Einführung in die Algebra
Blatt 5

Jendrik Stelzner

15. November 2013

Aufgabe 5.1.

Aufgabe 5.2.

Aufgabe 5.3.

Bemerkung 1. Sei R ein Ring mit mindestens zwei Elementen. Dann ist sind Null- und Einselement in R verschieden.

Beweis. Da R mindestens zwei Elemente besitzt, gibt es ein $a \in R$ mit $a \neq 0$. Es ist

$$1 \cdot a = a \neq 0 = 0 \cdot a,$$

also $0 \neq 1$. □

Bemerkung 2. Sei R ein kommutativer Ring und $a \in R$. Dann ist das von a erzeugte Ideal $\mathfrak{a} := (a)$ ein Ring ohne Eins (d.h. es ist möglich, aber nicht notwendig, dass $1 \in \mathfrak{a}$).

Beweis. Als Ideal ist $\mathfrak{a}$ eine additive Untergruppe der additiven Gruppe von R. Da $rs \in \mathfrak{a}$ für alle $r \in R$ und $s \in \mathfrak{a}$ ist $\mathfrak{a}$ inbesondere abgeschlossen bezüglich der Multiplikation. Die Assoziativität sowie Distributivität der Multiplikation vererben sich aus R. □

Es gilt zunächst zu bemerken, dass ein Ring, wie er in der Aufgabenstellung beschrieben ist, nicht existiert: Da R mindestens zwei Elemente besitzt, folgt aus Bemerkung 1, dass $0 \neq 1$. Jedoch muss $0 \subseteq R$ nach Aufgabenstellung das Einselement von R beinhalten, also $0 = 1$. Im Folgenden wird daher davon ausgegangen, dass die entsprechende Aussage für diesen Sonderfall ausgeschlossen wird.
Nach Aufgabenstellung ist R bereits ein kommutativer Ring mit 1. Da R mindestens zwei Elemente besitzt folgt aus Bemerkung 1, dass $0 \neq 1$. Es gilt also nur noch zu zeigen, dass es für jedes $a \in R$ mit $a \neq 0$ ein multiplikativ Inverses Element $b \in R$ mit $ab = 1$ gibt.
Sei $a \in R$ mit $a \neq 0$ beliebig aber fest. Es sei $\mathfrak{a} := (a)$ das von a erzeugte Ideal. Aus der Nullteilerfreiheit von R folgt, dass $\mathfrak{a} \neq 0$. Es ist $\mathfrak{a} = R$: Ist $\mathfrak{a} \neq R$, so folgt aus Bemerkung 2 und der Aufgabenstellung, dass $1 \in \mathfrak{a}$. Da $\mathfrak{a}$ ein Ideal ist, ist daher

$r = r \cdot 1 \in \mathfrak{a}$ für alle $r \in R$. Da $aR = \mathfrak{a} = R$ gibt es insbesondere ein $b \in R$ mit $ab = 1$.
Man bemerke, dass die für den Beweis die aus der Aufgabenstellung ebenfalls folgende Endlichkeit von $\mathfrak{a} = R$ nicht benötigt wird: Ich kann nur vermuten, dass ursprünglich, d.h. bevor die Aufgabenstellung geändert wurde, die Nullteilerfreiheit in Kombination mit der Endlichkeit einer entsprechenden Teilmenge dazu genutzt werde sollte, aus der folgenden Injektivität der Linksmultiplikation mit a auch deren Surjektivität zu folgern, und damit dann analog zu oben die Existenz eines multiplikativ Inversen. In der jetzigen Version folgt aus der aus der Endlichkeit allerdings, dass $\mathfrak{a} = R$ endlich ist.

Aufgabe 5.4.

(ii)

Für alle $a \in R$ ist

$$a^2 + 1 = a + 1 = (a+1)^2 = a^2 + 2a + 1,$$

also $2a = 0$. Insbesondere ist $a = -a$.

(i)

Für alle $a, b \in R$ ist

$$ab - ba = ab + ba = (a+b)^2 - a^2 - b^2 = a + b - a - b = 0,$$

also $ab = ba$, und daher R kommutativ.

(iii)

Seien $a, b \in R$ mit $a \neq b$. Es ist

$$(a-b)ab = a^2b - ab^2 = ab - ab = 0.$$

Da $a \neq b$ ist $a - b \neq 0$, wegen der Nullteilerfreiheit von R also $ab = 0$. Wegen der Nullteilerfreiheit ist also $a = 0$ oder $b = 0$. Aus der Beliebigkeit von a und b folgt, dass es neben 0 nur ein weiters Element in R gibt. Also ist $R = \{0, 1\}$. Betrachtet man die Verknüpfungstabellen von R,

$$\begin{array}{|c|c|c|} \hline + & 0 & 1 \\ \hline 0 & 0 & 1 \\ \hline 1 & 1 & 0 \\ \hline \end{array} \quad \text{und} \quad \begin{array}{|c|c|c|} \hline \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ \hline 1 & 0 & 1 \\ \hline \end{array},$$

so ist R offenbar isomorph zu $\mathbb{F}_2$.

Aufgabe 5.5.

(i)

Da $\mathfrak{a}$ ein Ideal in R ist, ist $ar \in \mathfrak{a}$ für alle $a \in \mathfrak{a}$ und $r \in R$. Es ist nun

$$\begin{aligned}\mathfrak{b} = (\mathfrak{a}) &= \sum_{a\in\mathfrak{a}} aR[X] = \sum_{a\in\mathfrak{a}} \left\{ a \sum_{i=0}^{n} a_i X^i : n \geq 0, a_i \in R \right\} \\ &= \sum_{a\in\mathfrak{a}} \left\{ \sum_{i=0}^{n} a a_i X^i : n \geq 0, a_i \in R \right\} = \left\{ \sum_{i=0}^{n} a_i X^i : n \geq 0, a_i \in \mathfrak{a} \right\}. \quad (1)\end{aligned}$$

Dabei ergibt sich die Gleichheit bei (1) wie folgt:
Für alle $f = \sum_{i=0}^{n} a a_i X^i \in aR[X]$ ist $a a_i \in \mathfrak{a}$, da $a \in \mathfrak{a}$ und $\mathfrak{a}$ ein Ideal in R ist, also f ein Polynom mit Koeffizienten in $\mathfrak{a}$.
Andererseits ist jedes Polynom $f = \sum_{i=0}^{n} a_i X^i$ mit Koeffizienten $a_0, \dots, a_n \in \mathfrak{a}$ die Summe der Monome $f_i := a_i X^i \in a_i R[X]$. Also ist $f \in \sum_{i=1}^{n} a_i R[X]$.

(ii)