Aufgabe 1.

Zu zeigen: Die Summe der ersten n ungeraden natürlichen Zahlen ist gleich n^2.
Aus der Vorlesung ist bekannt:

$$\forall\, n \in \mathbb{N}: \quad \sum_{k=1}^{n} k = \frac{n(n+1)}{2}\,.$$

Die k-te ungerade Zahl kann man in der Form $2k-1$ darstellen. Es gilt

$$\sum_{k=1}^{n}(2k-1) = 2\sum_{k-1}^{n} k - \sum_{k=1}^{n} 1 = 2\frac{n(n+1)}{2} - n = n^2$$

q.e.d.

Aufgabe 2.

Sei G eine Gruppe und $a \in G$. Zeigen Sie, dass die Abbildung $f : G \to G$ mit $f(b) = a \circ b \circ a^{-1}$ einen Isomorphismus von Gruppen darstellt.

<u>Beweis</u>:
Seien $b, c \in G$ und e das neutrale Element von G. Dann ist

$$\begin{aligned} f(b \circ c) &= a \circ (b \circ c) \circ a^{-1} \\ &= a \circ b \circ e \circ c \circ a^{-1} \\ &= (a \circ b \circ a^{-1}) \circ (a \circ c \circ a^{-1}) \\ &= f(b) \circ f(c) \end{aligned}$$

Also ist f ein Gruppenhomomorphismus. Bleibt noch die Bijektivität von f zu zeigen.

$$\begin{aligned} \mathrm{Kern}(f) &= \{b \in G \mid a \circ b \circ a^{-1} = e\} \\ &= \{b \in G \mid a \circ b = a\} \\ &= \{b \in G \mid b = e\} \\ &= \{e\} \end{aligned}$$

Somit ist f injektiv. f ist auch surjektiv, denn für ein $b \in G$ ist

$$f(a^{-1} \circ b \circ a) = a \circ (a^{-1} \circ b \circ a) \circ a^{-1} = b.$$

Insgesamt ist f also bijektiv und damit ein Isomorphismus. $\square$

Aufgabe 3.

a) Gesucht ist eine Permutation $\sigma \in S_4$ mit $\min\{i < 0 \mid \sigma^i = \mathrm{id}\} = 4$.

Also sucht man eine Permutation σ mit der Ordnung 4. Wähle $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$.

Beh.: $\mathrm{ord}(\sigma) = 4$.

Bew.: durch Nachrechnen:

$$\sigma^1 = \sigma \neq \mathrm{id}$$

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \neq \mathrm{id}$$

$$\sigma^3 = \sigma^2 \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \neq \mathrm{id}$$

$$\sigma^4 = \sigma^3 \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \mathrm{id}$$

b) Vorüberlegungen, die beim Finden des Homomorphismus hilfreich sind (zur Lösung der Aufgabe reicht es, φ anzugeben und die geforderten Eigenschaften nachzurechnen):

Die Verknüpfung auf $\mathbb{Z}/4\mathbb{Z}$ muss die Addition sein, da $\mathbb{Z}/4\mathbb{Z}$ nur dann eine Gruppe ist. Die Verknüpfung auf der S_4 ist wie üblich die Komposition/Hintereinanderausführung der Abbildungen.

Zur Konstruktion des Gruppenhomomorphismus:

1. Idee: $\varphi(0 + 4\mathbb{Z}) = \mathrm{id}$, da φ ein Homomorphismus sein muss.
2. Idee: $\varphi(2 + 4\mathbb{Z}) = \varphi(1 + 4\mathbb{Z}) \circ \varphi(1 + 4\mathbb{Z})$, ebenfalls wegen der Homomorphieeigenschaft.
3. Idee: $\varphi(0 + 4\mathbb{Z}) = \varphi(4 + 4\mathbb{Z})$
$= \varphi(1 + 4\mathbb{Z}) \circ \varphi(1 + 4\mathbb{Z}) \circ \varphi(1 + 4\mathbb{Z}) \circ \varphi(1 + 4\mathbb{Z})$
$= \varphi^4(1 + 4\mathbb{Z})$
$\Rightarrow \mathrm{ord}(\varphi(1 + 4\mathbb{Z})) = 4$.

