Lösungen zur
Modulprüfung zur
Elementaren Algebra/Zahlentheorie II

Weiterbildung für Lehrer an der FU

Dozent: V.Schulze 3. 12. 2020 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

Gegeben seien die Permutationen $\pi := (1,2,3), \sigma := (2,3)$ und die Identität id aus der symmetrischen Gruppe $(S_3, \circ)$ vom Index 3.
Es bezeichne $\circ$ die Hintereinanderschaltung von Abbildungen.
(i) Man stelle $\sigma \circ \pi$ und $\sigma \circ \pi^2$ als Produkt elementefremder Zyklen dar.
Man ergänze die folgende Verknüpfungstafel:

$\circ$	id	π	π^2	σ	$\sigma \circ \pi$	$\sigma \circ \pi^2$
id	id	π	π^2	σ	$\sigma \circ \pi$	$\sigma \circ \pi^2$
π	π	π^2	id	$\sigma \circ \pi^2$	σ	$\sigma \circ \pi$
π^2	π^2	id	π	$\sigma \circ \pi$		σ
σ	σ	$\sigma \circ \pi$	$\sigma \circ \pi^2$	id	π	π^2
$\sigma \circ \pi$	$\sigma \circ \pi$	$\sigma \circ \pi^2$	σ		id	π
$\sigma \circ \pi^2$	$\sigma \circ \pi^2$	σ	$\sigma \circ \pi$	π	π^2	id

(ii) Man betrachte die sechselementige Menge $G = \{id, \pi, \pi^2, \sigma, \sigma \circ \pi, \sigma \circ \pi^2\}$.
Man zeige: $(G, \circ)$ ist eine Gruppe.
Ist die Untergruppe $U := \{id, \pi, \pi^2\}$ von G Normalteiler von G ?
Besitzt G eine Untergruppe der Ordnung 4 ?

Lösung Aufgabe 1

(i) Es gilt $\sigma \circ \pi = (1,3)$ und $\sigma \circ \pi^2 = (1,2)$.
Ferner gilt

$\circ$	id	π	π^2	σ	$\sigma \circ \pi$	$\sigma \circ \pi^2$
id	id	π	π^2	σ	$\sigma \circ \pi$	$\sigma \circ \pi^2$
π	π	π^2	id	$\sigma \circ \pi^2$	σ	$\sigma \circ \pi$
π^2	π^2	id	π	$\sigma \circ \pi$	$\sigma \circ \pi^2$	σ
σ	σ	$\sigma \circ \pi$	$\sigma \circ \pi^2$	id	π	π^2
$\sigma \circ \pi$	$\sigma \circ \pi$	$\sigma \circ \pi^2$	σ	π^2	id	π
$\sigma \circ \pi^2$	$\sigma \circ \pi^2$	σ	$\sigma \circ \pi$	π	π^2	id

(ii) Die Verknüpfung zweier Elemente aus G liegt wieder in G. Dies zeigt die Verknüpfungstafel.
Die Hintereinanderschaltung zweier Abbildungen ist stets assoziativ. Also ist $(G, \circ)$ eine Halbgruppe.
In jeder Zeile und jeder Spalte der Verknüpfungstafel tritt jedes Element aus G genau ein Mal auf. Nach Vorlesung ist also $(G, \circ)$ eine Gruppe.
Nach Lagrange besitzt die Untergruppe U von G den Index 2. Nach Vorlesung ist dann U Normalteiler von G.
Die Ordnung einer Untergruppe ist stets Teiler der Gruppenordnung. Da 4 nicht Teiler von 6 ist, besitzt G keine Untergruppe der Ordnung 4.

Aufgabe 2

(i)Man zeige: Der Restklassenring $\mathbb{Z}_{100}$ besitzt genau 40 Einheiten.
Man bestimme die Ordnung von 49 (mod 100) in der Einheitengruppe von $\mathbb{Z}_{100}$.
(ii) Man betrachte den Unterring $\mathbb{Z}[\sqrt{3}] := \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ von $(\mathbb{R}, +, \cdot)$ und den Restklassenring $\mathbb{Z}_7$.
Die Abbildung $f : \mathbb{Z}[\sqrt{3}] \to \mathbb{Z}_7$ sei definiert durch
$f(a + b\sqrt{3}) := 2b \pmod 7$ für alle $a + b\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$.
Man zeige: f ist relationstreu bezüglich $+$.
Ist f ein Ring-Homomorphismus ?

