Aufgabe 1 (Frühjahr 1985)**.** Seien R ein kommutativer Integritätsring und $a, b \in R$ mit $b \neq 0$. Beweise die Äquivalenz folgender Aussagen:

(a) Es gibt $c, d \in R$ mit $d \neq 0$, $\frac{a}{b} = \frac{c}{d}$ (im Quotientenkörper von R) und $Rc + Rd = R$.

(b) $Ra + Rb$ ist ein Hauptideal.

Lösung. **(a) $\Rightarrow$ (b):** Nach Voraussetzung ist $ad = bc$ (da R integritätsring ist) und es gibt $r_1, r_2 \in R$ mit $r_1c + r_2d = 1$. Dann ist

$$\begin{aligned} a &= a \cdot 1 = a(r_1c + r_2d) = r_1ac + r_2ad = r_1ac + r_2bc = c(r_1a + r_2b) \\ b &= b \cdot 1 = b(r_1c + r_2d) = r_1bc + r_2bd = r_1ad + r_2bd = d(r_1a + r_2b) \end{aligned}$$

Es folgt, daß das Ideal $Ra + Rb = (a, b)$ von dem Element $\xi = r_1a + r_2b$ erzeugt wird, denn nach obiger Rechnung ist $a, b \in (\xi)$, also $(a, b) \subset (\xi)$, und $(\xi) \subset (a, b)$ ist klar.

(b) $\Rightarrow$ (a): Ist $Ra+Rb$ ein Hauptideal, dann gibt es $\xi \in R$ mit $(\xi) = R\xi = Ra+Rb = (a, b)$. Insbesondere gibt es $c, d \in R$ mit $a = c\xi$ und $b = d\xi$, und da $b \neq 0$ ist auch $d \neq 0$ und $\xi \neq 0$. Also ist

$$ad\xi = bc\xi$$

und mit der Kürzungsregel in Integritätsringen ist

$$ad = bc.$$

Also stimmen die Äquivalenzklassen $\frac{a}{b}$ und $\frac{c}{d}$ überein.
Da ξ in dem Ideal $Ra + Rb$ liegt, gibt es $r_1, r_2 \in R$ mit $\xi = r_1a + r_2b$. Einsetzen von $a = c\xi$ und $b = d\xi$ ergibt

$$\xi = r_1a + r_2b = r_1c\xi + r_2d\xi$$

und Kürzen, da $\xi \neq 0$

$$1 = r_1c + r_2d.$$

Also ist $R = Rc + Rd$.

Aufgabe 2 (Herbst 1987)**.** Man zeige: Der Körper $\mathbb{Q}$ enthält keinen echten Unterkörper.

Lösung. Sei $K \hookrightarrow \mathbb{Q}$ ein Unterkörper von $\mathbb{Q}$. Also sind $0, 1 \in K$. Es folgt, daß $2 = 1 + 1 \neq 0$ ebenfalls in K ist. Angenommen $n \in K$. Dann ist $n + 1 = (1 + \ldots + 1) + 1$ nach Induktion ebenfalls in K. Es folgt $\mathbb{N} \subset K$. Da $(K, +)$ eine abelsche Gruppe ist, ist für $n \in \mathbb{N}$ auch das additive Inverse $-x \in K$. Es folgt $\mathbb{Z} \hookrightarrow K$, und dies ist ein Ringhomomorphismus. Das Bild der multiplikativ abgeschloßenen Menge $S = \mathbb{Z}\backslash\{0\}$ unter diesem Ringhomomorphismus ist in $K\backslash\{0\} = K^\times$ enthalten. Nach der universellen Eigenschaft von Quotientenringen, gibt es also einen eindeutigen Ringhomomorphismus $\mathbb{Q} \to K$, so daß das Diagramm

$$\begin{tikzcd} \mathbb{Z} \arrow[rr] \arrow[dr] & & \mathbb{Q} \arrow[dl] \\ & K & \end{tikzcd}$$

kommutiert. Dieser ist invers zu $K \hookrightarrow \mathbb{Q}$. Also ist $K = \mathbb{Q}$.

Aufgabe 3. Sei $A = \left\{\frac{m}{n} \,;\, m \in \mathbb{Z}, n \in 2\,\mathbb{N}+1\right\}$. Zeigen Sie, daß $(A, +, \cdot)$ ein Ring ist und bestimmen Sie seine invertierbaren Elemente.

Lösung. **A ist ein Unterring von $\mathbb{Q}$:** Sei $x = \frac{m}{n}, y = \frac{m'}{n'} \in A$. Dann ist

$$\begin{aligned} x - y &= \frac{mn' - m'n}{nn'} \\ xy &= \frac{mm'}{nn'} \end{aligned}$$

Da $n, n' \equiv 1 \mod 2$ ist auch $nn' \equiv 1 \mod 2$, also $x - y, xy \in A$. Außerdem $1 = \frac{1}{1} \in A$, insbesondere ist $A \neq \varnothing$.

