Lösungen zur
Modulprüfung zur
Elementaren Algebra/Zahlentheorie II

Weiterbildung für Lehrer an der FU

Dozent: V.Schulze Datum:17.12.2021 Bearbeitungszeit: 90 Minuten

Name	Vorname	Unterschrift	Matr.Nr.

Aufgabe	1	2	3	4		Punktsumme	Note
Punkte							

Bearbeiten Sie drei der folgenden vier Aufgaben.
Anmerkung: Pro Aufgabenteil werden maximal 5 Punkte vergeben,
pro Aufgabe also maximal 10 Punkte; insgesamt also maximal 30 Punkte.
Zur vollständigen Bearbeitung einer Aufgabe gehört auch die stilistisch einwandfreie Darstellung des Gedankenganges.

Aufgabe 1

(i) Gegeben sei die Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 4 & 1 & 2 \end{pmatrix}.$$

Man stelle π als Produkt elementefremder Zyklen dar.
Man stelle π als Produkt von Transpositionen dar.
Man stelle π^{-1} als Produkt elementefremder Zyklen dar.
(ii) Gegeben seien die beiden Permutationen $\pi_1 = (1,4)$ und $\pi_2 = (2,4,3)$.
Man bestimme eine Permutation π_3 , so dass gilt $\pi_1 \circ \pi_3 = \pi_2$.
Ist π_3 eindeutig bestimmt ?

Lösung zu Aufgabe 1

(i) Es gilt $\pi = (1,3,5)(2,6), \pi = (1,3)(3,5)(2,6), \pi_1^{-1} = (1,5,3)(6,2)$.
(ii) Es gilt $\pi_3 = \pi_1^{-1} \circ \pi_2 = (4,1)(2,4,3) = (1,4,3,2)$.
Aus $\pi_1 \circ \pi_3 = \pi_2$ folgt $\pi_3 = \pi_1^{-1} \circ \pi_2$, also ist π_3 eindeutig bestimmt.

Aufgabe 2

Die Teilmenge M von $\mathbb{R}$ sei definiert durch $M := \{2a + b\sqrt{5} \,|\, a, b \in \mathbb{Z}\}$.
(i) Man zeige : M ist eine Untergruppe von $(\mathbb{R}, +)$.

Ist M ist ein Unterring von $(\mathbb{R}, +, .)$?
(ii) Die Abbildung $f : M \to \mathbb{Z}$ sei definiert durch
$f(2a + b\sqrt{5}) := a + b$ für alle $a, b \in \mathbb{Z}$
Man zeige : f ist bezüglich + ein Gruppenhomomorphismus.
Ist f surjektiv ?
Ist f injektiv ?.

Lösung zu Aufgabe 2

(i) Offenbar liegt die Summe zweier Elemente aus M wieder in M; genauer gilt $(2a + b\sqrt{5}) + (2c + d\sqrt{5}) = (2(a + c) + (b + d)\sqrt{5})$ und mit a, b, c, d liegen auch $a + c$ und $b + d$ in $\mathbb{Z}$.
Das neutrale Element $0 = 2 \cdot 0 + 0\sqrt{5}$ liegt in M.
Mit $2a + b\sqrt{5}$ liegt auch das Negative $2(-a) - b\sqrt{5}$ in M.
Das Assoziativgesetz überträgt sich von $\mathbb{R}$ auf M.
M ist kein Unterring von $(\mathbb{R}, +, .)$, da gilt: $\sqrt{5} \in M$, aber $(\sqrt{5}) \cdot (\sqrt{5}) = 5 \notin M$.
Also ist M bezüglich $\cdot$ nicht abgeschlossen.
(ii) Es gilt $f((2a+b\sqrt{5})+(2c+d\sqrt{5})) = f((2(a+c)+(b+d)\sqrt{5}) = 2(a+b)+(c+d) = f((2a + b\sqrt{5}) + f(2c + d\sqrt{5})$, also ist f relationstreu bezüglich + und damit ein Gruppenhomomorphismus.
Sei $b \in \mathbb{Z}$. Dann ist $2 \cdot 0 + b\sqrt{5}$ Urbild von b, also ist f surjektiv.
Offenbar ist f nicht injektiv; zum Beispiel besitzen $2 \cdot 0 + 0\sqrt{5}$ und $2 \cdot 1 - 1\sqrt{5}$ dasselbe Bild.

