Einführung in die Algebra
Blatt 6

Jendrik Stelzner

26. November 2013

Aufgabe 6.1.

Es sei $n > 1$ so dass
$$a^n = a \text{ für alle } a \in R, \tag{1}$$
und $\mathfrak{p}$ ein Primideal in R. Da $\mathfrak{p}$ ein Primideal ist, ist $R/\mathfrak{p}$ ein Integritätsring, sowie $R/\mathfrak{p} \neq 0$, da $\mathfrak{p}$ von R verschieden ist. Da R kommutativ ist, ist es auch $R/\mathfrak{p}$, und es ist offensichtlich, dass die Bedingung (1) auf $R/\mathfrak{p}$ vererbt wird. Da für alle $r \in R/\mathfrak{p}$ mit $r \neq 0$
$$r \cdot r^{n-1} = r^n = r = r \cdot 1,$$
folgt, wie bereits letzte Woche gezeigt, wegen der Nullteilerfreiheit von $R/\mathfrak{p}$, dass $r^{n-1} = 1$ für alle $r \in R/\mathfrak{p}$. Als ist für alle $r \in R/\mathfrak{p}$ mit $r \neq 0$
$$rr^{n-2} = r^{n-1} = 1,$$
d.h. alle $r \in R/\mathfrak{p}$ mit $r \neq 0$ sind multiplikativ invertierbar. Zusammen mit der Kommutativität von $R/\mathfrak{p}$ und $R/\mathfrak{p} \neq 0$ zeigt dies, dass $R/\mathfrak{p}$ ein Körper ist. Dies ist äquivalent dazu, dass $\mathfrak{p}$ ein maximales Ideal ist.

Aufgabe 6.2.

Bemerkung 1. *Sei R ein nicht notwendigerweise kommutativer Ring. Für $x, y \in R$ ist genau dann $xy \in R^*$, wenn $x, y \in R^*$.*

Beweis. Sind $x, y \in R^*$ so ist auch $xy \in R^*$, da die Einheitengruppe unter Multiplikation abgeschlossen ist.
Sei andererseits $c := xy \in R^*$. Da $c \in R^*$ gibt es $c^{-1} \in R^*$ mit $cc^{-1} = 1$. Es ist daher
$$x(yc^{-1}) = (xy)c^{-1} = cc^{-1} = 1,$$
also $x \in R^*$ mit $x^{-1} = yc^{-1}$. Damit ist auch
$$y(c^{-1}x) = (yc^{-1})x = x^{-1}x = 1,$$
also auch $y \in R^*$. □

Für alle $a \in \ker\varphi$ ist $1-a$ multiplikativ invertierbar: Für $n \geq 1$ mit $a^n = 0$ ergibt sich, dass

$$(1+a+a^2+\ldots+a^{n-1})(1-a) = 1-a^n = 1 \text{ und}$$
$$(1-a)(1+a+a^2+\ldots+a^{n-1}) = 1-a^n = 1.$$

Folglich ist

$$1+\ker\varphi = 1-\ker\varphi \subseteq R^*.$$

Wir bemerken auch, dass

$$x \in 1+\ker\varphi \Leftrightarrow \varphi(x) = 1,$$

denn da $1 \in \varphi^{-1}(\{1\})$ ist $1+\ker\varphi$ als Nebenklasse von 1 bezüglich $\ker\varphi$ die Faser $\varphi^{-1}(\{1\})$ von $1 \in S$ unter φ.
Bekanntermaßen induziert φ einen Gruppenhomomorphismus $\varphi_{|R^*} : R^* \to S^*$ der entsprechenden Einheitengruppen. Die Surjektivität von φ vererbt sich dabei auf $\varphi_{|R^*}$: Für $s \in S^*$ gibt es $r, r' \in R$ mit $\varphi(r) = s$ und $\varphi(r') = s^{-1}$. Es ist

$$\varphi(rr') = \varphi(r)\varphi(r') = ss^{-1} = 1,$$

also wie oben bemerkt $rr' \in 1+\ker\varphi \subseteq R^*$. Nach Bemerkung 1 ist daher $r \in R^*$. Es ist nun nach den obigen Beobachtungen

$$\begin{aligned}\ker\varphi_{|R^*} &= \{x \in R^* : \varphi(x) = 1\} = R^* \cap \varphi^{-1}(\{1\}) \\ &= R^* \cap (1+\ker\varphi) = 1+\ker\varphi.\end{aligned}$$