Setze also $\varphi(1 + 4\mathbb{Z}) := \sigma$ mit dem σ aus Teil a).

Beh.: Sei $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$. Dann ist

$$\varphi : \begin{cases} \mathbb{Z}/4\mathbb{Z} & \to & S_4 \\ a + 4\mathbb{Z} & \mapsto & \sigma^a \end{cases}$$

ein injektiver Gruppenhomomorphismus.

Bew.:

i) Wohldefiniertheit: Für $a, b \in \mathbb{Z}$ mit $a + 4\mathbb{Z} = b + \mathbb{Z}$ gilt:
$\exists k \in \mathbb{Z}: \; a = b + 4k$. Damit:

$$\sigma^a = \sigma^{b+4k} = \sigma^b \circ \sigma^{4k} = \sigma^b \circ \left(\sigma^4\right)^k = \sigma^b \circ \mathrm{id}^k = \sigma^b$$

ii) Homomorphieeigenschaft: Seien $a + 4\mathbb{Z}, b + 4\mathbb{Z} \in \mathbb{Z}/4\mathbb{Z}$. Dann gilt:

$$\begin{aligned} \varphi\left((a+4\mathbb{Z}) + (b+4\mathbb{Z})\right) &= \varphi\left((a+b)+4\mathbb{Z}\right) \\ &= \sigma^{a+b} \\ &= \sigma^a \circ \sigma^b \\ &= \varphi\left(a+4\mathbb{Z}\right) \circ \varphi\left(b+4\mathbb{Z}\right) \end{aligned}$$

iii) Injektivität: Seien $a + 4\mathbb{Z}, b + 4\mathbb{Z} \in \mathbb{Z}/4\mathbb{Z}$ mit $\sigma^a = \sigma^b$. Dann gilt:

$$\begin{aligned} &\mathrm{id} = \sigma^a \circ \left(\sigma^b\right)^{-1} = \sigma^a \circ \sigma^{-b} = \sigma^{a-b} \\ \Rightarrow\; &a - b = 4k, \text{ für ein } k \in \mathbb{Z} \\ \Rightarrow\; &a \in b + 4\mathbb{Z} \\ \Rightarrow\; &a + 4\mathbb{Z} = b + 4\mathbb{Z} \end{aligned}$$

$\square$

Aufgabe 5.

Behauptung: $\mathrm{ggT}(f_n, f_{n+1}) = 1 \quad \forall\, n \in \mathbb{N}.$

Beweis per vollständiger Induktion.

Induktionsanfang ($n = 1$): $\mathrm{ggT}(f_1, f_2) = \mathrm{ggT}(1, 1) = 1.$

Induktionsvoraussetzung (I.V.): $\mathrm{ggT}(f_n, f_{n+1}) = 1.$

Indutktionsschritt ($n \mapsto n+1$):

$$\mathrm{ggT}(f_{n+1}, f_{n+2}) = \mathrm{ggT}(f_{n+1}, f_{n+1} + f_n) = \mathrm{ggT}(f_{n+1}, f_n) = \mathrm{ggT}(f_n, f_{n+1}) \overset{\text{I.V.}}{=} 1$$

q.e.d.

Hier noch eine didaktisch bessere Formulierung:

Im Induktionsschritt zeigen wir:

'Wenn f_n und f_{n+1} teilerfremd sind, dann sind auch f_{n+1} und f_{n+2} teilerfremd.'

Es sei dazu $g := \mathrm{ggT}(f_{n+1}, f_{n+2})$. Da $f_{n+2} = f_{n+1} + f_n$ gilt, folgt nun aus $g | f_{n+2}$ und $g | f_{n+1}$, dass g auch f_n teilt. Also gilt $g | \mathrm{ggT}(f_{n+1}, f_n) = 1 \Rightarrow g = 1$.

