1.Aufgabe

Sei K ein Körper, $A \in M(n\times n, K)$. Dann gibt es $P, Q \in M(n\times n, K)$ invertierbar mit: $D := PAQ$ ist eine Diagonalmatrix mit Koeffizienten 0 und 1. Dann ist $D^2 = D$. Setze $B := QP$. Dann ist:

$$ABA = P^{-1}PAQPAQQ^{-1} = P^{-1}DDQ^{-1} = P^{-1}DQ^{-1} = A.$$

2.Aufgabe

(a)Sei $A = \begin{pmatrix} 1001 & 0 \\ 0 & 1001 \end{pmatrix}$.

- In $\mathbb{Z}/3\mathbb{Z}$ ist $\overline{A} = \begin{pmatrix} \overline{2} & 0 \\ 0 & \overline{2} \end{pmatrix}$ invertierbar, da $\det \overline{A} = \overline{1}$ invertierbar ist.
- In $\mathbb{Z}/5\mathbb{Z}$ ist $\overline{A} = \begin{pmatrix} \overline{1} & 0 \\ 0 & \overline{1} \end{pmatrix}$ invertierbar, da $\det \overline{A} = \overline{1}$ invertierbar ist.
- In $\mathbb{Z}/7\mathbb{Z}$ ist $\overline{A} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ nicht invertierbar, da $\overline{A}$ die Nullmatrix ist.
- In $\mathbb{Z}/11\mathbb{Z}$ ist $\overline{A} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ nicht invertierbar, da $\overline{A}$ die Nullmatrix ist.
- In $\mathbb{Z}/13\mathbb{Z}$ ist $\overline{A} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ nicht invertierbar, da $\overline{A}$ die Nullmatrix ist.

(b) Zu zeigen: Eine Matrix $A \in M(n \times n, \mathbb{Z})$ ist genau dann über $\mathbb{Z}$ invertierbar, wenn A modulo jeder Primzahl invertierbar ist.

- Sei $A \in M(n \times n, \mathbb{Z})$ über $\mathbb{Z}$ invertierbar, dann ist $\det(A)$ in $\mathbb{Z}$ invertierbar, d.h: es gibt $\det(A)^{-1}$. Sei p eine beliebipe Primzahl. Dann ist in $\mathbb{Z}/p\mathbb{Z}$:
$$\overline{\det(A)}\,\overline{\det(A)^{-1}} = \overline{\det(A)\det(A)^{-1}} = \overline{1}.$$
Also ist $\overline{\det(A)}$ invertierbar und damit auch die Matrix $\overline{A}$.
- Sei A nicht invertierbar über $\mathbb{Z}$. Dann ist $\det(A) \neq 1$ und $\det(A) \neq -1$. Damit gibt es eine Primzahl p mit $p|\det(A)$. Dann ist in $\mathbb{Z}/p\mathbb{Z}$: $\overline{\det(A)} = 0$. Also ist $\overline{A}$ nicht invertierbar.

3.Aufgabe

Sei $n \in \mathbb{N}_1$. Zu zeigen: $\mathbb{Z}/n\mathbb{Z}$ besitzt genau dann nichttriviale nilpotente Elemente, wenn es eine Primzahl p mit $p^2|n$ gibt.

- Sei $n = p^2k$ mit $k \in \mathbb{N}$. Dann ist:

$$(pk)^2 = p^2k^2 = nk.$$

Also wird $(pk)^2$ von n geteilt, pk allerdings nicht, da $pk < n$. Also ist in $\mathbb{Z}/n\mathbb{Z}$ $\overline{pk}$ ein von Null verschiedenes nilpotentes Element.

- Sei nun $0 < r < n$ und $t \in \mathbb{N}_1$ mit: $\overline{r}^t = 0$. r lässt sich in seine Primfaktoren zerlegen:

$$r = \prod_{i=1}^{n} p_i^{l_i}.$$

Dann ist:

$$r^t = \prod_{i=1}^{n} p_i^{tl_i}.$$

Da $n|r^t$, besteht die Primfaktorzerlegung von n nur aus den gleichen Primzahlen jedoch mit anderen Vielfachheiten $l_i' \in \mathbb{N}_0$.

$$n = \prod_{i=1}^{n} p_i^{l_i'}$$

Angenommen alle $l_i < 2$. Dann würde $n|r$ und damit $\overline{r} = 0$ gelten, was ein Widerspruch ist. Es gibt also ein i mit $l_i' > 1$. Damit gilt: $p_i^2|n$.

4.Aufgabe

Sei K ein Körper. $a_i \in K$ für $i = 0, \ldots, n$ paarweise verschieden.

(a) Zu zeigen: Es gibt ein Polynom $f \in K[X]$ mit $\deg(f) = n$, $f(a_0) = 1$ und $f(a_i) = 0$ für $i = 1, \ldots, n$.
Sei

$$f := \prod_{i=1}^{n} \frac{X - a_i}{a_0 - a_i}$$

Dann ist:

$$f(a_0) = \prod_{i=1}^{n} \frac{a_0 - a_i}{a_0 - a_i} = 1$$

und für $j = 1, \ldots, n$:

$$f(a_j) = \prod_{i=1}^{n} \frac{a_j - a_i}{a_0 - a_i} = 0.$$

Das Polynom f hat Grad n und erfüllt auch die anderen Bedingungen.

