Aufgabe 1 (Herbst 1989)**.** Seien

$$\begin{aligned} f &:= X^3 + 2X^2 - X - 1 \\ g &:= X^2 + X - 3 \end{aligned}$$

Polynome in $\mathbb{Q}[X]$. Man zeige, daß es Polynome $a, b \in \mathbb{Q}[X]$ gibt mit

$$af + bg = 1;$$

man gebe a, b explizit an. (3 Punkte)

Lösung. Der Polynomring $\mathbb{Q}[X]$ ist ein Euklidischer Ring mit Norm gegeben durch den Polynomgrad. Wir werden mit Hilfe des Euklidischen Algorithmus einen ggT von f und g bestimmen.

$$\begin{aligned} (X^3 + 2X^2 - X - 1) &= (X+1)(X^2 + X - 3) + (X+2) & \qquad r_{-1} &= q_1 r_0 + r_1 \\ (X^2 + X - 3) &= (X-1)(X+2) + (-1) & r_0 &= q_2 r_1 + r_2 \\ (X+2) &= (-X-2)(-1) + 0 & r_1 &= q_3 r_2 + 0 \end{aligned}$$

Nach drei Schritten ist der Euklidische Algorithmus beendet und wir sehen, daß $r_2 = -1$ ein ggT von f und g in $\mathbb{Q}[X]$ ist. Da -1 und 1 (wie alle invertierbaren Elemente von $\mathbb{Q}$) in $\mathbb{Q}[X]$ assoziiert sind, ist auch 1 ein ggT, also gibt es a und b wie gewünscht.
Mit Hilfe der Gleichungen des Euklidischen Algorithmus bestimmen wir nun rekursiv a und b. Es ist

$$r_2 = r_0(1 + q_1 q_2) - r_{-1} q_2$$

also

$$\begin{aligned} -1 &= (X^2 + X - 3)(1 + (X+1)(X-1)) - (X^3 + 2X^2 - X - 1)(X-1) \\ 1 &= (X^2 + X - 3)(-X^2) + (X^3 + 2X^2 - X - 1)(X-1) \end{aligned}$$

Aufgabe 2 (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.

(3 Punkte)

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 3 (Herbst 1981)**.** Sei R ein nullteilerfreier kommutativer Ring (nicht notwendig mit 1). Man beweise: Gibt es $a, c \in R$ mit $a \neq 0$ und $ac = a$, dann hat R ein Einselement, nämlich c. (3 Punkte)

Lösung. Wir müssen zeigen, daß für jedes Element $x \in R$ gilt $xc = x$. Dann gilt automatisch $cx = x$ wegen der Kommutativität von R. Die Gleichung $ac = a$ ist äquivalent zu

$$ac - a = 0.$$

(Es ist zu beachten, daß man hier **nicht** a ausklammern kann, also $\cancel{a(c-1) = 0}$ da R a priori keine 1 hat.) Wir multiplizieren x nun mit $0 = ac - a$

$$\begin{aligned} 0 = x \cdot 0 &= x(ac - a) \\ &= xac - xa \text{ (Distributivgesetz)} \\ &= axc - ax \text{ (Kommutativität)} \\ &= a(xc - x) \text{ (Distributivgesetz)} \end{aligned}$$

Da $a \neq 0$ und R nullteilerfrei ist, folgt $xc - x = 0$, also $xc = x$ wie gewünscht.

Aufgabe 4 (Frühjahr 1988)**.** (a) Sei R ein faktorieller Ring mit dem Quotientenkörper Q, sei weiter $f = f_0 + f_1X + \ldots + f_nX^n \in R[X]$ ein Polynom mit Koeffizienten in R. Eine Nullstelle von f sei $\frac{r}{s}$, wobei r und s teilerfremde Elemente aus R sind mit $s \neq 0$. Zeigen Sie, daß r Teiler von f_0 und s Teiler von f_n ist.

(b) Berechnen Sie alle rationalen Nullstellen von

$$f = 3X^4 + 4X^3 - 12X^2 + 4X - 15 \in \mathbb{Z}[X].$$

(c) Zeigen Sie: $qX^3 - p$ ist in $\mathbb{Z}[X]$ irreduzibel, wenn p und q verschiedene Primzahlen sind.

