10. Primideale und maximale Ideale

Definition: Es sei R ein kommutativer Ring. Ein Ideal P von R heißt Primideal, wenn $P \neq R$ und wenn für $a, b \in R$ die Implikation $ab \in P \Rightarrow a \in P \vee b \in P$ gilt.

Beispiele: 1) Ist p eine Primzahl, so ist $(p) = p\mathbb{Z}$ ein Primideal von $\mathbb{Z}$. (Sind $a, b \in \mathbb{Z}$, so gilt $ab \in (p) \Rightarrow p \mid ab \Rightarrow p \mid a \vee p \mid b \Rightarrow a \in (p) \vee b \in (p)$.)
2) Ist $m \in \mathbb{N} \setminus \{0, 1\}$ zusammengesetzt, so ist $(m) = m\mathbb{Z}$ kein Primideal von $\mathbb{Z}$. (Da m zusammengesetzt ist, $\exists\, a, b \in \mathbb{N}$ mit $1 < a, b < m$ und $m = ab$. Daher gilt $ab \in (m)$ aber weder $a \in (m)$ noch $b \in (m)$, da daraus $m \mid a$ oder $m \mid b$ folgen würde – was wegen $a < m$ und $b < m$ unmöglich ist.)
3) Ist R ein Integritätsbereich, so ist $(0) = \{0\}$ ein Primideal, da

$$ab \in \{0\} \Rightarrow ab = 0 \Rightarrow a = 0 \vee b = 0 \Rightarrow a \in \{0\} \vee b \in \{0\}.$$

4) Wegen Satz 59 folgt aus den vorangegangenen drei Beispielen, dass die Primideale von $\mathbb{Z}$ genau (0) und die Ideale der Gestalt (p) (mit p eine Primzahl) sind.
5) Ist R der Ring der reellen Polynomfunktionen, versehen mit punktweiser Addition und Multiplikation und $\alpha \in \mathbb{R}$, so ist $I_\alpha = \{p \in R \mid p(\alpha) = 0\}$ ein Primideal von R, denn

$$pq \in I_\alpha \Rightarrow (p \cdot q)(\alpha) = 0 \Rightarrow p(\alpha) \cdot q(\alpha) = 0 \Rightarrow p(\alpha) = 0 \vee q(\alpha) = 0 \Rightarrow p \in I_\alpha \vee q \in I_\alpha.$$

Definition: Es sei R ein kommutativer Ring mit Eins. Eine Menge $S \subseteq R$ heißt multiplikativ, wenn $1_R \in S$ und wenn $ab \in S \,\forall a, b \in S$.

Beispiele: 1) Ist p eine Primzahl, so ist $\left\{p^\alpha \,\middle|\, \alpha \in \mathbb{N} \cup \{0\}\right\}$ eine multiplikative Teilmenge von $\mathbb{Z}$.
2) Sind allgemeiner $p_1, \ldots, p_k$ (paarweise verschiedene) Primzahlen, so ist

$$\left\{p_1^{\alpha_1} \cdots p_k^{\alpha_k} \,\middle|\, \alpha_1, \ldots, \alpha_k \in \mathbb{N} \cup \{0\}\right\}$$

eine multiplikative Teilmenge von $\mathbb{Z}$.
3) Ist p eine Primzahl, so ist $\mathbb{Z} \setminus (p) = \left\{a \in \mathbb{Z} \,\middle|\, p \nmid a\right\}$ eine multiplikative Teilmenge von $\mathbb{Z}$, da $p \nmid 1$ und da $p \mid ab \Rightarrow p \mid a \vee p \mid b$ zur Implikation $p \nmid a \wedge p \nmid b \Rightarrow p \nmid ab$ äquivalent ist.
4) Ist R ein Integritätsbereich, so ist $R \setminus \{0\}$ eine multiplikative Teilmenge, da $1_R \neq 0$ und $a \neq 0 \wedge b \neq 0 \Rightarrow ab \neq 0$.