Die Inversen von A**:** Sei $x = \frac{m}{n} \in A$ invertierbar, also gibt es $y = \frac{m'}{n'}$ mit $xy = 1$, das heißt

$$\frac{mm'}{nn'} \frac{m}{n} \frac{m'}{n'} = 1$$

oder $mm' = nn'$. Da nn' ungerade ist, gilt das insbesondere auch für m.
Ist andererseits $x = \frac{m}{n} \in A$ mit m undgerade, dann ist $y = \frac{n}{m} \in A$ (falls $m > 0$ und $y = \frac{-n}{-m} \in A$ falls $m < 0$). Und $xy = 1$, also ist x invertierbar.
Insgesamt: die invertierbaren Elemente von A sind genau die $\frac{m}{n}$ mit $m \in \mathbb{Z}$, $n \in \mathbb{N}$, m, n ungerade.

Bemerkung: Die ungeraden ganzen Zahlen sind $S = \mathbb{Z} \backslash (2)$. Also ist A genau der Ring

$$\mathbb{Z}_S = \mathbb{Z}_{(2)} = \left\{ \frac{r}{s} \ ; \ r \in \mathbb{Z}, s \in S \right\} = \left\{ \frac{r}{s} \ ; \ r, s \in \mathbb{Z}, 2 \nmid s \right\}.$$

Aufgabe 4 (Frühjahr 1997)**.** Sei R ein Integritätsring mit Primring $\mathbb{Z}/(p)$, $p > 0$. Zeigen Sie, daß die Abbildung

$$F : R \to R, x \mapsto x^p$$

ein Ringhomomorphismus ist (der Frobenius).

Lösung. Es ist klar, daß $F(1) = 1$ ist und für alle $x, y \in R$ gilt $F(xy) = (xy)^p = x^p y^p = F(x)F(y)$, denn R ist kommutativ. Weiterhin berechnet man für $x, y \in R$

$$\begin{aligned} F(x+y) &= (x+y)^p \\ &= \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k} \end{aligned}$$

Es genügt nun nach dem vorherigen Beispiel zu zeigen, daß $p \big| \binom{p}{k}$ für $k = 1, \dots, p-1$. Nach Definition von $\binom{p}{k}$ gilt die Gleichheit

$$p! = \binom{p}{k} \cdot k! \cdot (p-k)!$$

Da offensichtlich $p \big| p!$, aber $p \nmid k!$ und $p \nmid (p-k)!$, und p eine Prmzahl ist, muß p $\binom{p}{k}$ teilen. Damit ist $\sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k} = 0$ und $F(x+y) = x^p + y^p = F(x) + F(y)$.

Aufgabe 5 (Herbs 1974)**.** (a) Sei K ein Körper der Charakteristik $\neq 0$. Zeigen Sie, daß dann die additive Gruppe von K nie isomorph zur multiplikativen Gruppe $K^\times$ sein kann.

(b) Sei K ein Körper der Charakteristik 0. Beweisen Sie, daß dann die additive Gruppe von K nie isomorph zur multiplikativen Gruppe $K^\times$ sein kann.

Lösung. **Zu (a):** Es ist $\mathrm{char}(K) = p$ eine Primzahl. Der Primkörper K_0 von K ist isomorph zu $\mathbb{F}_p = \mathbb{Z}/pZZ$.
Wir bemerken zunächst, daß für alle $x \in K$ gilt $px = 0$, denn $px = p(1 \cdot x) = (p \cdot 1)x = 0 \cdot x = 0$.
Angenommen $(K, +)$ und $(K \setminus \{0\}, \cdot)$ wären isomorph (als Gruppen), das heißt es gäbe einen Gruppenisomorphismus

$$\psi : K^\times \to K$$

Es gilt für $x, y \in K \setminus \{0\}$

$$\psi(x \cdot y) = \psi(x) + \psi(y)$$

Insbesondere ist

$$\psi(x^p) = p\psi(x) = 0$$

Also enthält $\ker(\psi)$ alle Elemente der Form x^p. Wir müssen nun ausschließen, daß alle x^p trivial sind.
Für $\mathbb{F}_p$ gilt nach dem kleinen Satz von Fermat $x^p = x$ für alle $x \in \mathbb{F}_p$. Also gilt dies auch für $K_0 \cong \mathbb{F}_p$.
Das heißt $\ker(\psi)$ enthält alle $x \in K_0^\times$, damit ist ψ nicht injektiv, also kein Isomorphismus.

Zu (b): Sei $\mathrm{char}(K) = 0$, dann ist $K_0 \cong \mathbb{Q}$.

Angenommen es gäbe einen Gruppenisomorphismus

$$\psi : K^\times \to K.$$

Wieder gilt $\psi(x \cdot y) = \psi(x) + \psi(y)$. In $\mathbb{Q}$ und somit auch in K_0 und in K gilt $-1 \neq 1$ und $(-1)^2 = (-1) \cdot (-1) = 1$. Also ist

$$0 = \psi(1) = \psi((-1)^2) = 2\psi(-1)$$

und es folgt $\psi(-1) = 0$. Und damit ist ψ nicht injektiv, also kein Isomorphismus.