Aufgabe 1

a)

$$(3,2,1)\cdot(4,5) = \begin{pmatrix}1&2&3&4&5\\3&1&2&4&5\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4&5\\1&2&3&5&4\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\3&1&2&5&4\end{pmatrix}$$

$$(5,4,3,2,1)\cdot(3,5) = \begin{pmatrix}1&2&3&4&5\\5&1&2&3&4\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4&5\\1&2&5&4&3\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\3&1&2&5&4\end{pmatrix}$$

b) Z.Z.: Sind $\sigma = (a_1,\dots,a_d), \tau = (b_1,\dots,b_e)$ zwei gleiche Zyklen, dann ist $e = d$.

Beweis. Zwei gleiche Abbildungen haben die gleiche Ursprungs-und Zielmenge, es ist also $\sigma \in \mathfrak{S}_n \implies \tau \in \mathfrak{S}_n$. Sein nun $N = \{k \in \mathbb{N} | 1 \leq k \leq n\}$, $M_\sigma = \{k \in N | \sigma(k) \neq k\}$ und $M_\tau = \{k \in N | \tau(k) \neq k\}$. Aus $\tau = \sigma$ folgt $M_\tau = M_\sigma$. Ferner gilt $\sigma(a_i) = a_j$ mit $1 \leq i,j \leq d, i \neq j$ und daraus folgt mit $\forall 1 \leq i,j \leq d, i \neq j : a_i \neq a_j$ sofort $\sigma(a_i) \neq a_i$. Für alle anderen $k \in N$ ist aber nach Definition des Zyklus $\sigma(k) = k$. Daraus folgt $M_\sigma = \{a_i | 1 \leq i \leq d\}$ und schließlich $\#M_\sigma = d$. Analog erhalten wir $\#M_\tau = e$. Mit $M_\tau = M_\sigma$ folgt sofort $e = d$. □

c) Z.Z.: Für einen Zyklus σ der Länge d gibt es genau d Darstellungen $\sigma = (a_1,\dots,a_d)$.

Beweis. Im folgenden bezeichne $\forall k \in \mathbb{N} : R(k)$ den Rest von k modulo d, insbesondere ist also $R(d+1) = 1$.

- Z.Z.: Es gibt d verschiedene Darstellungen.
  Bew.: Wir bezeichnen mit $(a_1, a_2, \dots, a_d)$ eine Darstellung von σ (es existiert auf jeden Fall eine). Alle Darstellungen $b_1, \dots b_d$ für die gilt: $\forall 1 \leq i,j,k \leq d : b_i = a_{R(i+k)} \implies b_j = a_{R(j+k)}$. Es gibt genau d verschiedene solche d-Tupel. Man erhält sie, wenn man $k = 1, 2, \dots, d$ wählt. Sobald $k = d+1$ ist die Darstellung äquivalent zu der Darstellung für $R(k) = R(d+1) = 1$.
  Damit aber alle diese d-Tupel den gleichen Zyklus darstellen, muss gelten $\forall 1 \leq i \leq d :$ $\sigma(a_i) = a_{R(i+1)}$. (Im Fall $i = d$ wird das zu $\sigma(a_d) = a_{R(d+1)} = a_1$). Es gilt:

  $$\sigma(a_i) \overset{\text{Es existiert stets ein geeignetes } k}{=} \sigma(b_{R(i+k)}) = b_{R(i+1+k)} = a_{R(i+1)}$$

  .
- Es gibt höchstens d verschiedene Darstellungen.
  Beweis durch Widerspruch: Annahme: Es gibt zusätzlich zu den d oben beschriebenen Darstellungen noch mindestens eine weitere Darstellung $(b_1, \dots, b_d)$. Da diese Darstellung nicht mehr der obigen Bedingung genügen kann, müssen O.B.d.A. $b_i = a_{R(i+k)}, bi + 1 \neq a_{R(i+1+k)}$ existieren. Damit erhalten wir allerdings $\sigma(a_i) = \sigma(b_{R(i+k)}) = b_{R(i+1+k)} \neq a_{R(i+1)}$, es folgt $\sigma \neq (b_1, \dots, b_d)$.