Satz 75: Es sei $R(\neq \{0\})$ ein kommutativer Ring mit Eins und P ein Ideal von R. Dann sind äquivalent:

(i) P ist ein Primideal,
(ii) $R \setminus P$ ist eine multiplikative Teilmenge von R.

Beweis: Es ist $P \neq R \Leftrightarrow 1 \notin P \Leftrightarrow 1 \in R \setminus P$ und

$$(ab \in P \Rightarrow a \in P \vee b \in P) \Longleftrightarrow (a \in R \setminus P \wedge b \in R \setminus P \Rightarrow ab \in R \setminus P).$$

Satz 76: Es sei $R(\neq \{0\})$ ein kommutativer Ring mit Eins und P ein Ideal von R. Dann sind äquivalent:

(i) P ist ein Primideal,
(ii) R/P ist ein Integritätsbereich.

Beweis: (i) $\Rightarrow$ (ii) Nach Satz 61 ist R/P ein kommutativer Ring mit Einselement $1_R + P$ und Nullelement $0+P = P$. Dabei ist $1_R+P \neq P$ (denn $1_R+P = P \Rightarrow 1_R \in P \Rightarrow P = R$, Widerspruch). Weiters gilt

$$\begin{aligned}(a+P)(b+P) = P &\Rightarrow ab+P = P \Rightarrow ab \in P \\ &\Rightarrow a \in P \vee b \in P \Rightarrow a+P = P \vee b+P = P,\end{aligned}$$

d.h. P ist der einzige Nullteiler von R/P.
(ii) $\Rightarrow$ (i) Da R/P ein Integritätsbereich ist, ist $1_R+P \neq 0+P(=P) \Rightarrow 1_R \notin P \Rightarrow P \neq R$. Weiters gilt

$$\begin{aligned}ab \in P &\Rightarrow ab+P = P \Rightarrow (a+P)(b+P) = P \\ &\Rightarrow a+P = P \vee b+P = P \Rightarrow a \in P \vee b \in P.\end{aligned}$$

Beispiele. 1) Ist p eine Primzahl, so ist $\mathbb{Z}/(p) = \mathbb{Z}_p$ ein Körper und daher ein Integritätsbereich.
2) Ist $m \in \mathbb{N} \setminus \{0,1\}$ zusammengesetzt, so ist $\mathbb{Z}/(m) = \mathbb{Z}_m$ zwar ein kommutativer Ring mit Eins, enthält aber Nullteiler $\neq 0$ und ist daher kein Integritätsbereich.
3) Ist R der Ring der reellen Polynomfunktionen, versehen mit punktweiser Addition und Multiplikation, $\alpha \in \mathbb{R}$ und $I_\alpha = \{p \in R \mid p(\alpha) = 0\}$, so ist $R/I_\alpha \cong \mathbb{R}$ ein Körper und daher ein Integritätsbereich (siehe Bsp. 4 nach Korollar 70).

Definition: Es sei R ein Ring. Ein Ideal M von R heißt maximales Ideal von R, wenn $M \neq R$ und wenn für ein Ideal I von R aus $M \subseteq I \subseteq R$ folgt, dass $I = M$ oder $I = R$.

