Erinnerung:

Definition: Ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist, heisst ein *Hauptidealring*.

Satz: Jeder Hauptidealring ist faktoriell.

4.4.6 Satz: *(Chinesischer Restsatz)* Seien $a_1, \ldots, a_n$ paarweise teilerfremde Elemente eines Hauptidealrings R. Dann ist die folgende Abbildung ein Ring-Isomorphismus:

$$\begin{array}{ccc} R/(a_1 \cdots a_n) & \longrightarrow & R/(a_1) \times \ldots \times R/(a_n), \\ x + (a_1 \cdots a_n) & \mapsto & \big(x + (a_1), \ldots, x + (a_n)\big). \end{array}$$

Beweis: $n=0$ $n=1$ ✓

$n=2$: Wähle $u_1, u_2 \in R$ mit $u_1 a_1 + u_2 a_2 = 1$.

Beh': Die Abb. $R/(a_1 a_2) \longleftarrow R/(a_1) \times R/(a_2)$

$u_2 a_2 x_1 + u_1 a_1 x_2 + (a_1 a_2) \longleftarrow (x_1 + (a_1), x_2 + (a_2))$

ist eine beidseitige Inverse.

Beweis: Wohldefiniertheit: Ändere x_1 um $y_1 a_1 \Rightarrow$ Ändere linke Seite um $u_2 a_2 y_1 a_1$ ✓

" — x_2 — $y_2 a_2 \Rightarrow u_1 a_1 y_2 a_2$ ✓

Die Abb ist eine Rechtsinverse: $x + (a_1 a_2) \longmapsto (x + (a_1), x + (a_2))$

$\swarrow$

$u_2 a_2 x + u_1 a_1 x + (a_1 a_2)$

$= \underbrace{(u_2 a_2 + u_1 a_1)}_{=1} x + (a_1 a_2)$

Die Abb ist eine Linksinverse: $(x_1 + (a_1), x_2 + (a_2)) \mid$

$\swarrow$

$u_2 a_2 x_1 + u_1 a_1 x_2 + (a_1 a_2) \mid \rightarrow (u_2 a_2 x_1 + \cancel{u_1 a_1 x_2} + (a_1),$

$\cancel{u_2 a_2} x_1 + u_1 a_1 x_2 + (a_2))$

$= ((1 - a_1 u_1) x_1 + (a_1),$

$(1 - a_2 u_2) x_2 + (a_2)) \mid$

$= (x_1 + (a_1), x_2 + (a_2)) \mid .$

Also gilt die Bch, somit ist die Abb aus dem ch. Restsatz bijektiv.
$\Rightarrow$ Also ist sie ein Isomorphismus.

$n \geq 3 \Rightarrow a_1, \dots, a_n$ teilerfremd $\Rightarrow a_1 \cdots a_{n-1}, a_n$ teilerfremd

$$\Rightarrow \quad \frac{R}{\cancel{(a_1, \dots, a_n)}\ (a_1 \cdots a_n)} \xrightarrow{\sim} \frac{R}{(a_1 \cdots a_{n-1})} \times \frac{R}{(a_n)}$$

$$\downarrow ?$$

$$\vdots$$

$$\xrightarrow{\sim} \frac{R}{(a_1)} \times \cdots \times \frac{R}{(a_n)} \qquad \square$$

4.5 Euklidische Ringe

4.5.1 Definition: Ein *euklidischer Ring* ist ein Integritätsbereich R zusammen mit einer Abbildung $\delta\colon R \setminus \{0\} \to \mathbb{Z}^{\geqslant 0}$, so dass gilt

$$\forall a \in R\ \forall b \in R \setminus \{0\}\colon\ \exists q, r \in R;\ \ a = bq + r \text{ und } (r = 0 \text{ oder } \delta(r) < \delta(b)).$$

Dieser Prozess heisst *Division mit Rest*, nämlich *Division von a durch b mit Quotient q und Rest r*. Die Funktion δ misst die Grösse oder Komplexität eines Elements.

4.5.2 Satz: Jeder euklidische Ring ist ein Hauptidealring.

Bew: Sei $I \lhd R$ ein Ideal.
Wenn $I = (0)$ ist, so ist I ein Hauptid. Sei also $I \neq (0)$.
Nehme jetzt ein $d \in I$, sodass $\delta(d)$ minimal ist.
(Warum geht das? $\delta: R\setminus\{0\} \to \mathbb{Z}_{\geq 0}$)
Sei nun $e \in I$. Wir wenden Div. mit Rest auf (e,d)
Also ex. $q, r \in R$: $e = d\cdot q + r$.
1. Fall: $r \neq 0$, dann ist $\delta(r) < \delta(d)$. ↯
2. Fall: $r = 0$, dann ist $e = d\cdot q$, also $e \in (d)$
$\Rightarrow I \subseteq (d)$
$\Rightarrow I = (d)$.

4.5.3 Beispiel: Der Ring $\mathbb{Z}$ ist euklidisch mit der Funktion $\delta(a) := |a|$.

(a) Seine Ideale sind genau die Ideale $(n) = n\mathbb{Z}$ für alle $n \geqslant 0$.