(b) Zu zeigen: Sind $b_0, \ldots, b_n \in K$, so gibt es ein eindeutig bestimmtes Polynom $g \in K[X]$ mit $\deg(g) \leq n$ und $g(a_i) = b_i$ für $i = 0, \ldots, n$.
Existenz: Nach Teil (a) gibt es Polynome f_j mit $f_j(a_i) = \delta_{ij}$ für $j = 0, \ldots, n$. (Um das Polynom f_j zu erhalten muss man a_0 und a_j vertauschen.) Setze nun:

$$g := \sum_{i=0}^{n} b_i f_i$$

Dann ist g als Summe von Polynomen n-ten Grades höchstens ein Polynom n-ten Grades mit:

$$g(a_j) = \sum_{i=0}^{n} b_i f_i(a_j) = \sum_{i=0}^{n} b_i \delta_{ij} = b_j$$

für j=0,. . . ,n.
Eindeutigkeit: Sei $h \in K[X]$ ein weiteres Polynom mit Grad $\leq n$ und $h(a_i) = b_i$. Dann ist: $\deg(g - h) \leq n$, und außerdem:

$$(g - h)(a_i) = g(a_i) - h(a_i) = b_i - b_i = 0.$$

Also existiern $n+1$ Nullstellen von $g-h$ und damit ist $g-h$ das Nullpolynom. Also muss $g = h$ gelten.

5.Aufgabe

Sei $K = \{a_0, \ldots, a_{q-1}\}$ ein Körper. Sei $\Pi_q = \{p \in K[X] | \deg(p) < q\}$. Sei ϵ die Auswertungsabbldung:

$$\epsilon : \Pi_q \longrightarrow K \text{ mit } \epsilon(f)(a) = f(a) \text{ für } f \in \Pi_q, a \in K$$

Zu zeigen: ϵ ist biektiv.
Surjektivität: Sei $h : K \longrightarrow K$ eine beliebige Abbildung. Dann gibt es nach Aufgabe 4(b) ein Polynom g mit Grad $< q$ und $g(a_i) = h(a_i)$ für $i = 0, \ldots, q-1$. Dann gilt, dass $\epsilon(g)(a) = g(a) = h(a)$ ist für alle $a \in K$. Also ist $\epsilon(g) = h$.
Injektivität: Seien $f, g \in \Pi_q$ mit $\epsilon(f) = \epsilon(g)$. Dann sind f und g zwei Polynome mit Grad $< q$ und $f(a_i) = g(a_i)$ für $i = 0, \ldots, q-1$. Nach Aufgabe 4(b) ist ein Polynom durch diese Eigenschaften eindeutig bestimmt. Also ist $f = g$ und damit ist ϵ injektiv.

6.Aufgabe

Gesucht sind alle irriduziblen Polynome fünften Grades in $\mathbb{Z}/2\mathbb{Z}[X]$. Von einem Polynom in $\mathbb{Z}/2\mathbb{Z}[X]$ lässt sich genau dann ein Linearfaktor abspalten, wenn es

eine Nullstelle besitzt. Das ist genau dann der Fall, wenn der niedrigste Koeffizient 0 ist oder die Summe aller Koefizienten 0 ist. Da ein Polynom zweiten oder dritten Grades genau dann irreduzibel ist, wenn es man einen Linearfaktor abspalten kann, gibt es folgende irreduziblen Polynome vom Grad 2 und 3:

- $X^2 + X + 1$
- $X^3 + X^2 + 1$
- $X^3 + X + 1$

Ein Polynom fünften Grades ist genau dann irreduzibel, wenn sich kein Linearfaktor abspalten lässt und es nicht in ein irreduzibles Polynom zweiten Grades und ein irreduzibles Polynom dritten Grades zerfällt. Die Polynom fünften Grades ohne Nullstelle sind:

- $X^5 + X + 1$
- $X^5 + X^2 + 1$
- $X^5 + X^3 + 1$
- $X^5 + X^4 + 1$
- $X^5 + X^4 + X^3 + X^2 + 1$
- $X^5 + X^4 + X^3 + X + 1$
- $X^5 + X^4 + X^2 + X + 1$
- $X^5 + X^3 + X^2 + X + 1$

Von diesen Polynomen muss man noch Produkte irreduzibler Polynome vom Grad zwei und drei ausschließen. Das sind:

- $(X^2 + X + 1)(X^3 + X^2 + 1) = X^5 + X + 1$
- $(X^2 + X + 1)(X^3 + X + 1) = X^5 + X^4 + 1$

Also sind die irrduziblen Polynome vom Grad fünf:

- $X^5 + X^2 + 1$
- $X^5 + X^3 + 1$
- $X^5 + X^4 + X^3 + X^2 + 1$
- $X^5 + X^4 + X^3 + X + 1$
- $X^5 + X^4 + X^2 + X + 1$
- $X^5 + X^3 + X^2 + X + 1$