Algebraische Zahlentheorie I

Prof. Dr. Alexander Schmidt

Wintersemester 2021/22

Inhaltsverzeichnis

0tens: Begriffe aus der Algebra:

- Ring, hier immer kommutativ mit 1
- R-Modul, $R \times M \to M$
- Ideal: $\mathfrak{a} \subset R$, R-Untermodul
- $x \in R \rightsquigarrow (x) = Rx = \{rx \mid r \in R)$ das von x erzeugte Hauptideal
- R heißt nullteilerfrei: wenn $xy = 0 \Rightarrow x = 0$ oder $y = 0$
- Einheitengruppe: $R^\times = \{r \in R \mid \exists\, s \in R : rs = 1\}$
- R nullteilerfrei: $(x) = (y) \iff x = ey$, $e \in R^\times$
- $\mathfrak{p} \subset R$ heißt Primideal $\iff R/\mathfrak{p}$ nullteilerfrei
- $\mathfrak{m} \subset R$ Maximalideal $\iff R/\mathfrak{m}$ Körper
- $f : R \to R'$ Ringhomomorphismus und $\mathfrak{p}' \subset R'$ Primideal $\Rightarrow f^{-1}(\mathfrak{p}') \subset R'$ Primideal (gilt nicht für Maximalideal).
- jeder Ring $\neq 0$ besitzt ein Maximalideal
- jedes Ideal $\neq R$ ist in einem Maximalideal enthalten
- jede Nichteinheit ist in einem Maximalideal enthalten
- $a, b \in R$, $a \mid b \overset{\text{df}}{=}$ es existiert ein $c \in R$ mit $ac = b \iff (b) \subset (a)$
- $a \mathrel{\hat{=}} b$ (assoziiert) $\overset{\text{df}}{=} a \mid b$ und $b \mid a \iff (a) = (b)$, R nullteilerfrei: $a \mathrel{\hat{=}} b \iff a = be$, $e \in R^\times$.

Definition 0.1. Sei R nullteilerfrei und $a, b \in R$. Ein Element $d \in R$ heißt **größter gemeinsamer Teiler** von a und b, wenn gilt

(i) $d \mid a$ und $d \mid b$
(ii) $(e \mid a$ und $e \mid b)) \Rightarrow e \mid d$.

Der ggT ist, wenn er existiert, bis auf Assoziiertheit eindeutig.

Definition 0.2. R heißt **Hauptidealring** wenn R nullteilerfrei ist, und jedes Ideal in R ist ein Hauptideal.

Bemerkung 0.3. Ist R ein Hauptidealring so existiert der ggT und es gilt

$$(a) + (b) = (\mathrm{ggT}(a, b)).$$

Insbesondere läßt sich $\mathrm{ggT}(a, b)$ linear aus a und b kombinieren. (Erinnerung: $\mathfrak{a} + \mathfrak{b} = \{\alpha + \beta \mid \alpha \in \mathfrak{a},\ \beta \in \mathfrak{b}\}$

Begründung: $(a)+(b) = (d)$ für ein $d \in R$, weil R Hauptidealring. Es gilt also $d|a$, $d|b$. Gilt nun $e|a$ und $e|b$, so folgt $(a) \subset (e)$ und $(b) \subset (e)$ also $(d) = (a) + (b) \subset (e) \Rightarrow e|d$ □

Definition 0.4. Ein nullteilerfreier Ring R heißt **euklidisch**, wenn es eine Funktion $\nu : R \setminus \{0\} \to \mathbb{N}$ gibt, so dass zu $a, b \in R$, $b \neq 0$ stets $q, r \in R$ mit $a = qb + r$ und $r = 0$ oder $\nu(r) < \nu(b)$ gibt $\rightsquigarrow$ erhalten („Euklidischen“) Algorithmus zur Bestimmung des ggT.

Satz 0.5. *(LA 2) Jeder euklidische Ring ist ein Hauptidealring.*

Definition 0.6. R nullteilerfrei $\pi \in R \setminus (\{0\} \cup R^\times)$ heißt

- Primelement, wenn (π) Primideal
- irreduzibel, falls $\pi = ab \Rightarrow a \in R^\times$ oder $b \in R^\times$.

