Protokoll zur Vorlesung Kryptographie
SS 2025

W. Bley

24. April 2025

1 Algebraische Grundlagen

1.1 Teilbarkeit in Integritätsbereichen

Definition 1.1.1 Sei R ein kommutativer Ring mit 1.

(a) R heißt nullteilerfrei, falls für alle $x, y \in R$ gilt:

$$xy = 0 \implies x = 0 \text{ oder } y = 0.$$

Man nennt dann R auch einen Integritätsbereich.

(b) $u \in R$ heißt Einheit, falls es ein $v \in R$ mit $uv = 1$ gibt. Mit $R^\times$ bezeichnen wir die Menge der Einheiten.

(c) Zwei Elemente $x, y \in R$ heißen assoziiert, falls es eine Einheit $u \in R^\times$ mit $x = uy$ gibt. Wir schreiben dann $x \sim y$.

Satz 1.1.2 *Sei R ein Integritätsbereich und $x, y \in R \setminus \{0\}$. Dann gilt:*

$$x \mid y \text{ und } y \mid x \iff x \sim y.$$

Definition 1.1.3 Sei R ein Integritätsbereich und $x_1, \ldots, x_n \in R$.

1. Ein Element $d \in R$ heißt ggT von $x_1, \ldots, x_n$, falls gilt:
   (a) $d \mid x_i$ für $i = 1, \ldots, n$.
   (b) Für jedes Element $d' \in R$ mit $d' \mid x_i$ für $i = 1, \ldots, n$ gilt $d' \mid d$.

Remark 1.1.4 Zwei ggT sind zueinander assoziiert.

Definition 1.1.5 Ein Integritätsbereich heißt euklidischer Ring, falls es eine Funktion

$$\beta \colon R \setminus \{0\} \longrightarrow \mathbb{N}_0$$

gibt, so daß gilt: Für je zwei Elemente $x, y \in R$, $y \neq 0$, gibt es Elemente $q, r \in R$ so daß

$$x = qy + r \text{ mit } r = 0 \text{ oder } \beta(r) < \beta(y).$$

Satz 1.1.6 *In einem euklidischen Ring R existieren größte gemeinsame Teiler.*

Definition 1.1.7 Eine nicht-leere Teilmenge I eines kommutativen Rings R heißt Ideal, falls gilt:

1. I ist eine additive Untergruppe.

2. Für alle $x \in I, a \in R$ gilt $ax \in I$.

Definition 1.1.8 1. Seien $x_1, \ldots, x_n \in R$. Dann nennt man

$$(x_1, \ldots, x_n) := Rx_1 + \ldots Rx_n = \left\{ \sum_{i=1}^{n} a_i x_i \mid a_i \in R \right\}$$

das von $x_1, \ldots, x_n$ erzeugte Ideal. Für $x \in R$ nennt man (x) das von x erzeugte Hauptideal.

2. Ein Hauptidealring ist ein nullteilerfreier Ring, in dem jedes Ideal ein Hauptideal ist.

Satz 1.1.9 *Jeder euklidische Ring ist ein Hauptidealring.*

Satz 1.1.10 *Sei R ein Integritätsbereich.*

1. *Für $x, y \in R$ gilt:*
$$x \mid y \iff (y) \subseteq (x).$$
2. *$x, y \in R \setminus \{0\}$ sind genau dann assoziiert, wenn $(x) = (y)$ gilt.*
3. *Für $u \in R$ gilt:*
$$u \in R^\times \iff (u) = R.$$

Satz 1.1.11 *Sei R ein Hauptidealring und seien $x_1, \ldots, x_n \in R \setminus \{0\}$. Sei $(x_1, \ldots, x_n) = (d)$. Dann ist d ein ggT von $x_1, \ldots, x_n$. Insbesondere existieren größte gemeinsame Teiler in Hauptidealringen.*

1.2 Primfaktorzerlegung

Definition 1.2.1 Sei R ein Integritätsbereich.

1. Ein Element $a \in R \setminus (R^\times \cup \{0\})$ heißt irreduzibel, falls es keine Zerlegung $a = xy$ mit $x, y \in R \setminus R^\times$ gibt.
2. Ein Element $a \in R \setminus (R^\times \cup \{0\})$ heißt prim, falls für alle $a, b \in R$ gilt:
$$p \mid ab \implies p \mid a \text{ oder } p \mid b.$$

Satz 1.2.2 *Sei R ein Integritätsbereich. Dann gilt:*

1. *Jedes Primelement ist irreduzibel.*
2. *Im HIR gilt auch die Umkehrung.*