2. Teil: Ringe

7. Definitionen und einfache Eigenschaften

Definition: Es sei $R \neq \varnothing$ eine Menge und $+ : R \times R \to R$ und $\cdot : R \times R \to R$ zwei binäre Verknüpfungen auf R. Gelten die drei Eigenschaften

1) $(R, +)$ ist eine abelsche Gruppe,

2a) $(R, \cdot)$ ist eine Halbgruppe,

3) $a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c \ \forall a, b, c \in R$ (Distributivgesetze),

so wird $(R, +, \cdot)$ als Ring bezeichnet.

Gilt zusätzlich zu 1), 2a) und 3) die Bedingung

4) $a \cdot b = b \cdot a \ \forall a, b \in R$ (Kommutativität der Multiplikation),

so wird $(R, +, \cdot)$ als kommutativer Ring bezeichnet.

Gelten 1) und 3) und statt 2a) die stärkere Bedingung

2b) $(R, \cdot)$ ist ein Monoid,

so wird $(R, +, \cdot)$ als Ring mit Eins(element) bezeichnet.

Gelten die vier Bedingungen 1), 2b), 3) und 4) wird $(R, +, \cdot)$ als kommutativer Ring mit Eins(element) bezeichnet.

Notationen und Bezeichnungen: 1) Für die abelsche Gruppe $(R, +)$ verwendet man die Bezeichnungen einer (additiv geschriebenen) abelschen Gruppe, die im ersten Teil eingeführt wurden. Insbesondere schreibt man 0 für das neutrale Element dieser Gruppe und nennt es das Nullelement des Rings R. Weiters schreibt man $-a$ für das zu $a \in R$ bezüglich der Addition inverse Element.
2) Sind $a, b \in R$, so schreibt man kurz $a - b$ für $a + (-b) \in R$, d.h. man setzt $a - b := a + (-b)$.
3) Ebenso verwendet man für die Halbgruppe $(R, \cdot)$ die im ersten Teil eingeführen Bezeichnungen. Ist $(R, +, \cdot)$ ein Ring mit Eins, so verwendet man die im ersten Teil eingeführten Bezeichnungen für das Monoid $(R, \cdot)$. Für das neutrale Element des Monoids $(R, \cdot)$ schreibt man 1 und nennt es das Einselement des Rings R (d.h. es gilt $1 \cdot a = a \cdot 1 = a \ \forall a \in R$). Besteht die Gefahr von Verwechslungen, schreibt man auch 1_R für das Einselement des Rings R. Ist $a \in R$ ein invertierbares Element des Monoids $(R, \cdot)$, so nennt man es kurz invertierbares Element des Rings R und schreibt (wie im ersten Teil) a^{-1} für sein inverses Element.

Beispiele: 1) Jeder Körper ist ein kommutativer Ring mit Eins, also insbesondere $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ und $(\mathbb{Z}_p, +, \cdot)$ für jede Primzahl p.

2) Ist $m \in \mathbb{N} \setminus \{0,1\}$, so ist $(\mathbb{Z}_m, +, \cdot)$ ein kommutativer Ring mit Eins.
3) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Eins.
4) Es bezeichne $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$. Dann ist $\mathbb{Z}[i]$ mit der üblichen Addition und Multiplikation komplexer Zahlen ein kommutativer Ring mit Eins, der als Ring der Gaußschen ganzen Zahlen bezeichnet wird.
5) Es sei $d \in \mathbb{Z}$, $d > 1$ quadratfrei (d.h. es gibt keine Primzahl p mit der Eigenschaft $p^2 \mid d$) und es bezeichne $\mathbb{Z}\big[\sqrt{d}\big] := \big\{a+b\sqrt{d} \,\big|\, a, b \in \mathbb{Z}\big\}$. Dann ist $\mathbb{Z}\big[\sqrt{d}\big]$ mit der üblichen Addition und Multiplikation reeller Zahlen ein kommutativer Ring mit Eins.
6) Es sei $d \in \mathbb{Z}$, $d < 0$ quadratfrei und es bezeichne $\mathbb{Z}\big[\sqrt{d}\big] := \big\{a+bi\sqrt{|d|} \,\big|\, a, b \in \mathbb{Z}\big\}$. Dann ist $\mathbb{Z}\big[\sqrt{d}\big]$ mit der üblichen Addition und Multiplikation komplexer Zahlen ein kommutativer Ring mit Eins. (Für $d = -1$ erhält man als Spezialfall Bsp. 4.)
7) Es sei K ein Körper und $M_n(K)$ bezeichne die Menge aller $n \times n$-Matrizen mit Eintragungen aus K. Dann ist $M_n(K)$ mit der üblichen Addition und Multiplikation von Matrizen ein Ring mit Eins, der für $n \geq 2$ nicht kommutativ ist.
8) Es sei V ein K-Vektorraum und $\mathrm{End}(V) = \{\varphi : V \to V \mid \varphi \text{ ist } K\text{-linear}\}$. Dann ist $\big(\mathrm{End}(V), +, \circ\big)$ ein Ring mit Eins, der der Endomorphismenring des Vektorraums V genannt wird. Dabei sind die Verknüpfungen folgendermaßen definiert:

