Lösungen zur
Modulprüfung zur
Algebra/Zahlentheorie II

Weiterbildung für Lehrkräfte an der FU
Dozent: V.Schulze Datum: 10.1.2023
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) Es sei $G = \{e, a, b, c\}$ eine Menge und $(G, \circ)$ eine Gruppe.
Man ergänze die folgende Verknüpfungstafel:

$\circ$	e	a	b	c
e	e	a	b	c
a	a			e
b	b			
c	c			

Man gebe eine Untergruppe U von $(G, \circ)$ der Ordnung 2 an.
(ii) Gegeben sei die Permutation $\pi := (1, 3, 5) \circ (3, 4, 2)$
aus der symmetrischen Gruppe $(S_5, \circ)$ vom Index 5.
Man stelle π als Produkt elementefremder Zyklen dar.
Man stelle π^{-1} als Produkt von Transpositionen dar.

Lösung zu Aufgabe 1

(i) Nach Vorlesung tritt in jeder Zeile und jeder Spalte der Verknüpfungstafel jedes Element aus G genau ein Mal auf.
Dies liefert die Verknüpfungstafel

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Offenbar ist $b \circ b = e$, also ist $U = \{e, b\}$ die von b erzeugte Untergruppe von $(G, \circ)$.
(ii) Es gilt $\pi = (1,3,4,2,5), \pi^{-1} = (1,5,2,4,3)$ und $\pi^{-1} = (1,5,2,4)(4,3) = (1,5,2)(2,4)(4,3)$.

Aufgabe 2

(i) Die Abbildung $f : \mathbb{Z} \to \mathbb{Z}_{14}$ sei definiert durch
$f(a) := 7a^2 \pmod{14}$ für alle $a \in \mathbb{Z}$.
Man zeige: f ist relationstreu bezüglich $+$.
Man zeige: f ist ein Ring-Homomorphismus.
(ii) Man bestimme den Kern von f.
Man bestimme das Bild von f.

Lösung zu Aufgabe 2

(i) Es gilt $f(a+b) = 7(a+b)^2 (mod 14) = 7a^2 + 14ab + 7b^2 mod(14) = 7a^2 + 7b^2 (mod 14) = f(a) + f(b)$, also ist f ist relationstreu bezüglich $+$.
Zu zeigen bleibt : f ist relationstreu bezüglich $\cdot$.
Wegen $7^2 \equiv 7 \pmod{14}$ gilt $f(ab) = 7a^2b^2 (mod 14) = 7a^2 \cdot 7b^2 (mod 14) = f(a)f(b)$.
(ii) $7a^2 \equiv 0 \pmod{14}$ ist gleichwertig mit $a \in 2\mathbb{Z}$.
Also ist $Kern f = 2\mathbb{Z}$.
Das Bild von f ist $\{0(mod 14), 7(mod 14)\}$.

Aufgabe 3

(i) Man zeige: $58 \pmod{193}$ ist Einheit in $\mathbb{Z}_{193}$.
Man berechne das zu $58 \pmod{193}$ in $\mathbb{Z}_{193}$ multiplikativ inverse Element.
(ii) Es bezeichne φ die Eulersche $\varphi-$ Funktion.
Man zeige : $\varphi(48) = 16$.
Gilt $7^{18} \equiv 1 \pmod{48}$?

Lösung zu Aufgabe 3

(i) $58 \pmod{193}$ ist Einheit in $\mathbb{Z}_{193}$ genau dann, wenn $ggT(58, 193) = 1$ ist.
Man bestimme den ggT mit Hilfe des Euklidischen Algorithmus:

$193 = 3 \cdot 58 + 19$
$58 = 3 \cdot 19 + 1$
$19 = 19 \cdot 1 + 0.$
Der letzte von 0 verschiedene Rest ist 1, dies ist auch der ggT.
Man stelle 1 als Linearkombination von 58 und 193 dar mit Hilfe der obigen Gleichungen: $1 = 58 - 3(193 - 3 \cdot 58) = 10 \cdot 58 - 3 \cdot 193$.
Also ist $1 \equiv 10 \cdot 58 \pmod{193}$ und das zu $58 \pmod{193}$ in $\mathbb{Z}_{193}$ multiplikativ inverse Element ist $10(mod 193)$.
(ii) Es gilt $\varphi(48) = \varphi(2^4) \cdot \varphi(3) = 2^3 \cdot 2 = 16$.
Nach dem Satz von Euler gilt $7^{16} \equiv 1 \pmod{48}$, also $7^{18} \equiv 49 \equiv 1 \pmod{48}$.

Aufgabe 4

(i) Man zeige : $x^2 + x + 1 \in \mathbb{Z}_2[x]$ ist irreduzibel.
Gibt es weitere irreduzible Polynome in $\mathbb{Z}_2[x]$ vom Grad 2 ?
(ii) Sei α Nullstelle von $x^2 + x + 1$ in einer Körpererweiterung von $\mathbb{Z}_2$.
Man zeige : $\{1, \alpha\}$ ist Basis der Körpererweiterung $\mathbb{Z}_2(\alpha) : \mathbb{Z}_2$.
Ist $\mathbb{Z}_2(\alpha) = \{0, 1, \alpha, \alpha^2\}$?

Lösung zu Aufgabe 4

(i) Da der Grad des Polynoms 2 ist, ist nur zu zeigen: $x^2 + x + 1 \in \mathbb{Z}_2[x]$ hat in $\mathbb{Z}_2$ keine Nullstelle. Dies ergibt sich durch Einsetzen der Werte $0, 1$.
Sei $ax^2 + bx + c \in \mathbb{Z}_2[x]$ irreduzibel vom Grad 2.
Dann ist $a = 1$, da der Grad 2 sein soll.
Weiter ist $c = 1$ wegen der Irreduzibiliät.
Weiter ist dann $b = 1$, da das Polynom sonst 1 als Nullstelle hätte.
(ii) Nach (i) ist offenbar $x^2 + x + 1$ das Minimalpolynom von α über $\mathbb{Z}_2$.
Nach Vorlesung folgt daraus die Behauptung über die Basis.
Da α Nullstelle von $x^2 + x + 1 \in \mathbb{Z}_2[x]$ ist , folgt $\alpha^2 = \alpha + 1$, und damit $\mathbb{Z}_2(\alpha) = \{0, 1, \alpha, \alpha^2\}$.