□

d) Z.Z. Jede Permutation $\sigma = \begin{pmatrix}1&2&\dots&n\\\sigma_1&\sigma_2&\dots&\sigma_n\end{pmatrix} \in \mathfrak{S}_n$ lässt sich als Produkt von Zyklen der Länge 2 schreiben.

Beweis.
Induktionsanfang: siehe Aufgabenblatt
Induktionsannahme: Jedes Element der $\mathfrak{S}_n$ lässt sich als Produkt von Zyklen der Länge 2 schreiben.
Induktionsschluss: Wir betrachten die Permutation $\sigma = \begin{pmatrix} 1 & 2 & \dots & n & n+1 \\ \sigma_1 & \sigma_2 & \dots & \sigma_n & \sigma_{n+1} \end{pmatrix} \in \mathfrak{S}_{n+1}$.
Fall 1: $n+1 = \sigma_{n+1}$.
Die Permutation $\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma_1 & \sigma_2 & \dots & \sigma_n \end{pmatrix} \in \mathfrak{S}_n$ lässt sich nach Induktionsvoraussetzung als Produkt $\prod_{i=1}^{k} p_i$ mit $k \in \mathbb{N}$ und $p_i \in \mathfrak{S}_n$ schreiben, wobei jedes p_i ein Zyklus der Länge zwei ist. Sei $f : \mathfrak{S}_n \to \mathfrak{S}_{n+1}, z \mapsto z$ ein Homomorphismus. Dann ist $f(p)_i$ ebenfalls ein Zyklus der Länge zwei und $\prod_{i=1}^{k} f(p_i) = \begin{pmatrix} 1 & 2 & \dots & n & n+1 \\ \sigma_1 & \sigma_2 & \dots & \sigma_n & n+1 \end{pmatrix} \in \mathfrak{S}_{n+1} = \sigma$ ist das gesuchte Produkt.
Fall 2: $\sigma_{n+1} \neq n+1$.
Der letze Zyklus in dem zu konstruierenden Produkt von Zweierzyklen sei $z_1 = (n+1, \sigma_{n+1}) \in \mathfrak{S}_{n+1}$. Es existiert genau ein k, sodass $\sigma(k) = n+1$. (Das wird sofort aus unserer Darstellungsweise einer Permutation ersichtlich). Dieses k ist außerdem $< n+1$. Zudem ist $\sigma_{n+1} < n+1$. Nach Induktionsvoraussetzung wissen wir, dass $\begin{pmatrix} 1 & 2 & \dots & k & \dots & n \\ 1 & 2 & \dots & \sigma_{n+1} & \dots & n \end{pmatrix} = \prod_{i=1}^{k} p_i$ mit $k \in \mathbb{N}$ und p_i ein Zyklus der Länge zwei aus $\mathfrak{S}_n$. Analog zu Fall 1 erhalten wir $z_2 = \prod_{i=1}^{k} f(p_i) = \begin{pmatrix} 1 & 2 & \dots & k & \dots & n & n+1 \\ \sigma_1 & \sigma_2 & \dots & \sigma_{n+1} & \dots & \sigma_n & n+1 \end{pmatrix} \in \mathfrak{S}_{n+1}$. Das gesuchte Produkt ist $z_2 \cdot z_1 = \begin{pmatrix} 1 & 2 & \dots & k & \dots & n & n+1 \\ \sigma_1 & \sigma_2 & \dots & \sigma_{n+1} & \dots & \sigma_n & n+1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & \dots & \sigma_{n+1} & \dots & n & n+1 \\ 1 & 2 & \dots & n+1 & \dots & n & \sigma_{n+1} \end{pmatrix}$
$= \begin{pmatrix} 1 & 2 & \dots & k & \dots & n & n+1 \\ \sigma_1 & \sigma_2 & \dots & n+1 & \dots & \sigma_n & \sigma_{n+1} \end{pmatrix}$. Da $\sigma(k) = n+1$, ist $n+1 = \sigma_k$.
$z_2 \cdot z_1 = \begin{pmatrix} 1 & 2 & \dots & k & \dots & n & n+1 \\ \sigma_1 & \sigma_2 & \dots & \sigma_k & \dots & \sigma_n & \sigma_{n+1} \end{pmatrix} = \sigma$ □

Aufgabe 2

Nach Bemerkung 1.28 im Skript ist $gH = \{g' \in G | g' = g * h, h \in H\}$.