$$\varphi + \psi : V \to V,\ (\varphi + \psi)(v) = \varphi(v) + \psi(v) \text{ und } \varphi \circ \psi : V \to V,\ (\varphi \circ \psi)(v) = \varphi\big(\psi(v)\big).$$

9) Es sei $m \in \mathbb{N} \setminus \{0,1\}$. Dann ist $m\mathbb{Z}$ mit der üblichen Addition und Multiplikation ganzer Zahlen ein kommutativer Ring (aber kein Ring mit Eins).
10) Es sei $[a,b] \subseteq \mathbb{R}$ ein Intervall. Die Menge aller Funktionen $f : [a,b] \to \mathbb{R}$, versehen mit der punktweisen Addition und Multiplikation (d.h. $(f+g)(x) = f(x) + g(x)$ und $(f \cdot g)(x) = f(x) \cdot g(x)$) ist ein kommutativer Ring mit Eins. (Ebenso bilden die Mengen der differenzierbaren bzw. Riemann-integrierbaren Funktionen $f : [a,b] \to \mathbb{R}$, jeweils mit punktweiser Addition und Multiplikation, einen kommutativen Ring mit Eins.)
11) Es sei $R = \{0\}$ versehen mit den Verknüpfungen $0 + 0 = 0$ und $0 \cdot 0 = 0$. Dann ist $(R, +, \cdot)$ ein kommutativer Ring mit Eins mit der Eigenschaft $0 = 1$. Tatsächlich ist das der einzige Ring mit Eins mit dieser Eigenschaft. Ist nämlich $(S, +, \cdot)$ ein Ring mit Eins, in dem $0 = 1$ gilt, so ist $a = a \cdot 1 = a \cdot 0 = 0\ \forall a \in S$. (Den Beweis, dass in einem Ring stets $a \cdot 0 = 0$ gilt, werden wir in Kürze in Lemma 48 nachholen.)
12) Es sei $(G, +)$ eine abelsche Gruppe und

$$\mathrm{End}(G) = \{\varphi : G \to G \mid \varphi \text{ ist ein Gruppenhomomorphismus}\}.$$

Dann ist $\big(\mathrm{End}(G), +, \circ\big)$ ein Ring mit Eins. Dabei sind die beiden Verknüpfungen wie in Bsp. 8 definiert, d.h. $(\varphi+\psi)(x) = \varphi(x)+\psi(x)$ und $(\varphi\circ\psi)(x) = \varphi\big(\psi(x)\big)$ für $\varphi, \psi \in \mathrm{End}(G)$ und $x \in G$.

13) Es sei

$$R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in 2\mathbb{Z} \right\} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{Z} \text{ sind gerade} \right\}.$$

Dann ist R, versehen mit der üblichen Addition und Multiplikation von Matrizen, ein Ring, der nicht kommutativ ist und kein Einselement besitzt.
14) Es sei K ein Körper und $K[X]$ bezeichne die Menge aller Polynome mit Koeffizienten in K, d.h.

$$K[X] = \{a_n X^n + \cdots + a_1 X + a_0 \mid a_0, a_1, \ldots, a_n \in K\}.$$

Dann ist $K[X]$, versehen mit der üblichen Addition und Multiplikation von Polynomen, ein kommutativer Ring mit Eins.

