Aufgabe 1 (Frühjahr 2015)**.** Ein Ring R mit Eins heißt idempotent, wenn $a \cdot a = a$ für alle $a \in R$ gilt Beweisen Sie:

(a) $-1 = 1$ in R. *(Haben wir bereits besprochen.)*

(b) Jeder idempotente Ring ist kommutativ. *(Haben wir bereits besprochen.)*

(c) Jeder idempotente Integritätsbereich is isomorph zu $\mathbb{F}_2$, dem Körper mit zwei Elementen.

Lösung. **Zu (c):** Wir haben bereits in (b) gezeigt, daß R kommutativ ist. Da R ein Integritätsbereich ist, gilt $1 \neq 0$, also hat R mindestens zwei Elemente. Wir zeigen, daß dies die einzigen Elemente sind. Sei $x \in R$ ein beliebiges Element. Da R idempotent ist, gilt

$$x^2 = x \qquad \Leftrightarrow x^2 - x = 0.$$

Mit dem Distributivgesetz gilt

$$x(x-1) = x^2 + x = 0.$$

Da R ein Integritätsring ist, ist aber dann $x = 0$ oder $x - 1 = 0$, also $x = 0$ oder $x = 1$.
Es folgt, daß R als Menge gegeben ist durch $\{0, 1\}$.
Man muß nun zeigen, daß R die RIngstruktur von $\mathbb{F}_2$ hat:
Es ist klar, daß

$$\begin{aligned} 0 + 0 &= 0 \\ 0 + 1 = 1 &= 1 + 0 \\ 0 \cdot 0 &= 0 \\ 0 \cdot 1 = 0 &= 1 \cdot 0 \end{aligned}$$

Da 0 das neutrale Element der Addition ist.
Weiterhin wissen wir, daß $(R, +)$ eine Gruppe der Ordnung 2 ist, also

$$2 \cdot 1 = 1 + 1 = 0.$$

Schließlich wissen wir, daß R idempotent ist, also

$$1 \cdot 1 = 1.$$

Aufgabe 2 (Frühjahr 2013)**.** Beweisen Sie, daß jeder endliche Integritätsbereich ein Körper ist.
Hinweis: Man betrachte eine durch Multiplikation gegebene Abbildung.

Lösung. Wir müssen zeigen, daß jedes Element $0 \neq s \in R$ invertierbar ist. Für ein solches s betrachte die Abbildung

$$\varphi : R \to R, r \mapsto rs.$$

Diese ist injektiv wegen der „Kürzungsregel“ in Integritätsringen:
ist $\varphi(r_1) = \varphi(r_2)$, also $r_1 s = r_2 s$, so ist $r_1 = r_2$.
Da R endlich ist, ist die gegebene Abbildung auch surjektiv, also bijektiv.
Demnach hat die 1 ein Urbild r unter dieser Abbildung, es gilt also $rs = 1$. Insbesondere ist s invertierbar.
Da s ein beliebiges Element $\neq 0$ war, folgt, daß alle Elemente $\neq 0$ invertierbar sind.

Aufgabe 3 (Frühjahr 1978)**.** Sei A ein Integritätsbereich, der eine endlichdimensionale $\mathbb{R}$-Algebra mit Dimension $n \geqslant 2$ ist. Man identifiziere $\mathbb{R}$ mit dem Untervektorraum $\mathbb{R}.1_A = \langle 1_A \rangle \subset A$.

(a) Man zeige, daß jedes Element $0 \neq a \in A$ invertierbar ist.

(b) Sei $a \in A \setminus \mathbb{R}$. Man zeige, daß die Familie $\{1_A, a\}$ linear unabhängig ist, die Familie $\{1_A, a, a^2\}$ aber linear abhängig.

(c) Man schließe daraus, daß $i_A \in \langle 1_A, a \rangle$ existiert mit $i_A^2 = -1$.

(d) Man zeige, daß $\dim(A) = 2$ und $A \cong \mathbb{C}$.

Lösung. Da A kommutativ ist, müssen wir uns keine Gedanken über das Zentrum von A machen, sondern können A sehen als Ring, der Gleichzietig ein $\mathbb{R}$-Vektorraum ist. Für $r \in \mathbb{R}$ und $a, b \in A$ schreiben wir die Skalarmultiplikation als $r.a$ und die Ringmultiplikation in A als ab.