Aufgabe 6.

Eine Nullstelle ist 1. Verifiziere durch Einsetzen:

$$1^5 - 1^4 + 2 \cdot 1^3 - 2 \cdot 1^2 + 1 - 1 = 1 - 1 + 2 - 2 + 1 - 1 = 0$$

Somit ist $(x-1)$ Primfaktor.
Benutze Polynomdivision:

$$\begin{array}{l}
(x^5 - x^4 + 2x^3 - 2x^2 + x - 1) : (x - 1) \quad = \quad x^4 + 2x^2 + 1 \\
-\underline{(x^5 - x^4)} \\
\qquad\quad 0 + 2x^3 - 2x^2 \\
\qquad\qquad -\underline{(2x^3 - 2x^2)} \\
\qquad\qquad\qquad\qquad 0 + x - 1 \\
\qquad\qquad\qquad\qquad\quad -\underline{(x - 1)} \\
\qquad\qquad\qquad\qquad\qquad\quad 0
\end{array}$$

Zerlege das Ergebnis weiter:

$$x^4 + 2 \cdot x^2 + 1 = (x^2 + 1) \cdot (x^2 + 1)$$

Zeige $(x^2 + 1)$ ist irreduzibel ber $\mathbb{R}$, indem man zeigt, da in $\mathbb{R}$ keine Nullstelle existiert.

$$x^2 + 1 = 0 \iff x^2 = -1 \iff x_{1/2} = \pm i$$

Also ist auch $(x^2 + 1)$ ein Primfaktor und die Primfaktorzerlegung sieht wie folgt aus:

$$(x^5 - x^4 + 2 \cdot x^3 - 2 \cdot x^2 + x - 1) = (x - 1) \cdot (x^2 + 1) \cdot (x^2 + 1)$$

Aufgabe 7.

Gegeben war das lineare Gleichungssystem

$$\begin{array}{rcrcrcl} x & + & y & + & z & = & 0 \\ a\,x & + & b\,y & + & c\,z & = & 0 \\ a^2x & + & b^2y & + & c^2z & = & 0 \end{array}$$

mit $a, b, c \in \mathbb{Q}$. Zu zeigen war, dass dieses homogene GLS genau dann eine eindeutige Lösung besitzt, wenn die Zahlen a, b, c paarweise verschieden sind.

Vorbereitung:
In unserer 'Kurzschreibweise' ergibt sich also:

$$\begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{pmatrix}.$$

Wir multiplizieren die erste Zeile mit $-a$ und addieren diese dann zur zweiten Zeile. Ausserdem multiplizieren wir die erste Zeile mit $-a^2$ und addieren diese dann zur dritten Zeile und erhalten:

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & b-a & c-a \\ 0 & b^2-a^2 & c^2-a^2 \end{pmatrix}$$

Da $b^2 - a^2 = (b-a)\cdot(b+a)$, multiplizieren wir die zweite Zeile mit $-(b+a)$ und addieren diese dann zur dritten Zeile und erhalten:

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & b-a & c-a \\ 0 & 0 & c^2-a^2-(b+a)(c-a) \end{pmatrix}$$

Da $c^2 - a^2 - (b+a)(c-a) = (c-a)(c+a) - (b+a)(c-a) = (c-a)(c-a-b+a) = (c-a)(c-b)$, folgt also

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & b-a & c-a \\ 0 & 0 & (c-a)(c-b) \end{pmatrix}$$

Nun zu der Behauptung:

"$\Rightarrow$" Das Gleichungssystem besitze eine eindeutige Lösung. Da das GLS homogen ist, ist diese Lösung der Nullvektor $(0,0,0)^t$, also $x = y = z = 0$.
An der dritten Zeile kann man gut erkennen, dass z im Falle $c = a$ oder $c = b$ beliebig wählbar wäre. Folglich $c \neq a$ und $c \neq b$.
Aus der zweiten Zeile folgt analog $a \neq b$, da ansonsten y beliebig wählbar wäre im Widerspruch zur Voraussetung. Also: $a \neq b$ <u>und</u> $b \neq c$ <u>und</u> $a \neq c$, welches gleichbedeutend mit a, b, c paarweise verschieden ist.