- Z.Z.: Es existiert eine bijektive Abbildung $f : H \to gH, h \to g * h$.

  Beweis. Die Abbildung ist offensichtlich wohldefiniert. Angenommen, f wäre nicht surjektiv. Dann gäbe es ein $g' = g * h \in gH$ und $h \in H$, sodass es kein $h \in H$ mit $g * h = g' \in gH$ gäbe. $\lightning$. Angenommen, die Abbildung wäre nicht injektiv, dann gäbe es $g, g' \in G$ **mit** $h \neq h'$, sodass $f(h) = f(h') \implies g * h = g * h'$. Sei g^{-1} das Inverse zu g (es existiert laut den Gruppenaxiomen). Dann ist $g^{-1} * g * h = g^{-1} * g * h'$ und damit $h = h' \lightning$. □

  Da es eine bijektive Abbildung von $H \to gH$ gibt, ist $\#H = \#gH$.

- Z.Z.: $\#G = \#H \cdot \#(G/H)$.

Beweis.

$$
\begin{aligned}
G &= \dot{\bigcup_{M \in G/H}} && \text{folgt aus den Axiomen für Äquivalenzrelationen} \\
\implies \#G &= \sum_{M \in G/H} \#M && \#M = \#gH = \#H \quad \forall M \in G/H \\
\#G &= \sum_{M \in G/H} \#H && \text{Diese Summe addiert } \#(G/H) \text{ mal } \#H \\
\#G &= \#(G/H) \cdot \#H
\end{aligned}
$$

□

Aufgabe 3

a) *Beweis.*

$$
\begin{aligned}
a + b = (a+b)^2 &= a^2 + ab + ba + b^2 = a + ab + ba + b \\
0 &= ab + ba \\
ab &= -ba && (1) \\
a + a = (a+a)^2 &= a^2 + a^2 + a^2 + a^2 = a + a + a + a \\
0 &= a + a \\
a &= -a && (2)
\end{aligned}
$$

Wir setzen (2) in (1) ein und erhalten

$$ab = ba \tag{3}$$

□

b) *Beweis.* In einem Körper K gilt $\forall x \neq 0 \exists x^{-1}$ mit $x \cdot x^{-1} = 1_K$. Sei K ein Körper. Sei $x \in R$.
Fall 1: $x = 0_R$. $0_R^2 = 0_R$✓
Fall 2: $x \neq 0_R$. Da R ein Körper ist, existiert ein x^{-1} mit $x \cdot x^{-1} = 1_R$. Ferner ist

$$
\begin{aligned}
x * x &= x && | * x^{-1} \\
x * x * x^{-1} &= x * x^{-1} \\
x &= 1_R
\end{aligned}
$$

R enthält also nur 0_R und 1_R. □

Aufgabe 4

a) Wir zeigen die Ringaxiome.

Beweis. R1) Da die Addition komponentenweise definiert ist und $(\mathbb{Q}, +, 0)$ eine abelsche Gruppe ist, muss auch $(\mathbb{Q} \times \mathbb{Q}, +_{K_d}, (0,0))$ eine abelsche Gruppe sein.

R2)

$$\begin{aligned}
&((a_0,a_1)\cdot_{K_d}(b_0,b_1))\cdot_{K_d}(c_0,c_1)\\
=&(a_0b_0+a_1b_1d,a_1b_0+a_0b_1)\cdot_{K_d}(c_0,c_1)\\
=&((a_0b_0+a_1b_1d)c_0+(a_1b_0+a_0b_1)c_1d,(a_1b_0+a_0b_1)c_0+(a_0b_0+a_1b_1d)c_1)\\
=&(a_0b_0c_0+a_1b_1c_0d+a_1b_0c_1d+a_0b_1c_1d,a_1b_0c_0+a_0b_1c_0+a_0b_0c_1+a_1b_1c_1d)\\
=&(a_0(b_0c_0+b_1c_1d)+a_1(b_1c_0+b_0c_1)d,a_0(b_1c_0+b_0c_1)+a_1(b_0c_0+b_1c_1d))\\
=&(a_0,a_1)\cdot_{K_d}(b_0c_0+b_1c_1d,b_1c_0+b_0c_1)\\
=&(a_0,a_1)\cdot_{K_d}((b_0,b_1)\cdot_{K_d}(c_0,c_1))
\end{aligned}$$

