Aufgabe 1 (Einstimmung)**.** Seien $p(X) = X^{500} - 2X^{301} + 1$ und $q(X) = X^2 - 1$ in $\mathbb{Q}[X]$. Man berechne den Rest von $p(X)$ bei Division mit $q(X)$.

Lösung. Dazu betrachten wir den Faktorring $\mathbb{Q}[X]/(q)$, und bemerken, daß zwei Elemente $f_1, f_2 \in \mathbb{Q}[X]$ modulo (q) gleich sind, wenn sie bei Division durch q den gleichen Rest haben, bzw. wenn $f_1 - f_2$ durch q teilbar ist. Insbesondere ist jedes Polynom $f \in \mathbb{Q}[X]$ modulo (q) gleich seinem Rest bei Division durch q. Sei nun r der Rest von p bei Division durch q, dh. $p = sq + r$ in $\mathbb{Q}[X]$ mit $\deg(r) < \deg(q) = 2$. Dann gilt

$$r + (q) = p + (q).$$

Wir finden r, indem wir einen bezüglich des Grads minimalen Repräsentanten der Klasse $p+(q)$ berechnen. Dafür bemerken wir noch, dass gilt $x^2 + (q) = 1 + (q)$.

$$\begin{aligned} p + (q) &= X^{500} - 2X^{301} + 1 + (q) \\ &= (X^{500} + (q)) - (2 + (q)) \cdot (X^{301} + q) + (1 + (q)) \\ &= ((X^2)^{250} + (q)) - (2 + (q)) \cdot ((X^2)^{150} + q)(X + (q)) + (1 + (q)) \\ &= (1^{250} + (q)) - (2 + (q)) \cdot (1^{150} + q)(X + (q)) + (1 + (q)) \\ &= (1 + (q)) - (2 + (q)) \cdot (1 + q)(X + (q)) + (1 + (q)) \\ &= (1 + (q)) - (2X + (q)) + (1 + (q)) = 2 - 2X + (q) \end{aligned}$$

Also ist die Differenz $r - (2 - 2X)$ durch q teilbar. Da aber beide Grad < 2 haben, gilt $r - (2 - 2X) = 0$ und $r = 2 - 2X$.

Aufgabe 2 (Frühjahr 2014)**.** Es seien K ein Körper und $K[X]$ der Polynomring in einer Unbekannten. Sei $n, m \in \mathbb{N}_0$. Zeigen Sie:
Ist $m > 1$, dann ist $X^r - 1$ der Rest bei Division von $X^n - 1$ durch $X^m - 1$, wobei r der Rest bei Division von n durch m ist.

Lösung. Sei $n = qm + r$ im euklidischen Ring $\mathbb{Z}$ mit $r < m$. Und sei $X^n - 1 = g(X^m - 1) + h$ mit $\deg(h) < \deg(X^m - 1) = m$. Diesmal arbeiten wir im Restklassenring $K[X]/(X^m - 1)$. Es gilt wieder $X^n - 1 \equiv h \mod (X^m - 1)$ und $X^m \equiv 1 \mod (X^m - 1)$. Damit berechnen wir einen minimalen Repräsentanten:

$$\begin{aligned} X^n - 1 &= X^{mq+r} - 1 \\ &= (X^m)^q X^r - 1 \\ &\equiv X^r - 1 \mod (X^m - 1) \end{aligned}$$

Es folgt für den Rest h, daß $h \equiv X^r - 1 \mod (X^m - 1)$, also ist die Differenz $h - (X^r - 1)$ durch $X^m - 1$ teilbar. Aber da sowohl h, als auch $X^r - 1$ Grad kleiner m haben, gilt $h - (X^r - 1) = 0$, also $h = X^r - 1$.

Aufgabe 3 (Herbst 1987)**.** R sei ein kommutativer Ring mit Eins und d eine Derivation von R, das heißt eine Abbildung $d : R \to R$ mit

$$d(x + y) = dx + dy \quad , \qquad d(x \cdot y) = x \cdot dy + y \cdot dx \quad \text{für alle } x, y \in R.$$

(a) Zeigen Sie, daß $\ker(d) := \{x \in R;\ dx = 0\}$ eine Unterring von R ist, der die Eins enthält.

(b) Beweisen Sie die Formel $d(x^n) = nx^{n-1}dx$ für $x \in R$, $n \in \mathbb{Z}, n > 0$.

(c) Zeigen Sie daß der Ring $\mathbb{Z}[X]/(X^2)$ eine nicht-triviale Derivation besitzt.