Bemerkung 0.7. Primelemente sind irreduzibel

Grund: $\pi = ab \Rightarrow \pi \mid a$ oder $\pi \mid b$. Gelte OE $\pi \mid a$. Wegen $a \mid \pi$ gilt $a \hat{=} \pi$, also $a = \pi u$, $u \in R^\times$. Nun gilt $\pi = ab = \pi ub$, also $\pi(1 - ub) = 0 \Rightarrow 1 = ub \Rightarrow b \in R^\times$.

Definition 0.8. R (nullteilerfrei) heißt **faktoriell**, wenn jedes $a \in R\backslash\{0\}$ eine bis auf Einheiten und Reihenfolge eindeutige Zerlegung in das Produkt irreduzibler Elemente besitzt.

Satz 0.9. *(i) In einem faktoriellen Ring ist jedes irreduzible Element Primelement. (Algebra 1, 2.20)*

(ii) Hauptidealringe sind faktoriell. (LA 2)

(iii) R faktoriell $\Rightarrow R[T]$ faktoriell. (Algebra 1, 2.42)

Sei R ein Ring und $\mathfrak{a} \subset R$ ein Ideal. Die Elemente des Faktorrings $R/\mathfrak{a}$ heißen Restklassen modulo $\mathfrak{a}$. Die Gruppe $(R/\mathfrak{a})^\times$ heißt Gruppe der *primen Restklassen* modulo $\mathfrak{a}$. Für $\mathfrak{a}, \mathfrak{b} \subset R$ gilt

$$\mathfrak{a}\mathfrak{b} \stackrel{df}{=} \left\{ \sum_{\text{endl.}} a_i b_i \mid a_i \in \mathfrak{a},\ b_i \in \mathfrak{b} \right\}.$$

$\mathfrak{a}$ und $\mathfrak{b}$ heißen teilerfremd (auch koprim), wenn $\mathfrak{a} + \mathfrak{b} = (1)$ gilt.

Lemma 0.10. *(Algebra 2, 1.15 (ii)) Es gilt*

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subset \mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}.$$

Insbesondere gilt $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$ falls $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremd sind.

Seien $R_1, \ldots, R_n$ Ringe. Dann ist $R = \prod_{i=1}^{n} R_i$ mit komponentenweiser Addition und Multiplikation ein Ring. Sei R ein Ring und $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subset R$ Ideale. Wir betrachten den Ringhomomorphismus

$$\phi : R \longrightarrow \prod_{i=1}^{n} R/\mathfrak{a}_i$$

der durch $r \mapsto (r + \mathfrak{a}_1, \ldots, r + \mathfrak{a}_n)$ gegeben ist.

Satz 0.11. *(Algebra 2, 1.16)*

(i) *Sind die* $\mathfrak{a}_i$ *paarweise relativ prim, so gilt* $\prod_{i=1}^{n} \mathfrak{a}_i = \bigcap_{i=1}^{n} \mathfrak{a}_i$.

(ii) ϕ *ist surjektiv* $\Longleftrightarrow$ *die* $\mathfrak{a}_i$ *sind paarweise relativ prim.*

(iii) ϕ *ist injektiv* $\Longleftrightarrow \bigcap \mathfrak{a}_i = (0)$.

Als Korollar erhält man:

Chinesischer Restklassensatz: *Seien* $r_1, \ldots, r_n \in R$ *und* $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subset R$ *paarweise teilerfremde Ideale. Dann hat das System von Kongruenzen*

$$\begin{aligned} x &\equiv r_1 \mod \mathfrak{a}_1 \\ &\vdots \\ x &\equiv r_n \mod \mathfrak{a}_n \end{aligned}$$

eine Lösung $x \in R$ *und* x *ist eindeutig bestimmt modulo* $\mathfrak{a}_1 \cdots \mathfrak{a}_n$.

Beweis. Dies ist eine Umformulierung der Tatsache, dass unter den gegebenen Bedingungen $R/(\mathfrak{a}_1 \cdots \mathfrak{a}_n) \longrightarrow \prod_{i=1}^{n} R/\mathfrak{a}_i$ ein Isomorphismus ist. □