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.

(b) Jeder idempotente Ring ist kommutativ.

(c) Jeder idempotente Integritätsbereich is isomorph zu $\mathbb{F}_2$, dem Körper mit zwei Elementen. *(Dies werden wir später besprechen.)*

Lösung. **Zu (a):** Für beliebige $x, y \in R$ gilt wie in jedem Ring $xy = (-x)(-y)$, denn

$$(-x)y + xy = ((-x) + x) \cdot y = 0 \cdot y = 0 = x \cdot 0 = x \cdot ((-y) + y) = x(-y) + xy.$$

das heißt $-xy = (-x)y = x(-y)$, und damit

$$xy = -(-xy) = -(x(-y)) = (-x)(-y).$$

Also insbesondere $1 \cdot 1 = (-1)(-1)$ und wegen Idempotenz folgt

$$1 = 1 \cdot 1 = (-1)(-1) = -1.$$

Zu (b): Um die Kommutativität zu zeigen, betrachten wir für $x, y \in R$

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y.$$

Nach Subtraktion von x und y auf beiden Seiten erhält man $0 = xy + yx$, also $yx = -xy = (-1)xy = 1 \cdot xy$.

Aufgabe 2 (Herbst 1999)**.** Die Menge $\mathbb{Z}^2$ ist ein Ring bezüglich komponentenweiser Addition und Multiplikation. Wir untersuchen hier seine Ideale.

(a) Sei $I \lhd \mathbb{Z}^2$ ein Ideal und

$$\begin{aligned} I_1 &= \{x \in \mathbb{Z} \mid (x, 0) \in I\} \\ I_2 &= \{y \in \mathbb{Z} \mid (0, y) \in I\} \end{aligned}$$

Man zeige, daß I_1 und I_2 Ideale von $\mathbb{Z}$ sind.

(b) Man zeige $I = I_1 \times I_2$.

(c) Man bestimme die Ideale von $\mathbb{Z}^2$

Lösung. **Zu (a):** I_1 is nicht-leer, da $(0, 0) \in I$, also $0 \in I_1$.
Sei $x, y \in I_1$ und $k \in \mathbb{Z}$. Dann ist $(x, 0), (y, 0) \in I$, also $(x - y, 0) = (x, 0) - (y, 0) \in I$, da $I \subset \mathbb{Z}^2$ ein Ideal ist. Es folgt $x - y \in I_1$.
Weiter ist für $l \in \mathbb{Z}$ beliebig $(kx, 0) = (k, l)(x, 0) \in I$, also $kx \in I_1$.
Ähnlich für I_2.
Zu (b): Sei $(x, y) \in I_1 \times I_2$. Dann ist $(x, 0), (0, y) \in I$. Also $(x, y) = (x, 0) + (0, y) \in I$, und damit $I_1 \times I_2 \subset I$.
Andererseits ist für $(x, y) \in I$ auch $(x, 0) = (1, 0)(x, y) \in I$ und $(0, y) = (0, 1)(x, y) \in I$, also $x \in I_1$ und $y \in I_2$. Damit $(x, y) \in I_1 \times I_2$ und $I \subset I_1 \times I_2$.
Zu (c): Wir wissen, daß die Ideale von $\mathbb{Z}$ genau die Untergruppen sind, also gibt es $a, b \in \mathbb{Z}$ mit $I_1 = a\,\mathbb{Z}$ und $I_2 = b\,\mathbb{Z}$. Wir folgern, daß jedes Ideal von $\mathbb{Z}^2$ die Form $I = a\,\mathbb{Z} \times b\,\mathbb{Z} = (a, b)\,\mathbb{Z}^2$ hat.

Aufgabe 3 (??)**.** Sei $A \in M_n(\mathbb{R})$ eine $n \times n$-Matix über den reellen Zahlen. Sei

$$K_A := \{M \in M_n(\mathbb{R}) \mid AM = MA\}$$

die Menge der mit A vertauschbaren Matrizen.
Zeigen Sie, daß K_A eine $\mathbb{R}$-Agebra ist.