Lösung. **Zu (a):** Da $d(1) = d(1 \cdot 1) = 1d(1) + 1d(1)$, folgt $0 = d(1)$, also $1 \in \ker(d)$.
Sei $x, y \in \ker(d)$. Dann ist $d(x - y) = d(x) - d(y) = 0 - 0 = 0$ und $d(xy) = xd(y) + yd(x) = 0 + 0 = 0$, also $x - y, xy \in \ker(d)$, und $\ker(d)$ ist ein Unterring.

Zu (b): Mit Induktion nach n. Klar für $n = 1$. Angenommen wir wissen $d(x^{n-1}) = (n-1)x^{n-2}dx$. Schreibe

$$d(x^n) = d(x^{n-1}x) = x^{n-1}d(x) + xd(x^{n-1}) = x^{n-1}d(x) + x(n-1)x^{n-2}dx = nx^{n-1}dx.$$

Zu (c): Wir definieren zunächst eine nicht-triviale Derivation von $\mathbb{Z}[X]$ und zeigen, daß diese eine nicht-triviale Derivation von $\mathbb{Z}[X]/(X^2)$ induziert. (Wir überlegen uns zunächst folgendes:
Für eine solche Derivation gilt, daß $d(n) = 0$, für alle $n \in \mathbb{Z}$, da nach (a) $1 \in \ker(d)$, und $d(n) = d(1+\ldots+1) = d(1)+\ldots+d(1)$. Da $\mathbb{Z}[X]$ eine $\mathbb{Z}$-Algebra ist, genügt es eine Derivation auf X zu definieren: für die Monome X^n kann man $d(X^n)$ dann mit dem Resultat aus (b) berechnen. Damit kann man dann für beliebige Polynome $\sum_{i=0}^n a_i X^i$ den Wert $d(\sum_{i=0}^n a_i X^i)$ mithilfe der "Summenformel" bestimmen. Damit dies dann eine Derivation auf $\mathbb{Z}[X]/(X^2)$ induziert, sollten Elemente aus dem Ideal (X^2) auf Elemente in (X^2) selbst geschickt werden.)
Betrachte nun die Derivation definiert durch

$$X \mapsto d(X) = X.$$

Dann ist nach der "Produktformel" (oder genauer Aufgabe (b))

$$d(X^n) = nX^{n-1}d(X) = nX^n.$$

Mit der Summenformel erhalten wir für $f = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$

$$d(f) = \sum_{i=0}^{n} i a_i X^i.$$

Insbesondere ist das Bild des Ideals (X^2) unter d wieder in dem Ideal selbst enthalten. Also induziert $d : \mathbb{Z}[X] \to \mathbb{Z}[X]$ eine Derivation auf $\mathbb{Z}[X]/(X^2)$ und das Diagramm

$$\begin{array}{ccc} \mathbb{Z}[X] & \xrightarrow{d} & \mathbb{Z}[X] \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{Z}[X]/(X^2) & \xrightarrow{d} & \mathbb{Z}[X]/(X^2) \end{array}$$

wobei π die knonische Projektion ist, kommutiert.

Aufgabe 4 (Frühjahr 1972)**.** Sei $P(x) \in \mathbb{Z}[x]$ ein Polynom mit der Eigenschaf, daß es ganze Zahlen a, b gibt mit $P(a) - P(b) = q$, wobei q eine Primzahl ist. Zeigen Sie, daß $a - b$ nur einen der Werte $-q, -1, 1, q$ annehmen kann.

Lösung. Zunächst bemerken wir, daß $a \neq b$ sein muß.
Sei $P(x) = a_0 + a_1 x^1 + \ldots + a_n x^n$. Nach Voraussetzung ist

$$q = P(a) - P(b) = (a_0 + \ldots + a_n a^n) - (a_0 + \ldots + a_n b^n) = a_1(a-b) + a_2(a^2 - b^2) + \ldots a_n(a^n - b^n).$$

Nun wissen wir, daß für $i \geqslant 1$

$$(a^i - b^i) = (a-b)(a^{i-1} + a^{i-2}b + \ldots + ab^{n-2} + b^{n-1}).$$

Also teilt $(a-b)$ die rechte Seite der obigen Gleichung. Damit ist $(a-b)$ ein Teiler von q. Da aber q eine Primzahl ist, muß $(a-b) \in \{q, -q, 1, -1\}$ liegen.