Folglich ist $1+\ker\varphi$ ein Normalteiler von R^* und

$$R^*/(1+\ker\varphi) \cong S^*.$$

Bemerkung

Bemerkung 2. *Ist R ein kommutativer Ring, so ist jedes echte Ideal $\mathfrak{a} \subsetneq R$ in einem maximalen Ideal von R enthalten.*

Beweis. Es sei R ein kommutativer Ring und $\mathfrak{a} \subseteq R$ ein Ideal mit $\mathfrak{a} \neq R$. Die Menge

$$\mathcal{I} := \{I \subseteq R : I \text{ ist ein Ideal in } R \text{ mit } I \neq R \text{ und } \mathfrak{a} \subseteq I\} \subseteq \mathcal{P}(R).$$

ist bezüglich der Teilmengenrelation $\subseteq$ partiell geordnet. Da $\mathfrak{a} \in \mathcal{I}$ ist $\mathcal{I}$ nichtleer. Es sei $\mathcal{C} \subseteq \mathcal{I}$ eine nichtleere Kette. $\mathcal{C}$ besitzt ein obere Schranke in $\mathcal{I}$. Um dies zu zeigen, nutzen wir die folgende Bemerkung:

Bemerkung 3. *Sei G eine abelsche Gruppe, und $(G_i)_{i\in I}$ eine Kette von Untergruppen von G, d.h. für alle $i \in I$ ist G_i eine Untergruppe von G und für $i, j \in I$ ist $G_i \subseteq G_j$ oder $G_j \subseteq G_i$. Dann ist*

$$\sum_{i\in I} G_i = \bigcup_{i\in I} G_i.$$

Beweis. Für alle $i \in I$ ist $G_i \subseteq \bigcup_{j\in I} G_j$, also ist auch $\sum_{i\in I} G_i \subseteq \bigcup_{i\in I} G_i$. Für $x \in \sum_{i\in I} G_i$ gibt es Indizes $i_1, \ldots, i_n \in I$ und Elemente $g_{i_1} \in G_{i_1}, \ldots, g_{i_n} \in G_{i_n}$ mit $x = \sum_{j=1}^n g_{i_j}$. Da die G_i bezüglich $\subseteq$ total geordnet sind, gibt es ein $k \in \{1, \ldots, n\}$ mit $G_{i_j} \subseteq G_{i_k}$ für $j = 1, \ldots, n$. Insbesondere ist $g_{i_j} \in G_{i_k}$ für $j = 1, \ldots, n$, also auch $x \in G_{i_k}$. Damit ist $x \in \bigcup_{i\in I} G_i$, also $\sum_{i\in I} G_i \subseteq \bigcup_{i\in I} G_i$. □

Aus dieser Behauptung folgt, dass

$$C := \bigcup_{I \in \mathcal{C}} I = \sum_{I \in \mathcal{C}} I$$

ein Ideal in R ist. Für alle $I \in \mathcal{C}$ gilt, dass $I \neq R$, also $1 \notin I$, und daher auch $1 \notin C$, also $C \neq R$. Auch ist $\mathfrak{a} \subseteq I \subseteq C$ für $I \in C$. Es ist also $C \in \mathcal{I}$, und deshalb C eine obere Schrankte für $\mathcal{C}$ in $\mathcal{I}$.
Mit dem Lemma von Zorn folgt, dass es ein $M \in \mathcal{I}$ gibt, dass bezüglich $\subseteq$ maximal in $\mathcal{I}$ ist. M ist ein maximales Ideal in R: Für jedes Ideal M' mit $M \subseteq M' \subsetneq R$ ist $\mathfrak{a} \subseteq M \subseteq M'$ und $M' \neq R$, also $M' \in \mathcal{I}$. Wegen der Maximalität von M in $\mathcal{I}$ ist daher $M' = M$. $\square$

Aufgabe 6.3.

Bemerkung 4. *Für alle $a \in R$ ist a genau dann eine Einheit, wenn a in keinem maximalen Ideal in R enthalten ist.*

Beweis. Ist a keine Einheit, so ist $(a) \neq R$; wäre nämlich $(a) = R$, so gebe es insbesondere ein $b \in R$ mit $ab = 1$. Da (a) ein echtes Ideal in R ist, folgt aus Bemerkung 2, dass es ein maximales Ideal $\mathfrak{m}$ in R mit

$$a \in (a) \subseteq \mathfrak{m}$$

gibt.
Ist andererseits a eine Einheit mit inversen Element a', so folgt für jedes Ideal $\mathfrak{a} \subseteq R$ mit $a \in \mathfrak{a}$, dass $1 = aa' \in \mathfrak{a}$, also $\mathfrak{a} = R$. Insbesondere ist $\mathfrak{a}$ nicht maximal. $\square$

