8. Unterringe, Ideale und Faktorringe

Definition: Es sei $(R,+,\cdot)$ ein Ring und $S \subseteq R$, $S \neq \varnothing$. Ist S mit den Verknüpfungen von R selbst ein Ring, so wird S Unterring von R genannt.

Satz 52: Es sei $(R,+,\cdot)$ ein Ring und $S \subseteq R$, $S \neq \varnothing$. Dann sind äquivalent:

(i) S ist Unterring von R,
(ii) $a-b \in S\ \forall a,b \in S$ und $a \cdot b \in S\ \forall a,b \in S$.

Beweis: (i) $\Rightarrow$ (ii) Trivial.
(ii) $\Rightarrow$ (i) Aus $a-b \in S\ \forall a,b \in S$ folgt (wegen Satz 10), dass $(S,+)$ eine (abelsche) Untergruppe von $(R,+)$ ist. Wegen $a \cdot b \in S\ \forall a,b \in S$ ist S bezüglich der Multiplikation abgeschlossen. Die Assoziativität der Multiplikation und die Distributivgesetze gelten allgemein.

Beispiele: 1) $(\mathbb{Z},+,\cdot)$ ist ein Unterring von $(\mathbb{Q},+,\cdot)$, $(\mathbb{Q},+,\cdot)$ von $(\mathbb{R},+,\cdot)$ und $(\mathbb{R},+,\cdot)$ von $(\mathbb{C},+,\cdot)$.
2) Für jedes $m \in \mathbb{Z}$ ist $m\mathbb{Z}$ ein Unterring von $(\mathbb{Z},+,\cdot)$.
3) $M_n(\mathbb{Q})$ ist ein Unterring von $\big(M_n(\mathbb{R}),+,\cdot\big)$.
4) Ist $d \in \mathbb{Z}$, $d > 1$ quadratfrei, so ist $\mathbb{Z}\big[\sqrt{d}\big]$ ein Unterring von $(\mathbb{R},+,\cdot)$.
5) Ist $d \in \mathbb{Z}$, $d < 0$ quadratfrei, so ist $\mathbb{Z}\big[\sqrt{d}\big]$ ein Unterring von $(\mathbb{C},+,\cdot)$.

Bemerkungen: 1) Ist $(R,+,\cdot)$ ein Ring mit Eins und S ein Unterring von R, so muss S kein Einselement besitzen. Z.B. ist $(2\mathbb{Z},+,\cdot)$ ein Unterring von $(\mathbb{Z},+,\cdot)$, besitzt aber kein Einselement.
2) Ist $(R,+,\cdot)$ ein Ring mit Eins, S ein Unterring von R und S ein Ring mit Eins, so kann $1_S \neq 1_R$ gelten. Z.B. ist $R = \mathbb{Z} \times \mathbb{Z}$, versehen mit komponentenweiser Addition und Multiplikation $(x_1,y_1)+(x_2,y_2) = (x_1+x_2, y_1+y_2)$ und $(x_1,y_1)\cdot(x_2,y_2) = (x_1x_2, y_1y_2)$ ein Ring mit Einselement $(1,1)$. Setzt man $S = \big\{(x,0)\,\big|\,x \in \mathbb{Z}\big\}$, so ist S ein Unterring von R und besitzt das Einselement $(1,0)$.

Lemma 53: Ist R ein Integritätsbereich, $S(\neq \{0\})$ ein Unterring von R und S ein Ring mit Eins, so gilt $1_S = 1_R$.

Beweis: Es ist $1_S \cdot 1_S = 1_S = 1_S \cdot 1_R$. Da $1_S \neq 0$ folgt $1_S = 1_R$ wegen Lemma 50.

Definition: Es sei R ein Ring und $I \subseteq R$ ein Unterring von R.

1) I heißt Linksideal von R, wenn $\alpha x \in I\ \forall \alpha \in R\ \forall x \in I$,
2) I heißt Rechtsideal von R, wenn $x\alpha \in I\ \forall \alpha \in R\ \forall x \in I$,
3) I heißt Ideal von R, wenn es Links- und Rechtsideal von R ist.

Satz 54: Es sei R ein Ring und $I \subseteq R$, $I \neq \varnothing$.

(i) I ist Linksideal von $R \iff x - y \in I \ \forall x, y \in I \quad$ und $\quad \alpha x \in I \ \forall \alpha \in R \ \forall x \in I$,

(ii) I ist Rechtsideal von $R \iff x - y \in I \ \forall x, y \in I \quad$ und $\quad x\alpha \in I \ \forall \alpha \in R \ \forall x \in I$,

(iii) I ist Ideal von $R \iff x - y \in I \ \forall x, y \in I, \quad \alpha x \in I \ \forall \alpha \in R \ \forall x \in I$
und $\quad x\alpha \in I \ \forall \alpha \in R \ \forall x \in I$.