(6 Punkte)

Lösung. **Zu (a):** Da $\frac{r}{s}$ Nullstelle von f über K ist, ist $X - \frac{r}{s}$ ein Teiler von f. Es gibt also $g \in K[X]$ mit

$$f = (X - \frac{r}{s})g = (sX - r)\frac{1}{s}g.$$

Insbesondere ist $sX - r$ ein Teiler von f in $K[X]$. Da aber f und $sX - r \in R[X]$ und $sX - r$ primitiv ist, ist $sX - r$ auch ein Teiler von f in $R[X]$, das heißt $h := \frac{1}{s}g \in R[X]$. Insbesondere sind der konstante Koeffizient h_0 und der höchste Koeffizient h_{n-1} von h in R. Wir erhalten Gleichungen in R:

$$\begin{aligned} f_0 &= -rh_0 \\ f_n &= sh_{n-1} \end{aligned}$$

Also ist r Teiler von f_0 und s Teiler von f_n.
Zu (b): Die Teiler von 3 sind $\{\pm 1, \pm 3\}$. Die Teiler von 15 sind $\{\pm 1, \pm 3, \pm 5, \pm 15\}$. Also Nulstellen kommen also nach (a) in Frage:

$$\{\pm 1, \pm 3, \pm 5, \pm 15, \pm\frac{1}{3}, \pm\frac{5}{3}\}$$

Wir berechnen:

$$\begin{aligned} f(1) &= -16 \\ f(-1) &= -32 \\ f(3) &= 240 \\ f(-3) &= 0 \\ f(5) &= 2080 \\ f(-5) &= 1040 \\ f(15) &= 162720 \\ f(-15) &= 135600 \\ f(\frac{1}{3}) &= -14\frac{22}{27} \\ f(-\frac{1}{3}) &= -17\frac{21}{27} \\ f(\frac{5}{3}) &= 0 \\ f(-\frac{5}{3}) &= -50\frac{10}{27} \end{aligned}$$

Also sind die rationalen Nullstellen $\{-3, \frac{5}{3}\}$.

Zu (c): Da q und p relativ prim sind, also $\mathrm{ggT}(p,q) = 1$, ist das Polynom $qX^3 - p$ primitiv. Es genügt daher zu zeigen, daß $qX^3 - p$ irreduzibel in $\mathbb{Q}[X]$ (nach einer Folgerung aus dem Satz von Gauß).
Ein Polynom dritten Grades ist genau dann irreduzibel, wenn es keine Nullstelle hat. Nach (a) müsste für eine Nullstelle $\frac{r}{s}$ (mit $r, s \in \mathbb{Z}$ teilerfremd $s \neq 0$) gelten:

$$\begin{aligned} r \big| p &\text{ also } r \in \{1, -1, p, -p\} \\ s \big| q &\text{ also } s \in \{1, -1, q, -q\}. \end{aligned}$$

Es wäre also $\frac{r}{s} \in \{\pm 1, \pm p, \pm\frac{1}{q}, \pm\frac{p}{q}\}$. Durch Einsetzten sieht man leicht, daß keines davoin eine Nullstelle von $qX^3 - p$ sein kann. Also ist $qX^3 - p$ irreduzibel in $\mathbb{Q}[X]$ und damit auch in $\mathbb{Z}[X]$.
Oder: wende das Eisenstienkriterium an.

Zusatzaufgabe (Herbst 1989)**.** Man untersuche

$$f := X^3 - 5X^2 + 25X + 10$$

auf Irreduzibilität in den Ringen $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ und $\mathbb{C}[X]$ (eine kurze Begründung genügt jeweils). (4 Punkte)

Lösung. **Über $\mathbb{Z}$:** f ist ein Eisensteinpolynom für $p = 5$, also über $\mathbb{Z}$ irreduzibel.

Über $\mathbb{Q}$: Da $\mathbb{Q}$ der Quotientenkörper des faktoriellen Rings $\mathbb{Z}$ ist, und f irreduzibel über $\mathbb{Z}$, ist f auch irreduzibel über $\mathbb{Q}$ (folgt aus dem Satz von Gauß).

Über $\mathbb{R}$: Jedes kubische Polynom über $\mathbb{R}$ hat mindestens eine reelle Nullstelle, spaltet also einen Linearfaktor ab und ist damit reduzibel.

Über $\mathbb{C}$: Über dem algebraisch abgeschlossenen Körper $\mathbb{C}$ zerfällt jedes Polynom in Linearfaktoren. f ist also reduzibel.