Aufgabe 3

(i) Es bezeichne φ die Eulersche $\varphi-$ Funktion.
Man zeige : $\varphi(35) = 24$.
Gilt $3^{24} \equiv 3 \cdot 24 \pmod{35}$?
(ii) Man zeige mit Hilfe des Euklidischen Algorithmus:
Der ggT von 1001 und 497 ist 7.
Man zeige : $497 \cdot x \equiv 7 \pmod{1001}$ ist lösbar .
Man gebe eine Lösung von $497 \cdot x \equiv 7 \pmod{1001}$ an.

Lösung zu Aufgabe 3

(i) Es gilt $\varphi(5 \cdot 7) = \varphi(5) \cdot \varphi(7) = 4 \cdot 6 = 24$.
Nach dem Satz von Euler gilt $3^{24} \equiv 1 \pmod{35}$, aber $3 \cdot 24 \equiv 72 \equiv 2 \pmod{35}$, also ist $3^{24} \equiv 3 \cdot 24 \pmod{35}$ falsch.
(ii) Der Euklidische Divisionsalgorithmus liefert
$1001 = 2 \cdot 497 + 7$,
$497 = 71 \cdot 7 + 0$.
Der letzte von 0 verschiedene Rest ist 7. Dies ist auch der ggT von 1001 und 497.

Die Kongruenz $497 \cdot x \equiv 7 \pmod{1001}$ ist lösbar, da 7 Teiler von $ggT(1001, 497)$ ist.
Betrachtet man die obige Gleichung $1001 = 2 \cdot 497 + 7$ modulo 1001, so ergibt sich -2 als Lösung von $497 \cdot x \equiv 7 \pmod{1001}$.

Aufgabe 4

(i) Man gebe ein irreduzibles normiertes Polynom $f(x) \in \mathbb{Q}[x]$ vom Grad 4 an.
Sei $\alpha \in \mathbb{R}$ Nullstelle von $f(x)$.
Man zeige : $\{1, \alpha, \alpha^2, \alpha^3\}$ ist Basis der Körpererweiterung $\mathbb{Q}(\alpha) : \mathbb{Q}$.
(ii) Sei $\alpha \in \mathbb{R}$ Nullstelle von $x^3 + 6x + 12 \in \mathbb{Q}[x]$
Man zeige : $\{1, \alpha, \alpha^2\}$ ist Basis der Körpererweiterung $\mathbb{Q}(\alpha) : \mathbb{Q}$.
Man stelle α^{-1} als Linearkombination der Basiselemente dar.

Lösung zu Aufgabe 4

(i) Nach Eisenstein (wähle $p = 2$) ist $f(x) = x^4 + 2 \in \mathbb{Q}[x]$ irreduzibel.
Es gilt $Irr(\alpha, \mathbb{Q}) = f(x)$, da $f(x) \in \mathbb{Q}[x]$ normiert, irreduzibel ist und α als Nullstelle besitzt. Da $Grad f(x) = 4$ ist, folgt aus der Vorlesung:
$\{1, \alpha, \alpha^2, \alpha^3\}$ ist Basis der Körpererweiterung $\mathbb{Q}(\alpha) : \mathbb{Q}$.
(ii) Nach Eisenstein (wähle $p = 3$) ist $x^3 + 6x + 12 \in \mathbb{Q}[x]$ irreduztibel.
Dann folgt analog zu (i) :
$\{1, \alpha, \alpha^2\}$ ist Basis der Körpererweiterung $\mathbb{Q}(\alpha) : \mathbb{Q}$.
Da α Nullstelle von $x^3 + 6x + 12$ ist, folgt $\alpha(\alpha^2 + 6) = -12$, also $\alpha^{-1} = -\frac{\alpha^2}{12} - \frac{1}{2}$.