Lösungen zur
Modulprüfung zur
Elementaren Algebra/Zahlentheorie II

Weiterbildung für Lehrkräfte an der FU

Dozent: V.Schulze Datum: 14.1.2025 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) Die Verknüpfung $\otimes$ auf $\mathbb{Z}$ sei definiert durch
$a \otimes b := a + a^2b^2 + b$ für alle $a, b \in \mathbb{Z}$.
Gilt $(1 \otimes 1) \otimes 2 = 1 \otimes (1 \otimes 2)$?
Man zeige: 0 ist neutrales Element von $(\mathbb{Z}, \otimes)$.
Besitzt 1 in $(\mathbb{Z}, \otimes)$ ein inverses Element ?
(ii) Man stelle $(1, 2, 3)(4, 2)$ als Produkt elementefremder Zyklen dar.
Man stelle $(1, 2, 3)(4, 2)$ als Produkt von Transpositionen dar.
Wie viele Linksnebenklassen besitzt die Untergruppe $U := \{id, (1, 2)\}$ in der symmetrischen Gruppe S_4 vom Index 4?

Lösung von Aufgabe 1

(i) Es gilt $(1 \otimes 1) \otimes 2 = 3 \otimes 2 = 41, 1 \otimes (1 \otimes 2) = 1 \otimes 7 = 57$, also nicht $(1 \otimes 1) \otimes 2 = 1 \otimes (1 \otimes 2)$.
Es gilt $0 \otimes a = a, a \otimes 0 = a$, also ist 0 neutrales Element.
Annahme : a ist zu 1 invers.
Dann folgt $a \otimes 1 = 0$, also $a + 1 + a^2 = 0$. Diese quadratische Gleichung ist aber in $\mathbb{Z}$ nicht lösbar. Also besitzt 1 kein inverses Element.
(ii) Es gilt $(1, 2, 3)(4, 2) = (1, 2, 4, 3)$ und $(1, 2, 3)(4, 2) = (1, 2)(2, 3)(4, 2)$.

Die Darstellung als Produkt von Transpositionen ist natürlich nicht eindeutig.
U enthält 2 Elemente ,S_4 enthält 4! Elemente. Nach Lagrange besitzt U genau $\frac{4!}{2} = 12$ Linksnebenklassen.

Aufgabe 2

(i) Die Abbildung $f : \mathbb{Z} \to \mathbb{Z}_{12}$ sei definiert durch
$f(a) := 4a \pmod{12}$ für alle $a \in \mathbb{Z}$.
Man zeige: f ist ein Gruppenhomomorphismus bezüglich +.
Man bestimme den Kern von f.
Ist f ist ein Ring-Homomorphismus ?
(ii) Man bestimme die Anzahl der Einheiten des Restklassenringes $\mathbb{Z}_{12}$.
Man gebe alle Einheiten von $\mathbb{Z}_{12}$ an.

Lösung von Aufgabe 2

(i) Wendet man die Zuordnungsvorschrift für f und die Rechenregeln in $\mathbb{Z}_{12}$ an, so ergibt sich $f(a + b) = 4(a + b) \pmod{12} = 4a \pmod{12} + 4b \pmod{12} = f(a) + f(b)$ für alle $a, b \in \mathbb{Z}$.
Also ist f ein Gruppenhomomorphismus bezüglich +.
Nach Definition enthält der Kern von f alle Elemente aus $\mathbb{Z}$, die auf 0 (mod 12) abgebildet werden.
Also liegt $a \in \mathbb{Z}$ im Kern von f genau dann, wenn $4a$ Vielfaches von 12 ist oder gleichwertig a Vielfaches von 3 ist. Also ist $Kern(f) = 3\mathbb{Z}$.
Es gilt $f(a)f(b) = 4a \pmod{12} \cdot 4b \pmod{12} = 16ab \pmod{12} = 4ab \pmod{12} = f(ab)$.
Also ist f relationstreu bezüglich $\cdot$.
Der Gruppenhomomorphismus ist also auch Ringhomomorphismus.
(ii) Es bezeichne φ die Eulersche φ - Funktion.
Nach Vorlesung ist $\varphi(12)$ die Anzahl der Einheiten von $\mathbb{Z}_{12}$.
Es gilt $\varphi(12) = \varphi(4)\varphi(3) = 2 \cdot 2 = 4$.
Die Anzahl der Einheiten des Restklassenringes $\mathbb{Z}_{12}$ ist also 4.
Nach Vorlesung ist $a \pmod{12}$ Einheit von $\mathbb{Z}_{12}$ genau dann, wenn $ggT(a, 12) = 1$ ist.
Die Einheiten des Restklassenringes $\mathbb{Z}_{12}$ sind also $1 \pmod{12}, 5 \pmod{12}, 7 \pmod{12}, 11 \pmod{12}$.