Zu (a): Dies kann man ähnlich wie in Aufgabe 2 zeigen.
Sei $a \in A \setminus \{0\}$. Die Abbildung

$$\varphi : A \to A, x \mapsto ax$$

ist ein injektiver Ringhomomorphismus wegen der „Kürzungsregel“ in Integritätsringen:
ist

$$ax_1 = \varphi(x_1) = \varphi(x_2) = ax_2,$$

, so ist $x_1 = x_2$.
Außerdem ist klar, daß φ ein $\mathbb{R}$-Vektorraumhomomorphismus ist. Da A ein endlichdimensionaler $\mathbb{R}$-Vektorraum ist, ist φ sogar surjektiv, also bijektiv (ein Automorphismus). Also gibt es $x \in A$, mit $ax = \varphi(x) = 1_A$. Dies zeigt, daß a invertierbar ist.

Zu (b): Das Element $1_A \in A$ ist $\neq 0$, da A ein Integritätsring ist. Das Element $a \in A$ ist $\neq 0$, da $a \notin \mathbb{R} \ni 0$. Da $a \notin \langle 1 \rangle$ sind $\{1_A, a\}$ linear unabhängig.
Die Familie $\{1_A, a, a^2, \ldots, a^n\}$ von $n+1$ Elementen ist dagegen linear abhängig, da $\dim(A) = n$. Das heiß es gibt $r_0, \ldots, r_n \in \mathbb{R}$, mindestens eines davon ungleich 0, so daß

$$r_0.1_A + r_1.a + r_2.a^2 + \ldots + r_n.a^n = 0.$$

Berachte das Polynom $f = r_0 + r_1X + r_2X^2 + \ldots + r_nX^n \in \mathbb{R}[X]$. Nach Konstruktion ist $f \neq 0$ und a Nullstelle von f, d.h. $f(a) = 0$.
Faktorisiere f in irreduzible Polynome über $\mathbb{R}$, also $f = f_1 \cdots f_r$. Es gilt

$$f_1(a) \cdots f_r(a) = f(a) = 0 \in A$$

Da A ein Integritätsring ist, ist einer der Faktoren $= 0$, also gibt es k mit $f_k(a) = 0$. Da f_k ein irreduzibles Polynom über $\mathbb{R}$ ist, ist $\deg(f_k) \leqslant 2$. Es ist nicht möglich, daß $\deg(f_k) = 0$ (also f_k konstant), denn sonst wäre $f_k = 0$ und damit $f = 0$. Es ist ebenso unmöglich, daß $\deg(f_k) = 1$, denn sonst wären 1 und a linear abhängig. Also ist $\deg(f_k) = 2$, d.h. von der Form $f_k = s_0 + s_1X + s_2X^2$, $s_2 \neq 0$ nicht trivial, also $s_0.1_A + s_1.a + s_2.a^2 = 0$ und damit sind $\{1_A, a, a^2\}$ linear abhängig.

Zu (c): Ohne Einschränkung nehmen wir an, daß $s_2 = 1$ in dem Polynom f_k. Dann ist $f_k = X^2 + s_1X + s_0$, und die Diskriminante $\Delta = s_1^2 - 4s_0 < 0$ sonst wäre f_k nicht irreduzibel. Wir berechnen nun (mit der „Mitternachtsformel“):

$$\begin{aligned} 0 = f_k(a) &= a^2 + s_1a + s_0 \\ &= \left(a^2 + 2a\frac{s_1}{2} + \frac{s_1^2}{4}\right) - \frac{s_1^2 - 4s_0}{4} \end{aligned}$$

also

$$\left(a + \frac{s_1}{2}\right)^2 = \frac{s_1^2 - 4s_0}{4}$$

oder

$$-1 = \left(\frac{2a + s_1}{\sqrt{4s_0 - s_1^2}}\right)^2.$$

Wir setzen $i_A := \frac{2a+s_1}{\sqrt{4s_0-s_1^2}} = \frac{2}{\sqrt{4s_0-s_1^2}}.a + \frac{s_1}{\sqrt{4s_0-s_1^2}}.1_A$. Dann gilt $i \in \langle 1_A, a \rangle$, aber auch $a \in \langle 1_A, i \rangle$.