R3)

$$\begin{aligned}
&(a_0,a_1)\cdot_{K_d}((b_0,b_1)+_{K_d}(c_0,c_1))\\
=&(a_0,a_1)\cdot_{K_d}(b_0+c_0,b_1+c_1)\\
=&(a_0(b_0+c_0)+a_1(b_1+c_1)d,a_1(b_0+c_0)+a_0(b_1+c_1))\\
=&(a_0b_0+a_1b_1d+a_0c_0+a_1c_1d,a_1b_0+a_0b_1+a_1c_0+a_0c_1)\\
=&(a_0b_0+a_1b_1d,a_1b_0+a_0b_1)+_{K_d}(a_0c_0+a_1c_1d,a_1c_0+a_0c_1)\\
=&(a_0,a_1)\cdot_{K_d}(b_0,b_1)+_{K_d}(a_0,a_1)\cdot_{K_d}(c_0,c_1)
\end{aligned}$$

Damit der Ring unitär ist, muss es ein neutrales Element 1_{K_d} bezüglich der Multiplikation geben.
Behauptung $1_{K_d}=(1,0)$.
Bew.:

$(1,0)\cdot_{K_d}(a_0,a_1)=(1\cdot a_0+0\cdot a_1\cdot d,1\cdot a_1+0\cdot a_0)=(a_0,a_1)=(a_0\cdot 1+a_1\cdot 0\cdot d,a_1\cdot 1+a_0\cdot 0)=(a_0,a_1)\cdot_{K_d}(1,0)$

□

b) Z.Z.: $\iota:\mathbb{Q}\to K_d, x\mapsto(x,0)$ ist ein unitärer Ringhomomorphismus.

Beweis. $\mathbb{Q}$ und K_d sind beides unitäre Ringe. Es gilt $\forall p,q\in\mathbb{Q}$:

$$\begin{aligned}
\iota(p+q)&=(p+q,0)=(p,0)+_{K_d}(q,0)=\iota(p)+_{K_d}\iota(q)\\
\iota(p\cdot q)&=(pq,0)=(pq+0\cdot 0\cdot d,0\cdot q+p\cdot 0)=(p,0)\cdot_{K_d}(q,0)=\iota(p)\cdot_{K_d}\iota(q)\\
\iota(1_{\mathbb{Q}})&=\iota(1)=(1,0)=1_{K_d}
\end{aligned}$$

□

Z.Z.: $X^2-\iota(d)=0$ hat eine Lösung in K_d.

Beweis. Behauptung $X=(0,1)$ löst die Gleichung.

$$\begin{aligned}
&X^2-d\\
=&(0,1)\cdot_{K_d}(0,1)-(d,0)\\
=&(0^2+1^2d,1\cdot 0+0\cdot 1)-(d,0)\\
=&(0,0)
\end{aligned}$$

□

c)

(i)→(ii) Das folgt sofort aus Lemma 1.15.

(ii)→(iii) Wir zeigen die Kontraposition: Wenn die Gleichung $X^2 - d = 0$ eine Lösung in $\mathbb{Q}$ hat, dann gibt es $a, b \in K_d \setminus \{0_{K_d}\}$ mit $a \cdot b = 0$. Wenn die Gleichung $X^2 - d = 0$ eine Lösung in $\mathbb{Q}$ hat, können wir $a_0, a_1 \in \mathbb{Q}, a_1 \neq 0$ so wählen, dass $\left(\frac{a_0}{a_1}\right)^2 - d = 0$. Sei außerdem $b \neq 0$.
Behauptung: Dann ist $(a_0, a_1) \cdot (b, -\frac{a_1}{a_0}b) = (0, 0)$

Beweis.

