Erinnerung: $p \sim q \iff \exists u \in R^\times : q = pu.$

4.2.6 Proposition: Sei R faktoriell, und sei $\{p_i \mid i \in I\}$ ein Repräsentantensystem seiner Primelemente unter Assoziiertheit.

(a) Jedes Element von $R \smallsetminus \{0\}$ kann man auf eindeutige Weise schreiben in der Form

$$\boxed{a \;=\; u \cdot \prod_{i\in I}{}' \, p_i^{\mu_i}}$$

für eine Einheit $u \in R^\times$ und Exponenten $\mu_i \in \mathbb{Z}^{\geqslant 0}$, fast alle gleich 0.

(b) Für $a = u \cdot \prod'_{i\in I} p_i^{\mu_i}$ und $b = v \cdot \prod'_{i\in I} p_i^{\nu_i}$ mit $u, v \in R^\times$ gilt $a|b$ genau dann, wenn für alle i gilt $\mu_i \leqslant \nu_i$.

(c) Jedes Element von $\mathrm{Quot}(R) \smallsetminus \{0\}$ kann man auf eindeutige Weise schreiben in der Form

$$\boxed{a \;=\; u \cdot \prod_{i\in I}{}' \, p_i^{\mu_i}}$$

für eine Einheit $u \in R^\times$ und Exponenten $\mu_i \in \mathbb{Z}$, fast alle gleich 0.

4.3 Grösster gemeinsamer Teiler

Sei R faktoriell.

4.3.1 Proposition-Definition: Betrachte Elemente $a_1, \ldots, a_n \in R$.

(a) Ein Element $b \in R$ mit $\forall i\colon b|a_i$ heisst ein *gemeinsamer Teiler von $a_1, \ldots, a_n$*.

(b) Es existiert ein gemeinsamer Teiler b von $a_1, \ldots, a_n$, so dass für jeden gemeinsamen Teiler b' von $a_1, \ldots, a_n$ gilt $b'|b$.

(c) Dieser *grösste gemeinsame Teiler von $a_1, \ldots, a_n$* ist eindeutig bis auf Assoziiertheit. Wir bezeichnen jeden solchen mit $\mathrm{ggT}(a_1, \ldots, a_n)$.

Da der ggT nur eindeutig bis auf Assoziiertheit ist, sollte man ihn immer nur auf Assoziiertheit testen und nicht auf Gleichheit.

Beweis: Jedes $a_j = 0$ können wir ignorieren. Wähle Rep. Syst. $\{p_i \mid i \in I\}$ wie oben.

Jedes $0 \neq a_j = u_j \cdot \prod'_{i \in I} p_i^{\mu_{ij}}$ mit $u_j \in R^\times$, $\mu_{ij} \in \mathbb{Z}^{\geq 0}$, fast alle 0.

Sind alle $a_j = 0$, dann tut es $b = 0$.

Sonst ist jeder gemeinsame Teiler $b' \neq 0$, und $b' = v \cdot \prod_{i \in I} p_i^{\nu_i}$ mit $\forall j\colon \nu_i \leq \mu_{ij}$.

Setze $b := \prod_{i \in I} p_i^{\min\{\mu_{ij} \mid 1 \leq j \leq n\}}$.

Das tut's $\Rightarrow$ (b).

(c) Seien b, b' grösste gemeinsame Teiler. Dann ist $b'|b$ und $b|b'$ $\Rightarrow$ $b \sim b'$.

qed.

4.3.2 Proposition: Für alle $a_1, \ldots, a_n, x_1, \ldots, x_n \in R$ gilt

$$\mathrm{ggT}(a_1, \ldots, a_n) \sim \mathrm{ggT}(a_1, \ldots, a_n, \textstyle\sum_{i=1}^n x_i a_i).$$

Bew.: Jeder gemeinsame Teiler von $a_1, \ldots, a_n$ teilt auch $\sum_i x_i a_i$.
Also sind die gemeinsamen Teiler auf beiden Seiten die gleichen,
$\Rightarrow$ ebenso der ggT. qed.

Folge: $\mathrm{ggT}(a_1, \ldots, a_n) = \mathrm{ggT}(a_1, \ldots, a_{n-1}, a_n + \sum_{i=1}^{n-1} x_i a_i)$.

4.3.3 Definition: Elemente $a_1, \ldots, a_n \in R$ mit

(a) $\mathrm{ggT}(a_1, \ldots, a_n) \sim 1$ heissen *teilerfremd.*

(b) $\mathrm{ggT}(a_i, a_j) \sim 1$ für alle $i \neq j$ heissen *paarweise teilerfremd.*

Bsp.: $6, 10, 15 \in \mathbb{Z}$ sind teilerfremd,
aber nicht paarweise teilerfremd.

4.3.4 Proposition-Definition: Betrachte Elemente $a_1, \ldots, a_n \in R$.

(a) Ein Element $b \in R$ mit $\forall i\colon a_i | b$ heisst *gemeinsames Vielfaches von $a_1, \ldots, a_n$*.

