist Hauptidealring.

3.6.2 Bemerkung

Hauptidealringe sind noethersch.

3.6.3 Satz

In einem Hauptidealring sind irreduzible Elemente prim.

Beweis: Sei p irreduzibel, $p \mid ab$. Es gilt $\langle p \rangle \subset \langle p, a \rangle$, $\langle p \rangle \subset \langle p, b \rangle$. Wäre $\langle p, a \rangle = R = \langle 1 \rangle = \langle p, b \rangle$, so gäbe es r_i, s_i mit $r_1 a + s_1 p = 1 = r_2 b + s_2 p$

$\Rightarrow \quad 1 = (r_1 a + s_1 p)(r_2 b + s_2 p) =$

$r_1 r_2 ab + r_1 s_2 ap + r_2 s_1 bp + s_1 s_2 p^2$

$\in \langle p \rangle$, da $ab \in \langle p \rangle$ $\lightning$ da

p keine Einheit.

Also ist $\mathbb{C}$ $\langle p, a \rangle \subsetneq R$.

Da R Hauptidealring ist, $\exists$

d: $\langle p, a \rangle = \langle d \rangle \subsetneq R$. Damit

$d \notin R^*$. Dann $\exists$ c, e:

$p = c \cdot d$, $a = e \cdot d$. Da p irreduzibel

ist, folgt $c \in R^* \Rightarrow$

$a = ed = e c^{-1} c d = e c^{-1} p$

$\in \langle p \rangle$ also $p \mid a$.

Damit ist p prim. $\square$

<u>3.6.4 Korollar</u>

Hauptidealringe sind faktoriell.

<u>Beweis</u>: Hauptidealringe sind noethersch

wegen 3.6.2 und nullteilerfrei n. V.

Da wegen 3.6.3 irreduzible

Element prim sind, folgt mit Satz 3.5.13, daß Hauptidealringe faktoriell sind. $\square$

3.6.5 Satz

Sei R ein Hauptidealring, $a_1, \dots, a_r \in R$

1) $\langle a_1, \dots, a_r \rangle = \langle ggT(a_1, \dots, a_r) \rangle$

Insbesondere gibt es eine Darstellung

$ggT(a_1, \dots, a_r) = x_1 a_1 + \dots + x_r a_r$

2) $\langle a_1 \rangle \cap \dots \cap \langle a_r \rangle = \langle kgV(a_1, \dots, a_r) \rangle$

Beweis:

1) Da R Hauptidealring ist, ist $\langle a_1, \dots, a_r \rangle = \langle d \rangle$ für ein d.

Es gilt $a_i \in \langle d \rangle \; \forall i \Rightarrow d | a_i \; \forall i$

Außerdem $d \in \langle a_1, \dots, a_r \rangle \Rightarrow$

$\exists x_i \in R: \; d = x_1 a_1 + \dots + x_r a_r$.

Sei d' ein Teiler von $a_i \; \forall i$, dann gilt d' teilt $x_1 a_1 + \dots + x_r a_r = d$.

Damit ist $d = ggT(a_1, \dots, a_r)$.

2) Der Schnitt ist ein Ideal, daher $\exists m: \langle a_1 \rangle \cap \dots \cap \langle a_r \rangle = \langle m \rangle$.

$\Rightarrow \quad m \in \langle a_i \rangle \ \forall i \Rightarrow a_i | m \ \forall i.$

Gilt $a_i | m' \ \forall i$ für ein m', so folgt $m' \in \langle a_i \rangle \ \forall_i \Rightarrow m' \in \langle a_1 \rangle \cap \dots \cap \langle a_r \rangle = \langle m \rangle \Rightarrow m | m'$

$\Rightarrow m = \mathrm{kgV}(a_1, \dots, a_r).$ $\square$

<u>Bsp</u>:

1) In $\mathbb{Z}$ ist $\langle 6, 15 \rangle = \langle 3 \rangle = \langle \mathrm{ggT}(6,15) \rangle$
$\langle 6 \rangle \cap \langle 15 \rangle = \langle 30 \rangle = \langle \mathrm{kgV}(6,15) \rangle$

2) $\mathbb{C}[x,y]$ ist kein Hauptidealring.
$\langle x, y \rangle$ kann nicht von einem Polynom erzeugt werden.
$\mathbb{C}[x,y]$ ist faktoriell (ohne Beweis)
also existiert $\mathrm{ggT}(x,y) = 1$.
Aber $\langle x,y \rangle \subsetneq \langle 1 \rangle = \mathbb{C}[x,y]$.