Bemerkung: Für die abelsche Gruppe $(R,+)$ und die Halbgruppe bzw. das Monoid $(R,\cdot)$ gelten alle Rechenregeln und Eigenschaften, die im ersten Teil bewiesen wurden.

Lemma 48: Es sei $(R,+,\cdot)$ ein Ring. Dann gelten:

(i) $0 \cdot a = a \cdot 0 = 0 \ \forall a \in R$,
(ii) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b) \ \forall a,b \in R$,
(iii) $(-a) \cdot (-b) = a \cdot b \ \forall a,b \in R$,
(iv) $a \cdot (b-c) = a \cdot b - a \cdot c$ und $(a-b) \cdot c = a \cdot c - b \cdot c \ \forall a,b,c \in R$,
(v) $(na) \cdot b = a \cdot (nb) = n(a \cdot b) \ \forall n \in \mathbb{Z} \ \forall a,b \in R$,
(vi) Für alle $a_1, \ldots, a_n, b_1, \ldots, b_m \in R$ ist

$$\left(\sum_{i=1}^{n} a_i \right) \cdot \left(\sum_{j=1}^{m} b_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j.$$

Beweis: (i) Aus $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$ folgt

$$0 = 0 \cdot a + \big(-(0 \cdot a)\big) = 0 \cdot a + 0 \cdot a + \big(-(0 \cdot a)\big) = 0 \cdot a.$$

Die Identität $a \cdot 0 = 0$ kann analog bewiesen werden.
(ii) Es ist

$$a \cdot b + (-a) \cdot b = \big(a + (-a)\big) \cdot b = 0 \cdot b \overset{\text{(i)}}{=} 0.$$

Aus der Eindeutigkeit des (additiven) Inversen folgt $-(a \cdot b) = (-a) \cdot b$.
Die Identität $a \cdot (-b) = -(a \cdot b)$ kann analog bewiesen werden.
(iii) Folgt aus

$$(-a) \cdot (-b) \overset{\text{(ii)}}{=} a \cdot \big(-(-b)\big) \overset{\text{Satz 4 (i)}}{=} a \cdot b.$$

(iv) Gilt wegen

$$a \cdot (b-c) = a \cdot \big(b + (-c)\big) = a \cdot b + a \cdot (-c) \overset{\text{(ii)}}{=} a \cdot b + \big(-(a \cdot c)\big) = a \cdot b - a \cdot c.$$

bzw.

$$(a-b) \cdot c = \big(a + (-b)\big) \cdot c = a \cdot c + (-b) \cdot c \overset{\text{(ii)}}{=} a \cdot c + \big(-(b \cdot c)\big) = a \cdot c - b \cdot c.$$

(v) Die Behauptung gilt für $n = 0$, da

$$(0 \cdot a) \cdot b = 0 \cdot b = 0,\ a \cdot (0 \cdot b) = a \cdot 0 = 0 \text{ und } 0 \cdot (a \cdot b) = 0.$$

(Beachten Sie, dass 0 und $\cdot$ hier jeweils zwei Bedeutungen haben. In allen drei Gleichungsketten ist nur die jeweils erste Null in $\mathbb{Z}$. Es ist also z.B. $(0_{\mathbb{Z}} \cdot a) \cdot b = 0_R \cdot b \overset{\text{(i)}}{=} 0_R$.)

Den Fall $n > 0$ beweisen wir mit Induktion. Die Behauptung ist trivial für $n = 1$ und folgt sofort aus den Distributivgesetzen für $n = 2$. Schließlich ist

$$\big((n+1)a\big)b = (na + a)b = (na)b + ab \overset{\text{IV}}{=} n(ab) + ab = (n+1)ab$$

bzw.

$$a\big((n+1)b\big) = a(nb + b) = a(nb) + ab \overset{\text{IV}}{=} n(ab) + ab = (n+1)ab.$$

Der Fall $n < 0$ gilt wegen

$$(na)b = \big(|n|(-a)\big)b = |n|\big((-a)b\big) = |n|\big(-(ab)\big) = n(ab)$$

und

$$a(nb) = a\big(|n|(-b)\big) = |n|\big(a(-b)\big) = |n|\big(-(ab)\big) = n(ab).$$