Beweis: Folgt sofort aus Satz 52 und der vorangegangenen Definition.

Beispiele: 1) Jeder Ring R enthält die beiden Ideale $\{0\}$ und R.

2) Für jedes $m \in \mathbb{Z}$ ist $m\mathbb{Z}$ ein Ideal von $\mathbb{Z}$.

3) Ist R der Ring der reellen Polynomfunktionen, d.h.

$$R = \big\{ p : \mathbb{R} \to \mathbb{R} \,\big|\, p(x) = a_n x^n + \cdots + a_1 x + a_0 \text{ für gewisse } a_0, a_1, \ldots, a_n \in \mathbb{R} \big\},$$

versehen mit punktweiser Addition und Multiplikation und $\alpha \in \mathbb{R}$, so ist

$$I_\alpha = \{ p \in R \mid p(\alpha) = 0 \}$$

ein Ideal von R.

4) Ist K ein Körper, $R = M_2(K)$,

$$I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \,\middle|\, a, b \in K \right\} \quad \text{und} \quad J = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \,\middle|\, a, b \in K \right\},$$

so ist I ein Linksideal von R (aber kein Rechtsideal von R) und J ein Rechtsideal von R (aber kein Linksideal von R), denn

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \in I, \quad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \in J \quad \text{aber} \quad \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in R \setminus (I \cup J).$$

Lemma 55: Es sei R ein Ring und $\mathcal{I} \neq \varnothing$ eine (Index)Menge.

(i) Ist S_i ein Unterring von R für alle $i \in \mathcal{I}$, so ist $\bigcap\limits_{i \in \mathcal{I}} S_i$ ein Unterring von R.

(ii) Ist I_i ein Linksideal (bzw. Rechtsideal bzw. Ideal) von R für alle $i \in \mathcal{I}$, so ist $\bigcap\limits_{i \in \mathcal{I}} I_i$ ein Linksideal (bzw. Rechtsideal bzw. Ideal) von R.

Beweis: (i) $x, y \in \bigcap\limits_{i \in \mathcal{I}} S_i \Rightarrow x, y \in S_i \ \forall i \in \mathcal{I} \Rightarrow x - y \in S_i \ \forall i \in \mathcal{I}$ und $xy \in S_i \ \forall i \in \mathcal{I}$
$\Rightarrow x - y \in \bigcap\limits_{i \in \mathcal{I}} S_i$ und $xy \in \bigcap\limits_{i \in \mathcal{I}} S_i$. Die Behauptung folgt aus Satz 52.

(ii) Aus (i) folgt sofort, dass $\bigcap\limits_{i \in \mathcal{I}} I_i$ ein Unterring von R ist.

$\alpha \in R$ und $x \in \bigcap\limits_{i \in \mathcal{I}} I_i \Rightarrow x \in I_i \ \forall i \in \mathcal{I} \Rightarrow \alpha x \in I_i \ \forall i \in \mathcal{I}$ (bzw. $x\alpha \in I_i \ \forall i \in \mathcal{I}$)
$\Rightarrow \alpha x \in \bigcap\limits_{i \in \mathcal{I}} I_i$ (bzw. $x\alpha \in \bigcap\limits_{i \in \mathcal{I}} I_i$). Die Behauptung folgt aus Satz 54.

Definition: Es sei R ein Ring und $X \subseteq R$. Dann heißt

$$(X) = \bigcap_{\substack{X \subseteq I \\ I \text{ ist Ideal von } R}} I$$

das von X erzeugte Ideal von R. Ist X endlich (d.h. $\exists x_1, \dots, x_n \in R : X = \{x_1, \dots, x_n\}$), so schreibt man auch $(x_1, \dots, x_n)$ statt (X).
Ein Ideal I von R, das von einem einzelnen Element erzeugt wird (d.h. $\exists x \in R : I = (x)$) heißt Hauptideal. Ein Ring, in dem jedes Ideal Hauptideal ist, wird Hauptidealring genannt. Ein Integritätsbereich, der ein Hauptidealring ist, wird Hauptidealbereich genannt.