<u>3.6.6 Lemma</u> Sei R Hauptidealring, $a \in R \setminus (R^* \cup \{0\})$. Dann ist

$\langle a \rangle$ maximal $\Leftrightarrow$ a irreduzibel

<u>Beweis</u>: „$\Rightarrow$" Lemma 3.5.8 (R nullteilerfrei n. V.).

„$\Leftarrow$" Sei a irreduzibel, sei
$\langle a \rangle \subset \langle b \rangle \subset R \Rightarrow a \in \langle b \rangle$
$\Rightarrow \exists c: \; a = bc \Rightarrow b \in R^*$
oder $c \in R^*$
1. Fall: $b \in R^* \Rightarrow \langle b \rangle = R$
2. Fall: $c \in R^* \Rightarrow \langle a \rangle = \langle b \rangle$
$\Rightarrow \langle a \rangle$ ist maximal. $\square$

3.7 Euklidische Ringe

3.7.1 Def Ein nullteilerfreier Ring heißt euklidisch, wenn
$\exists v: R \setminus \{0\} \longrightarrow \mathbb{N}$,
$\forall a, b \in R \setminus \{0\}$ mit $v(a) \geq v(b)$
$\exists q, r \in R$:

1) $a = qb + r$
2) $r = 0$ oder $v(r) < v(b)$.

1) heißt dann Division mit Rest,
v heißt euklidische Norm.

Bsp

1) $\mathbb{Z}$ ist euklidisch mit $v: a \mapsto |a|$

2) $K[x]$ ist euklidisch mit $v = \deg$.

Bsp für eine Polynomdivision:

$$(x^4-1) : (x^2+2x+1) = x^2-2x+3$$
$$\begin{array}{l} -(x^4+2x^3+x^2) \\ \hline -2x^3-x^2-1 \\ -(-2x^3-4x^2-2x) \\ \hline 3x^2+2x-1 \\ -(3x^2+6x+3) \\ \hline -4x-4 \quad \text{Rest} \end{array}$$

$$\underbrace{(x^4-1)}_{a} = \underbrace{(x^2-2x+3)}_{q} \cdot \underbrace{(x^2+2x+1)}_{b} + \underbrace{(-4x-4)}_{r}$$

Dabei gilt $\deg r < \deg b$.

Für das Verfahren benötigen wir, daß K ein Körper ist, denn man muß durch Leitkoeffizienten teilen.

3.7.2 Satz

Euklidische Ringe sind Hauptidealringe.

Beweis: $I = \langle 0 \rangle$ ist von 0 erzeugt.

Sei $I \neq \langle 0 \rangle$. Wähle $m \in I$ mit minimalem ν.

Beh: $I = \langle m \rangle$

„$\supset$" klar

„$\subset$" Sei $b \in I$. Division mit Rest mit m liefert $b = q \cdot m + r$ mit $\nu(r) < \nu(m)$ oder $r = 0$

$\Rightarrow r = b - qm \in I$

Da m minimales ν hatte, folgt $r = 0 \Rightarrow b = qm \Rightarrow b \in \langle m \rangle$. $\square$

Bsp

$R = \mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$

der Ring der ganzen Gaußschen Zahlen

Setze $\nu : R \setminus \{0\} \longrightarrow \mathbb{N}$:

$a+bi \longmapsto a^2+b^2 = |a+bi|^2$

Beh: ν ist euklidische Norm.