"$\Leftarrow$" Seien nun a, b, c paarweise verschieden, also $a \neq b$, $b \neq c$ und $a \neq c$.
Aus der dritten Zeile folgt dann $z = 0$, und damit dann aus der zweiten Zeile $y = 0$, und schließlich aus der ersten Zeile $x = 0$, also ist das GLS eindeutig lösbar. $\square$

Aufgabe 8.

Gegeben war das lineare Gleichungssystem

$$(\star) \qquad \begin{array}{lclclcl} (1+1)x & + & y & + & z & = & 0 \\ x & + & (1+1)y & + & z & = & 0 \\ x & + & y & + & (1+1)z & = & 0 \end{array}$$

Wir übersetzen dieses homogene Gleichungssystem in unsere 'Kurzschreibweise'

$$\begin{pmatrix} (1+1) & 1 & 1 \\ 1 & (1+1) & 1 \\ 1 & 1 & (1+1) \end{pmatrix}.$$

Wir subtrahieren die dritte Zeile von der zweiten einmal und von der ersten Zeile zweimal

$$\begin{pmatrix} 0 & -1 & -(1+1+1) \\ 0 & 1 & -1 \\ 1 & 1 & (1+1) \end{pmatrix} \overset{(1)}{\sim} \begin{pmatrix} 1 & 0 & (1+1+1) \\ 0 & 1 & -1 \\ 0 & 0 & -(1+1+1+1) \end{pmatrix}.$$

In (1) addieren wir die zweite Zeile zur ersten Zeile, subtrahieren die zweite Zeile von der dritten Zeile und tauschen die erste Zeile mit der dritten Zeile. Nun interpretieren wir diese Umformungen.

a) In $\mathbb{F}_2$ gilt $1+1=0$ und $-1=1$, d.h. wir erhalten $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$. Somit ist die $z \in \mathbb{F}_2$ frei wählbar und die Lösungsmenge von $(\star)$ ist

$$\mathbb{L} = \left\{ z(1,1,1)^t \in \mathbb{F}_2^3 \;\middle|\; z \in \mathbb{F}_2 \right\} = \{(0,0,0)^t,\ (1,1,1)^t\} \subset \mathbb{F}_2^3 \Rightarrow |\mathbb{L}| = 2.$$

Es gibt daher genau zwei Lösungen.

b) In $\mathbb{F}_3$ gilt $1+1+1=0$ und $-1=2$, d.h. wir erhalten $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix}$. Es ergibt sich somit $z=0 \Rightarrow y=0 \Rightarrow x=0$, d.h. es existiert nur die triviale Lösung $\mathbb{L} = \{(0,0,0)^t\} \subset \mathbb{F}_3^3 \Rightarrow |\mathbb{L}| = 1$.

c) In $\mathbb{F}_4$ gilt $1+1=0$ und $-1=1$, d.h. wir erhalten $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$. Somit ist die $z \in \mathbb{F}_4$ frei wählbar und die Lösungsmenge von $(\star)$ ist
$\mathbb{L} = \left\{ z(1,1,1)^t \in \mathbb{F}_4^3 \;\middle|\; z \in \mathbb{F}_4 \right\} = \{(0,0,0)^t,\ (1,1,1)^t,\ (2,2,2)^t,\ (3,3,3)^t\}$
$\Rightarrow |\mathbb{L}| = 4$. Es gibt daher genau vier Lösungen.
Man beachte, dass $2 \neq 0$ in $\mathbb{F}_4$. Wir haben hier die vier Elemente in $\mathbb{F}_4$ nur einfach mit $0, 1, 2$ und 3 benannt. Das hat nichts mit $\mathbb{Z}/4\mathbb{Z}$ zu tun.