Zu (d): Wäre $\dim(A) > 2$, dann gäbe es $b \in A$, so daß die Familie $\{1_A, a, b\}$ linear unabhängig wären. Wie in (c) findet man für ein solches b ein $j \in \langle 1, b \rangle$ mit $j^2 = -1$. Aber dann wäre

$$0 = -1 + 1 = i^2 - j^2 = (i + j)(i - j).$$

Da A ein Integritätsbereich ist, wäre dann $i + j = 0$ oder $i - j = 0$, also $i = -j$ oder $i = j$. In beiden Fällen folgt $j \in \langle 1_A, a \rangle$ und dann auch $b \in \langle 1_A, j \rangle \subset \langle 1_A, a \rangle$. Widerspruch zur linearen Unabhängigkeit

von $\{1_A, a, b\}$. Also ist $\dim(A) = 2$. Insbesondere gilt $A = \langle 1_A, a\rangle = \langle 1_A, i_A\rangle$ als Vektorraum.

Wir definieren einen $\mathbb{R}$-Vektorraumhomomorphismus durch

$$A \to \mathbb{C}, \begin{cases} 1_A \mapsto 1_{\mathbb{C}}, \\ i_A \mapsto i_{\mathbb{C}}. \end{cases}$$

Dies ist ein $\mathbb{R}$-Vektorraumisomorphismus, da A und $\mathbb{C}$ beide Dimension 2 über $\mathbb{R}$ haben.
Man sieht leicht, daß ies sogar ein $\mathbb{R}$-Algebrenhomomorphismus ist, da $i_A^2 = -1 = i_{\mathbb{C}}^2$.

Aufgabe 4 (??)**.** Sei A ein Integritätsring, der nur eine endliche Anzahl von Idealen hat. Zeigen Sie, daß A bereits ein Körper ist.

Lösung. Sei $x \in A\backslash 0$. Betrachte die Ideale $I_n = (x^n) \subset A$. Da A nur endlich viele Ideale besitzt, muß es $n < m \in \mathbb{N}$ geben, so daß die von x^n und x^m erzeugten Ideale übereinstimmen, dh. $(x^n) = (x^m) \subset A$. Insbesondere ist $x^m \in (x^n)$, das heißt, es gibt $a \in A$ it $x^n = x^m a$. Es folgt

$$x^n(1 - x^q a) = x^n - x^m a = 0,$$

mit $q = m - n > 0$. Da A ein Integritätsring ist, folgt $x^q a = 1$. Also ist x in A invertierbar mit Inversem $x^{q-1}a$.

Aufgabe 5 (Herbst 1998)**.** Betrachten Sie das Gitter

$$R = \left\{ n + m\frac{1+\sqrt{-7}}{2} \ ; \ n, m \in \mathbb{Z} \right\}$$

n der komplexen Ebene $\mathbb{C}$.

(a) Zeigen Sie, daß R ein Ring ist.

(b) Sei

$$d(z, R) = \min\{|z - r| \ ; \ r \in R\}$$

der Abstand einer komplexen Zahl vom Gitter R. Bestimmen Sie das Maximum dieser Abstände, also

$$d = \max_{z \in \mathbb{C}} d(z, R),$$

und zeigen Sie $d < 1$.

(c) Folgern Sie aus (b) daß R ein euklidischer Ring ist, wobei die euklidische Wertfunktion auf R der Absolutbetrag der komplexen Zahlen sei.

Lösung. **Zu (a):** Da $\mathbb{C}$ als Körper insbesondere ein Ring ist, genügt es zu zeigen, daß R ein Unterring ist.

- Es ist $1 = 1 + 0\frac{1+\sqrt{-7}}{2} \in R$.
- Sei $r_1 = n_1 + m_1\frac{1+\sqrt{-7}}{2} \in R$ und $r_2 = n_2 + m_2\frac{1+\sqrt{-7}}{2} \in R$. Dann ist

$$r_1 - r_2 = (n_1 - n_2) + (m_1 - m_2)\frac{1+\sqrt{-7}}{2} \in R.$$

- Sei $r_1 = n_1 + m_1\frac{1+\sqrt{-7}}{2} \in R$ und $r_2 = n_2 + m_2\frac{1+\sqrt{-7}}{2} \in R$. Dann ist

$$r_1 r_2 = (n_1 n_2 - 4m_1 m_2) + (n_1 m_2 + m_1 n_2 + 2m_1 m_2)\frac{1+\sqrt{-7}}{2} \in R.$$