Seien $a+bi,\ c+di \in \mathbb{Z}[i]$,
betrachte $\frac{a+bi}{c+di} =: x+iy$ mit

$$x = \frac{ac+bd}{c^2+d^2}, \quad y = \frac{bc-ad}{c^2+d^2} \in \mathbb{Q}.$$

Wähle $p, q \in \mathbb{Z}$ mit $|p-x| \leq 1/2$, $|q-y| \leq 1/2$.

Dann ist $|x+iy-(p+qi)|^2 =$
$(x-p)^2 + (y-q)^2 \leq 1/4 + 1/4 < 1$

$$\Rightarrow \left| \frac{a+ib}{c+id} - (p+qi) \right|^2 < 1 \quad \Rightarrow$$

$$| a+ib - (p+qi)(c+di)|^2 < |c+di|^2$$

Setze $a+bi - (p+qi)(c+di)$ als Rest, dann erfüllt $(\mathbb{Z}[i], \nu)$ Def 3.7.1.

Damit ist $\mathbb{Z}[i]$ Hauptidealring und faktoriell.

<u>Bsp</u> $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ ist Hauptidealring, aber nicht euklidisch (ohne Beweis).

3.7.3 Satz (Euklidischer Algorithmus)

Sei R mit $v: R\setminus\{0\} \to \mathbb{N}$ euklidisch.
Seien $a, b \in R\setminus\{0\}$ mit $v(a) \geq v(b)$

1. Schritt: $a_1 := a$, $b_1 := b$

2. Schritt: Berechne eine Division mit Rest $a_1 = q_1 b_1 + r_1$
Wenn $r_1 = 0$ dann ist $ggT(a,b) = b_1$, stop.
Sonst setze $a_2 := b_1$, $b_2 := r_1$ und wiederhole Schritt 2 mit diesen.

Rückwärtseinsetzen liefert eine Darstellung $ggT(a,b) = xa + yb$.

Beweis wie in $\mathbb{Z}$.

Bsp: Wir berechnen in $\mathbb{Z}[i]$ den ggT von $3+4i$ und $-1+12i$

$$\frac{-1+12i}{3+4i} = \frac{(-1+12i)(3-4i)}{9+16} = \frac{45+40i}{25}$$

$$\left|2 - \frac{45}{25}\right| = \left|\frac{5}{25}\right| = \left|\frac{1}{5}\right| \leq 1/2$$

$$\left|2 - \frac{40}{25}\right| = \left|\frac{10}{25}\right| = \left|\frac{2}{5}\right| \leq 1/2$$

$\Rightarrow (-1+12i) = (2+2i)(3+4i) + r$

mit $r = (-1+12i) - (2+2i)(3+4i) =$

$(-1+12i) - (-2+14i) = 1-2i$

$1-2i \neq 0$, weiter:

$$\frac{3+4i}{1-2i} = \frac{(3+4i)(1+2i)}{5} = \frac{-5+10i}{5} = -1+2i$$

$\Rightarrow (3+4i) = (-1+2i)(1-2i) + 0$

$\Rightarrow ggT(3+4i, -1+12i) = 1-2i$

Dies ist nur eindeutig bis auf

Einheiten $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Andere ggT sind $-1+2i$, $2+i$, $-2-i$.

3.8 Der Chinesische Restsatz

3.8.1 Def Sei R ein kommutativer Ring mit 1, I_1, I_2 Ideale in R.
Wir definieren die Summe
$$I_1 + I_2 = \{a + b \mid a \in I_1, b \in I_2\}$$
und das Produkt
$$I_1 \cdot I_2 = \langle ab \mid a \in I_1, b \in I_2 \rangle,$$
das sind jeweils Ideale in R.