(vi) Wir zeigen zunächst den Fall $n = 1$ mit Induktion nach m, d.h.

$$a_1 \sum_{j=1}^{m} b_j = \sum_{j=1}^{m} a_1 b_j. \qquad (1)$$

Diese Behauptung ist trivial für $m = 1$ und folgt aus einem der Distributivgesetze für $m = 2$. Schließlich ist

$$a_1 \sum_{j=1}^{m+1} b_j = a_1 \left(\sum_{j=1}^{m} b_j + b_{m+1} \right) = a_1 \sum_{j=1}^{m} b_j + a_1 b_{m+1} \overset{\text{IV}}{=} \sum_{j=1}^{m} a_1 b_j + a_1 b_{m+1} = \sum_{j=1}^{m+1} a_1 b_j.$$

Völlig analog kann man den Fall $m = 1$ mit Induktion nach n zeigen, d.h.

$$\left(\sum_{i=1}^{n} a_i \right) b_1 = \sum_{i=1}^{n} a_i b_1. \qquad (2)$$

Mit Hilfe dieser beiden Spezialfälle folgt nun

$$\left(\sum_{i=1}^{n} a_i \right) \cdot \left(\sum_{j=1}^{m} b_j \right) \overset{(2)}{=} \sum_{i=1}^{n} a_i \left(\sum_{j=1}^{m} b_j \right) \overset{(1)}{=} \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j.$$

Definition: Es sei $(R, +, \cdot)$ ein Ring mit Eins.
Ist $a \in R$ invertierbar (d.h. $\exists a^{-1} \in R : a \cdot a^{-1} = a^{-1} \cdot a = 1$), so wird a eine Einheit von R genannt. Weiters wird $(R^*, \cdot)$ als Einheitengruppe des Rings R bezeichnet, wobei

$$R^* = \{a \in R \mid a \text{ ist invertierbar}\} = \{a \in R \mid a \text{ ist eine Einheit}\}.$$

Bemerkung: Dass $(R^*, \cdot)$ eine Gruppe ist, wurde in Übungsbeispiel 15 bewiesen.

Definition: Ist $K(\neq \{0\})$ ein Ring mit Eins, in dem jedes $a \in K \setminus \{0\}$ invertierbar ist, so wird K ein Schiefkörper genannt. Ist $K(\neq \{0\})$ ein kommutativer Ring mit Eins, in dem jedes $a \in K \setminus \{0\}$ invertierbar ist, so ist K ein Körper.

Bemerkung: Wir haben den Begriff des Körpers bis jetzt vorausgesetzt und bereits mehrfach in Beispielen verwendet. Wir haben ihn an dieser Stelle trotzdem noch einmal definiert, um ihn in die Theorie einzufügen.

Beispiele: 1) Ist K ein Schiefkörper, so ist $K^* = K \setminus \{0\}$ nach Definition. Ist K sogar ein Körper, so ist $(K^*, \cdot) = \big(K \setminus \{0\}, \cdot\big)$ eine abelsche Gruppe.
2) Ist $m \in \mathbb{N} \setminus \{0, 1\}$, so ist $(\mathbb{Z}_m^*, \cdot)$ die prime Restklassengruppe (siehe Zahlentheorie).
3) $\mathbb{Z}^* = \{-1, +1\}$.
4) Man kann zeigen, dass $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$.
5) Man kann zeigen, dass

$$\mathbb{Z}\big[\sqrt{2}\big]^* = \big\{\pm\big(1+\sqrt{2}\big)^n \,\big|\, n \in \mathbb{Z}\big\} = \big\{\varepsilon\big(1+\sqrt{2}\big)^n \,\big|\, n \in \mathbb{Z}, \varepsilon \in \{+1, -1\}\big\}.$$

6) Ist K ein Körper, so ist $M_n(K)^* = \mathrm{GL}_n(K)$.

Bemerkung: Beachten Sie, dass die Bedeutung der Bezeichnungen $\mathbb{Q}^*$, $\mathbb{R}^*$ und $\mathbb{C}^*$ mit der an der Schule üblichen übereinstimmt, da es sich bei $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ um Körper handelt. Das stimmt aber nicht für die Bedeutung der Bezeichnungen $\mathbb{Z}^*$ und $\mathbb{N}^*$, die man aus diesem Grund im Rahmen der Algebra nicht für die Mengen $\mathbb{Z} \setminus \{0\}$ und $\mathbb{N} \setminus \{0\}$ verwenden sollte.