Beispiele: 1) Ist p eine Primzahl, so ist $(p) = p\mathbb{Z}$ ein maximales Ideal von $\mathbb{Z}$. (Es sei I ein Ideal von $\mathbb{Z}$ mit der Eigenschaft $(p) \subseteq I \subseteq \mathbb{Z}$. Wegen Satz 59 $\exists\, a \in \mathbb{Z} : I = (a)$ und daher $(p) \subseteq (a) \Rightarrow p \in (a) \Rightarrow a \mid p \Rightarrow a \in \{1,-1,p,-p\}$. Falls $a \in \{1,-1\}$, so $I = (a) = \mathbb{Z}$ und falls $a \in \{p,-p\}$, so $I = (a) = (p)$.)
2) Ist $m \in \mathbb{N} \setminus \{0,1\}$ zusammengesetzt, so ist $(m) = m\mathbb{Z}$ kein maximales Ideal von $\mathbb{Z}$. (Da m zusammengesetzt ist, $\exists\, a,b \in \mathbb{N}$ mit $1 < a,b < m$ und $m = ab$. Nun ist $(m) \subsetneqq (a) \subsetneqq \mathbb{Z}$. Die erste Mengeninklusion folgt sofort daraus, dass offensichtlich jedes Vielfache von m auch ein Vielfaches von a ist. Aus $m \nmid a$ folgt $a \notin (m)$ und daher $(m) \neq (a)$. Wegen $1 \notin (a)$ ist $(a) \neq \mathbb{Z}$.)

3) Ist K ein Körper, so ist $(0) = \{0\}$ ein maximales Ideal nach Satz 60 (i).

Satz 77: Es sei $R(\neq \{0\})$ ein kommutativer Ring mit Eins und M ein Ideal von R. Dann sind äquivalent:

(i) M ist ein maximales Ideal,
(ii) R/M ist ein Körper.

Beweis: (i) $\Rightarrow$ (ii) Wieder nach Satz 61 ist R/M ein kommutativer Ring mit Einselement $1 + M \neq M$. Für ein $a \in R$ sei $a + M \neq M$, d.h. $a \notin M$. Setze

$$J := M + (a) = \{x + ab \mid x \in M, b \in R\}.$$

Wegen Lemma 71 ist J ein Ideal von R. Offensichtlich gilt $M \subseteq J$ und (da $a \in J \setminus M$) sogar $M \subsetneqq J$. Da M ein maximales Ideal ist, folgt $J = R$. Daher ist $1 \in J$ und $\exists x \in M \, \exists b \in R : 1 = x + ab$. Somit ist

$$1 + M = x + ab + M = ab + M = (a + M)(b + M),$$

d.h. $b + M = (a + M)^{-1}$ in R/M.
(ii) $\Rightarrow$ (i) Wie im Beweis von Satz 76 zeigt man $M \neq R$. Es sei I ein Ideal von R mit der Eigenschaft $M \subsetneqq I \subseteq R$. Dann $\exists a \in I \setminus M$ und daher $a + M \neq M$. Da R/M ein Köper ist,

$$\exists b \in R : 1 + M = (a + M)(b + M) = ab + M$$

und daher $1 - ab \in M (\subseteq I)$. Aus $a \in I$ folgt $ab \in I$ und daraus $1 = (1 - ab) + ab \in I$. Daraus erhält man sofort $I = R$ und M ist somit ein maximales Ideal.

Beispiele: 1) Ist p eine Primzahl, so ist $\mathbb{Z}/(p) = \mathbb{Z}_p$ ein Körper.
2) Ist R der Ring der reellen Polynomfunktionen, versehen mit punktweiser Addition und Multiplikation, $\alpha \in \mathbb{R}$ und $I_\alpha = \{p \in R \mid p(\alpha) = 0\}$, so ist I_α ein maximales Ideal, da $R/I_\alpha \cong \mathbb{R}$ ein Körper ist (siehe Bsp. 4 nach Korollar 70).

Korollar 78: Es sei $R(\neq \{0\})$ ein kommutativer Ring mit Eins und I ein Ideal von R. Ist I ein maximales Ideal von R, so ist I auch ein Primideal von R.

Beweis: Da I ein maximales Ideal ist, ist R/I nach Satz 77 ein Körper und daher ein Integritätsbereich. Wegen Satz 76 ist I ein Primideal.