3.8.2 Def

I_1, I_2 heißen koprim $:\Longleftrightarrow$
$$I_1 + I_2 = \langle 1 \rangle$$

Bsp

1) Für Hauptideale $I_1 = \langle a \rangle$, $I_2 = \langle b \rangle$ gilt
$$I_1 + I_2 = \langle a, b \rangle$$
$$I_1 \cdot I_2 = \langle a \cdot b \rangle$$

2) Sei R ein Hauptidealring.
$\langle a \rangle, \langle b \rangle$ sind koprim $\Longleftrightarrow$

$\text{ggT}(a,b) = 1$ (Satz 3.6.5) $\Longleftrightarrow$

$\text{kgV}(a,b) = a \cdot b \Longleftrightarrow$

$\langle a \rangle \cdot \langle b \rangle = \langle ab \rangle = \langle \text{kgV}(a,b) \rangle$

$= \langle a \rangle \cap \langle b \rangle$

<u>3.8.3 Satz</u> (Chinesischer Restsatz)

Sei R ein kommutativer Ring mit 1, $I_1, \dots, I_r$ paarweise koprime Ideale. Dann ist

$$\varphi : R \longrightarrow R/I_1 \times \dots \times R/I_r$$

$$a \longmapsto ([a], \dots, [a]) = (a + I_1, \dots, a + I_r)$$

surjektiv, $\text{Ker}\,\varphi = I_1 \cap \dots \cap I_r = I_1 \cdot \dots \cdot I_r$.

Insbesondere

$$R/_{I_1 \cap \dots \cap I_r} \cong R/I_1 \times \dots \times R/I_r$$

Erinnerung Satz 1.8, Chinesischer Restsatz für $\mathbb{Z}$:

$n_1, \dots, n_r$ paarweise teilerfremd

$\Longleftrightarrow \langle n_1 \rangle, \dots, \langle n_r \rangle$ paarweise koprim dann ist $x \equiv a_1 \mod n_1, \dots, x \equiv a_r \mod n_r$ für $a_1, \dots, a_r \in \mathbb{Z}$ lösbar und die Lösung ist eindeutig mod $n_1 \cdots n_r$

$$\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}/\langle n_1 \rangle \times \dots \times \mathbb{Z}/\langle n_r \rangle$$
$$a \longmapsto ([a], \dots, [a])$$
$$= (a_1, \dots, a_r)$$

φ surjektiv $\Rightarrow \exists$ Lösung $a \in \mathbb{Z}$.

Eindeutig mod $n_1 \cdots n_r \Leftrightarrow$

$$\mathbb{Z}/(n_1 \cdots n_r) \cong \mathbb{Z}/\langle n_1 \rangle \times \dots \times \mathbb{Z}/\langle n_r \rangle$$

ist Isomorphismus. Hier $\langle n_1 \rangle \cap \dots \cap \langle n_r \rangle = \langle n_1 \cdots n_r \rangle$.

<u>Beweis:</u> Sei $a_i + I_i \in R/I_i \;\forall i$,

wir suchen $a \in R$ mit

$a + I_i = a_i + I_i \;\forall i$.

N.V. $\exists\; s_{ij} \in I_i,\; t_{ij} \in I_j$:

$$s_{ij} + t_{ij} = 1$$

Betrachte $k_j = \prod_{i \neq j} s_{ij} = \prod_{i \neq j} (1 - t_{ij})$.

Es gilt $k_j \in I_i \;\forall i \neq j$,

$k_j \in 1 + I_j$.

Setze $a = \sum_{j=1}^{r} a_j k_j$, dann ist

$a + I_j = \sum_{\ell=1}^{r} a_\ell k_\ell + I_j = a_j k_j + I_j$

$= (a_j + I_j)(k_j + I_j) = (a_j + I_j)(1 + I_j) =$

$a_j + I_j$

$\Rightarrow \varphi$ ist surjektiv.

$\ker \varphi = I_1 \cap \dots \cap I_r$ klar.

Noch zz: $I_1 \cap \dots \cap I_r = I_1 \cdot \ldots \cdot I_r$

„$\supset$" klar

„$\subset$" Induktion nach r.

IA: $r = 2$: $s_{12} + t_{12} = 1$, $s_{12} \in I_1$, $t_{12} \in I_2$.