(b) Es existiert ein gemeinsames Vielfaches b von $a_1, \ldots, a_n$, so dass für jedes gemeinsame Vielfache b' von $a_1, \ldots, a_n$ gilt $b|b'$.

(c) Dieses *kleinste gemeinsame Vielfache von $a_1, \ldots, a_n$* ist eindeutig bis auf Assoziiertheit. Wir bezeichnen jedes solche mit $\mathrm{kgV}(a_1, \ldots, a_n)$.

4.3.5 Proposition: Für alle $a, a_1, \ldots, a_n \in R$ gilt

$$\begin{aligned} \mathrm{ggT}(aa_1, \ldots, aa_n) &\sim a \cdot \mathrm{ggT}(a_1, \ldots, a_n), \\ \mathrm{kgV}(aa_1, \ldots, aa_n) &\sim a \cdot \mathrm{kgV}(a_1, \ldots, a_n). \end{aligned}$$

Beweis: Seien $a_j = u_j \prod_{i \in I} p_i^{r_{ij}}$ wie in 4.3.1

Ist $a = 0$, so gilt $\mathrm{ggT}(0, \ldots, 0) \sim 0 \sim 0 \cdot \mathrm{ggT}(\ldots)$

Sei $0 \neq a = u \cdot \prod_i p_i^{r_i}$

$\Rightarrow a a_i = u_i u \prod p_i^{r_i + r_{ij}}$

$\Rightarrow \mathrm{ggT}(aa_1, \ldots, aa_n) \sim \prod_i p_i^{\min\{r_i + r_{ij} \mid j\}}$

$= \underbrace{\prod_i p_i^{r_i}}_{\sim\, a} \cdot \underbrace{\prod_i p_i^{\min\{r_{ij} \mid j\}}}_{\sim\, \mathrm{ggT}(a_1, \ldots, a_n)}$.

kgV analog. qed.

4.3.6 Proposition: Für alle $a_1, a_2 \in R$ gilt

$$\mathrm{ggT}(a_1, a_2) \cdot \mathrm{kgV}(a_1, a_2) \sim a_1 \cdot a_2.$$

Beweis: Ist $a_1 = 0$, ist $\mathrm{ggT}(a_1, a_2) \sim a_2$ und $\mathrm{kgV}(a_1, a_2) \sim 0$ und $a_2 \cdot 0 = 0 \cdot a_2$. ✓

Analog falls $a_2 = 0$

Sind $a_1, a_2 \neq 0$, so ist $\mathrm{ggT}(a_1, a_2) \sim \prod_i p_i^{\min\{r_{i1}, r_{i2}\}}$

$\mathrm{kgV}(a_1, a_2) \sim \prod_i p_i^{\max\{r_{i1}, r_{i2}\}}$

$\Rightarrow \mathrm{ggT}(a_1, a_2) \cdot \mathrm{kgV}(a_1, a_2) \sim \prod_i p_i^{r_{i1} + r_{i2}} \sim a_1 \cdot a_2$.

$\forall i : \min\{r_{i1}, r_{i2}\} + \max\{r_{i1}, r_{i2}\} = r_{i1} + r_{i2}$

qed.

4.4 Hauptidealringe

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

4.4.2 Beispiel: Für jeden Körper K ist $K[[X]]$ ein Hauptidealring. Genauer sind seine Ideale das Nullideal (0) sowie die Ideale (X^n) für alle $n \geqslant 0$.

Erinnerung: $K[[X]]^\times = \{ \sum_{i \geq 0} a_i X^i \mid a_i \in K, \ a_0 \neq 0 \}$.

Jedes $0 \neq f \in K[[X]]$ ist gleich $X^n \cdot g$ für $n \geq 0$ und $g \in K[[X]]^\times$.

Sei $\mathfrak{a} \subset K[[X]]$ ein Ideal. Ist $\mathfrak{a} \neq 0$, wähle n maximal, so dass für alle $f \in \mathfrak{a}$ gilt $X^n \mid f$. Dann enthält $\mathfrak{a}$ ein $f \in X^n \cdot K[[X]]^\times$ $\Rightarrow X^n \in \mathfrak{a}$ und $\mathfrak{a} = (X^n)$.

4.4.3 Satz: Sei R ein Hauptidealring.

(a) Jede aufsteigende Folge von Idealen $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \ldots$ wird stationär, das heisst, es existiert $n_0 \geqslant 0$ mit $\mathfrak{a}_n = \mathfrak{a}_{n_0}$ für alle $n \geqslant n_0$. (Ein Ring mit dieser Eigenschaft heisst *noethersch.*) Emmy Noether.

(b) Für jedes $a \in R \setminus (\{0\} \cup R^\times)$ existiert ein Primelement $p \in R$ mit $p|a$.

(c) Der Ring R ist faktoriell.

Bew.: (a) $\mathfrak{a} := \bigcup_{n \geq 0} \mathfrak{a}_n$ ist ein Ideal.

Schreibe $\mathfrak{a} = (a)$ für ein $a \in R$.