Definition: Es sei R ein Ring. Ein $a \in R$ wird Linksnullteiler (bzw. Rechtsnullteiler) genannt, wenn $\exists x \in R \setminus \{0\} : ax = 0$ (bzw. $\exists x \in R \setminus \{0\} : xa = 0$). Ein $a \in R$ wird Nullteiler genannt, wenn es sowohl Links- als auch Rechtsnullteiler ist.

Bemerkung: Die Definition der Begriffe Linksnullteiler, Rechtnullteiler und Nullteiler ist in der Literatur nicht einheitlich. Sehr oft wird das Nullelement (wegen Lemma 48 (i)) von vornherein ausgeschlossen. Weiters wird ein $a \in R$ manchmal schon Nullteiler genannt, wenn es entweder Links- oder Rechtsnullteiler ist.

Beispiele: 1) Ist $R \neq \{0\}$ ein Ring, so ist (wegen Lemma 48 (i)) 0 ein Nullteiler (zumindest nach der in dieser Vorlesung verwendeten Definition).

2) Es sei $m \in \mathbb{N} \setminus \{0,1\}$. Dann ist jedes Element von $\mathbb{Z}_m \setminus \mathbb{Z}_m^*$ ein Nullteiler im Ring $(\mathbb{Z}_m, +, \cdot)$. Ist nämlich $1 \leq a \leq m-1$ und $d = \mathrm{ggT}(a,m) > 1$, so gilt $m/d < m$ und daher

$$\overline{m/d} \neq \overline{0} \quad \text{und} \quad \overline{a} \cdot \overline{m/d} = \overline{am/d} = \overline{a/d} \cdot \overline{m} = \overline{a/d} \cdot \overline{0} = \overline{0}.$$

Ist z.B. $m = 12$, so ist $\mathbb{Z}_{12} \setminus \mathbb{Z}_{12}^* = \{\overline{0}, \overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{8}, \overline{9}, \overline{10}\}$ und $\overline{0} \cdot \overline{1} = \overline{0}$ sowie

$$\overline{2} \cdot \overline{6} = \overline{3} \cdot \overline{4} = \overline{8} \cdot \overline{3} = \overline{9} \cdot \overline{4} = \overline{10} \cdot \overline{6} = \overline{0}.$$

3) Es sei K ein Körper. Dann ist jedes Element von $M_n(K) \setminus \mathrm{GL}_n(K)$ Nullteiler im Ring $\big(M_n(K), +, \cdot\big)$. Ist nämlich $A \in M_n(K) \setminus \mathrm{GL}_n(K)$, so gilt (nach der Linearen Algebra) $\det A = 0$ und es gibt $x_1, \ldots, x_n \in K$ (die nicht alle $= 0$ sind) und $y_1, \ldots, y_n \in K$ (die ebenfalls nicht alle $= 0$ sind) mit den Eigenschaften

$$(x_1, \ldots, x_n)A = (0, \ldots, 0) \text{ und } A(y_1, \ldots, y_n)^T = (0, \ldots, 0)^T.$$

(Dabei bezeichnet $(y_1, \ldots, y_n)^T$ die Transponierte des Zeilenvektors $(y_1, \ldots, y_n)$, d.h. den Spaltenvektor mit den Eintragungen $y_1, \ldots, y_n$.) Es sei nun $X \in M_n(K)$ die Matrix

$$X := \begin{pmatrix} x_1y_1 & x_2y_1 & \cdots & x_ny_1 \\ x_1y_2 & x_2y_2 & \cdots & x_ny_2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1y_n & x_2y_n & \cdots & x_ny_n \end{pmatrix}$$

