Aufgabe 1 (Herbst 1998)**.** Sei p eine Primzahl.

(a) Zeigen Sie, daß das Polynom $f = X^p - X - 1$ irreduzibel über dem endlichen Körper $\mathbb{F}_p$ ist.

(b) Ist f auch irreduzibel über $\mathbb{Z}$? Die Antwort ist zu begründen.

Lösung. **Zu (a):** Es ist klar, daß f keine Nullstellen (Wurzeln) in $\mathbb{F}_p$ hat, denn nach dem kleinen Satz von Fermat ist für $a \in \mathbb{F}_p$ immer $a^p = a$, also $f(a) = -1$. Sei α eine Nullstelle in einem Erweiterungskörper, dann kann man alle Nullstellen von f angeben:

$$\{\alpha, \alpha + 1, \alpha + 2, \ldots, \alpha + p - 1\}$$

also $f = (X - \alpha)(X - \alpha - 1)\cdots(X - \alpha - p + 1)$. Sei

$$f = gh, \text{ mit } g, h \in \mathbb{F}_p[X] \text{ und } \deg g = d$$

eine Faktorisierung von f über $\mathbb{F}_p$. In dem gleichen Erweiterungskörper wie oben zerfällt g, und man kann schreiben

$$g = (X - \alpha)(X - \alpha - c_1))\cdots(X - \alpha - c_d) = X^d - \sum_{i=1}^{d}(\alpha + c_i)X^{d-1} + \ldots + (-1)^d \prod_{i=1}^{d}(\alpha + c_i),$$

mit $\{c_1, \ldots, c_d\} \subsetneq \mathbb{F}_p$. Der Koeffizient von X^{d-1} in g ist also

$$-\sum_{i=1}^{d}(\alpha + c_i) = -(d\alpha + \sum_{i=1}^{d} c_i) \in \mathbb{F}_p\,.$$

Da die $c_i \in \mathbb{F}_p$ muß also auch $d\alpha \in \mathbb{F}_p$. Ist $d \not\equiv 0 \mod p$, müss also $\alpha \in \mathbb{F}_p$, unmöglich. Also ist $d = 0$ oder $d = p$ und damit die Faktorisierung trivial.

Zu (b): Nach dem Reduktionskriterium ist f irreduzibel über $\mathbb{Z}$, da es irreduzibel über $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ist.

Aufgabe 2 (Frühjahr 1992)**.** Sei K ein Körper, a ein Element von K, und seine m und n zwei natürliche Zahlen $\neq 0$, die relativ prim zueinander sind. Zeigen Sie, daß das Polynom $X^{mn} - a$ genau dann irreduzibel über K ist, wenn die Polynome $g_m = X^m - a$ und $g_n = X^n - a$ irreduzibel über K sind.
Nur eine Richtunug möglich ohne Galoistheorie/Körpertheorie. Die zweite werden wir später anschauen.

Lösung. Es ist $X^{nm} - a = (X^n)^m - a = (X^m)^n - a$. Ist also $Y^n - a$ (oder $Y^m - a$) reduzibel mit $Y^n - a = f(Y)g(Y)$, so ist

$$X^{nm} - a = (X^m)^n - a = f(X^m)g(X^m)$$

reduzibel. Dies zeigt: Ist $X^{nm} - a$ irreduzibel, so auch $X^n - a$ und $X^m - a$.

Aufgabe 3 (Herbst 1998)**.** Ist das Polynom

$$3X^3 - 6X^2 + \frac{3}{2}X - \frac{3}{5}$$

in $\mathbb{Q}[X]$ irreduzibel?