Wähle $n \geq 0$ mit $a \in \mathfrak{a}_n$.

Dann ist $\mathfrak{a} = (a) \subset \mathfrak{a}_n \subset \mathfrak{a} \Rightarrow \mathfrak{a} = \mathfrak{a}_n$

und $\mathfrak{a} = \mathfrak{a}_n = \mathfrak{a}_{n+1} = \ldots = \mathfrak{a}$.

(b) Es ist $(a) \subsetneqq R$. Krull $\Rightarrow \exists$ max. Ideal $(a) \subset \mathfrak{m} \subsetneqq R$. Schreibe $\mathfrak{m} = (p)$ für ein $p \in R$.

Dann ist $R/(p) = R/\mathfrak{m}$ ein Körper $\Big\} \Rightarrow p$ prim.
$(a) \neq 0 \Rightarrow \mathfrak{m} \neq (0) \Rightarrow p \neq 0$

Wegen $a \in \mathfrak{m} = (p)$ ist $p \mid a$.

(c) Sei $a \in R \setminus \{0\}$.

Konstruiere Folge $a = a_0, a_1, \ldots, a_n \in R \setminus \{0\}$ wie folgt:

Wenn a_n gegeben ist: Ist $a_n \in R^\times \longrightarrow$ Stop.

Sonst wähle nach (b) ein Primelement p_{n+1} und $\boxed{a_n = a_{n+1} \cdot p_{n+1}}$ für ein $a_{n+1} \in R \setminus \{0\}$.

Damit ist $(a_n) \subset (a_{n+1})$. Wäre $(a_n) = (a_{n+1})$, dann wäre $a_{n+1} = \kappa a_n$ für ein $\kappa \in R$

$\Rightarrow \quad a_n = a_{n+1} p_{n+1} = a_n \kappa p_{n+1}$.

Also ist $(a_n) \subsetneq (a_{n+1})$.

$a_n \neq 0 \Rightarrow 1 = \kappa p_{n+1} \Rightarrow p_{n+1} \in R^\times$ $\lightning$

da p_{n+1} prim.

Nach (a) kann nicht immer der zweite Fall eintreten,

also $\exists n$: $a_n \in R^\times$.

$$a_0 = a_1 p_1 = a_2 p_2 p_1 \cdots = \underset{\in R^\times}{a_n} \cdot \overbrace{p_n \cdots p_1}^{\text{prim}}$$

<u>qed.</u>

4.4.4 Proposition: Ist R ein Hauptidealring, so gilt für alle $a_1, \dots, a_n \in R$

$$(\mathrm{ggT}(a_1, \dots, a_n)) = (a_1, \dots, a_n).$$

Insbesondere existieren $x_1, \dots, x_n \in R$ mit

$$\mathrm{ggT}(a_1, \dots, a_n) = x_1 a_1 + \dots + x_n a_n.$$

Bew.: Schreibe $(a_1, \dots, a_n) = (a)$.
Dann ist $\forall i$: $a_i \in (a) \Rightarrow a \mid a_i$
Und $a = \sum_i x_i a_i$ für $x_i \in R$.

$$\Rightarrow \mathrm{ggT}(a_1, \dots, a_n) \overset{4.3.2}{=} \mathrm{ggT}(a_1, \dots, a_n, a) \overset{4.3.2}{=} \mathrm{ggT}(a) \sim a.$$

qed.

4.4.5 Bemerkung: Nicht jeder faktorielle Ring ist ein Hauptidealring. Zum Beispiel ist für jeden Körper K der Ring $K[X, Y]$ faktoriell, aber sein Ideal (X, Y) ist kein Hauptideal. In diesem Fall ist $\mathrm{ggT}(X, Y) \sim 1$, aber $(X, Y) \neq (1)$. Der ggT lässt sich hier nicht als Linearkombination von X und Y darstellen.

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:

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

wohldef, da $(a_1 \cdots a_n) \subset (a_i)$
Ringhom.

Der älteste bekannte Beleg dieses Satzes ist eine mathematische Veröffentlichung in China im 5. Jahrhundert unserer Zeitrechnung. Gemäss einer Legende benutzte ein chinesischer General den Satz für $R = \mathbb{Z}$, um seine Soldaten zu zählen. Er liess sie in Reihen von $a_1 := 19$ aufstellen und erhielt den Rest 1, in Reihen von $a_2 := 17$ mit dem Rest 14, sowie in Reihen von $a_3 := 12$ mit dem Rest 1. Da er auch die ungefähre Grössenordnung wusste, konnte er die Gesamtzahl bestimmen, nämlich 3193 gegenüber $19 \cdot 17 \cdot 12 = 3876$.

Computeralgebrasysteme benutzen den chinesischen Restsatz, um eine Rechnung mit grossen Zahlen in $\mathbb{Z}$ durch mehrere voneinander unabhängige Rechnungen in endlichen Körpern $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ zu ersetzen. Je nach Situation kann das den Rechenaufwand deutlich verringern; ausserdem eignet sich die Methode gut für parallele Programmierung.