Da es $i, j \in \{1, \ldots, n\}$ mit den Eigenschaften $x_i \neq 0$ und $y_j \neq 0$ gibt, ist $x_iy_j \neq 0$ und daher $X \neq 0$. Da $XA = AX = 0$, ist A ein Nullteiler.
Ist z.B. $A = \left(\begin{smallmatrix} 2 & -2 \\ 1 & -1 \end{smallmatrix}\right)$, so kann man z.B. $(1 \ -2)A = (0 \ 0)$ und $A(1 \ 1)^T = (0 \ 0)^T$ wählen. Daraus erhält man $X = \left(\begin{smallmatrix} 1 & -2 \\ 1 & -2 \end{smallmatrix}\right)$ sowie

$$XA = \begin{pmatrix} 1 & -2 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 2 & -2 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ und } AX = \begin{pmatrix} 2 & -2 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -2 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

4) Es sei R der Ring der Funktionen $f : [0,1] \to \mathbb{R}$ mit punktweiser Addition und Multiplikation. Es seien $f, g \in R \setminus \{0\}$ definiert als

$$f(x) = \begin{cases} 1 & \text{für } x \in \big[0, \frac{1}{2}\big], \\ 0 & \text{für } x \in \big(\frac{1}{2}, 1\big], \end{cases} \quad \text{und} \quad g(x) = \begin{cases} 0 & \text{für } x \in \big[0, \frac{1}{2}\big], \\ 1 & \text{für } x \in \big(\frac{1}{2}, 1\big]. \end{cases}$$

Dann gilt offenbar $f \cdot g = 0$ und f und g sind Nullteiler im Ring R.

Lemma 49: Es sei $R(\neq \{0\})$ ein Ring mit Eins. Dann enthält seine Einheitengruppe R^* weder Links- noch Rechtsnullteiler.

Beweis: Ist $a \in R^*$ und $ax = 0$ für ein $x \in R$, so folgt

$$x = 1 \cdot x = (a^{-1}a)x = a^{-1}(ax) = a^{-1} \cdot 0 = 0,$$

d.h. a kann kein Linksnullteiler sein. Dass a kein Rechtsnullteiler ist, kann man analog beweisen.

Definition: Ist $R(\neq \{0\})$ ein kommutativer Ring mit Eins, in dem 0 der einzige Nullteiler ist, so wird R Integritätsbereich genannt.

Bemerkung: Diese Definition wird oft so formuliert, dass R *nullteilerfrei* sein muss, was man bei der in dieser Vorlesung verwendeten Definition des Nullteilers nicht ganz wörtlich nehmen darf.

Beispiele: 1) Jeder Körper ist ein Integritätsbereich.
2) $\mathbb{Z}$ ist ein Integritätsbereich.
3) $\mathbb{Z}[i]$ ist ein Integritätsbereich.
4) Allgemeiner gilt: Ist $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei, so ist $\mathbb{Z}\left[\sqrt{d}\right]$ ein Integritätsbereich.

Lemma 50: Es sei $R(\neq \{0\})$ ein kommutativer Ring mit Eins. Dann sind äquivalent:

(i) R ist ein Integritätsbereich,
(ii) Es gilt folgende Kürzungsregel: Aus $ab = ac$ und $a \neq 0$ folgt $b = c$ (mit $a, b, c \in R$).

Beweis: (i) $\Rightarrow$ (ii) Wenn $ab = ac$ dann $a(b - c) = ab - ac = 0$. Da $a \neq 0$, muss $b - c = 0$ und daher $b = c$ sein.
(ii) $\Rightarrow$ (i) Wenn $ab = 0$ und $a \neq 0$, so ist $ab = a \cdot 0$ und daher $b = 0$.

Satz 51: Jeder endliche Integritätsbereich ist ein Körper.

Beweis: Es sei R ein endlicher Integritätsbereich mit n Elementen und $R = \{a_1, \ldots, a_n\}$. Ist $a \in R \setminus \{0\}$, dann ist auch $R = \{aa_1, \ldots, aa_n\}$. (Ist $aa_i = aa_j$, so folgt nach Lemma 50 $a_i = a_j$. Daher ist $aa_i \neq aa_j$ für $1 \leq i, j \leq n$ und $i \neq j$. Also enthält $\{aa_1, \ldots, aa_n\} (\subseteq R)$ ebenfalls n Elemente und stimmt daher mit R überein.) Also gibt es ein $i \in \{1, \ldots, n\}$ mit der Eigenschaft $aa_i = a_i a = 1$.

Bemerkung: Man kann zeigen, dass jeder endliche Schiefkörper ein Körper ist (Satz von Wedderburn).