Lösung. Da

$$f = 3X^3 - 6X^2 + \frac{3}{2}X - \frac{3}{5} = \frac{3}{10}(10X^3 - 20X^2 + 5X - 2) = u \cdot \widetilde{f}$$

ist, mit $\widetilde{f} = 10X^3 - 20X^2 + 5X - 2 \in \mathbb{Z}[X]$, genügt es zu zeigen, daß $\widetilde{f}$ irreduzibel über $\mathbb{Z}$ ist.
Bemerke: $\widetilde{f} = 10X^3 - 20X^2 + 5X - 2 \in \mathbb{Z}[X]$ primitiv, es spaltet also über $\mathbb{Z}$ kein konstantes nichttriviales Polynom ab. Es ist mglich das Reduktionskritrium anzuwenden mit $p = 3$:

$$\widetilde{f} \equiv X^3 + X^2 + 2X + 1 \mod 3.$$

Ein primitives Polynom dritten Grades über einem Körper ist genau dann irreduzibel, wenn es keine Nullstelle hat. Wir testen die drei möglichen Werte:

$$\widetilde{f}(0) = 1 \equiv 1 \mod 3$$
$$\widetilde{f}(1) = 5 \equiv 2 \mod 3$$
$$\widetilde{f}(2) = 17 \equiv 2 \mod 3$$

Also ist $\widetilde{f}$ irreduzibel über $\mathbb{Z}/3\mathbb{Z}$ und damit auch über $\mathbb{Z}$ und über $\mathbb{Q}$.

Aufgabe 4 (Herbst 1999). (a) Seien R ein Integritätsring und $a \in R$. Man zeige: Das Polynom $X^2 + a$ ist genau dann reduzibel in $R[X]$, wenn $-a$ ein Quadrat in R ist.

(b) Sei K ein Körper, der nicht Charakteristik 2 besitzt. Man zeige: Für alle $n \in \mathbb{N}$, $n \geqslant 3$, ist das Polynom $X_1^2 + X_2^2 + \ldots + X_n^2$ im Polynomring $K[X_1, \ldots, X_n]$ irreduzibel.

Lösung. **Zu (a):** Angenommen $-a$ ist ein Quadrat in R, das heißt es gibt $r \in R$ mit $r^2 = -a$. Dann ist

$$X^2 + a = (X + r)(X - r)$$

eine Zerlegung in R von $X^2 + a$ in Linearfaktoren.
Nehmen wir umgekehrt an, daß $X^2 + a$ reduzibel ist, also in Linearfaktoren zerfällt. Dann hat es in R eine Nullstelle r. Es gilt $r^2 + a = 0$, das heißt $r^2 = -a$. In anderen Worten $-a$ ist ein Quadrat in R.

Zu (b): Zunächst bemerken wir, daß für $n \in \mathbb{N}$ $K[X_1, \ldots, X_n]$ Integritätsring ist. Wir wenden Induktion nach n an.
Induktionsanfang: Wir stellen fest, daß $f_2 = X_1^2 + X_2^2 \in K[X_1, X_2]$ irreduzibel ist. Dazu identifizieren wir $K[X_1, X_2]$ mit dem Polynomring in einer Variablen $K[X_1][X_2]$ über dem Ring $K[X_1]$. Der konstante Koeffizient von f_2 ist X_1^2. Wäre f_2 reduzibel, so würde es über $K[X_1]$ in Linearfaktoren zerfallen, es hätte also eine Nullstelle in $K[X_1]$. Dies Nullstelle ist ein Teiler in $K[X_1]$ vom konstanten Koeffizienten X_1^2, also $\pm 1, \pm X_1, \pm X_1^2$. Man prüft leicht nach, daß keiner dieser Teiler Nullstelle von f_2 sein kann, da in K gilt $-1 \neq 1$ (da $\operatorname{char} K \neq 2$). Also ist f_2 irreduzibel, insbesondere ist $-f_2$ kein Quadrat in $K[X_1, X_2]$.
Induktionsschritt: Angenommen wir haben bereits gezeigt, daß $f_{n-1} = X_1^2 + \ldots + X_{n-1}^2$ irreduzibel in $K[X_1, \ldots, X_{n-1}]$ ist, insbesondere ist $-f_{n-1}$ kein Quadrat in diesem Ring. Wir betrachten $f_n = X_1^2 + X_2^2 + \ldots + X_n^2$ als Polynom in einer Variablen X_n über dem Ring $K[X_1, \ldots, X_{n-1}]$ mit konstantem Koeffizienten f_{n-1}. Da $-f_{n-1}$ kein Quadrat in $K[X_1, \ldots, X_{n-1}]$ ist, ist nach (a) also f_n ebenfalls irreduzibel.