Sei $k \in I_1 \cap I_2 \Rightarrow$

$k \cdot 1 = k(s_{12} + t_{12}) = k \cdot s_{12} + k \cdot t_{12} \in I_1 \cdot I_2$

IV: es gelte $I_1 \cap \dots \cap I_{r-1} = I_1 \cdot \dots \cdot I_{r-1}$.

IS: $r \geq 2$: $s_{ir} \in I_i$, $t_{ir} \in I_r$:

$s_{ir} + t_{ir} = 1$. Dann ist

$$1 = \prod_{i=1}^{r-1} (s_{ir} + t_{ir})$$

$$= \underbrace{s_{1r} \cdots s_{r-1r}}_{\in I_1 \cdot \dots \cdot I_{r-1}} + \underbrace{t_{1r} \cdots + t_{2r} \cdots}_{\in I_r}$$

$\Rightarrow I_1 \cdot \dots \cdot I_{r-1}$, I_r sind koprim

Mit dem IA erhalten wir

$$(I_1 \cdot \dots \cdot I_{r-1}) \cdot I_r = (I_1 \cdot \dots \cdot I_{r-1}) \cap I_r$$

$$\overset{IV}{=} (I_1 \cap \dots \cap I_{r-1}) \cap I_r$$

$\square$

<u>Bsp</u> $R = K[X]$, $u_1, \dots, u_n \in K$ paarweise verschieden. Setze $f_i = X - u_i \in K[X]$, die f_i sind paarweise teilerfremd.

Für $c_1, \dots, c_n \in K$ gibt es mit dem chinesischen Restsatz daher ein $g \in K[X]$:

$g \equiv c_i \mod (x-u_i) \iff$

$g(u_i) - c_i = 0 \iff g(u_i) = c_i$.

g ist dabei eindeutig mod $f = \prod f_i$,

dividiere g mit Rest durch f und

erhalte den Rest g' mit

$\deg(g') < n$, $g'(u_i) = c_i \ \forall i$.

Da $K[x]$ euklidisch ist, können

wir die s_{ij}, t_{ij} aus dem Beweis

des chinesischen Restsatzes bestimmen

und damit ist der Beweis

konstruktiv wie in $\mathbb{Z}$.

Wir setzen $\hat{f}_i = \prod_{j \neq i} f_j = \prod_{j \neq i} x - u_j$

Dann ist

$$\hat{f}_i \cdot \prod_{j \neq i} \frac{1}{u_i - u_j} = \prod_{j \neq i} \frac{x-u_j}{u_i - u_j} = \begin{cases} 1 \mod x-u_i \\ 0 \mod x-u_j \end{cases}$$

Damit gilt

$$g' = \sum_{i=1}^{n} c_i \prod_{j \neq i} \frac{x-u_j}{u_i-u_j}.$$

Dieses Polynom löst das Lagrange'sche Interpolationsproblem:

3.8.4 Satz (Lagrangescher Interpolationssatz)

Seien $u_1, \dots, u_n \in K$ paarweise verschieden, $c_1, \dots, c_n \in K$, dann

$\exists!\ g \in K[x]$, $\deg g < n$, $g(u_i) = c_i \ \forall i$.

3.9 Übersicht

nullteilerfreie Ringe $\qquad K[x,y,z,w]/\langle xy-zw\rangle$, $\mathbb{Z}[\sqrt{-3}]$

$\cup$

Noethersch, nicht faktoriell: $\mathbb{Z}[i\sqrt{5}]$

Faktoriell, nicht noethersch: $K[x_1, x_2, \dots]$

Faktorielle Ringe $\qquad K[x_1, \dots, x_n]$, $\mathbb{Z}[x]$

($\langle 2, x\rangle$ ist kein Hauptideal)

(ohne Beweis: Satz von Gauß: R faktoriell $\Rightarrow$ $R[x]$ faktoriell)

Noethersche Ringe $\qquad K[x_1, \dots, x_n]$

$\cup$

Hauptidealringe $\qquad \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$

$\cup$ $\qquad$ (ohne Beweis)

euklidische Ringe

$\mathbb{Z}$, $\mathbb{Z}[i]$, $K[x]$