$$\begin{aligned}
&(a_0, a_1) \cdot \left(b, -\frac{a_1}{a_0}b\right) \\
&= \left(a_0 b - a_1 \cdot \frac{a_1}{a_0} bd, -a_0 \cdot \frac{a_1}{a_0} \cdot b + a_1 \cdot b\right) \\
&= \left(b\frac{a_1^2}{a_0}\left(\frac{a_0^2}{a_1^2} - d\right), -a_1 b + a_1 b\right)
\end{aligned}$$

Nach unserer Wahl von a_0, a_1 gilt $\left(\frac{a_0}{a_1}\right)^2 - d = 0$.

$$= \left(b\frac{a_1^2}{a_0}(0), 0\right) = (0, 0)$$

□

$a_1 \implies (a_0, a_1) \neq (0, 0)$ und $b \neq 0 \implies \left(b, -\frac{a_1}{a_0}b\right) \neq (0, 0)$. Es gibt also $a, b \in K_d \setminus \{0_{K_d}\}$ mit $a \cdot b = 0_{K_d}$. Damit ist die Kontraposition $\neg(iii) \to \neg(ii)$ und somit auch die Implikation $(ii) \to (iii)$ bewiesen.

(iii) → (i) Behauptung: K_d ist ein Körper, wenn die Gleichung $X^2 - d = 0$ keine Lösung in $\mathbb{Q}$ hat.

Beweis. Da K_d ein unitärer Ring ist, müssen wir nur noch zeigen, dass es zu jedem $(a_0, a_1) \neq (0, 0) \in K_d$ ein multiplikatives Inverses $(a_0, a_1)^{-1} \in K_d$ gibt. Fall 1: $a_1 = 0 \implies a_0 \neq 0$. $(a_0, 0) \cdot \left(\frac{1}{a_0}, 0\right) = \left(a_0\frac{1}{a_0} + 0 \cdot 0 \cdot d, 0 \cdot \frac{1}{a_0} + a_0 \cdot 0\right) = (1, 0)$✓. Das Inverse existiert stets, da $a_0 \neq 0$.
Fall 2: $a_1 \neq 0$:

$$\begin{aligned}
&(a_0, a_1) \cdot_{K_d} \left(\frac{a_0}{a_1^2\left(\left(\frac{a_0}{a_1}\right)^2 - d\right)}, \frac{1}{-a_1\left(\left(\frac{a_0}{a_1}\right)^2 - d\right)}\right) \\
=&(a_0, a_1) \cdot_{K_d} \left(\frac{a_0}{a_0^2 - a_1^2 \cdot d}, \frac{a_1}{a_1^2 \cdot d - a_0^2}\right) \\
=&\left(\frac{a_0^2}{a_0^2 - a_1^2 \cdot d} + \frac{a_1^2 \cdot d}{a_1^2 \cdot d - a_0^2}, \frac{a_0 a_1}{a_1^2 \cdot d - a_0^2} + \frac{a_1 a_0}{a_0^2 - a_1^2 \cdot d}\right) \\
=&\left(\frac{a_0^2 - a_1^2 \cdot d}{a_0^2 - a_1^2 \cdot d}, \frac{a_0 a_1 - a_1 a_0}{a_1^2 \cdot d - a_0^2}\right) \\
=&(1, 0)✓
\end{aligned}$$

Da die Gleichung $X^2 - d = 0$ keine Lösung in $\mathbb{Q}$ hat, ist stets $\left(\frac{a_0}{a_1}\right)^2 - d \neq 0$. Da zusätzlich $a_1 \neq 0$, ist außerdem stets $a_1^2\left(\left(\frac{a_0}{a_1}\right)^2 - d\right) \neq 0$ und $-a_1\left(\left(\frac{a_0}{a_1}\right)^2 - d\right) \neq 0$. Daher gibt es stets ein Inverses $\left(\frac{a_0}{a_1^2\left(\left(\frac{a_0}{a_1}\right)^2 - d\right)}, \frac{1}{-a_1\left(\left(\frac{a_0}{a_1}\right)^2 - d\right)}\right)$. □

Aus $(i) \implies (ii) \implies (iii) \implies (i)$ folgt $(i) \iff (ii) \iff (iii)$.