Zu (b): Sei $z = \alpha + i\beta \in \mathbb{C}$. In der Basis $\{1, \frac{1+\sqrt{-7}}{2}\}$ können wir schreiben

$$z = \left(\alpha - \frac{\beta}{2\sqrt{7}}\right) + \frac{\beta}{\sqrt{7}}\left(\frac{1+\sqrt{-7}}{2}\right)$$

Sei

$$n_1 = \lfloor \alpha - \frac{\beta}{2\sqrt{7}} \rfloor$$
$$n_2 = \lceil \alpha - \frac{\beta}{2\sqrt{7}} \rceil = n_1 + 1$$
$$m_1 = \lfloor \frac{\beta}{\sqrt{7}} \rfloor$$
$$m_2 = \lceil \frac{\beta}{\sqrt{7}} \rceil = m_1 + 1$$

Dann ist z in dem Paralellogramm mit Eckpunkten

$$A = n_1 + m_1 \frac{1+\sqrt{-7}}{2}$$
$$B = n_2 + m_1 \frac{1+\sqrt{-7}}{2}$$
$$C = n_1 + m_2 \frac{1+\sqrt{-7}}{2}$$
$$D = n_2 + m_2 \frac{1+\sqrt{-7}}{2}$$

Ohne Einschränkung nehmen wir an $n_1 = 0 = m_1$ und $n_2 = 1 = m_2$. Wegen Symmetrie genügt es das Dreieck $\triangle(A, B, C)$ zu betrachten.
Wir suchen den Punkt, der von allen Eckpunkten des Dreiecks gleichweit entfernt ist. Dieser liegt auf den Geraden $\frac{1}{2} = x$ und $y = -\frac{1}{\sqrt{7}}x + \frac{2}{\sqrt{7}}$. Der Schnittpunkt ist demnach bei $(\frac{1}{2}, \frac{3}{2\cdot\sqrt{7}})$. Insbesondere ist dieser PUnkt innerhalb des Dreiecks, und

$$d = \sqrt{\frac{1}{4} + \frac{9}{4 \cdot 7}} = \frac{2}{\sqrt{7}}.$$

Die Längen der Diagonalen sind gegeben durch

$$|D - A| = \left|1 + \frac{1+\sqrt{-7}}{2}\right| = \sqrt{\frac{9}{4} + \frac{7}{4}} = 2$$
$$|C - B| = \left| -1 + \frac{1+\sqrt{-7}}{2}\right| = \sqrt{\frac{1}{4} + \frac{7}{4}} = \sqrt{2} < 2$$

Also ist $[D, A]$ die längere Diagonale, und jedes Punkt innerhalb des Parallelograms hat von dem nahegelegensten Gitterpunkt einen Abstand $< \frac{|D-A|}{2} = 1$.
Es folgt $d < 1$.

Zu (c): Sei $x_1 = n_1 + m_1 \frac{1+\sqrt{-7}}{2} \in R$ und $x_2 = n_2 + m_2 \frac{1+\sqrt{-7}}{2} \in R \setminus 0$. Es ist $\frac{x_1}{x_2} \in \mathbb{C}$ und nach (b) ist $d\left(\frac{x_1}{x_2}, R\right) < 1$. Es gibt also $q \in R$ mit $\left|\frac{x_1}{x_2} - q\right| < 1$. Setze $r = x_1 - qx_2$, oder $x_1 = qx_2 + r$. Dann ist $|r| = |x_1 - qx_2| < |x_2|$. Und damit ist R ein euklidischer Ring.

Aufgabe 6 (Herbst 1976)**.** Man zeige daß der Ring $\mathbb{R}[X, Y]$ der reellen Polynome in zwei Veränderlichen kein Hauptidealring ist.

Lösung. Das Ideal (X, Y) ist kein Hauptideal. Angenommen, es gäbe $d \in \mathbb{R}[X, Y]$ mit $(d) = (X, Y)$. Da dann $X, Y \in (d)$ gibt es $r_1, r_2 \in \mathbb{R}$ mit $r_1 d = X$ und $r_2 d = Y$, aber X und Y sind teilerfremd.