Lösung Aufgabe 2

(i)Es bezeichne φ die Eulersche $\varphi-$ Funktion.
Die Anzahl der Einheiten von $\mathbb{Z}_{100}$ ist dann $\varphi(100) = \varphi(2^2)\cdot\varphi(5^2) = 2\cdot 5\cdot 4 = 40$.
Es gilt $49 \cdot 49 \equiv 2401 \equiv 1 \pmod{100}$.
Die Ordnung von $49 \pmod{100}$ in der Einheitengruppe von $\mathbb{Z}_{100}$ ist also 2.
(ii) Es gilt $f(a + b\sqrt{3}) + f(c + d\sqrt{3}) = 2b \pmod 7 + 2d \pmod 7 = 2 \cdot (b + d) \pmod 7 = f((a + b\sqrt{3}) + (c + d\sqrt{3}))$.
Also ist f ist relationstreu bezüglich +.
Zum Beispiel gilt $f(\sqrt{3}\cdot\sqrt{3}) = f(3) = 0 \pmod 7$, aber $f(\sqrt{3})\cdot f(\sqrt{3}) = 2\cdot 2 \pmod 7 \neq 0 \pmod 7$.
Also ist f kein Ring-Homomorphismus.

Aufgabe 3

(i)Ist die Kongruenz $2430x \equiv 1 \pmod{7293}$ lösbar ?
Man zeige: Die Kongruenz $2430x \equiv 3 \pmod{7293}$ ist lösbar.
Man gebe eine Lösung von $2430x \equiv 3 \pmod{7293}$ an.
(ii) Es bezeichne φ die Eulersche $\varphi-$ Funktion.
Berechne $\varphi(40)$.
Für welche $a \in \mathbb{Z}$ gilt $a^{16} \equiv 1 \pmod{40}$?

Lösung Aufgabe 3

(i) Es gilt $7293 = 3 \cdot 2430 + 3$ und $2430 = 810 \cdot 3 + 0$.
Also ist $ggT(7293, 2430) = 3$.
Die Kongruenz $2430x \equiv 1 \pmod{7293}$ ist also nicht lösbar.
Die Kongruenz $2430x \equiv 3 \pmod{7293}$ ist lösbar.
Betrachtet man die Gleichung $7293 = 3 \cdot 2430 + 3$ modulo 7293 , so ergibt sich -3 als Lösung von $2430x \equiv 3 \pmod{7293}$.
(ii) Es gilt $\varphi(40) = \varphi(2^3 \cdot 5) = \varphi(2^3) \cdot \varphi(5) = 4 \cdot 4 = 16$.

Sei $ggT(a, 40) = 1$. Dann gilt wegen $\varphi(40) = 16$ nach Euler $a^{16} \equiv 1 \pmod{40}$.
Sei $ggT(a, 40) > 1$. Dann ist $a \pmod{40}$ keine Einheit in $\mathbb{Z}_{40}$ und $a^{16} \equiv 1 \pmod{40}$ kann nicht gelten.

Aufgabe 4

(i) Man zeige : $x^3 - x - 1 \in \mathbb{Q}[x]$ ist irreduzibel.
Für welche $a \in \mathbb{Z}$ ist $x^3 - ax - 1 \in \mathbb{Q}[x]$ irreduzibel ?
(ii)Sei $\alpha \in \mathbb{R}$ Nullstelle von $x^3 - x - 1 \in \mathbb{Q}[x]$.
Man zeige : $\{1, \alpha, \alpha^2\}$ ist Basis der Körpererweiterung $\mathbb{Q}(\alpha) : \mathbb{Q}$.
Man stelle α^3 als Linearkombination der Basiselemente dar.

Lösung Aufgabe 4

(i) Da das Polynom $x^3 - x - 1$ den Grad 3 besitzt, ist es in $\mathbb{Q}[x]$ irreduzibel g.d.w. es keine rationale Nullstelle besitzt. Als rationale Nullstellen kommen nur 1 und -1 in Frage, beide Elemente sind aber keine Nullstelle.
Analog kommen als rationale Nullstellen von $x^3 - ax - 1$ nur 1 und -1 in Frage. Also besitzt $x^3 - ax - 1$ eine rationale Nullstelle genau für $a = 0$ und $a = 2$.
(ii)Es gilt $x^3 - x - 1 = Irr(\alpha, \mathbb{Q})$, da $x^3 - x - 1 \in \mathbb{Q}[x]$ irreduzibel ist, normiert ist und α als Nullstelle besitzt.
Also folgt : $\{1, \alpha, \alpha^2\}$ ist Basis der Körpererweiterung $\mathbb{Q}(\alpha) : \mathbb{Q}$.
Da α Nullstelle von $x^3 - x - 1$ ist, gilt $\alpha^3 = \alpha + 1 = 0 \cdot \alpha^2 + \alpha + 1$. Dies ist die gesuchte Linearkombination.