Aufgabe 3

(i) Man zeige: $y^4 \equiv a \pmod{5}$ ist lösbar genau dann, wenn $a \equiv 0 \pmod{5}$ oder $a \equiv 1 \pmod{5}$ ist.
Man zeige: $x^2 - y^4 \equiv 2 \pmod{5}$ ist nicht lösbar.
Ist $x^2 - y^4 = 7$ in $\mathbb{Z}$ lösbar ?
(ii) Man zeige: 2863421 ist durch 11 teilbar.

Man zeige: 344256 ist durch 33 teilbar.
Ist die Kongruenz $344256 \cdot x \equiv 1 \pmod{2863421}$ lösbar ?

Lösung von Aufgabe 3

(i) Setzt man für y die Werte $0, 1, 2, 3, 4$ ein, so ergibt sich:
$y^4 \equiv a \pmod 5$ ist lösbar genau dann, wenn $a \equiv 0 \pmod 5$ oder $a \equiv 1 \pmod 5$ ist.
Setzt man für x die Werte $0, 1, 2, 3, 4$ ein, so ergibt sich:
$x^2 \equiv b \pmod 5$ ist lösbar genau dann, wenn $b \equiv 0 \pmod 5$ oder $b \equiv 1 \pmod 5$ oder $b \equiv 4 \pmod 5$ ist.
Aus den beiden obigen Ergebnissen ergibt sich:
$x^2 - y^4 \equiv c \pmod 5$ ist lösbar nur für $c \equiv 0, 1, 4, 3 \pmod 5$.
Die Gleichung $x^2 - y^4 = 7$ besitzt in $\mathbb{Z}$ keine Lösung, denn eine Lösung wäre auch Lösung von $x^2 - y^4 \equiv 2 \pmod 5$.
(ii)Die alternierende Quersumme von 2863421 ist $1-2+4-3+6-8+2 = 0 \equiv 0 \pmod{11}$.
Also ist 2863421 ist durch 11 teilbar.
Die alternierende Quersumme von 344256 ist $6 - 5 + 2 - 4 + 4 - 3 = 0 \equiv 0 \pmod{11}$.
Also ist 344256 ist durch 11 teilbar.
Die Quersumme von 344256 ist $6 + 5 + 2 + 4 + 4 + 3 = 0 \equiv 0 \pmod 3$.
Also ist 344256 durch 3 teilbar.
Zusammen folgt: 344256 ist durch 33 teilbar.
Ist die Kongruenz $344256 \cdot x \equiv 1 \pmod{2863421}$ ist nicht lösbar, da $ggT(344256, 2853421)$ nach den obigen Ergebnissen Vielfaches von 11 ist, also nicht 1 sein kann.

Aufgabe 4

Man betrachte das irreduzible Polynom $x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$.
Es sei α Nullstelle von $x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$
in einer Körpererweiterung von $\mathbb{Z}_2$.
(i) Man zeige : $\{1, \alpha, \alpha^2, \alpha^3\}$ ist Basis der Körpererweiterung $\mathbb{Z}_2(\alpha) : \mathbb{Z}_2$.
Wie viele Elemente besitzt der Körper $\mathbb{Z}_2(\alpha)$?
(ii) Ist α^2 zu α in $\mathbb{Z}_2(\alpha)$ multiplikativ invers ?
Man stelle α^4 als Linearkombination der Basiselemente dar.

Lösung von Aufgabe 4

(i) Das Polynom $x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$ ist irreduzibel und normiert, also ist $Irr(\alpha, \mathbb{Z}_2) = x^4 + x^3 + 1$. Der Grad des Minimalpolynoms ist also 4. Nach Vorlesung ist dann $\{1, \alpha, \alpha^2, \alpha^3\}$ ist Basis der Körpererweiterung $\mathbb{Z}_2(\alpha) : \mathbb{Z}_2$.
Die Anzahl der möglichen Linearkombinationen der 4 Basisvektoren ist also $2^4 = 16$. Also besitzt der Körper $\mathbb{Z}_2(\alpha)$ 16 Elemente.

(ii) Es gilt $\alpha^2 \cdot \alpha = \alpha^3 \neq 1$ beziehungsweise $\alpha^3 - 1 \neq 0$,da $\{1, \alpha, \alpha^2, \alpha^3\}$ Basis der Körpererweiterung $\mathbb{Z}_2(\alpha) : \mathbb{Z}_2$ ist.
Beachtet man, daß α Nullstelle von $x^4 + x^3 + 1$ ist, so ergibt sich $\alpha^4 = -\alpha^3 - 1$, dies ist die gesuchte Linearkombination.