(b) Die maximalen Ideale von $\mathbb{Z}$ sind die (p) für alle Primzahlen p, mit dem zugehörigen Restklassenkörper $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

(c) Das einzige weitere Primideal von $\mathbb{Z}$ ist das Nullideal (0).

(d) Die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ besteht aus den Restklassen $a+n\mathbb{Z}$ für alle zu n teilerfremden Zahlen a.

4.5.4 Beispiel: Für jeden Körper K ist $K[X]$ euklidisch mit der Funktion $\delta(f) := \deg(f)$.

4.5.5 Beispiel: Für eine natürliche Zahl $d \geqslant 1$ ist der Ring $\mathbb{Z}[i\sqrt{d}]$ euklidisch, bzw. ein Hauptidealring, bzw. faktoriell genau dann, wenn $d \leqslant 2$ ist. Die Funktion $\delta(a + i\sqrt{d} \cdot b) := a^2 + db^2$ erfüllt dann die gewünschte Bedingung.

$d=1$: $\delta(5 + i \cdot 6) = 25 + 36 = 61$

4.5.6 Vorsicht: Nicht jeder Hauptidealring lässt sich zu einem euklidischen Ring machen. Zum Beispiel ist $\mathbb{Z}\left[\frac{1}{2} \cdot (1 + i\sqrt{163})\right]$ ein Hauptidealring, aber nicht euklidisch.

4.5.7 Euklidischer Algorithmus: Sei (R, δ) euklidisch und betrachte Elemente $a_1, a_2 \in R$, nicht beide gleich Null. Wir setzen diese fort zu einer Folge $a_1, \ldots, a_n$ wie folgt. Ist das letzte konstruierte Element a_n gleich Null, so halte an. Andernfalls benutze Division mit Rest und schreibe $a_{n-1} = a_n q_n + a_{n+1}$ mit $a_{n+1} = 0$ oder $\delta(a_{n+1}) < \delta(a_n)$.

4.5.8 Proposition: Dieser Algorithmus endet nach endlich vielen Schritten, und für das letzte von Null verschiedene Element a_{m-1} gilt

$$a_{m-1} \sim \mathrm{ggT}(a_1, a_2).$$

Beweis: 1) $\delta : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$

2) Beh: $\mathrm{ggT}(a_n, a_{n+1}) \sim \mathrm{ggT}(a_{n+1}, a_{n+2})$ ✓

$a_n = a_{n+1} q_{n+1} + a_{n+2}$

$a_{n+2} = a_n - a_{n+1} \cdot q_{n+1}$

Sei N sodass $a_N = 0$ ✓ $\quad m = N$

$\mathrm{ggT}(a_{N-1}, a_N) \sim \mathrm{ggT}(a_{N-1}, 0) \sim a_{N-1}$

4.5.9 Bemerkung: Der euklidische Algorithmus produziert zusätzlich Elemente $u_n, v_n \in R$ mit $a_n = u_n a_1 + v_n a_2$, für alle $n \geqslant 1$, nämlich durch $(u_1, v_1) := (1, 0)$ und $(u_2, v_2) := (0, 1)$ und $(u_{n+1}, v_{n+1}) := (u_{n-1} - u_n q_n, v_{n-1} - v_n q_n)$, für alle $n \geqslant 2$. Für das letzte von Null verschiedene Element a_{m-1} liefert dies eine Linearkombination

$$\mathrm{ggT}(a_1, a_2) \sim a_{m-1} = u_{m-1} a_1 + v_{m-1} a_2.$$

4.5.8.: $ggt(a_{N-1}, a_N) \sim ggt(a_{N-2}, a_{N-1}) \sim \dots \sim ggt(a_1, a_2)$. $\square$

$\forall a \in R \forall b \in R \setminus \{0\} \exists q, r \in R : a = b \cdot q + r$ und $(r = 0$ oder $\delta(r) < \delta(b))$

4.5.10 Beispiel: (a) In $\mathbb{Z}$ ist $\mathrm{ggT}(2022, 1959) \sim 3 = 311 \cdot 2022 - 321 \cdot 1959$.

$(u_1, v_1) := (1, 0)$

$(u_2, v_2) := (0, 1)$

1) $a_1 = 2022, a_2 = 1959$

$a_1 = 2022 = 1959 \cdot 1 + 63$

$a_2 = 1959 = 63 \cdot q_3 + r_3$

$= 63 \cdot 31 + 6$

$(u_3, v_3) = (1 - 0, 0 - 1 \cdot 1)$

$= (1, -1)$

$n=3 \quad (u_4, v_4) = (0 - 1 \cdot 31, 1 - (-1) \cdot 31)$

$= (-31, 32)$

(b) In $\mathbb{Q}[X]$ ist $\mathrm{ggT}(X^{15} + 1, X^6 - 1) \sim X^3 + 1 = (X^{15} + 1) - (X^9 + X^3)(X^6 - 1)$.

$a_3 = 63 = 6 \cdot q_4 + r_4$

$= 6 \cdot 10 + 3$

$n=4 \quad (u_5, v_5) = (1 - (-31) \cdot 10, -1 - 32 \cdot 10)$

$= (311, -321)$

$6 = 3 \cdot 2 + 0$