Lösung. Die Menge $K_A$ist ein Unterring des Matrizenrings $M_n(\mathbb{R})$: sie enthält die Einheitsmatrix E_n (und die Nullmatrix 0_n), und für $B, C \in K_A$ gilt

$$(B-C)A = BA-CA = AB-AC = A(B-C) \quad \text{und } (BC)A = B(CA) = B(AC) = (BA)C = (AB)C = A(BC)$$

also $B - C \in K_A$ und $BC \in K_A$.
Des weiteren definiert die Abbildung

$$\varphi : \mathbb{R} \to K_A, \alpha \mapsto \alpha E_n$$

einen Ringhomomorphismus mit $\text{im}(\varphi) \subset Z(K_A)$, denn

$$\begin{aligned}
\varphi(0) &= 0_n \\
\varphi(1) &= E_n \\
\varphi(\alpha+\beta) &= (\alpha+\beta)E_n = \alpha E_n + \beta E_n = \varphi(\alpha) + \varphi(\beta) \\
\varphi(\alpha\cdot\beta) &= (\alpha\cdot\beta)E_n = \alpha E_n \cdot \beta E_n = \varphi(\alpha)\cdot\varphi(\beta) \\
\text{im}(\varphi) &\subset Z(M_n(\mathbb{R}))
\end{aligned}$$

Aufgabe 4 (Herbst 1978)**.** Sei E eine Menge und $A = \mathcal{P}(E)$ ihre Potenzmenge mit den Verknüpfungen

$$\begin{aligned}
E_1 \Delta E_2 &= \{e \in E \mid e \in E_1 \cup E_2, e \notin E_1 \cap E_2\} \\
E_1 \cap E_2
\end{aligned}$$

(a) Man zeige, daß $(A, \Delta, \cap)$ ein kommutativer Ring ist.

(b) Sei E endlich und $E' \subset E$. Man zeige, daß $I = \mathcal{P}(E')$ ein Ideal von A ist.

(c) Sei andererseits I ein Ideal von A. Sei $X, Z \in I$ und $Y \subset X$. Man zeige $Y \in I$ und $X \cup Z \in I$.

(d) Man zeige, daß es $E' \subset E$ gibt, so daß $I = \mathcal{P}(E')$.

(e) Sei E unendlich. Man zeige, dass die Menge der endlichen Teilmengen von E ein Ideal von A bilden, das nicht on der Form $\mathcal{P}(E')$ ist.

Lösung. **Zu (a):** Man muß die Axiome nachprüfen, da A kein Unterring eines bekannten Rings ist. Es ist klar, daß Δ und $\cap$ Verknüpfungen $A \times A \to A$ definieren, da $E_1 \Delta E_2 \subset E$ und $E_1 \cap E_2 \subset E$.
Wir zeigen, daß (A, Δ) eine abelsche Gruppe ist:

- Kommutativität: $E_1 \Delta E_2 = E_2 \Delta E_1$ nach Definition.
- Assoziativität:

$$\begin{aligned}
(E_1\Delta E_2)\Delta E_3 &= \{e \in E \mid e \in (E_1\Delta E_2) \cup E_3, e \notin (E_1\Delta E_2) \cap E_3\} \\
&= \{e \in E \mid e \in E_1 \cup E_2 \cup E_3, e \notin E_1 \cap E_2 \cup E_1 \cap E_3 \cup E_2 \cap E_3\} \\
E_1\Delta(E_2\Delta E_3) &= \{e \in E \mid e \in E_1\Delta(E_2 \cup E_3), e \notin E_1 \cap (E_2\Delta E_3)\} \\
&= \{e \in E \mid e \in E_1 \cup E_2 \cup E_3, e \notin E_1 \cap E_2 \cup E_1 \cap E_3 \cup E_2 \cap E_3\}
\end{aligned}$$

- Neutrales Element:

$$\varnothing \Delta E' = \{e \in E \mid e \in E' \cup \varnothing = E', e \notin E' \cap \varnothing = \varnothing\} = E'$$

- Inverses Element:

$$E' \Delta E' = \{e \in E \mid e \in E' \cup E' = E', e \notin E' \cap E' = E'\} = \varnothing$$

Wir zeigen, daß $(A, \cap)$ ein kommutatives Monoid ist:

- Kommutativität: klar.
- Assoziativität: klar.