Satz 56: Es sei R ein Ring und $X \subseteq R$.
(i) Es ist

$$(X) = \left\{ \sum_{i=1}^{I} \alpha_i x_i \beta_i + \sum_{j=1}^{J} \gamma_j y_j + \sum_{k=1}^{K} u_k \delta_k + \sum_{\ell=1}^{L} n_\ell v_\ell \;\middle|\; \begin{array}{l} \alpha_i, \beta_i \in R \text{ und } x_i \in X \text{ für } 1 \le i \le I, \\ \gamma_j \in R \text{ und } y_j \in X \text{ für } 1 \le j \le J, \\ \delta_k \in R \text{ und } u_k \in X \text{ für } 1 \le k \le K, \\ n_\ell \in \mathbb{Z} \text{ und } v_\ell \in X \text{ für } 1 \le \ell \le L \end{array} \right\}.$$

(ii) Es sei R ein kommutativer Ring, so ist

$$(X) = \left\{ \sum_{i=1}^{I} \alpha_i x_i + \sum_{j=1}^{J} n_j y_j \;\middle|\; \begin{array}{l} \alpha_i \in R \text{ und } x_i \in X \text{ für } 1 \le i \le I, \\ n_j \in \mathbb{Z} \text{ und } y_j \in X \text{ für } 1 \le j \le J \end{array} \right\}.$$

(iii) Es sei R ein Ring mit Eins, so ist

$$(X) = \left\{ \sum_{i=1}^{n} \alpha_i x_i \beta_i \;\middle|\; \alpha_i, \beta_i \in R \text{ und } x_i \in X \text{ für } 1 \le i \le n \right\}.$$

(iv) Ist R ein kommutativer Ring mit Eins, so ist

$$(X) = \left\{ \sum_{i=1}^{n} \alpha_i x_i \;\middle|\; \alpha_i \in R \text{ und } x_i \in X \text{ für } 1 \le i \le n \right\}.$$

Beweis: Übung.

Korollar 57: Es sei R ein Ring und $a \in R$.

(i) Es ist

$$(a) = \left\{ \alpha a + a\beta + na + \sum_{i=1}^{m} \gamma_i a \delta_i \;\middle|\; \alpha, \beta, \gamma_1, \dots, \gamma_m, \delta_1, \dots, \delta_m \in R, n \in \mathbb{Z} \right\}.$$

(ii) Ist R kommutativ, so ist $(a) = \{\alpha a + na \mid \alpha \in R, n \in \mathbb{Z}\}$.
(iii) Ist R ein Ring mit Eins, so ist

$$(a) = \left\{ \sum_{i=1}^{n} \alpha_i a \beta_i \;\middle|\; \alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in R \right\}.$$

(iv) $Ra = \{\alpha a \mid \alpha \in R\}$ ist ein Linksideal von R und $aR = \{a\alpha \mid \alpha \in R\}$ ist ein Rechtsideal von R (die aber beide a nicht enthalten müssen). Ist R ein Ring mit Eins, so ist $a \in Ra$ und $a \in aR$.
(v) Ist R ein kommutativer Ring mit Eins, so ist $(a) = Ra = aR$.

Beweis: (i), (ii) und (iii) Sind Spezialfälle von Satz 56 (i), (ii) und (iii).
(iv) Ra ist ein Linksideal von R, da

$$\alpha a - \beta a = (\alpha - \beta)a \in Ra \ \forall \alpha, \beta \in R \text{ und } \beta(\alpha a) = (\beta\alpha)a \in Ra \ \forall \alpha, \beta \in R.$$

Dass aR ein Rechtsideal ist, kann man analog zeigen.
Ist $R = 2\mathbb{Z}$ und $a = 2$, so ist $a \in R$, aber $2 = a \notin aR = Ra = 2 \cdot 2\mathbb{Z} = 4\mathbb{Z}$.
Ist R ein Ring mit Eins, so ist $a = 1 \cdot a \in Ra$ und $a = a \cdot 1 \in aR$.
(v) Nach (iv) ist $Ra = aR$ ein Ideal von R und $a \in Ra = aR$, woraus $(a) \subseteq Ra = aR$ folgt. Ist umgekehrt I ein Ideal von R und $a \in I$, so muss $\alpha a = a\alpha \in I \ \forall \alpha \in I$ gelten. Daraus folgt $Ra = aR \subseteq I$ und somit $Ra = aR \subseteq (a)$.

Lemma 58: (i) In jedem Ring R ist $\{0\} = (0)$ ein Hauptideal.
(ii) Ist R ein Ring mit Eins, so ist $R = (1)$ ein Hauptideal.

Beweis: (i) Es ist $0 \in \{0\}$ und $\{0\}$ ist offenbar ein Ideal von R. Ist I ein Ideal von R, so muss $0 \in I$ und daher $\{0\} \subseteq I$ gelten. Also ist $(0) = \{0\}$.
(ii) Ist I ein Ideal von R mit der Eigenschaft $1 \in I$, so folgt $a = a \cdot 1 \in I \ \forall a \in R$ und daher $R \subseteq I$. Also ist $I = R$ und somit $(1) = R$.