Aufgabe 5 (Herbst 1995). R sei ein kommutativer Ring, der einen Körper k enthält und somit auf natürliche Weise ein k-Vektorraum ist. Es sei $\dim_k R < \infty$. Man beweise:

(a) Alle Primideale von R sind maximal.

(b) R hat höchstens $\dim_k R$ maximale Ideale.

Lösung. **Zu (a):** Sei $P \subset R$ ein Primideal. Dann ist R/P ein Integritätsring. Wir zeigen, daß dies schon ein Körper ist. Da P als Primideal ein echtes Ideal von R ist, enthält es keine invertierbaren Element, insbesondere enthält es keine Elemente aus der multiplikativen Gruppek^*. Also ist die Komposition

$$k \hookrightarrow R \to R/P$$

injektiv und R/P ist ebenfalls ein endlichdimensionaler k-Vektorraum.
Wir zeigen, daß jedes Element $0 \neq \overline{a} \in RP$ invertierbar ist. Für ein solches $\overline{a}$ betrachte wie üblich den Ringhomomorphismus gegeben durch

$$\varphi : R/P \to R/P, \overline{r} \mapsto \overline{ra}.$$

Dieser ist injektiv wegen der „Kürzungsregel" in Integritätsringen:
ist $\varphi(\overline{r}_1) = \varphi(\overline{r}_2)$, also $\overline{r}_1\overline{a} = \overline{r}_2\overline{a}$, so ist $\overline{r}_1 = \overline{r}_2$.
Die Abbidlung φ ist auch ein k-Vektorraumhomomorphismus, genauer ein Endomorphismus von R/P. Da R/P endlich-dimensional ist, ist φ sogar surjektiv, also bijektiv. Also gibt es $\overline{x} \in R/P$, mit $\overline{ax} = \varphi(\overline{x}) = \overline{1}$. Dies zeigt, daß $\overline{a}$ invertierbar ist.

Zu (b): Sei $n = \dim_k R$. Je zwei verschiedene Primideal P_1 und P_2 von R sind paarweise fremd, da sie nach (a) maximale Ideale sind. Für j verschiedenen Primideale $P_1, \ldots P_j$ von R gilt also nach dem Chinesischen Restsatz

$$R/P_1 \cdots P_j \cong \prod_{i=1}^{j} R/P_i$$

als R-Algebren. Die $R/P_1 \cdots P_j$ und R/P_i sind k-Algebren mit

$$\dim_k R/P_1 \cdots P_j \leqslant \dim_k R = n$$
$$1 \leqslant \dim_k R/P_i \leqslant \dim_k R = n$$
$$j \leqslant \dim_k \prod_{i=1}^{j} R/P_i$$

Es folgt, daß $j \leqslant n$ sein muß, es also nur n verschiedenen Primideale in R geben kann.

Aufgabe 6 (??). Sei K ein Körper. Seien $n, m \in \mathbb{N}$ teilerfremd. Man zeige, daß das Polynom $f = X^n - Y^m \in K[X,Y]$ irreduzibel ist.