- Neutrales Element: $E' \cap E = E'$.
- (Außerdem ist $A = \mathcal{P}(E)$ idempotent: $E' \cap E' = E'$.)

Wir zeigen das Distributivgesetz:

$$\begin{aligned}(E_1 \Delta E_2) \cap E_3 &= \{e \in E \mid e \in (E_1 \cup E_2) \cap E_3, e \notin E_1 \cap E_2\} \\ &= \{e \in E \mid e \in (E_1 \cap E_3) \cup (E_3 \cap E_3), e \notin (E_1 \cap E_3) \cap (E_2 \cap E_3) = (E_1 \cap E_3)\Delta(E_2 \cap E_3)\end{aligned}$$

Zu (b): Wie oben sieht man, daß $\mathcal{P}(E')$ eine abelsche Gruppe ist, also insbesondere eine Untergruppe von $\mathcal{P}(E)$. Weiter ist für $X \in \mathcal{P}(E')$ und $Y \in A$

$$X \cap Y \subset X \subset E'$$

also $X \cap Y \in \mathcal{P}(E')$.
Zu (c): Sei $X \in I$ und $Y \subset X$, also $Y \in A$. Da I ein Ideal von A ist, ist $Y = Y \cap X \in I$.
Sei $X, Z \in I$, setze $X_1 = X \setminus Z$, dann sind X_1 und Z disjunkt, und es gilt

$$X \cup Z = X_1 \cup Z = X_1 \Delta Z \in I,$$

da $X_1 \subset X \in I$ und I ein Ideal ist.
Zu (d): Sei E' die Vereinigung aller Elemente in I. Natürlich ist $E' \subset E$ eine endliche Menge, und mit Iduktion folgt nach (c), daß $E' \in I$. Nach (c) is auch klar, daß $\mathcal{P}(E') \subset I$. Aber wenn $X \in I$ ist, ist auch $X \subset E'$, also $X \in \mathcal{P}(E')$. Damit $I = \mathcal{P}(E')$.
Zu (e): Die Menge der endlichen Teilmengen ist ein Ideal von A: diese Menge enthält die leere Menge und ist abgeschlossen unter Δ und für $X \in A$ und eine endliche Teilmenge $Y \subset E$ ist $X \cap Y$ endlich.
Sie ist nicht von der Form $\mathcal{P}(E')$: Angenommen dies wäre der Fall. Dann wäre für $x \in E$ und $X = \{x\}$ auch $X \in \mathcal{P}(E')$, das heißt $x \in E'$, in anderen Worten $E = E'$. Aber da das Ideal nur die endlichen Teilmengen von E enthält, kann es nicht $\mathcal{P}(E)$ sein.

Aufgabe 5 (Herbst 1975)**.** Sei R ein endlicher kommutativer Ring (nicht notwendig mit 1). Beweisen Sie, daß jedes Element $x \in R$ eine der drei folgenden Aussagen erfüllt:

(a) x ist 0 oder nilpotent,

(b) x ist eine Einheit in R,

(c) eine Potenz von x ist idempotent.

Lösung. Angenommen $x \in R$ ist nicht null, nicht nilpotent, und keine Einheit. Betrachte die Menge

$$\{x, x^2, x^3, \ldots\} \subset R.$$

Da R endlich ist, ist auch diese Menge endlich, und es gibt $a < b \in \mathbb{N}$ mit $x^a = x^b$. Sei $b = a + r$. Dann ist

$$x^a = x^{a+r} = x^a x^r = x^{a+r} x^r = x^{a+2r} = \ldots = x^{a+kr}$$

für alle $k \in \mathbb{N}_0$ und

$$x^{na} = x^{(n-1)a} x^a = x^{(n-1)a} x^{a+kr} = x^{na+kr}.$$

Wählen wir also $n = r$ und $k = a$, so erhalten wir

$$x^{ra} = x^{ra+ar} = x^{ar} x^{ar}.$$