Satz 59: Ist I ein Ideal des Rings $(\mathbb{Z}, +, \cdot)$, so gibt es ein $m \in \mathbb{Z}$, $m \geq 0$ mit der Eigenschaft $I = (m) = m\mathbb{Z}$. Insbesondere ist $\mathbb{Z}$ ein Hauptidealbereich.

Beweis: Ist $I = \{0\}$, so ist $I = (0)$. Ist $I \neq \{0\}$, so ist $(I, +)$ Untergruppe der zyklischen Gruppe $(\mathbb{Z}, +)$. Nach dem Beweis von Satz 35 (ii) hat I daher die Gestalt

$$I = \langle m \rangle = m\mathbb{Z} = (m),$$

wobei $m = \min\{k \in \mathbb{Z} \mid k > 0, k \in I\} > 0$. In der letzten Gleichung wurde Korollar 57 (v) verwendet.

Satz 60: (i) Ein Schiefkörper K besitzt nur die beiden Linksideale (bzw. Rechtsideale bzw. Ideale) $\{0\}$ und K.
(ii) Ist $R(\neq \{0\})$ ein Ring mit Eins und besitzt außer $\{0\}$ und R keine weiteren Links- oder Rechtsideale, so ist R ein Schiefkörper.

Beweis: (i) Es sei $I \neq \{0\}$ ein Linksideal von K. Dann gibt es ein $\alpha \in I \setminus \{0\}$. Für jedes $\beta \in K$ ist $\beta\alpha^{-1} \in K$ und daher $\beta = \beta\alpha^{-1} \cdot \alpha \in I$. Also ist $K \subseteq I$ und somit $I = K$. Der Beweis für Rechtsideale kann analog geführt werden. Die Behauptung für Ideale folgt sofort.
(ii) Es sei $a \in R \setminus \{0\}$. Nach Korollar 57 (iv) ist Ra ein Linksideal von R und $a \in Ra$. Also ist $Ra \neq \{0\}$ und nach Voraussetzung gilt $Ra = R$. Daher ist $1 \in Ra$ und es gibt ein $x \in R$ mit der Eigenschaft $xa = 1$. Analog kann man zeigen, dass es ein $y \in R$ mit der Eigenschaft $ay = 1$ gibt. Wegen $x = x \cdot 1 = x(ay) = (xa)y = 1 \cdot y = y$ ist a invertierbar.

Satz 61: Es sei R ein Ring und I ein Ideal von R. Versieht man die Faktorgruppe $(R/I, +)$ mit der Multiplikation $(a+I)\cdot(b+I) = ab+I$, so ist $(R/I, +, \cdot)$ ein Ring. Ist R kommutativ, so ist auch R/I kommutativ. Ist R ein Ring mit Eins, so ist auch R/I ein Ring mit Eins.

Beweis: Wir zeigen zunächst, dass die Multiplikation wohldefiniert ist. Angenommen, $a' + I = a + I$ und $b' + I = b + I$. Dann ist $a' - a, b' - b \in I$. Daher gibt es $i, j \in I$, derart dass $a' = a + i$ und $b' = b + j$ und somit $a'b' = (a + i)(b + j) = ab + aj + ib + ij$ und $a'b' - ab = aj + ib + ij \in I$, also $a'b' + I = ab + I$.
Die Multiplikation ist assoziativ, da

$$\big((a + I)(b + I)\big)(c + I) = (ab)c + I = a(bc) + I = (a + I)\big((b + I)(c + I)\big).$$

Das erste Distributivgesetz gilt, da

$$\begin{aligned}(a + I)\big((b + I) + (c + I)\big) &= a(b + c) + I = (ab + ac) + I \\ &= (ab + I) + (ac + I) = (a + I)(b + I) + (a + I)(c + I).\end{aligned}$$

Das zweite Distributivgesetz kann analog bewiesen werden. Ist R kommuativ, so folgt

$$(a + I)(b + I) = ab + I = ba + I = (b + I)(a + I).$$

Ist R ein Ring mit Einselement 1, so ist $1 + R$ Einselement des Rings R/I, da

$$(1 + I)(a + I) = (a + I)(1 + I) = a + I.$$

Definition: Es sei $(R, +, \cdot)$ ein Ring und I ein Ideal von R. Der Ring $(R/I, +, \cdot)$ wird Faktorring (oder Restklassenring) von R nach I genannt.

Beispiel: Ist $m \in \mathbb{N} \setminus \{0, 1\}$, so ist $\mathbb{Z}/(m) = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$, d.h. man erhält den aus der Zahlentheorie bekannten Ring der Restklassen $(\mathbb{Z}_m, +, \cdot)$ modulo m.