Lösung. Angenommen dies ist nicht der Fall, dann gibt es Polynome $g, h \in K[X,Y]$ mit $X^n - Y^m = f = g \cdot h$. Betrachte den K-Algebrenhomomorphismus

$$K[X,Y] \mapsto K[Z], X \mapsto Z^m, Y \mapsto Z^n.$$

Für das Bild von f unter diesem Homomorphismus gilt

$$0 = (Z^m)^n - (Z^n)^m = f(Z^m, Z^n) = g(Z^m, Z^n)h(Z^m, Z^n).$$

Da $K[Z]$ Integritätsring ist, muß eines der beiden Polynome $g(Z^m, Z^n)$ oder $h(Z^m, Z^n)$ das Nullpolynom sein. Ohne Einschränkung sei dies $g(Z^m, Z^n)$. Mit $g(X,Y) = \sum_{\substack{i,j \\ i<n, j<m}} a_{ij} X^i Y^j$ können wir also schreiben

$$g(Z^m, Z^n) = \sum_{\substack{i,j \\ i<n, j<m}} a_{ij} Z^{mi} Z^{nj} = \sum_k \sum_{\substack{i<n, j<m \\ mi+nj=k}} a_{ij} Z^k.$$

Damit $g(Z^m, Z^n)$ das Nullpolynom ist, müssen alle Koeffizienten der Z^k gleich 0 sein, es muß also für alle k gelten

$$\sum_{\substack{i<n, j<m \\ mi+nj=k}} a_{ij} = 0.$$

Es können jedoch für festes k in einer solche Summe nicht mehrere Summanden vorkommen, denn wäre $mi + nj = mi' + nj'$, so wäre $m(i - i') = n(j' - j)$. Dies bedeutet

$$\begin{aligned} i &\equiv i' \mod n \\ j &\equiv j' \mod m \end{aligned}$$

aber es gilt $i, i' \in \{0, \ldots, n-1\}$ und $j, j' \in \{0, \ldots, m-1\}$, so daß folgt $i = i'$ und $j = j'$. Also besteht die Summe $\sum_{\substack{i<n, j<m \\ mi+nj=k}} a_{ij}$ aus höchstem einem a_{ij}, und dieses muß dann gleich 0 sein. Also ist auch das Polynom $g(X,Y) = \sum_{\substack{i,j \\ i<n, j<m}} a_{ij} X^i Y^j$ gleich 0. Widerspruch.

Aufgabe 7. Eine natürliche Zahl heißt quadratfrei, wenn sie durch keine Quadratzahl ungleich 1 teilbar ist. Man zeige, daß es beliebig lange Abschnitte direkt aufeinander folgender natürlicher Zahlen gibt, in denen jedes Folgeglied nicht quadratfrei ist.

Lösung. Sei $\{p_1, p_2, \ldots, p_i, \ldots\} \subset \mathbb{N}$ die Menge der positiven Primzahlen in $\mathbb{Z}$. Sei n beliebig. Die Quadrate $p_1^2, p_2^2, \ldots, p_n^2$ sind paarweise relativ prim. Also ist nach dem Chinesischen Restsatz die Abbildung

$$\mathbb{Z}/(p_1^2 \cdots p_n^2) \to \prod_{i=1}^n \mathbb{Z}/(p_i^2), x + (p_1^2 \cdots p_n^2) \mapsto \left(x + (p_1^2), \ldots, x + (p_n^2)\right)$$

ein $\mathbb{Z}$-Algebrenisomorphismus, und für $b_1, \ldots, b_n \in \mathbb{Z}$ gibt es $x \in \mathbb{Z}$ mit $x \equiv b_i \mod p_i^2$.
Wählen wir für die Zahlen b_i die aufeinanderfolgenden Zahlen 0 bis $n-1$, also $b_1 = 0, b_2 = 1, \ldots, b_n = n-1$, so erhalten wir also $a_n \in \mathbb{Z}$ mit

$$\begin{aligned} a_n &\equiv 0 \mod p_1^2 \\ a_n &\equiv 1 \mod p_2^2 \\ &\vdots \\ a_n &\equiv n-1 \mod p_n^2 \end{aligned}$$

Für $1 \leqslant k \leqslant n$ ist also $a_n + k - 1$ durch p_k^2 teilbar , und damit nicht quadratfrei.
Wir haben also aufeinanderfolgende natürliche Zahlen $a_n, \ldots, a_n + n - 1$ konstruiert, die nicht quadratfrei sind.