Lösungen zur
Modulnachprüfung zur
Elementaren Algebra/Zahlentheorie II

Weiterbildung für Lehrer an der FU

Dozent: V.Schulze Datum: 8.1.2017 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

Es sei $(G, \circ)$ eine Gruppe und $\varphi : G \to G$ definiert durch $\varphi(g) = g^{-1}$ für alle $g \in G$.
(i) Man zeige: φ ist surjektiv.
Man zeige: φ ist injektiv.
(ii) Man zeige: φ ist ein Gruppen-Homomorphismus, falls die Gruppe $(G, \circ)$ kommutativ ist.
Ist φ auch ein Gruppen-Homomorphismus, falls die Gruppe $(G, \circ)$ nicht kommutativ ist?

Lösung

(i) Sei $\varphi(g) = g^{-1} = \varphi(h) = h^{-1}$.
Dann folgt durch Multiplikation mit h von links und mit g von rechts die Gleichung $g = h$. Also ist φ injektiv.
Wegen $(g^{-1})^{-1} = g$ ist g^{-1} Urbild von g. Also ist φ surjektiv.
(ii) Nach Vorlesung gilt für $g, h \in G$ stets $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$.
Also ist $\varphi(g \circ h) = (g \circ h)^{-1} = h^{-1} \circ g^{-1}$.
Ferner gilt $\varphi(g) \circ \varphi(h) = g^{-1} \circ h^{-1}$.
Ist $(G, \circ)$ kommutativ , so ist also φ ein Gruppen-Homomorphismus.
Sei nun $(G, \circ)$ nicht kommutativ. Dann existieren $g, h \in G$ mit $g \circ h \neq h \circ g$.
Dann ist φ kein Gruppen-Homomorphismus, denn es gilt

$h^{-1} \circ g^{-1} \neq g^{-1} \circ h^{-1}$. Dies ergibt sich wie folgt:
Annahme : $h^{-1} \circ g^{-1} = g^{-1} \circ h^{-1}$.
Dann folgt durch Multiplikation von links mit h und g und durch Multiplikation von rechts mit h und g die Gleichung $h \circ g = g \circ h$. Widerspruch.

Aufgabe 2

(i) Man zeige: Das Polynom $f(x) := 7x^3 + 25x + 5 \in \mathbb{Q}[x]$ ist irreduzibel.
Sei α Nullstelle von $f(x)$.
Man bestimme die Koordinaten von $(1 + \alpha^2)(2 + 7\alpha^2)$ bezüglich der Basis $\{1, \alpha, \alpha^2\}$ von $\mathbb{Q}(\alpha) : \mathbb{Q}$.
(ii) Ist $7x^3 + 25x + 5 \in \mathbb{Z}_3[x]$ irreduzibel?

Lösung

(i) Nach Eisenstein ($p = 5$) ist das Polynom $f(x) := 7x^3 + 25x + 5 \in \mathbb{Z}[x]$ irreduzibel, nach Vorlesung dann auch in $\mathbb{Q}[x]$.
Es gilt $(1 + \alpha^2)(2 + 7\alpha^2) = 2 + 9\alpha^2 + 7\alpha^4$.
Es gilt $7\alpha^3 + 25\alpha + 5 = 0$, also $7\alpha^4 + 25\alpha^2 + 5\alpha = 0$.
Es folgt $(1 + \alpha^2)(2 + 7\alpha^2) = 2 + 9\alpha^2 - 25\alpha^2 - 5\alpha = 2 - 5\alpha - 16\alpha^2$.
(ii) Das Polynom ist nicht irreduzibel, da -1 Nullstelle ist.

Aufgabe 3

(i) Man gebe die sechs Einheiten des Restklasenringes $\mathbb{Z}_9$ an.
Gibt es in der Einheitengruppe von $\mathbb{Z}_9$ ein Element der Ordnung 5 ?
(ii) Man zeige: 2 ist Primitivwurzel $mod 9$.
Ist -2 ebenfalls Primitivwurzel $mod 9$?

Lösung

(i) Die Restklase $a(mod 9)$ ist Einheit in $\mathbb{Z}_9$ genau dann, wenn $ggT(a, 9) = 1$ ist.
Die Einheiten von $\mathbb{Z}_9$ sind also $1(mod 9), 2(mod 9), 4(mod 9), 5(mod 9), 7(mod 9), 8(mod 9)$.
Die Einheitengruppe besitzt genau 6 Elemente.
Die Ordnung eines Gruppenelementes in einer endlichen Gruppe ist Teiler der Gruppenordnung.
Also kann es kein Gruppenelement der Ordnung 5 geben.
(ii) Die Potenzen von $2(mod 9)$ sind $1(mod 9), 2(mod 9), 4(mod 9), 8(mod 9), 7(mod 9), 5(mod 9)$.
Also ist 2 ist Primitivwurzel $mod 9$.
Die Potenzen von $-2(mod 9)$ sind $1(mod 9), -2(mod 9), 4(mod 9)$. Also ist -2 nicht Primitivwurzel $mod 9$.

Aufgabe 4

(i) Man zeige: Die Kongruenz $3713x \equiv 1(mod 7429)$ ist lösbar.

Man berechne eine Lösung der Kongruenz.
(ii) Man zeige: Die Kongruenz $-6x^2 \equiv 2(mod 7)$ ist lösbar.
Gibt es eine Lösung dieser Kongruenz, die gleichzeitig Lösung der Kongruenz aus (i) ist ?
Hinweis: Man verwende den chinesischen Restsatz.

Lösung

Die Kongruenz $3713x \equiv 1(mod 7429)$ ist lösbar genau dann, wenn $ggT(3713, 7429) = 1$ ist. Der $ggT(3713, 7429)$ wird mit Hilfe des Euklidischen Algorithmus berechnet:
$7429 = 2 \cdot 3713 + 3$
$3713 = 1237 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 1 \cdot 1 + 0$
Der letzte von 0 verchiedene Rest ist der gesuchte ggT. Also ist $ggT(3713, 7429) = 1$ und die Kongruenz $3713x \equiv 1(mod 7429)$ ist lösbar.
Zur Bestimmung einer Lösung der Kongruenz $3713x \equiv 1(mod 7429)$ wird 1 dargestellt als Linearkombination von 3713 und 7429 unter Verwendung der obigen Divisionsgleichungen. Es gilt
$1 = 3-2 = 3-(3713-1237 \cdot 3) = (7429-2 \cdot 3713)-(3713-1237 \cdot (7429-2 \cdot 3713))$.
Also ist $1 = 1238 \cdot 7429 + 3713(-2477)$.
Es folgt $1 \equiv 3713 \cdot (-2477)(mod 7429)$, also ist -2477 eine Lösung der Kongruenz $3713x \equiv 1\,(mod 7429)$.
(ii) Durch Einsetzen ergibt sich 3 als Lösung der Kongruenz $-6x^2 \equiv 2(mod 7)$.
Da 7 nicht Teiler von 7429 ist , gilt $ggT(7, 7429) = 1$.
Nach dem chinesischen Restsatz exisiert ein x_0 mit
$x_0 \equiv -2477\, mod(7429)$ und $x_0 \equiv 3\, mod(7)$.
Dann ist x_0 eine gemeinsame Lösung der Kongruenzen
$3713x \equiv 1\,(mod 7429)$ und $-6x^2 \equiv 2(mod 7)$.