Bemerkungen: 1) Die Umkehrung von Korollar 78 ist nicht korrekt. So ist z.B. (0) ein Primideal von $\mathbb{Z}$ aber kein maximales Ideal, da z.B. $(0) \subsetneqq (2) \subsetneqq \mathbb{Z}$.
2) Aus Korollar 78 folgt (gemeinsam mit anderen Beispielen oben), dass die maximalen Ideale von $\mathbb{Z}$ genau die Ideale der Gestalt (p) (mit p eine Primzahl) sind.

Satz 79: Es sei $R(\neq \{0\})$ ein Ring mit Eins und $I(\neq R)$ ein Ideal von R. Dann gibt es ein maximales Ideal M von R mit der Eigenschaft $I \subseteq M$.

Beweis: Es sei

$$\mathcal{M} := \big\{ J \,\big|\, J \text{ ist ein Ideal von } R \text{ und } I \subseteq J \subsetneq R \big\}.$$

Es ist $\mathcal{M} \neq \varnothing$, da $I \in \mathcal{M}$. Es sei $J_1 \subseteq J_2 \subseteq J_3 \subseteq \cdots$ eine aufsteigende Kette von Idealen in $\mathcal{M}$. Dann ist

$$\overline{J} := \bigcup_{i=1}^{\infty} J_i$$

ebenfalls in $\mathcal{M}$. (Sind $a, b \in \overline{J}$, so $\exists i, j \geq 1 : a \in J_i$ und $b \in J_j$ und daher $a, b \in J_{\max\{i,j\}}$, woraus $a - b \in J_{\max\{i,j\}} \subseteq \overline{J}$ folgt. Ist $a \in \overline{J}$ und $x \in R$, so $\exists i \geq 1 : a \in J_i$ und daher $ax, xa \in J_i \subseteq \overline{J}$, d.h. $\overline{J}$ ist ein Ideal. Klarerweise ist $I \subseteq \overline{J}$ und $\overline{J} \neq R$, da $1_R \notin J_i \, \forall i \geq 1$.) D.h. $\overline{J}$ ist obere Schranke der Kette $J_1 \subseteq J_2 \subseteq J_3 \subseteq \cdots$ und nach dem Lemma von Zorn besitzt $\mathcal{M}$ ein maximales Element M, das auch maximales Ideal von R sein muss.

Korollar 80: Es sei $R(\neq \{0\})$ ein Ring mit Eins. Dann enthält R ein maximales Ideal.

Beweis: Wende Satz 79 auf $I = \{0\}$ an.

Korollar 81: Es sei $R(\neq \{0\})$ ein kommutativer Ring mit Eins. Dann sind äquivalent:

(i) R ist ein Körper,
(ii) R enthält nur die Ideale $\{0\}$ und R,
(iii) $\{0\}$ ist maximales Ideal von R,
(iv) Ist S ein Ring und $\varphi : R \to S$ ein Homomorphismus, so ist entweder $\varphi(a) = 0 \, \forall a \in R$ oder φ ist ein Monomorphismus.

Beweis: (i) $\Leftrightarrow$ (ii) Folgt aus Satz 60.
(ii) $\Leftrightarrow$ (iii) Trivial.
(ii) $\Rightarrow$ (iv) Nach Lemma 68 (i) ist $\ker \varphi$ ein Ideal von R und daher $\ker \varphi = \{0\}$ oder $\ker \varphi = R$. Ist $\ker \varphi = \{0\}$, so ist φ ein Monomorphismus nach Lemma 68 (ii). Ist $\ker \varphi = R$, so ist $\varphi(a) = 0 \, \forall a \in R$.
(iv) $\Rightarrow$ (ii) Ist I ein Ideal von R mit $\{0\} \subsetneq I \subsetneq R$, so ist $\varphi : R \to R/I$, $\varphi(a) = a + I$ ein Homomorphismus. Da $I \neq R$, ist $1_R \notin I$ und daher $\varphi(1_R) = 1_R + I \neq I$. Da $\ker \varphi = I \neq \{0\}$, ist φ nicht injektiv.