Aufgabe 5 (Herbst 1981)**.** Lösen Sie folgende Gleichungen für Polynome $P, Q \in \mathbb{R}[X]$.

(a) $P(X^2) = (X^2+1)P(X)$.

(b) $Q(Q(X)) = Q(X)$.

Lösung. **Zu (a):** Das Nullpolynom ist offensichtlich eine Lösung. Weiterhin gilt für eine Lösung P

$$2\deg(P) = \deg(P) + 2.$$

Also ist P vom Grad 2. Wir schreiben $P(X) = aX^2 + bX + c$. Also

$$P(X^2) = aX^4 + bX^2 + c$$
$$(X^2+1)P(X) = aX^4 + bX^3 + (a+c)X^2 + bX + c$$

Indem wir diese gleichsetzen schließen wir, daß $b = 0$, und weiter $a + c = 0$. Also sind die Lösungen von der Form

$$P(X) = a(X^2 - 1)$$

für $a \in \mathbb{R}$.

Zu (b): Ist Q eine nichttriviale Lösung (also $\neq 0$), so ist $\deg(Q \circ Q) = \deg(Q)^2$, damit erhalten wir die Gleichung

$$\deg(Q)^2 = \deg(Q).$$

Damit $\deg(Q) = 1$ oder $\deg(Q) = 0$ (also konstant $\neq 0$). Wir schreiben $Q(X) = aX + b$, also

$$\begin{aligned} Q \circ Q(X) &= a(aX + b) + b = a^2X + (ab + b) \\ Q(X) &= aX + b \end{aligned}$$

Also $a^2 = a$, das heißt $a = 1$ oder $a = 0$, und $ab = 0$. Ist $a = 1$, so ist $b = 0$. Ist $a = 0$, so kann $b \in \mathbb{R}$ beliebig sein. Also sind die Lösungen der Gleichung die konstanten Polynome und das Polynom $Q(X) = X$.

Aufgabe 6 (Frühjahr 1993)**.** Für $P \in \mathbb{R}[X]$ und $a, b \in \mathbb{R}$, $a \neq b$, sei 1 der Rest bei Division von P durch $(X - a)$ und -1 der Rest bei Division von P durch $(X - b)$.
Was ist der Rest bei Division von P durch $(X - a)(X - b)$?

Lösung. Wir wissen, daß $P(X) = (X - a)Q_1(X) + 1$, also $P(a) = 1$. Ebenso $P(X) = (X - b)Q_2(X) - 1$, also $P(b) = -1$. Wir schreiben für die Division von $P(X)$ durch $(X - a)(X - b)$

$$P(X) = (X - a)(X - b)Q(X) + R(X)$$

wobei $\deg(R) < 2$. Schreibe $R(X) = \alpha x + \beta$. Wir setzten in die obige Gleichung a und b ein, und erhalten:

$$\begin{aligned} \alpha a + \beta &= 1 \\ \alpha b + \beta &= -1 \end{aligned}$$

Die Lsung dieses GLeichungssystmes ist

$$\begin{aligned} \alpha &= \frac{2}{a - b} \\ \beta &= \frac{-a - b}{a - b} \end{aligned}$$

Also ist der Rest bei Division von P durch $(X - a)(X - b)$ gleich

$$R(X) = \frac{2}{a - b}X + \frac{-a - b}{a - b}.$$

Aufgabe 7 (Frühjahr 1991)**.** Sei K ein Körper und $A, B, P \in K[X]$, P nicht konstant. Angenommen $A \circ P \big| B \circ P$. Man zeige $A \big| B$.

Lösung. Es gibt $Q, R \in K[X]$ mit $B = AQ + R$ und $\deg(R) < \deg(A)$. Komposition mit P ergibt die Gleichung

$$B \circ P = (A \circ P)(Q \circ P) + R \circ P.$$

Das Polynom $A \circ P \in K[X]$ hat den Grad $\deg(A \circ P) = \deg(A) \cdot \deg(P)$. Ebenso hat das Polynom $R \circ P$ den Grad $\deg(R \circ P) = \deg(R) \cdot \deg(P)$. Also ist $\deg(R \circ P) < \deg(A \circ P)$. Nach der Einduetigkeit der Division mit Rest, angewendet auf die Division von $B \circ P$ durch $(A \circ P)$, muss dann aber $R \circ P = 0$ sein. Dies ist aber nur möglich, wenn bereits $R = 0$ ist. Also $B = AQ$ und $A \big| B$ wie gewünscht.