Aufgrund von Bemerkung 4 reicht nun zu zeigen, dass $a \in R$ genau dann in jedem maximalen Ideal von R liegt, wenn $1 - ab$ für alle $b \in R$ in keinem maximalen Ideal von R liegt. Dabei wird im Folgenden der Fall $R = 0$ ausgeschlossen, da die Aussage in diesem Fall offenbar erfüllt ist. Nach Bemerkung 2 enthält $R \neq 0$ mindestens ein maximales Ideal, da $0 \subseteq R$ ein echtes Ideal ist.
Angenommen, a liegt in jedem maximalen Ideal von R. Gibt es ein maximales Ideal $\mathfrak{m}$ von R, und $b \in R$ mit $1 - ab \in \mathfrak{m}$, so ist wegen $a \in \mathfrak{m}$ auch $ab \in \mathfrak{m}$, also $1 = 1 - ab + ab \in \mathfrak{m}$. Damit ist $\mathfrak{m} = R$, was der Maximalität von R widerspricht. Also ist $1 - ab \notin \mathfrak{m}$ für jedes $b \in R$ und maximale Ideal $\mathfrak{m}$ von R.
Angenommen, es gibt ein maximals Ideal $\mathfrak{m}$ von R mit $a \notin \mathfrak{m}$. Dann ist $(a) + \mathfrak{m}$ ein Ideal von R mit $\mathfrak{m} \subsetneq (a) + \mathfrak{m}$, wegen der Maximalität von $\mathfrak{m}$ also $(a) + \mathfrak{m} = R$. Insbesondere gibt es ein $b \in R$ und $m \in \mathfrak{m}$ mit $ab + m = 1$. Es ist also $1 - ab = m \in \mathfrak{m}$ nach Bemerkung 4 keine Einheit.

Aufgabe 6.4.

Definition. *Sei R ein kommutativer Ring. Das* Jacobson-Radikal *von R ist der Schnitt über alle maximalen Ideale von R,*

$$J(R) := \bigcap_{\substack{\mathfrak{a} \subseteq R \\ \mathfrak{a} \text{ maximales} \\ \text{Ideal}}} \mathfrak{a}.$$

Wie in Aufgabe 6.3. gezeigt, ist diese Definition äquivalent zu

$$J(R) = \{a \in R : 1 - ab \in R^* \textit{ für alle } b \in R\}.$$

Es ist $J(R) = 0$: Aufgrund der Nullteilerfreiheit von R ist für alle $a \in J(R)$ mit $a \neq 0$ die Abbildung

$$R \to R^*, b \mapsto 1 - ab$$

injektiv. Dies ist aber nicht möglich, da R unendlich und R^* endlich ist. Also gibt es kein $a \in J(R)$ mit $a \neq 0$.

Angenommen R enthält nur endlich viele maximale Ideale $\mathfrak{m}_1, \dots, \mathfrak{m}_n$. Da maximale Ideale immer paarweise koprim sind, folgt aus dem chinesischen Restsatz, dass

$$R / \bigcap_{i=1}^{n} \mathfrak{m}_i \cong \prod_{i=1}^{n} R/\mathfrak{m}_i$$

Dabei ist $\bigcap_{i=1}^{n} \mathfrak{m}_i = J(R) = 0$. Also ergibt sich aus der obigen Gleichung, dass

$$R \cong \prod_{i=1}^{n} R/\mathfrak{m}_i. \tag{2}$$

Da die $\mathfrak{m}_i$ maximale Ideale von R sind, sind die Faktorringe $R/\mathfrak{m}_i$ Körper. Da R unendlich ist, muss mindestens einer dieser Körper unendlich sein. Durch passende Nummerierung der $\mathfrak{m}_i$ können wir o.B.d.A. davon ausgehen, dass $R/\mathfrak{m}_1$ unendlich ist. Insbesondere ist auch $(R/\mathfrak{m}_1)^* = R/\mathfrak{m}_1 \setminus \{0\}$ unendlich.

Da für jede Einheit $\lambda \in R/\mathfrak{m}_1$ das Element $(\lambda, 1, 1, \dots, 1) \in \prod_{i=1}^{n} R/\mathfrak{m}_i$ ebenfalls eine Einheit ist (das multiplikativ Inverse ist $(\lambda^{-1}, 1, 1, \dots, 1)$), folgt aus (2), dass R unendlich viele Einheiten besitzt. Dies ist ein Widerspruch zur Endlichkeit von R^*. Also besitzt R unendlich viele maximale Ideale.